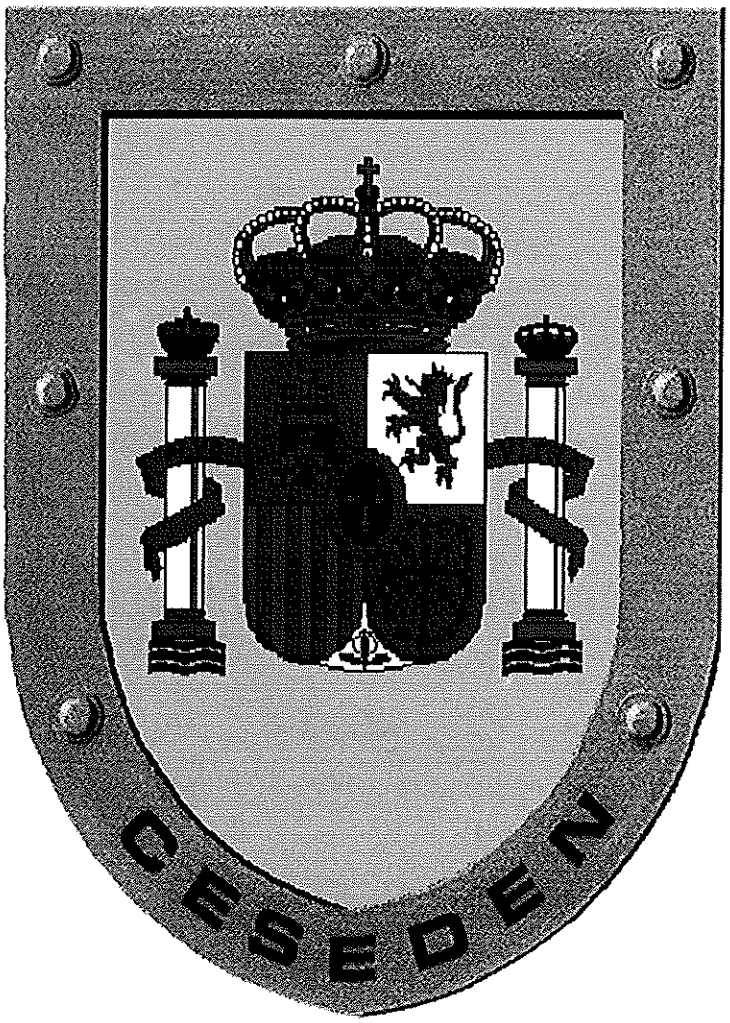
MINISTERIO
DE
DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR DE ESTUDIOS
DE LA DEFENSA NACIONAL



CURRÍCULO

CURSO DE ANALISIS FORENSE

Febrero 2017

CURRÍCULO

CURSO DE ANÁLISIS FORENSE DE CIBERDEFENSA

1. DESCRIPCIÓN GENERAL DEL CURSO.

Denominación: Curso de Análisis forense de Ciberdefensa.

Tipo de Curso: A efectos de aplicación del Real Decreto 339/2015, de 30 de abril, por el que se ordenan las enseñanzas de perfeccionamiento y de Altos Estudios de la Defensa Nacional, artículo 4 apartado d) 3, este curso tiene la consideración un curso militar conjunto y según lo señalado en el artículo 16, se trata de un curso informativo e indistinto.

Categoría del Curso: No aplicable por tratarse de un curso informativo.

Duración: 100 horas.

Fase a distancia: 50 horas en 4 semanas sin dedicar tiempo de la jornada laboral.

Fase presencial: 50 horas en 2 semanas.

Idioma: Español.

Centro responsable y lugar donde se imparte: La organización y dirección del curso corresponde al Centro Superior de Estudios de la Defensa Nacional (CESEDEN), siendo impartido en las instalaciones de la Escuela de Mando, Control y Telecomunicaciones del Ejército del Aire (EMACOT).

Modalidad de enseñanza: Semipresencial.

Número máximo de alumnos por curso: 15. Oficiales, suboficiales, tropa y personal civil de las Fuerzas Armadas.

2. JUSTIFICACIÓN.

2.1 Justificación del Curso.

En la actualidad no existen en el MINISDEF cursos que cubran las necesidades de formación expresadas en el Plan de Formación en Ciberdefensa para los analistas forenses de los CIS. Su misión fundamental comprobar el estado de los sistemas bajo su supervisión, controlando los eventos del sistema

Con la finalidad de optimizar la formación de dichos analistas forenses, se propone un curso que proporcionará las competencias necesarias para capacitar al alumno

en el desempeño de las Funciones de Análisis forense en aplicación del Plan de Formación en Ciberdefensa del Ministerio de Defensa (FORCIBE).

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. Siguiendo esta Directiva, se ha partido de la necesidad formativa en el área de análisis forense 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. PERFIL DE EGRESO.

El objetivo del curso es proporcionar la aptitud necesaria para el desempeño de funciones avanzadas de análisis forense de sistemas.

Los alumnos que completen el curso deberán ser capaces de realizar las siguientes tareas:

- Comparar las diferencias existentes en la obtención de evidencias forenses digitales procedentes de soportes de almacenamiento magnéticos y de estado sólido.
- Aplicar las herramientas de Sysinternals para examinar partes claves del sistema operativo incluyendo la programación de subprocesos, la paginación, la asignación de memoria virtual y memoria física.
- Describir el proceso de un análisis forense en general.
- Realizar análisis forense digital de medios de almacenamiento masivo.
- Realizar análisis forense digital de sistemas MS-Windows.
- Describir los métodos empleados por las últimas versiones del sistema Windows para guardar información de su funcionamiento centrándose en el log de eventos, archivos Prefetch, archivos de navegación y el registro del sistema.
- Realizar análisis forense sobre dispositivos móviles.
- Describir con precisión los aspectos legislativos del análisis forense.
- Redactar un informe de un análisis forense digital.

4. PERFIL DE INGRESO. ACCESO DE ALUMNOS.

4.1. Sistemas de información previa al curso

El currículo de este curso, una vez aprobado, se encontrará disponible en la Intranet de Defensa, en la página correspondiente al CESEDEN y a la Escuela de Técnicas de Mando Control y Telecomunicaciones (EMACOT) del EA.

4.2. Requisitos de acceso

El Curso se dirige a militares de todas las escalas y personal civil funcionario del Ministerio de Defensa, que tengan, o vayan a tener, cometidos técnicos relacionados con el análisis forense de sistemas.

Los alumnos deberán tener conocimientos avanzados en ciberdefensa que incluyan:

- Describir cómo se almacenan físicamente los datos en un sistema informático.
- Describir el funcionamiento de la RAM, ROM, memoria flash, CD, DVD, discos duros y Blue-Ray.
- Describir los métodos de particionado de discos duros y de gestión de volúmenes. Describir los formatos NTFS, EFS, FAT 12/16/32, exFAT, CDFS, UDFS, HFS, HFS+ centrándose en el método de almacenamiento de archivos, la gestión de directorios y la eliminación de archivos.
- Describir el diseño interno del sistema operativo Windows en sus últimas versiones centrándose en la arquitectura, el soporte de aplicaciones, la programación de subprocesos y la gestión de la memoria, la seguridad, las claves de registro y las entradas y salidas.
- Configurar y emplear máquinas virtuales.
- Describir los protocolos de comunicación por internet.
- Describir los diferentes tipos de malware y sus mecanismos de actuación.
- Los alumnos deberán estar en posesión de la habilitación de seguridad Reservado/NATO SECRET.
- Los alumnos deberán tener conocimientos de inglés técnico en la materia.

4.3. Admisión al curso.

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

Al inicio de la fase de presente del curso se evaluará:

- Los conocimientos avanzados en ciberdefensa descritos en el punto 4.2 de este documento, mediante una prueba escrita de 1 hora de duración. Se puntuará de uno (1) a diez (10) y supondrá un 80% de la nota final para ingreso.
- Un 10% se basará en haber realizado "Curso de Búsqueda de Evidencias" del CCN o acreditar poseer alguna de las certificaciones forenses siguientes: CHFI (ECCouncil) y CFFP (ISC)2.
- Conocimientos de idioma inglés. Se puntuará de uno (1) a diez (10) según el perfil SLP de los solicitantes, de acuerdo con la siguiente tabla y supondrá un 10% de la nota final para ingreso:

PUNTOS SLP	VALOR (Sobre 10)
12 o más	10
10-12	9
8-10	8
6-8	7

La suma, teniendo en cuenta su ponderación, de los tres conceptos anteriores debe ser superior a cinco (5) para poder optar a una plaza del curso, pudiendo quedarse plazas desiertas en ausencia de personal con esta puntuación mínima.

4.4. Procedimientos de acogida, apoyo y orientación a los alumnos

Antes del inicio de la fase a distancia, la Secretaría de la Dirección del curso (CESEDEN) y la EMACOT remitirán correos a la cuenta de correo oficial de la red de propósito general (WAN PG) del MINISDEF. informando a los alumnos 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 desde donde se va a impartir la fase a distancia y procedimientos de relación (correos, horarios y uso de la WAN PG).
- 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.

- Procedimiento para tramitación y liquidación de la comisión de servicio.

Al tratarse de un curso de perfeccionamiento no será necesario instruir a los alumnos en aspectos relativos al régimen de internado del Centro.

Parte de los aspectos relativos a la fase presencial en la EMACOT podrán remitirse durante el desarrollo de la fase a distancia.

4.5. Reconocimiento de créditos

No se efectuará reconocimiento de créditos de este curso.

5. PLAN DE ESTUDIOS

5.1 Estructura General

El Curso tendrá una fase previa a distancia a desarrollar en 4 semanas y una fase presencial con una duración de 50 horas a desarrollar en 2 semanas, en horario de mañana.

Estará dividido en 4 módulos:

Módulo 1.- Contenido teórico Analista Forense Digital. (50 horas). Se imparte durante la Fase a distancia

Módulo 2.- Procedimiento de actuación forense: escenario y tratamiento de evidencias. (9 horas) Fase Presencial

Módulo 3.- Análisis de sistemas y dispositivos móviles: forense postmortem y online. (30 horas) Presencial

Módulo 4.- Presentación de resultados y actuación pericial práctica. (9 horas) Presencial.

La distribución se detalla en el Anexo I "Resumen de Materias" y los contenidos y sesiones de cada módulo en el Anexo II "Plan de estudios".

Se realizarán 2 pruebas escritas de 1 sesión de duración cada una de ellas.

El curso comenzará con una sesión de apertura en la que además se expondrá el desarrollo del curso y se facilitará información sobre las instalaciones y servicios del Centro y otros aspectos administrativos. El Curso finalizará con un acto de clausura (1 sesión).

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. La duración de esta fase será de 4 semanas.

La fase presencial tendrá una duración de 50 horas, distribuidas en 2 semanas a razón de 5 horas diarias. Las exposiciones orales de los profesores cubren 5 horas. Para comprobar que los alumnos alcanzan los resultados de aprendizaje se programarán ejercicios prácticos. La duración total de estas prácticas será de 45 horas.

5.3. Criterios de Evaluación.

Los módulos de la fase presencial, se evaluarán mediante una evaluación continua de cada uno de los módulos que combinará:

- Evaluación por observación por parte del profesor de la resolución de problemas y prácticas realizadas durante las sesiones prácticas. Esta nota supondrá el 60% de la nota final.
- Dos pruebas escritas de carácter teórico, teórico–práctico o práctico cada una de ellas sobre el temario de dos módulos y cuya media supondrá el 40% de la nota final. En el caso que un alumno no supere una prueba se le podrá realizar una prueba complementaria.

Se considerará superado el Curso, cuando se haya obtenido una puntuación igual o superior a cinco (5) puntos, sobre una escala de cero (0) a diez (10) puntos en la media ponderada de las observaciones y prueba escrita de cada uno de los módulos. La no superación de un módulo supondrá la no superación del Curso.

Superado el Curso, el alumno recibirá un certificado acreditativo, procediéndose posteriormente a publicar en el BOD la superación del Curso.

6. RECURSOS DE PERSONAL

Director: La Escuela Superior de la Fuerzas Armadas nombrará un Director del Curso

Coordinador: La Escuela de Mando, Control y Telecomunicaciones del Ejército del Aire nombrará un Coordinador del Curso.

Personal docente:

- La fase a distancia será impartida por profesores militares, destinados en la EMACOT y pertenecientes al Departamento de TELYE de ese Centro.
- La fase presencial será impartida por personal de la empresa SIDERTIA SOLUTIONS apoyado por personal de la EMACOT

Personal de apoyo:

- La EMACOT facilitará los apoyos para administración, uso de los medios y servicios con personal propio del centro.

7. RECURSOS DE MATERIAL

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

Para la fase presencial: El curso se impartirá en aula de informática de la EMACOT, equipada con ordenadores y conexión a red e internet. Características del aula:

- Capacidad: 15 puestos + 1 puesto profesor, PCs con procesador i5 y 8 gigas de 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.

Se dispone del 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 EMACOT en el mismo horario que el resto de profesores y alumnos del centro.

Financiación: Este curso será financiado con los créditos del CESEDEN

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

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

Resultados previstos: Se trata de un curso de nueva creación, con contenidos relativos a un campo novedoso en el Ministerio de Defensa. Los alumnos son personal profesional, con experiencia y conocimientos previos en esta materia, que ya están trabajando en el ámbito de la ciberdefensa y que están interesados en completar su formación para continuar en este campo elegido voluntariamente y hacia el que posiblemente deseen orientar su carrera por lo que se prevé una tasa de éxito por encima del 92 %

La comprobación de resultados del aprendizaje se va a basar, según se detalla en el punto 5 (apartado "criterios de evaluación").

Efectos y servidumbres: La superación del Curso facultará al personal para:

- Desempeñar los cometidos de los puestos de ciberdefensa en la estructura del Ministerio de Defensa.
- Realizar algunas funciones relacionadas con seguridad de los sistemas TIC del Ministerio de Defensa.
- Ocupar destinos que exijan haber realizado este curso en la Relación de Puestos Militares (RPM) cuando así se definan.

9. SISTEMA DE GARANTÍA INTERNA DE CALIDAD.

Sistema de Garantía de Calidad del Plan de Estudios:

El Director y Coordinador del curso serán los responsables de gestionar, coordinar y realizar el seguimiento a este Plan de Estudios.

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 de la EMACOT, 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.

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 de la EMACOT implicado en la realización del curso.

Este informe y, en su caso, las observaciones del MCCD, órgano que genera la necesidad del curso, se utilizarán para realizar el informe de evaluación interna y proponer modificaciones. Los resultados de la evaluación interna se remitirán a DIGEREM.

10. CALENDARIO DE IMPLANTACIÓN.

El Primer Curso de Análisis Forense se ajustará a lo siguiente:

- Inicio Fase a distancia: 24ABR17.
- Fin Fase a Distancia: 26MAY17.
- Inicio Fase presencial: 29MAY17.

- Fin Fase presencial: 09JUN17.
- Remisión Informe Centro y Actas: NLT 30JUN17.
- Remisión informe a DIGEREM: TBD.

Madrid, a 23 de febrero 2017

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

Rafael Sánchez Ortega

ANEXOS:

ANEXO I: RESUMEN DE MATERIAS

ANEXO II: PLAN DE ESTUDIOS

ANEXO II: INFORME DE VIABILIDAD

INTENCIONADAMENTE EN BLANCO

CURRÍCULO CURSO DE ANÁLISIS FORENSE DE CIBERDEFENSA

ANEXO I: RESUMEN DE MATERIAS

ORGANIZACIÓN TEMPORAL DEL CURSO

MODULO	HORAS	ORGANIZACIÓN TEMPORAL
1.- Contenido teórico Analista Forense Digital	50	A Distancia
2.- Procedimiento de actuación forense: escenario y tratamiento de evidencias	9	Presencial
3.- Análisis de sistemas y dispositivos móviles: forense postmortem y online	30	Presencial
4.- Presentación de resultados y actuación pericial práctica.	9	Presencial

RELACIÓN ENTRE RESULTADOS, MÓDULOS Y MATERIAS DEL CURSO

RESULTADOS APRENDIZAJE	MODULOS	MATERIAS
Describe el proceso de un análisis forense en general.	1	Introducción Forense digital Peritaje y pericia Procedimiento forense
Compara las diferencias existentes en la obtención de evidencias forenses digitales procedentes de soportes de almacenamiento magnéticos y de estado sólido.	2	Forense digital sobre medios de almacenamientos masivos. Recogida de evidencias.
Aplica las herramientas de Sysinternals para examinar partes claves del sistema operativo incluyendo la programación de subprocesos, la paginación, la asignación de memoria virtual y memoria física	3	Análisis forense digital de sistemas MS Windows
Realiza análisis forense digital de medios de almacenamiento masivo.	2, 3	Forense digital sobre medios de almacenamiento masivos. Recogida de evidencias. Análisis de sistemas y dispositivos móviles: forense postmortem y online

RESULTADOS APRENDIZAJE	MODULOS	MATERIAS
Realiza análisis forense digital de sistemas MS-Windows	3	Análisis forense digital de sistemas MS Windows
Describe los métodos empleados por las últimas versiones del sistema Windows para guardar información de su funcionamiento centrándose en el log de eventos, archivos Prefetch, archivos de navegación y el registro del sistema.	3	Análisis forense digital de sistemas MS Windows
Realiza análisis forense sobre dispositivos móviles.	3	Análisis forense de dispositivos móviles. Análisis de aplicaciones móviles
Describe con precisión los aspectos legislativos del análisis forense.	4	Aplicación práctica de la Legislación en un caso forense
Redacta un informe de un análisis forense digital.	4	Elaboración de un informe asociado a un caso forense

CURRÍCULO CURSO DE ANÁLISIS FORENSE DE CIBERDEFENSA

ANEXO II: PLAN DE ESTUDIOS

MODULO	CONTENIDOS	DISTANCIA	PRESENCIAL		
		Teórica	Teórica	Práctica	Pruebas
1.- Contenido teórico Analista Forense Digital	1. Introducción 2. Forense digital 3. Peritaje y pericia 4. Procedimiento forense	50	x	x	x
2.- Procedimiento de actuación forense: escenario y tratamiento de evidencias	1. Introducción 2. Forense digital sobre medios de almacenamientos masivos. 3. Recogida de evidencias.	x	0,5	8,5	1 hora prueba escrita fase no presencial
3.- Análisis de sistemas y dispositivos móviles: forense postmortem y online	1. Análisis forense digital de sistemas MS Windows 2. Análisis forense digital de sistemas Linux 3. Análisis de memoria 4. Línea temporal 5. Análisis forense de dispositivos móviles 6. Análisis de aplicaciones móviles 7. Técnicas anti forenses	x	3	27	x
4.- Presentación de resultados y actuación pericial práctica	1. Elaboración de un informe asociado a un caso forense 2. Aplicación práctica de la Legislación en un caso forense	x	1,5	7,5	1
Total Horas		50	5	45	2

Al inicio de la fase presencial se realiza una prueba escrita de 1 hora de duración en la que se comprobará el perfil de ingreso y los conocimientos adquiridos en la fase a distancia.

Fase presencial: 50 horas (5 teóricas, 45 prácticas, 2 pruebas escritas [incluyendo la prueba correspondiente al módulo de la fase a distancia]), 1 hora para apertura y 1 hora para la clausura.

CURRÍCULO CURSO DE ANÁLISIS FORENSE DE CIBERDEFENSA

ANEXO III: INFORME DE VIABILIDAD

Nº de alumnos/año que se necesita formar: 15 alumnos.

Periodicidad del curso: Máximo 1 curso por año.

Coste de la acción formativa por curso:

Dietas Alumnos:	6.000 €
Locomoción:	2.500 €
Asistencias profesorado:	300 €
Sidertia Solutions:	6.200 €
Material de oficina:	1.000 €