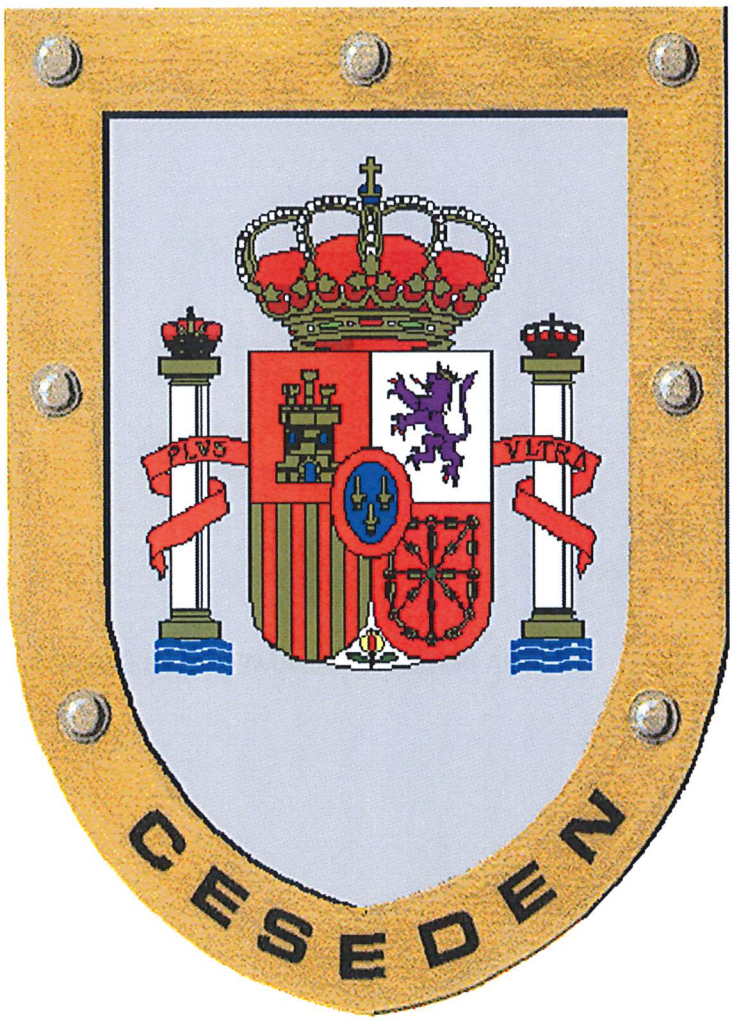
MINISTERIO
DE
DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR DE ESTUDIOS
DE LA DEFENSA NACIONAL



CURRÍCULO

CURSO DE AUDITORÍA DE SEGURIDAD DE CIBERDEFENSA

Enero 2018

PAGINA INTENCIONADAMENTE EN BLANCO

CURRÍCULO DEL CURSO DE AUDITORIA DE SEGURIDAD DE CIBERDEFENSA

1. DESCRIPCIÓN GENERAL DEL CURSO

1.1. Denominación

Curso de auditoría de seguridad de Ciberdefensa.

1.2. 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 conjunto, informativo e indistinto.

1.3. Categoría del Curso

No aplicable por tratarse de un curso informativo.

1.4. Duración

100 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.

La ciberdefensa en el ámbito del MINISDEF depende en gran medida de la calidad de la formación de aquellos que tienen responsabilidades en esta materia. Esta calidad se basa en una formación

orientada directamente a las funciones de cada uno de los puestos relacionados con las actividades de la ciberdefensa. La formación debe abarcar los aspectos técnicos y los eminentemente operativos.

Para conseguir que el personal dedicado a estas tareas adquiera, mejore y actualice las competencias necesarias en ciberdefensa, se ha redactado el Plan de Formación en Ciberdefensa (FORCIBE), que fue aprobado por el JEMAD en abril de 2015.

El objetivo fundamental del Plan es definir los requisitos de formación, en materia de ciberdefensa, que deberían alcanzar los profesionales del MINISDEF que ocupen puestos de trabajo relacionados con este ámbito.

En la redacción de este Plan FORCIBE se han tenido en cuenta:

- El estudio de los cometidos relacionados con la ciberdefensa del personal del MINISDEF.
- Las medidas de protección aplicables en los sistemas de información y telecomunicaciones para garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información, incluidas en el concepto de Seguridad de la Información y Telecomunicaciones (SEGINFOSIT). Estas medidas están identificadas en la normativa vigente y las guías desarrolladas por el Centro Criptológico Nacional;

Este plan posibilita, además, establecer unos itinerarios formativos que permitan alcanzar la capacitación necesaria para cada uno de los distintos grupos de formación identificados en él.

Al objeto de establecer las necesidades de formación se han identificado las funciones relacionadas con la ciberdefensa que desempeña el personal del MINISDEF. En base a éstas, se han definido los grupos funcionales que requieren una determinada formación. Dichos grupos funcionales están orientados a cubrir las capacidades definidas por el JEMAD en su documento "Visión sobre la Ciberdefensa" y que son de defensa, explotación y respuesta.

Dentro de los grupos con funciones técnicas, se encuentran los administradores de seguridad, cuya formación es el objeto del presente informe y que son responsables de realizar auditorías de seguridad a los sistemas, tanto en sus aspectos técnicos como procedimentales y de dirigir los equipos técnicos de inspección.

Una auditoría de un Sistema de Información (SI) es un estudio que consiste el análisis de las características de dicho sistema para para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Normalmente la auditoría de seguridad se hace en aplicación de una normativa concreta como puede ser una norma ISO. En el ámbito del Ministerio de Defensa pueden abarcar desde la inspección de sistemas acreditados o que pretenden serlo hasta sistemas no clasificados pero que tienen que cumplir estándares como los definidos en el Esquema Nacional de Seguridad (ENS).

Las auditorías de seguridad de un SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Desde el punto de vista de las Fuerzas Armadas el persona que cubra estas funciones debería tener conocimientos de análisis de vulnerabilidades, gestión de riesgos y de las normativas en cuya aplicación se pretende auditar (OTAN, de ámbito nacional y privadas).

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.

Su estudio se ha desarrollado a partir de un Grupo de trabajo que ha contado con expertos de Centros Docentes Militares y de organismos de defensa relacionados con la ciberdefensa.

Se han estudiado los siguientes cursos sobre la auditoria de seguridad de ciberdefensa:

- En el ámbito civil existe un curso prestigioso que se denomina "Curso de oficial preparación CISA (Certified Information System Auditor)", impartido por la Information Systems Audit and Control Association (ISACA), pero no cubre aspectos técnicos de interés como pueden ser el uso de herramientas de análisis de vulnerabilidades, ni la normativa STIC o del ENS).
- Otro curso de interés, el de Vulnerability Assessmente de la Escuela OTAN en Oberammergau, se orienta al análisis de vulnerabilidades de REDY no trata los aspectos normativos del curso mencionado anteriormente.
- Por último, igual sucede con el curso de SANS conocido como AUD507: Auditing & Monitoring Networks, Perimeters & Systems, sus carencias en aspectos normativos hace que no cubra exactamente la formación buscada.
- Dentro del marco de la OTAN, España participa a través del MCCD en el GT "Ciberdefence Education & Training" donde se ha identificado la necesidad de formación en el campo de la auditoría de seguridad de ciberdefensa, aunque no se han concretado acciones comunes o desarrollos de otras naciones.

Teniendo en cuenta todos estos factores, y siguiendo los requerimientos identificados por el MCCD, se hace recomendable llevar a cabo la organización y convocatoria de este curso de auditoría de seguridad de ciberdefensa.

3. PERFIL DE EGRESO

El objetivo general del curso es proporcionar las competencias necesarias para que los auditores de seguridad de las TIC de las FAS puedan comprobar la aplicación de las medidas de seguridad de los sistemas, tanto en sus aspectos técnicos como procedimentales y de dirigir los equipos técnicos de inspección.

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

- Describir los aspectos de un análisis de riesgos.
- Utilizar la herramienta PILAR de análisis de riesgos
- Identificar las fases de un análisis de vulnerabilidades.
- Realizar un diagnóstico técnico del estado de protección de un sistema a nivel técnico utilizando herramientas de análisis de vulnerabilidades
- Verificar la documentación de seguridad necesaria para la acreditación de un sistema.
- Instalar, configurar y mantener servidores Windows de forma segura.
- Aplicación de las guías y estándares de seguridad nacionales y OTAN.

- Redactar informes completos de auditoría de seguridad de un CIS.
- Elaborar propuestas de ciberdefensa de un CIS basado en la auditoría a un CIS.

4. SISTEMA DE ADMISIÓN AL CURSO

4.1. Perfil de ingreso

Para poder acceder al curso los alumnos deberán tener conocimientos avanzados en ciberdefensa que incluyan:

- Gestionar y administrar la seguridad en infraestructuras de red, servidores, estaciones de trabajo y dispositivos móviles.
- Configuración segura de sistemas operativos, aplicaciones, servicios y otros elementos que conforman un sistema de información.

También se requerirá un nivel de inglés mínimo equivalente a 6 puntos, obteniendo estos de la suma de los rasgos del perfil SLP.

4.2. Categoría y empleo militar de los alumnos

El Curso se dirige a oficiales, suboficiales y personal civil funcionario del Ministerio de Defensa que tengan o vayan a tener cometidos técnicos relacionados con la acreditación de la seguridad de los CIS.

4.3. Formación previa

Los alumnos deberán estar en posesión de la habilitación de seguridad Reservado/NATO SECRET.

Será recomendable estar en posesión de cursos relacionados con la informática y el ámbito Cibernético, como son el Diploma de Informática Militar, Curso Avanzado de Ciberdefensa o Curso de Administrador de Seguridad.

4.4. Sistema de selección

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

Al inicio del curso se realizará una prueba en la que se evaluarán los conocimientos descritos como requisitos de acceso mediante una prueba escrita. Se puntuará de uno (1) a (10) y supondrá un 80% de la nota final para ingreso.

Los conocimientos de idioma inglés se valorarán puntuando de uno (1) a diez (10) según el perfil SLP de los solicitantes, de acuerdo con la siguiente tabla. Supondrá un 20% 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 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.

4.5. Información previa al curso

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.

4.6. Apoyo y orientación al alumnado

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

El Curso constará de fase a distancia (50h) sin dedicar tiempo de la jornada de trabajo, y fase presencial (50h), estando dividido en 5 módulos cuyo detalle es:

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS

MODULO	HORAS	ORGANIZACIÓN TEMPORAL
1. Acreditación Sistemas	11	Al inicio de la fase presencial
2. Análisis de Riesgos	10	A continuación del módulo 1
3. Bastionado Sistemas	14	A continuación del módulo 2
4. Auditoría nivel 3 (análisis de vulnerabilidades).	22	A continuación del módulo 3
5. Auditoría nivel 4 y 5 (Test de penetración caja blanca y caja negra).	43	A continuación del módulo 4

5.2. Descripción de los módulos

DESCRIPCIÓN DE LOS MÓDULOS

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
1 Acreditación de Sistemas	**Fase Presencial:** - Información clasificada. Legislación (LSO 9/1968, Ley 48/1978, RD 242/1969, RD 421/2004, OM 76/2002). - Proceso de Acreditación (CCN-STIC 101): - Tipos de Auditorías de Seguridad de las TIC (niveles). - Estudio y revisión documentación de seguridad (CCN-STIC 202, 203, 204, 207). - Inspección INFOSEC: o SEGINFOINS (Ins. 95/2011) o SEGINFOPER (Ins. 9/2011) o SEGINFODOC (Ins. 51/2013) o SEGINFOSIT: ▪ Seguridad de las emanaciones (CCN-STIC 103, 150, 151, 153). ▪ Estructura de Seguridad (CCN-STIC 201). ▪ Evaluación de los Procedimientos Operativos de Seguridad (POS). ▪ Inspección CIS: ▪ Análisis local. ▪ Análisis remoto. ▪ Informe Auditoría **Fase a distancia:** - CCN-STIC series 000 (Políticas), 100 (Procedimientos) y 200 (Normas).	6	4	0	1
2 Análisis de Riesgos	**Fase Presencial:** – Conceptos básicos de Análisis y Gestión del Riesgo. – Elementos del Riesgo (activos, vulnerabilidades, amenazas, salvaguardas). – Metodologías de Análisis de Riesgos (MAGERIT, CRAMM, OCTAFVE, MEHARI, ISO 3100, NIST SP 800-30). – MAGERIT. – Herramienta PILAR. **Fase a distancia:** – CCN-STIC 410 (Análisis de riesgos en Sistemas de la Administración) y 470 (PILAR).	5	3	1	1
3 Bastionado de Sistemas	**Fase Presencial:** - Normativa Nacional. • CCN-STIC para sistemas con información clasificada. o CCN-STIC 301 Requisitos STIC. o CCN-STIC 302 Interconexión STIC. o Series 500 CCN-STIC (Windows). o Series 600 CCN-STIC (Otros).	9	3	1	1

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
	• ENS para administración. - Normativa Internacional. • OTAN (Guías NCIRC). **Fase a distancia:** - Elección, lectura y aplicación de 3 guías CCN-STIC de bastionado (series 400, 500 o 600) sobre el software que desee el alumno.				
4 Auditoría nivel 3 (Análisis de vulnerabilidades)	**Fase Presencial:** - Conceptos básicos de un Análisis de Vulnerabilidades. - Metodologías de Análisis de Vulnerabilidades (OSSTMM, ISSAF, NIST). - Fases de un Análisis de Vulnerabilidades. - Fase 1: Planificación. - Herramientas Fase 1 (Project). - Fase 2: Recopilación de información. - Herramientas Fase 2 (tanto online como offline). - Fase 3: Mapeo de Red. - Herramientas Fase 3 (nmap). - Fase 4: Identificación de Vulnerabilidades. - Herramientas Fase 4 (nessus, openvas, nikto). - Fase 5: Cumplimiento con normativa de seguridad. - Herramientas Fase 5 (Herramientas CLARA y ROCIO). - Ejemplo contenido de un Informe de Auditoría nivel 3 para la Acreditación de un Sistema. **Fase a distancia:** - Manual de la herramienta CLARA. - Temas 1, 2, 4, 5, 6 y 8 del libro "Nmap 6: Network Exploration and Security Auditing Cookbook". - Instalación de OpenVas y Nessus sobre Kali Linux, análisis de cada uno de ellos y comparativa de un escaneo remoto sobre una misma máquina objetivo.	12	4	5	1
5 Auditoría de nivel 4 y 5 (test de penetración caja blanca y caja negra)	**Fase Presencial:** - Conceptos básicos de Kali Linux. - Introducción a las fases de un Test de Penetración. - Fase 1: Reconocimiento. - Fase 2: Enumeración y Análisis de Vulnerabilidades. - Fase 3: Ganar acceso. - Fase 4: Elevación de privilegios. - Fase 5: Movimiento lateral y borrado de evidencias. - CTF y ejemplo del contenido de un Informe de Auditoría niveles 4 y 5 para la Acreditación de un Sistema. **Fase a distancia:** - Elección y ejecución de uno de los siguientes cursos gratuitos online de Offensive Security: "Metasploit Unleashed" o "Kali Linux Revealed".	18	11	13	1

MODULO	CONTENIDOS	Distancia	PRESENCIAL		
		Teórica	Teórica	Práctica	Prueba
	- Elección de una o varias máquinas virtuales de la página web "vulnhub.com" y realizarlas a modo CTF siguiendo las fases de un test de penetración.				
	Total	50	25	20	5

Horas: 100 horas (Fase a distancia: 50 horas. Fase presencial: 50 horas: 25 teóricas, 20 prácticas y 5 pruebas prácticas escritas). Fuera del currículo 2 sesiones: 1 sesión de inauguración y presentación del curso y agenda del mismo y 1 sesión para la clausura el último día.

Módulo 1 Acreditación de un Sistema (Se imparte en las fases a distancia y presencial) Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Conocer la legislación por la cual se ha de acreditar un sistema que maneje información clasificada.
- Conocer la normativa nacional vigente a aplicar en el Proceso de Acreditación de un Sistema (CCN-STICs).

Módulo 2. Análisis de Riesgos (Se imparte en las fases a distancia y presencial). Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Describir los conceptos básicos de Análisis y Gestión del Riesgo, así como los elementos del Riesgo.
- Conocer las principales metodologías de Análisis de Riesgos, en especial MAGERIT.
- Utilizar la herramienta PILAR para la realización de Análisis de Riesgos.

Módulo 3. Bastionado de un Sistema (Se imparte en las fases a distancia y presencial) Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Conocer la normativa nacional vigente a aplicar en el bastionado de un Sistema que maneje información clasificada (CCN-STICs).
- Aplicar las guías CCN-STICs correspondientes para bastionar un sistema en función de su Sistema Operativo, rol, servicios.
- Auditar un sistema utilizando las listas de comprobación de las guías CCN-STIC.
- Conocer el Esquema Nacional de Seguridad a aplicar en las Administraciones Públicas.
- Conocer la existencia de guías internacionales como las NCIRC de OTAN.

Módulo 4. Auditoría nivel 3 análisis de vulnerabilidade. (Se imparte en las fases a distancia y presencial) Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Describir los conceptos básicos de un análisis de vulnerabilidades.
- Conocer las metodologías más conocidas de análisis de vulnerabilidades.
- Ejecutar un análisis de vulnerabilidades con todas y cada una de sus fases.
- Utilizar las herramientas nmap, nessus, openvas, nikto, appdetective.

- Utilizar las herramientas del CCN CLARA y ROCIO.
- Realizar el Informe y conclusiones de la Auditoría Nivel 3. Recoger en un informe ejecutivo los aspectos más importantes hallados en la auditoría nivel 3.
- Detallar las deficiencias encontradas en un informe técnico y realizar las recomendaciones y/o acciones correctivas correspondientes derivadas de la auditoría.

Módulo 5 Auditoría de nivel 4 y 5 Test de penetración de caja blanca y caja negra. (Se imparte en las fases a distancia y presencial) Resultado del Módulo: Al finalizar la materia el alumno será capaz de:

- Conocer qué es la plataforma de análisis Kali, cómo manejarse en un entorno Linux y qué herramientas contiene para realizar un Test de Penetración.
- Saber diferenciar las diferentes fases de un Test de Penetración: Reconocimiento, Enumeración y Análisis de Vulnerabilidades, Ganar acceso, Elevación de Privilegios, Movimiento lateral y borrado de evidencias.
- Entender las diferentes formas de Reconocimiento.
- Comprender los diferentes tipos de Escaneos de Red.
- Entender y realizar ataques de Infraestructura de Red y DNS, para posteriormente saber cómo defenderse de ellos.
- Comprender las diferentes Vulnerabilidades de Corrupción de Memoria y sus protecciones.
- Entender y practicar los diferentes ataques a Aplicaciones Web para saber cómo protegerse de ellos.
- Comprender los diferentes ataques al Cliente.
- Entender y practicar los diferentes tipos de ataques Password.
- Comprender y utilizar las diferentes formas de redirección, tunelizado y encapsulado de tráfico.
- Saber manejar Metasploit Framework.
- Saber usar Exploits públicos que no estén incluidos dentro de Metasploit.
- Realizar bypassing de Antivirus.
- Borrar evidencias del Test de Penetración.
- Elaborar Informe y conclusiones Auditoría Nivel 4 y 5.
- Realizar un CTF reducido (4h) y recoger en un informe ejecutivo los aspectos más importantes hallados en la auditoría nivel 4 y 5, explicando al cliente en qué condiciones se encuentra el objetivo víctima planteado.
- Detallar las deficiencias encontradas en un informe técnico.
- Realizar las recomendaciones y/o acciones correctivas correspondientes derivadas de la auditoría.

5.3. Metodología de enseñanza-aprendizaje.

El curso se impartirá en formato semipresencial.

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.

5.4. Criterios de Evaluación.

El curso evaluará mediante el sistema de evaluación continua que combinará:

- Evaluación por observación por parte del profesor de la resolución de problemas y trabajos prácticos realizados durante las sesiones prácticas. Esta nota supondrá el 60% de la nota final del curso.
- Cinco (5) pruebas escritas, cuya media ponderada supondrán el 40% de la nota final del curso. Se considerará aprobada cuando se haya obtenido una puntuación igual o superior a cinco (5) puntos, sobre una escala de cero (0) a diez (10) puntos en cada una de las pruebas escritas.

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 pruebas escritas.

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

6. REQUISITOS DEL PROFESORADO Y PERSONAL DE APOYO

6.1. Personal académico.

La fase a distancia será impartida por 2 profesores militares, destinados en la EMACOT y pertenecientes al Departamento de Telecomunicación y Electrónica de ese centro. Deberán tener conocimientos a nivel gestor de la plataforma Moodle, a emplear esta fase.

La fase presencial será impartida por personal de la empresa SIDERTIA con titulación superior en áreas relacionadas con la informática y telecomunicaciones complementadas con acreditaciones de las principales empresas de software y seguridad de sistemas. Se requieren 4 profesores.

6.2. Otro personal personal.

Director: El CESEDEN nombrará un Director del Curso que pertenecerá a su Escuela Superior de las Fuerzas Armadas.

Coordinador: La EMACOT nombrará un Coordinador del Curso.

Personal de apoyo: No se requiere personal de apoyo para las clases. Los apoyos para administración, y servicios serán facilitados por personal propio de la ESTAER sin necesidad de dedicarlos en exclusividad al curso.

7. RECURSOS MATERIALES Y SERVICIOS

Para la fase a distancia: Los alumnos deberán disponer de conexión a la WAN PG del Ministerio de Defensa, con ordenador 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.

Sus resultados se emplearán como base para la redacción del informe final. Esta encuesta incluye la posibilidad de formular sugerencias por parte de los alumnos.

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 Escuela de Técnicas de Mando Control y Telecomunicaciones (EMACOT) del EA.

10. CALENDARIO DE IMPLANTACIÓN.

Curso de Auditoría de Seguridad de Ciberdefensa:

- Convocatoria: febrero 2.018.
- Designación de alumnos: febrero 2.018.
- Inicio del curso: abril 2.018.
- Fin del curso: junio 2.018.
- Remisión Informe Centro y Actas: junio 2.018.
- Remisión informe a DIGEREM: junio 2.018.

Madrid, a 16 de Enero 2.018

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

Rafael Sánchez Ortega

ANEXOS:

ANEXO I: INFORME DE VIABILIDAD

ANEXO II: DILIGENCIA DE VERIFICACIÓN

- 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

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

- Tasa de Éxito (TE) prevista: 88%
- Tasa de Bajas Académicas (TBA) prevista: 6%
- Tasa de Bajas a Petición Propia (TBPS) Prevista: 6%
- Tasa de Abandono (TA) prevista: 12%

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 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.

Debido a su carácter informativo, este curso no tiene servidumbres de ocupación de destinos ni de tiempos de servicios.

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 los resultados de aprendizaje definidos 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.

ANEXO III MODELO DE CERTIFICADO ACREDITATIVO DE SUPERACIÓN DEL CURSO

ANEXO I: INFORME DE VIABILIDAD

MINISTERIO
DE DEFENSA

USO OFICIAL

SUBSECRETARÍA DE DEFENSA
DIGEREM
SIGI ENSEÑANZA MILITAR
Código DIR3: EA0052928

FIRMA ELECTRÓNICA MINISDEF-EC-IUPG-PKI:
DIRECTOR GENERAL DE RECLUTAMIENTO Y ENSEÑANZA MILITAR
Jerónimo de Gregorio y Monmeneu
FECHA DE LA FIRMA: 20/07/2017

CESEDEN		MINISDEF-DIGEREM	
	FECHA DE REGISTRO (CET)		FECHA DE REGISTRO (CET)
ENTRADA	20/07/2017 18:37:23	SALIDA	20/07/2017 18:20:21
D-EM-CG-22000000-E-17-004277		D-CC-SB-4300000-S-17-009483	

OFICIO

S/REF.	2200-GG/SPC [..]S-17-002203 de 03/07/2017
N/REF.	455 / DYC1
FECHA	20/07/2017
ASUNTO	Re: INFORME VIABILIDAD CURSO AUDITORÍA SEGURIDAD (CIBERDEFENSA)
DESTINATARIO	DIRECTOR DEL CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL
COPIA	JEFE DEL ÁREA DE DIRECCIÓN GESTIÓN Y PROGRAMACIÓN DOCENTE DE LA DIGEREM

Como contestación a su escrito de la referencia le comunico que el Curso Auditoría Seguridad (CIBERDEFENSA) se considera como "Acción Formativa Viable", por lo que se puede continuar con el procedimiento indicado en la Orden DEF/464/2017, de 19 de mayo, por la que se aprueban las normas que regulan la enseñanza de perfeccionamiento y de Altos Estudios de la Defensa Nacional, para la aprobación tanto del currículo como de los perfiles de ingreso y egreso.

EL DIRECTOR GENERAL DE RECLUTAMIENTO Y ENSEÑANZA MILITAR

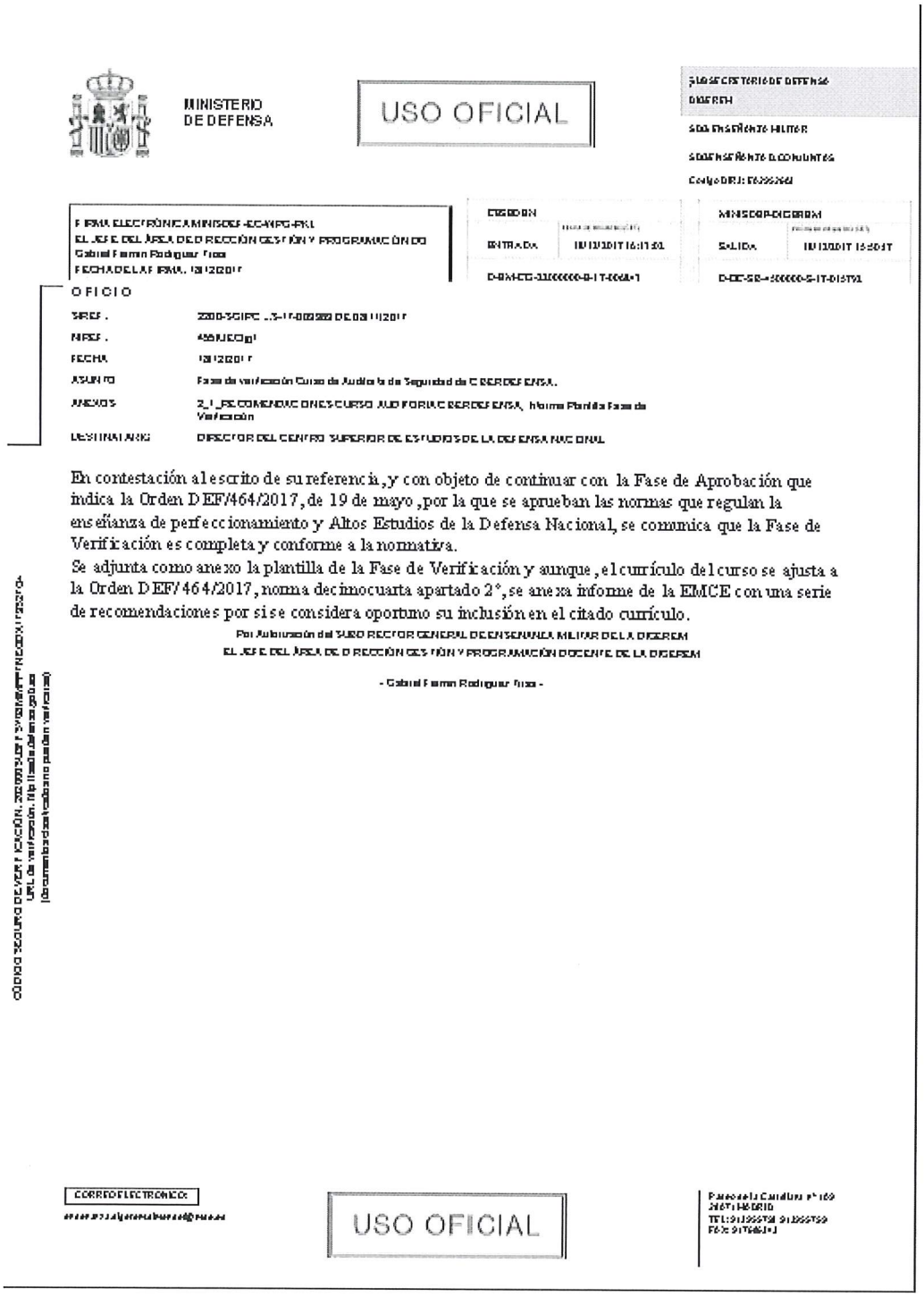
- Jerónimo de Gregorio y Monmeneu -

ANEXO II: DILIGENCIA DE VERIFICACIÓN

En virtud de lo dispuesto en la Orden DEF/469/2017, de 19 de mayo, por la que se aprueban las normas que regulan la enseñanza de perfeccionamiento y de Altos Estudios Militares, para dar cumplimiento a los dispuesto en su norma "Decimocuarta, y una vez se ha determinado que la acción formativa es viable a los efectos de lo dispuesto en la norma "Decimotercera" punto 3, se propone tras realizar la verificación a la que se hace mención en el punto 2 de la norma "Decimocuarta", el currículo del curso de "Auditoría de Seguridad (Ciberdefensa)",

SEA INFORMADO FAVORABLEMENTE

Al objeto de continuar con el proceso de aprobación de este currículo.



MINISTERIO
DE DEFENSA

USO OFICIAL

SUBSECRETARÍA DE DEFENSA
DIGEREM
SDG ENSEÑANZA MILITAR
SDGENSEÑANZA DOCUMENTOS
Código DIR3: E06956501

FIRMA ELECTRÓNICA MINISDEF-ECAMPG-PKI
EL JEFE DEL ÁREA DE DIRECCIÓN GESTIÓN Y PROGRAMACIÓN DO
Gabriel Fermín Rodríguez Ynsa
FECHA DE LA FIRMA: 19/12/2017

ORIGEN
ENTRADA 19/12/2017 16:11:01
D-ENTRADA-31000000-S-17-000491

MINISDEF-DIGEREM
SALIDA 19/12/2017 15:20:17
D-DE-SR-2000000-S-17-015791

OFICIO

SIREF.	2200-SGIPC-3-17-000589 DE 08/11/2017
NIPEF.	455NJECOg1
FECHA	19/12/2017
ASUNTO	Fase de verificación Curso de Auditor/a de Seguridad de CIBERDEFENSA.
ANEXOS	2_1_RECOMENDACIONES CURSO AUDITOR/A CIBERDEFENSA, Informe Plantilla Fase de Verificación
DESTINATARIO	DIRECTOR DEL CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

En contestación al escrito de su referencia, y con objeto de continuar con la Fase de Aprobación que indica la Orden DEF/464/2017, de 19 de mayo, por la que se aprueban las normas que regulan la enseñanza de perfeccionamiento y Altos Estudios de la Defensa Nacional, se comunica que la Fase de Verificación es completa y conforme a la normativa.

Se adjunta como anexo la plantilla de la Fase de Verificación y aunque, el currículo del curso se ajusta a la Orden DEF/464/2017, norma decimocuarta apartado 2°, se anexa informe de la EMCE con una serie de recomendaciones por si se considera oportuno su inclusión en el citado currículo.

Por Autorización del SUBDIRECTOR GENERAL DE ENSEÑANZA MILITAR DE LA DIGEREM
EL JEFE DEL ÁREA DE DIRECCIÓN GESTIÓN Y PROGRAMACIÓN DOCENTE DE LA DIGEREM

- Gabriel Fermín Rodríguez Ynsa -

CÓDIGO SEGURO DE VERIFICACIÓN: [illegible]

CORREO ELECTRÓNICO:
[illegible]

USO OFICIAL

Paseo de la Castellana nº 109
28071 MADRID
TFL: 91 3956758 91 3956759
FAX: 91 7960814

ANEXO III: MODELO DE CERTIFICADO ACREDITATIVO DE SUPERACIÓN DEL CURSO

Estado Mayor de la Defensa

Centro Superior de Estudios de la Defensa Nacional

Por cuanto el Empleo Cuerpo

D. Nombre y Apellidos

El Director del curso certifica que ha realizado del día y mes inicio al día y mes fin de año

I Curso de Auditoría de Seguridad de Ciberdefensa

Cuatro Vientos, a día y mes fin de año
El Coronel Director del Curso,

Fdo.: Nombre y Apellidos

Vº Bº
El General de División Director de la ESFAS

Nombre y Apellidos

NOTA PARA DESPACHO

CURRÍCULO DEL CURSO DE AUDITORÍA DE SEGURIDAD DE CIBERDEFENSA

De acuerdo con lo establecido en la Orden DEF 464/2017, el currículo ha sido verificado por DIGEREM.

De acuerdo con lo especificado en el OFICIO 455/UEC/jgf de DIGEREM "Fase de verificación Curso de Auditoría de Seguridad de CIBERDEFENSA" de 18 de diciembre de 2.017, que se adjunta a esta NOTA y que va incluido en el Currículo, **"la fase de verificación es completa y conforme a normativa y que el currículo del curso se ajusta a la Orden DEF 464/2017"**.

La Escuela Militar de Ciencias de la Información, (EMCE), Centro al que DIGEREM ha encomendado la realización del informe, hace una serie de recomendaciones por si se considera oportuno su inclusión. Con relación a éstas (incluidas en documento que se adjunta para despacho) se hacen las siguientes precisiones:

3 PERFIL DE EGRESO.

La modificación de este párrafo del currículo para hacer referencia a resultados de aprendizaje en vez a competencias haría necesario consultar a los órganos técnicos que han intervenido en su redacción, modificación del texto y, posiblemente volver a someterlo a verificación. Toda vez que DIGEREM ha determinado que el currículo del curso se ajusta a los requisitos, no se va a proceder a esta modificación.

Se tendrá en cuenta esta observación cuando se acometa la revisión del currículo.

4. SISTEMA DE ADMISIÓN AL CURSO.

Se ha modificado la redacción de los párrafos propuestos, salvo en lo relativo a "Reconocimientos o convalidaciones y homologaciones", que no figura en el Anexo a la Orden DEF 464/2017, que establece el formato del currículo y por el que se rige su redacción y tramitación.

Las modificaciones propuestas para el resto de párrafos han sido incluidas.

Se trata de un curso militar, indistinto, conjunto, de perfeccionamiento e informativo. **Una vez realizados los trámites** marcados en la Orden DEF 464/2017, **la autoridad para aprobar el currículo del curso recae en DICESEDEN**.

Se tiene previsto que la primera convocatoria del curso se realice para comenzar el 3 de abril de 2.018

10 de enero de 2.018