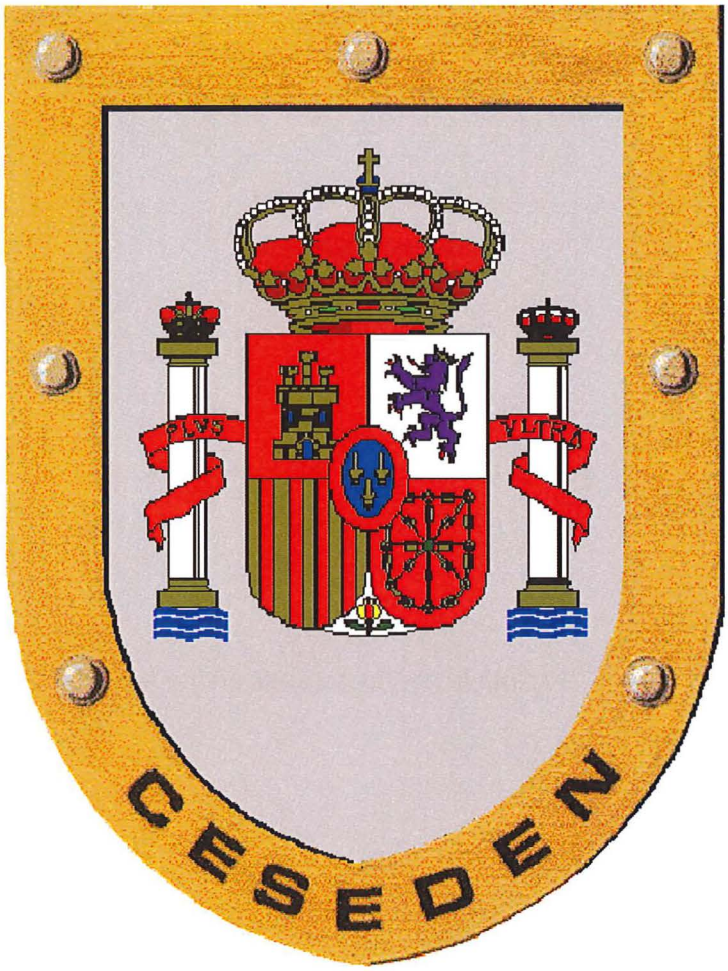
MINISTERIO
DE DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR DE ESTUDIOS
DE LA DEFENSA NACIONAL



CURRÍCULO

CURSO "BÁSICO DE CIBERDEFENSA"

Abril 2019

PAGINA INTENCIONADAMENTE EN BLANCO

CURRÍCULO DEL CURSO "BÁSICO DE CIBERDEFENSA"

1. DESCRIPCIÓN GENERAL DEL CURSO

Denominación: Curso "BÁSICO DE CIBERDEFENSA".

Tipo de Curso: A efectos de aplicación del RD 339/2015, de 30 de abril, de ordenamiento de las enseñanzas de perfeccionamiento y de Altos Estudios de la Defensa Nacional, artículos 4 y 13, el curso tiene la consideración de curso militar de perfeccionamiento, conjunto, informativo e indistinto.

Objetivos del curso: El objetivo general del curso es proporcionar competencias para la realización de tareas de apoyo a las operaciones en el Ciberespacio. También iniciar en la Ciberdefensa al personal sin formación previa o asignado a otras funciones relacionadas con las TIC.

Duración: Fase previa no presencial 63 horas. Fase presencial 75 horas.

Idioma: español.

Centro Docente Militar responsable del desarrollo del curso: La organización y dirección del curso corresponde al Centro Superior de Estudios de la Defensa Nacional, siendo impartido en la Escuela de Especialidades de la Armada "Antonio de Escaño".

Modalidad de enseñanza: Semipresencial.

Número máximo de alumnos por curso: 20 alumnos por curso.

2. JUSTIFICACIÓN DEL CURSO

2.1. Justificación.

Por Orden Ministerial 10/2013, de 19 de febrero, se crea el Mando Conjunto de Ciberdefensa (MCCD) de las Fuerzas Armadas. Este Mando, en coordinación con los ejércitos y otros organismos elaboró el Plan de Formación de Ciberdefensa (FORCIBE) que fue aprobado por el Jefe de Estado Mayor de la Defensa el 16 de marzo de 2015. Este Plan es un documento para uso interno de las Fuerzas Armadas.

Los cursos desarrollados en dicho plan se fueron implantando de manera escalonada. De esta manera, algunos de los planes de estudios se desarrollaron en base a la normativa anterior. La norma decimosexta de la Orden DEF 464/2017 especifica el procedimiento a seguir con los currículos de los cursos que se encuentran en esta circunstancia. El curso Básico de Ciberdefensa se encuentra en esta situación.

La Ciberdefensa es un nuevo ámbito de las operaciones. Como tal, existe un énfasis creciente en desarrollar expertos que puedan planear y ejecutar misiones en el ciberespacio. La formación de dichos expertos está todavía

desarrollándose dentro de MINISDEF pero hay una amplia oferta formativa externa (universidades y centros de estudios privados).

Adicionalmente, la Directiva de JEMAD para Orientar la Preparación de la Fuerza Conjunta de JEMAD (Ref. f.) hace mención expresa a la necesidad de proporcionar conocimientos básicos de Ciberdefensa dentro de la enseñanza de formación, pero también potenciando esta nueva disciplina en la enseñanza de perfeccionamiento. La Ciberdefensa es una capacidad de carácter conjunto. Tanto es así que hay una integración cada vez mayor entre las dimensiones de la seguridad y de la defensa hasta el punto de que ha fomentado la aparición de los nuevos conceptos de "guerra híbrida" y "operaciones híbridas".

Una de las carencias en formación más importantes que se han detectado, sin embargo, implica precisamente al personal que no es experto en la materia, o al menos no lo es aún, pero desarrolla labores relacionadas en mayor o menor medida con la Ciberdefensa. Se puede afirmar que la práctica totalidad del personal de MINISDEF es usuaria de servicios digitales en el ciberespacio pero la mayoría desconoce sus características, limitaciones y vulnerabilidades.

Es necesaria una formación base que faculte al personal relacionado con la Ciberdefensa para entender la terminología y los conceptos básicos, y que también permita obtener las competencias necesarias para enlazar con formación más avanzada que conduzca a una posible especialización en Ciberdefensa y a otros cursos más específicos para puestos concretos de acuerdo con los itinerarios diseñados en el Plan de Formación.

2.2. Descripción de los procedimientos de consulta.

El currículo se ha elaborado a tenor de lo dispuesto en la Directiva 03/16 del JEMAD y en la Orden DEF/464/2017. Así, se ha partido de la necesidad formativa detectada por el MCCD, plasmada en el Plan FORCIBE y concretada en un Documento de Necesidad Operativa (DNO). Este documento ha sido redactado por el MCCD y estudiado por el CESEDEN y la Jefatura de Recursos Humanos del EMAD. En su estudio se ha consultado a expertos de Centros Docentes Militares y de organismos de defensa relacionados con la Ciberdefensa.

3. RESULTADOS DE APRENDIZAJE

Los alumnos que completen el curso deberán ser capaces de:

- Relacionar la terminología y los conceptos básicos, tanto desde el punto de vista conceptual como técnico en materia de Ciberdefensa.
- Distinguir la seguridad de los Sistemas de las TIC y las amenazas y vulnerabilidades que representan las nuevas tecnologías.
- Evaluar el estado de seguridad de un sistema, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos.
- Explicar de manera básica y con una garantía suficiente, los aspectos de seguridad relativos a la infraestructura de red basada en elementos de comunicaciones (concentradores, enrutadores,...), dispositivos inalámbricos y redes privadas virtuales (VPN) introduciendo los conceptos de cortafuegos, sistemas de detección de intrusos (IDS) y dispositivos trampa (honeypots y honeynets).
- Explicar de manera básica y con una garantía suficiente, los aspectos de seguridad relativos a la configuración básica de dispositivos móviles, comunicaciones inalámbricas, sistemas operativos de escritorio, aplicaciones y servicios de usuario.

- Gestionar y administrar sistemas operativos Windows y Linux.

4. SISTEMA DE ADMISIÓN AL CURSO

4.1. Categoría y empleo militar

El curso se dirige a oficiales, suboficiales, MTM y personal civil que tengan, o vayan a tener, cometidos generales o técnicos de apoyo relacionados con la Ciberdefensa.

4.2. Perfil de ingreso

Los alumnos deberán tener conocimientos básicos de informática, como son:

- Identificar y organizar los componentes físicos y lógicos que conforman un sistema microinformático y/o red de transmisión de datos, clasificados según su función para acoplarlos según su finalidad.
- Reconocer las herramientas del sistema operativo y periféricos manejándolas para realizar configuraciones y resolver problemas siguiendo las instrucciones del fabricante.
- Conocer las aplicaciones ofimáticas de uso en las FAS.

Los alumnos deberán estar en posesión de la habilitación de seguridad Reservado/NATO SECRET y tener conocimientos de inglés técnico en la materia.

4.3. Sistema de selección.

Los alumnos serán designados de forma directa. La relación de designados será publicada en el BOD, pudiendo adelantarse mediante mensaje oficial.

4.4. Apoyo y orientación al alumnado

El currículo de este curso, una vez aprobado, se encontrará disponible en la Intranet de Defensa, en la página correspondiente al CESEDEN y en el campus virtual de la Escuela Naval Militar de la Armada.

En el momento de su designación, la secretaría de la dirección del curso remitirá una comunicación a la cuenta de correo oficial de cada alumno (red de propósito general (WAN PG) del Ministerio de Defensa). En esta comunicación se informará al alumno de:

- Estructura del curso, director, coordinador.
- Dirección (postal, telefónica y correo electrónico) donde dirigirse para trámites administrativos.
- Plan de Estudios, competencias a alcanzar y sistema de evaluación.
- Centro donde se va impartir la fase presencial, ubicación, horarios generales, acceso y normas para el uso de los servicios del centro.
- Departamento del centro encargado del curso, calendario.
- Otros aspectos como ceremonias de apertura y clausura, uniformidad.

5. PLAN DE ESTUDIOS

5.1. Estructura general del Plan de Estudios

Este curso tendrá una fase previa no presencial con una carga lectiva de 63 horas a desarrollar en 25 días hábiles y una fase presencial con una carga lectiva de 75 horas (50 de clase y 25 de estudio) a desarrollar en 10 días hábiles, en horario de mañana.

El curso está dividido en cuatro módulos:

- Introducción a la seguridad de la información.
- Aspectos básicos de legislación, estructura y normativa de Ciberdefensa.
- Conceptos básicos de Ciberseguridad y Ciberdefensa.
- Introducción a la criptología.

Módulo 1. Introducción a la seguridad de la información.

Duración total de 13 horas, en la fase a distancia.

Contenido:

- Introducción y conceptos básicos.
- Organización y gestión de la seguridad.
- Acreditación de sistemas.
- Documentación de seguridad.
- Seguridad física, documental y de personal.
- Procedimiento de inspecciones de seguridad.
- Gestión de incidencias de seguridad.

Resultado del módulo: Identificar la terminología de seguridad de la información.

Módulo 2. Aspectos básicos de legislación, estructura y normativa de Ciberdefensa.

Duración total de 24 horas durante la fase a distancia.

Contenido:

- Políticas de seguridad.
- Estrategia Nacional de Seguridad.
- Estrategia Nacional de Ciberseguridad.
- Plan Nacional de Ciberseguridad.
- Esquema Nacional de Ciberseguridad.
- Otra normativa nacional y OTAN relativa a la Ciberseguridad.
- Organismos relacionados con la Ciberdefensa en España.
- Normativa y procedimientos del MINISDEF.
- Regulación nacional en el ciberespacio (nivel básico, generalidades)
- Leyes aplicables al ciberespacio en el ámbito internacional.

Resultado del módulo: Identificar la legislación y normativa de Ciberdefensa así como reconocer la estructura española en Ciberdefensa.

Módulo 3. Conceptos básicos de Ciberseguridad y Ciberdefensa.

Duración total: 45 horas, 13 en la fase a distancia y 25 en la fase de presente.

Contenido:

- Terminología y conceptos básicos.
- Introducción a la Ciberdefensa.
- Amenazas y vulnerabilidades.
- Descripción básica de los diferentes tipos de malware.
- Estudio de los tipos de ataque de manera general.
- Conocimiento e identificación de los vectores de ataque.

Resultado del módulo: Identificar los conceptos básicos de Ciberseguridad y Ciberdefensa.

Módulo 4. Introducción a la criptología.

Duración total: 45 horas, 13 en la fase a distancia y 25 en la fase de presente.

Contenido:

- Terminología y conceptos básicos.
- Seguridad criptográfica.
- Definición de criptosistema.
- Clasificación de los criptosistemas.
- Criterio de diseño de un criptosistema.
- Modos de empleo de la cifra.
- Estenografía.

Resultado del módulo: Identificar los conceptos básicos de criptología.

5.2. Metodología de enseñanza-aprendizaje.

El Curso se impartirá en formato semipresencial con una fase a distancia y una fase presencial.

La fase a distancia se realizará compatibilizándose con los cometidos propios del destino que estén ocupando los alumnos designados. El trabajo autónomo del alumno de esta fase tiene una duración de 63 horas.

El coordinador del curso realizará una presentación de una hora al inicio de la fase presencial.

La fase presencial tendrá una duración de 50 horas de clase más 25 horas de estudio del alumno. Las exposiciones orales de los profesores cubren 20 horas lectivas. Para comprobar que los alumnos alcanzan los resultados de aprendizaje se programarán ejercicios prácticos. La duración total de estas prácticas será de 30 horas.

El curso finalizará con un juicio crítico y clausura (1 hora).

5.3. Criterios de Evaluación.

Se realizará un examen teórico previo de una hora al inicio de la fase de presente y otro al final de la misma para valorar el progreso del aprendizaje.

Para asistir a la fase de presente será necesario haber superado el examen previo.

Las prácticas del curso se evaluarán con la observación directa del profesor.

Para la obtención de la calificación de APTO, será necesario superar dos pruebas, una al inicio de la fase de presente sobre los contenidos de la fase a distancia y otra al final en la que se acrediten los conocimientos adquiridos durante el curso.

6. RECURSOS DEL PROFESORADO Y PERSONAL DE APOYO

Director: El CESEDEN nombrará un Director del Curso que pertenecerá a la ESFAS.

Coordinador: La Escuela de Especialidades de la Armada "Antonio de Escaño" nombrará un Coordinador del Curso.

Personal docente: Ambas fases serán impartidas por personal docente universitario con la acreditada formación y experiencia en ciberdefensa.

Personal de apoyo: La Escuela de Especialidades de la Armada "Antonio de Escaño" facilitará los apoyos para administración, uso de los medios y servicios con personal propio del centro.

7. RECURSOS MATERIALES Y SERVICIOS NECESARIOS PARA IMPARTIR EL CURSO

Fase a distancia: Los alumnos deberán disponer de conexión a la WAN PG del Ministerio de Defensa y acceso a internet.

Fase presencial: El curso se impartirá en un aula equipada con ordenadores y conexión a red e internet. Las características del aula deben ser:

- Capacidad: 25 puestos + 1 puesto profesor, PCs con al menos procesador Intel i5 (o equivalente) y 8 GB de memoria RAM.
- Conectividad: Conexión en red local con conexión a internet por medio de fibra óptica con velocidad de 50 megas simétricos.
- Suelo técnico.
- Pizarra electrónica con proyector integrado.
- Apoyo de la biblioteca del Centro y los fondos de los departamentos relacionados con informática y comunicaciones.

Los profesores y alumnos del curso tendrán acceso a los servicios de la Escuela en el mismo horario que el resto de profesores y alumnos del centro.

Financiación: El curso será financiado por el EMAD

Convocatoria: La relación de concurrentes seleccionados se hará pública en el BOD.

8. EFECTOS DE LA SUPERACIÓN DE LA ACTIVIDAD FORMATIVA Y RESULTADOS PREVISTOS

8.1. Efectos y servidumbres

La superación del Curso facultará al personal para:

- Desempeñar los cometidos de su puesto teniendo en cuenta las particularidades de la Ciberdefensa.
- Acceder a cursos de mayor nivel tecnológico relacionados con la Ciberdefensa.

8.2. Resultados previstos

Se trata de un curso con contenidos relativos a un campo novedoso en el Ministerio de Defensa. Los alumnos son personal profesional, con experiencia y conocimientos previos en su campo. Muchos ya están trabajando en el ámbito de la Ciberdefensa y están interesados en completar su formación para continuar en este campo, previéndose los siguientes resultados:

- Tasa de Éxito (TE) prevista: 92%
- Tasa de Bajas Académicas (TBA) prevista: 4%
- Tasa de Bajas a Petición Propia (TBPS) Prevista: 4%
- Tasa de Abandono (TA) prevista: 8%

9. SISTEMA DE GARANTÍA INTERNA DE LA CALIDAD.

9.1. Responsables del sistema de garantía de la calidad del plan de estudios

Los director y coordinador del curso serán los responsables de gestionar, coordinar y realizar el seguimiento de este plan de estudios.

9.2. Procedimientos de evaluación, mejora y análisis

De acuerdo con la Instrucción 03/16 del JEMAD para los cursos de perfeccionamiento en el ámbito conjunto, el CESEDEN con el apoyo del profesorado del curso, llevará a cabo una evaluación interna con el objeto de comprobar que el curso y su desarrollo cumplen con los objetivos establecidos y que el alumno obtiene las competencias definidas en el perfil de egreso.

Antes de la finalización del curso la dirección del curso pasará una encuesta a los alumnos. Esta encuesta cubre aspectos administrativos, de organización del curso, curriculares y sobre la docencia. Sus resultados se emplearán en la redacción del informe final.

Inmediatamente después de la finalización del curso, el Centro de Enseñanza remitirá al CESEDEN un informe final, elaborado mediante encuestas a los alumnos durante la realización del curso y las observaciones de los profesores. En este informe se incluirán las observaciones aportadas por el personal de apoyo, mandos y resto de personal implicado en la realización del curso.

Al año de haber finalizado el curso, los egresados que estén ocupando una vacante relacionada con la Ciberdefensa, elevarán un informe por su cadena orgánica en el que se refleje la utilidad de las enseñanzas recibidas en dicho curso. Los resultados de este informe se remitirán al CESEDEN para ser utilizados en la revisión y mejora del plan de estudios del curso.

9.3 Mecanismos de publicidad del curso

De acuerdo con el Artículo 11 del RD 339/2015, el curso estará incluido en el "Registro de Centros, Cursos y Títulos" y se podrá acceder a este registro a través de la intranet del Ministerio de Defensa, en la página correspondiente al CESEDEN y en el aula a distancia del CUD de la Escuela Naval de Marín de la Armada.

10. CALENDARIO DE IMPLANTACIÓN.

Este curso viene realizándose satisfactoriamente desde el año 2016.

Madrid, a 25 de abril 2019

El Teniente General Director de Centro Superior de Estudios de la Defensa Nacional

- Rafael Sanchez Ortega -

ANEXO I: ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS Y DESCRIPCIÓN DE LOS MÓDULOS

ANEXO I: ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS Y DESCRIPCION DE LOS MÓDULOS

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS

MODULO	HORAS	ORGANIZACIÓN TEMPORAL
1. Introducción a la seguridad de la información	13	Fase a distancia
2. Aspectos básicos de legislación, estructura y normativa de ciberdefensa	24	Fase a distancia
3. Conceptos básicos de ciberseguridad y ciberdefensa	38	Fases a distancia y presencial
4. Introducción a la criptología	38	Fases a distancia y presencial

DESCRIPCIÓN DE LOS MÓDULOS

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
1. Introducción a la seguridad de la información	- Introducción y conceptos básicos - Organización y gestión de la seguridad - Acreditación de sistemas - Documentación de seguridad - Seguridad física, documental y de personal - Procedimiento de inspecciones de seguridad. - Gestión de incidencias de seguridad	13			
2. Aspectos básicos de legislación, estructura y normativa de ciberdefensa	- Políticas de seguridad - Estrategia nacional de seguridad - Estrategia nacional de ciberseguridad - Plan nacional de ciberseguridad - Esquema nacional de ciberseguridad - Otra normativa nacional y OTAN relativa a la ciberseguridad - Organismos relacionados con la ciberdefensa en España. - Normativa y procedimientos del MINISDEF - Regulación nacional legal en el ciberespacio (nivel básico, generalidades) - Leyes aplicables al ciberespacio en el ámbito internacional	24			

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
3. Conceptos básicos técnicos de ciberseguridad y ciberdefensa	- Terminología y conceptos básicos - Introducción ciberdefensa - Amenazas y vulnerabilidades - Descripción básica de los diferentes tipos de malware - Estudio de los tipos de ataque de manera general - Conocimiento e identificación de los vectores de ataque	13	10	14	1
4. Introducción a la criptología	- Terminología y conceptos básicos - Seguridad criptográfica - Definición de criptosistema - Clasificación de los criptosistemas - Criterio de diseño de un criptosistema - Modos de empleo de la cifra - Estenografía	13	10	14	1
	Total	63	20	28	2