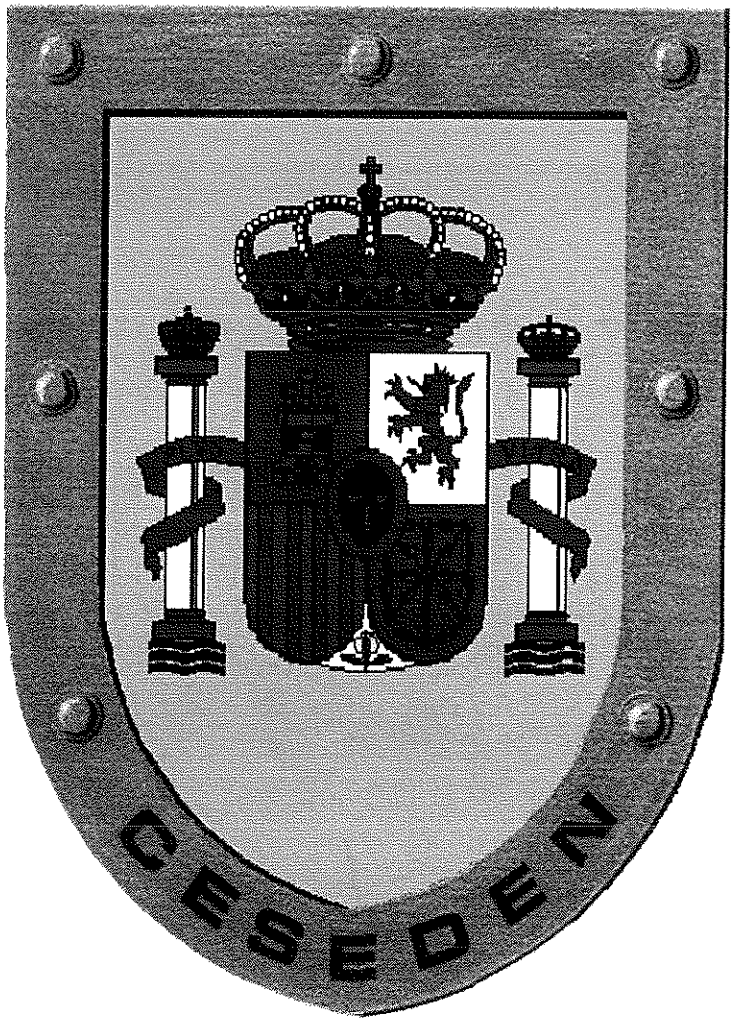
MINISTERIO
DE
DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR DE
ESTUDIOS DE LA DEFENSA
NACIONAL



CURRÍCULO

CURSO DE OPERADOR DE MONITORIZACIÓN DE CIBERDEFENSA

Abril 2017

PAGINA INTENCIONADAMENTE EN BLANCO

CURRÍCULO DEL CURSO DE OPERADOR DE MONITORIZACIÓN DE CIBERDEFENSA

1. DESCRIPCIÓN GENERAL DEL CURSO

1.1. Denominación

Curso de operador de monitorización de Ciberdefensa.

1.2. 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.

1.3. Categoría del Curso

No aplicable por tratarse de un curso informativo.

1.4. Duración

Fase a distancia: 50 horas. Fase presencial: 50 horas.

1.5. Idioma

Español, pudiendo impartirse alguna materia en inglés.

1.6. Centro responsable y lugar donde se imparte

El responsable del curso es el Centro de Estudios Superiores de la Defensa (CESEDEN), siendo impartido en la Escuela de Mando, Control y Telecomunicaciones del Ejército del Aire (EMACOT).

1.7. Modalidad de enseñanza

Semipresencial.

1.8. Número máximo de alumnos por curso

15.

2. JUSTIFICACIÓN

2.1. Justificación del curso.

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 FORCIBE es un documento para uso interno de las Fuerzas Armadas.

En la actualidad no existen en el MINISDEF cursos que cubran las necesidades de formación expresadas en el punto 4.1 del Plan FORCIBE para los operadores de monitorización de los CIS, cuya misión fundamental es comprobar el estado de los sistemas bajo su supervisión, controlando los eventos del sistema. Este curso proporcionará las competencias necesarias para capacitar al alumno en el desempeño de las funciones de operador de monitorización

Se trata de un curso sin precedentes en el sistema de enseñanza militar y la necesidad de desarrollar este curso de nueva creación está aprobada por el JEMAD cuando de acuerdo con los puntos 4 y 5 de su Directiva 03/16 para la puesta en marcha de cursos de perfeccionamiento en el ámbito conjunto, se ha identificado la necesidad operativa y se ha analizado la viabilidad del curso.

2.2. Descripción de los procedimientos de consulta.

El currículo se ha elaborado basándose en las directrices marcadas en la Directiva 03/16 del JEMAD. Siguiendo esta Directiva, se ha partido de la necesidad formativa para operadores de monitorización de los CIS 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 general del curso es proporcionar las competencias necesarias para que los operadores de monitorización de los CIS puedan comprobar el estado de los sistemas bajo su supervisión, controlando los eventos del sistema.

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

- Describir como se hace la gestión de vulnerabilidades y qué herramientas se utilizan.
- Describir el ciclo de vida en la gestión de vulnerabilidades.
- Describir el procedimiento de monitorización, detección de incidentes y su gestión.
- Clasificar los incidentes de seguridad.
- Describir el proceso de monitorización, identificando qué se debe monitorizar, y las amenazas prestando especial atención a las más frecuentes y a las nuevas
- Investigar los registros de actividad (logs) de los dispositivos de un CIS tales como: IDS/IPS, Firewall, Proxy, DNS, Controlador de Dominio u otros.
- Explicar el funcionamiento de un SIEM.
- Describir la configuración de un SIEM.
- Instalar y administrar los sistemas de monitorización como IDS/IPS
- Operar y administrar los SIEM corporativos de MDEF, desarrollando reglas de correlación y el parseo de nuevas fuentes.
- Analizar los eventos que se producen en un SIEM detectando las posibles intrusiones.
- Interpretar la monitorización de eventos en equipos y dispositivos individuales

- Operar herramientas de monitorización y ticketing como LUCIA, CARMEN y REYES
- Describir los aspectos legales de la monitorización y manejo de información clasificada.

4. PERFIL DE INGRESO

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 y pruebas de admisión

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 la monitorización los CIS.

Los alumnos deberán tener conocimientos avanzados en ciberdefensa que incluyan:

- Describir de manera precisa los elementos de la infraestructura de un CIS: routers, IDS, switches, firewall y otros.
- Describir los servicios de un CIS tales como: servidores web, bases de datos, correo electrónico, DHCP, DNS, controlador de dominio.
- Describir servicios, mecanismos y protocolos de seguridad más comunes en las redes (SSH, SCP, FTP, TELNET, HTTP/S y otros).
- Utilizar herramientas básicas de administración de sistemas como Vterminal, Putty o Citrix.
- Identificar los distintos tipos de tecnologías inalámbricas.
- Describir los dispositivos y software específicos de seguridad com Antivirus, Firewall, VPN, IDS/IPS, SIEM, Data Loss Protection, Network Access Control, Web Application Firewall y otros.
- Describir y aplicar las estrategias de sensorización para distintos elementos de un sistema en red y analizar de manera básica los eventos observados.
- Describir la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas y procedimientos de seguridad.
- Describir los procedimientos técnicos para la implantación, configuración y mantenimientos de redes de manera segura.
- Describir y aplicar los conceptos básicos relativos a los test de penetración/ análisis de vulnerabilidades.
- Identificar las técnicas de ocultación de ataques a sistemas y redes.
- Fundamentos de programación en C#, y Python.
- Administrar sistemas operativos: Unix, Microsoft Windows, Android, IOS.
- Administrar entornos virtuales.

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

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 presencial del curso se evaluará:

- Los conocimientos avanzados en ciberdefensa descritos como requisitos de acceso, 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.
- 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 20% de la nota final para ingreso:

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

La suma, teniendo en cuenta su ponderación, de los dos 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.

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

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 electrónica) 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.

4.4. Reconocimiento de créditos

No se efectuará reconocimiento de créditos de este curso.

5. PLAN DE ESTUDIOS

5.1. Estructura general del Plan de Estudios

Este Curso tendrá 2 fases. Fase a distancia con una duración de 50 horas, a desarrollar en 4 semanas sin dedicar tiempo de la jornada laboral y fase presencial con una duración de 50 horas, a desarrollar en 2 semanas.

El Curso está dividido en cuatro Módulos, descritos en el Anexo II.

5.2. Descripción de los módulos

Ver Anexo II.

5.3. 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. La materia se impartirá a partir de clases teóricas en las que el profesor expondrá a los alumnos la materia, combinadas con clases prácticas en las que los estudiantes resolverán ejercicios prácticos relacionados con esa materia. En total se dedicarán 11 horas a las exposiciones teóricas de estas materias y 36 a las clases prácticas. Quedaran 3 horas para la realización de pruebas escritas.

5.4. Criterios de Evaluación.

El módulo 1, impartido en la fase a distancia se evaluará junto con la prueba escrita del módulo 2. Los módulos de la fase presencial, se evaluarán mediante una evaluación continua de cada uno de ellos que combinará:

- Evaluación por observación por parte del profesor de la resolución de problemas y prácticas realizadas durante las sesiones prácticas del módulo. Esta nota supondrá el 60% de la nota final del módulo.
- Una prueba escrita de carácter teórico, teórico-práctico o práctico a la finalización de cada módulo que supondrá el 40% de la nota final del módulo. 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 ESFAS nombrará un Director del Curso

Coordinador: La EMACOT 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 Telecomunicación y Electrónica de ese centro.
- La fase presencial será impartida por personal de la empresa SIDERTIA.

Personal de apoyo:

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

7. RECURSOS MATERIALES Y SERVICIOS

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: 25 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.

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

8.1. 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.

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

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%

8.2. 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 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.

9.1. 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.

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 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.

Antes de la finalización del curso la dirección del curso pasará una encuesta a los alumnos. Esta encuesta cubrirá 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 de la EMACOT 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 está incluido en el "Registro de centros, cursos y títulos" y se puede acceder a este registro a través de la intranet del Ministerio de Defensa, en la página correspondiente al CESEDEN y a la EMACOT del EA.

10. CALENDARIO DE IMPLANTACIÓN.

Curso de operador de monitorización de Ciberdefensa:

- Convocatoria: septiembre 2017.
- Designación de alumnos: septiembre 2017.
- Inicio del curso: octubre 2017.
- Fin del curso: noviembre 2017.
- Remisión Informe Centro y Actas: noviembre 2017.
- Remisión informe a DIGEREM: noviembre 2017.

Madrid, a 28 de abril 2017

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

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL
DIRECTOR

Rafael Sanchez Ortega

ANEXOS:

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

PAGINA INTENCIONADAMENTE EN BLANCO

ANEXO I: INFORME DE VIABILIDAD

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

Periodicidad del curso: Máximo 1 curso por año. (15 alumnos por curso aproximadamente).

Coste de la acción formativa por curso:

Docencia profesores empresa:	7.000 €
Asistencias profesorado:	300 €
Dietas Alumnos:	8.500 €
Material de oficina:	1.200 €

PAGINA INTENCIONADAMENTE EN BLANCO

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

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS

MODULO	HORAS	ORGANIZACIÓN TEMPORAL
1. Operaciones de monitorización de seguridad.	50	Fase a distancia
2. Operaciones de monitorización y gestión de incidentes	14	Al inicio de la fase presencial
3. Intrusiones y monitorización de la seguridad de una infraestructura TIC	20	A continuación del módulo 2
4. Vulnerabilidades y explotación	14	A continuación del módulo 3

DESCRIPCIÓN DE LOS MÓDULOS

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
Operaciones de monitorización de seguridad	- Introducción - Seguridad y monitorización - Gestión de incidentes - Triage y resolución de incidencias - IDS/IPS - SIEM - Vulnerabilidades de seguridad	50			
Operaciones de monitorización y gestión de incidentes	- Introducción a las operaciones de monitorización - Monitorización de eventos. - Gestión de incidentes - Triage y resolución de incidencias - Respuesta ante incidentes de seguridad		3	10	1
Intrusiones y monitorización de la seguridad de una infraestructura TIC	- Sistemas de detección de intrusiones: IDS/IPS - Implantación y puesta en producción de sistemas IDS/IPS. - Sistemas SIEM - Operaciones sobre un sistema SIEM		4	16	1
Vulnerabilidades y explotación	- Vulnerabilidades de seguridad - Análisis y gestión de vulnerabilidades		4	10	1
	- Clausura				
	Total	50	11	36	3

Horas de clase:

Fase a distancia: 50 horas.

Fase presencial: 50 horas (11 teóricas, 36 prácticas y 3 pruebas escritas [la primera prueba escrita corresponderá a los módulos 1 (fase a distancia) y 2]).

Hay que añadir 2 sesiones. 1 Sesión de inauguración y presentación del curso el primer día y 1 sesión para la clausura el último día.

Módulo 1 Operaciones de monitorización de seguridad. Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Describir los aspectos legales de la monitorización y manejo de información clasificada.
- Clasificar los incidentes de seguridad.
- Investigar los registros de actividad (logs) de los dispositivos de un CIS tales como: IDS/IPS, Firewall, Proxy, DNS, Controlador de Dominio u otros.

Módulo 2. Operaciones de monitorización y gestión de incidentes. Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Describir el proceso de monitorización, identíficando qué se debe monitorizar, y las amenazas prestando especial atención a las más frecuentes y a las nuevas
- Operar herramientas de monitorización y ticketing como LUCIA, CARMEN y REYES

Módulo 3 Intrusiones y monitorización de la seguridad de una infraestructura TIC. Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Explicar el funcionamiento de un SIEM.
- Describir la configuración de un SIEM.
- Instalar y administrar los sistemas de monitorización como IDS/IPS
- Operar y administrar los SIEM corporativos de MDEF, desarrollando reglas de correlación y el parseo de nuevas fuentes.

Módulo 4 Vulnerabilidades y explotación. Contenidos: Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Describir la gestión de vulnerabilidades y qué herramientas se utilizan.
- Describir el ciclo de vida en la gestión de vulnerabilidades.
- Analizar los eventos que se producen en un SIEM detectando intrusiones.
- Interpretar la monitorización de eventos en equipos y dispositivos individuales.