MINISTERIO
DE DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR DE ESTUDIOS
DE LA DEFENSA NACIONAL

CURRÍCULO

CURSO "AVANZADO DE CIBERDEFENSA"

Junio 2019

PAGINA INTENCIONADAMENTE EN BLANCO

CURRÍCULO DEL CURSO "AVANZADO DE CIBERDEFENSA"

REFERENCIAS

A. 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
B. Real Decreto 1111/2015, de 11 de diciembre, por el que se aprueba el Reglamento de adquisición y pérdida de la condición de militar y situaciones administrativas de los militares profesionales
C. 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.

1. DESCRIPCIÓN GENERAL DEL CURSO

Denominación

Curso Avanzado de Ciberdefensa.

Tipo de Curso

A efectos de aplicación del RD 339/2015 de la referencia A, artículos 4 y 13, el curso tiene la consideración de curso militar de perfeccionamiento, conjunto, de especialización e indistinto.

Objetivos del curso

El objetivo general del curso es proporcionar las competencias que capaciten para continuar la formación en cursos específicos para funciones técnicas del plan FORCIBE.

Adicionalmente, facilitará la adaptación y desarrollo dentro de la ciberdefensa de otras funciones críticas no exclusivas de este ámbito, como son la inteligencia, la logística, el planeamiento y conducción de operaciones, el adiestramiento, etc.

Categoría del curso

Categoría A, según el Real Decreto de la referencia B.

Duración

Fase previa no presencial

50 horas, en 4 semanas, sin dedicar tiempo de la jornada laboral.

Fase presencial

195 horas, en 8 semanas, y 175 horas de trabajo del alumno, más 5 horas no lectivas durante la fase presencial correspondientes a temas administrativos, conferencias especiales y ceremonias de inauguración y clausura, en total 375.

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 por personal con la acreditada cualificación y en el centro que se determine.

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, siendo el curso Avanzado de Ciberdefensa uno de ellos.

La ciberdefensa es un nuevo ámbito de las operaciones. Como tal, es fundamental contar con expertos que puedan planear y ejecutar misiones en el ciberespacio. La formación de este personal está todavía desarrollándose dentro del 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".

Desde la perspectiva de los cuadros de mando que deben planear y operar en el ámbito del ciberespacio, continúa existiendo la necesidad de dar una formación general de mayor profundidad y calado que el curso Básico de Ciberdefensa. En este sentido la necesidad de un curso avanzado surge de las mismas motivaciones que el curso básico pero incrementa los contenidos para servir de fundamento a la especialidad de Ciberdefensa, exigible en vacantes asociadas a este tipo de operaciones.

2.2. Descripción de los procedimientos de consulta

El currículo se ha elaborado a tenor de lo dispuesto en la Orden DEF/464/2017, partiendo de la necesidad formativa detectada por el MCCD. 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

Resultados de aprendizaje

Los alumnos que completen el curso deberán ser capaces de:

- Aplicar los mecanismos de cifrado y estenografía pertinentes para proteger los datos residentes en un sistema o en tránsito por una red
- Configurar, efectuar la carga de claves y administrar equipos de cifra
- Aplicar los mecanismos y procedimientos en la gestión de equipos de cifra
- Emplear los procedimientos de gestión de claves (generación, distribución, almacenamiento y destrucción de claves)
- Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto
- Describir los procedimientos técnicos para la implantación, configuración y mantenimiento de redes de manera segura
- Diferenciar los distintos tipos de tecnologías inalámbricas e identificar las amenazas y riesgos asociadas a las mismas, así como las medidas de protección
- Describir la normativa técnica y las disposiciones legales de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas y procedimientos de seguridad
- Identificar los aspectos a contemplar en el diseño de una estrategia de seguridad
- Elaborar concisa, clara y razonadamente documentos, planes y proyectos técnicos de trabajo en el ámbito de la ciberseguridad
- Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS)
- Describir de manera global los requisitos y el procedimiento de certificación de sistemas seguros
- Utilizar de manera básica las herramientas de ciberseguridad, tanto SW como HW
- Identificar las principales anomalías y firmas de ataques en los sistemas y redes
- Describir y aplicar las estrategias de sensorización para distintos elementos de un sistema en red y analizar de manera básica los eventos observados
- Describir y aplicar las generalidades del procedimiento y la gestión de incidentes de seguridad, diferenciando las fases
- Aplicar de manera básica las capacidades y procedimientos de reacción frente a ciberataques
- Aplicar el procedimiento de análisis de vulnerabilidades
- Reconocer las evidencias de ataques en los sistemas informáticos

- Describir los procedimientos que permitan preservar las evidencias y mantener la cadena de custodia de las mismas
- Identificar y aplicar las técnicas de investigación de ciberataques a un sistema específico
- Identificar las técnicas de ocultación de ataques a sistemas y redes
- Reconocer los mecanismos necesarios de prevención de fugas de información
- Identificar los aspectos básicos de configuración de seguridad de los Sistemas Operativos (SO) Windows y Linux
- Describir los aspectos básicos de configuración de seguridad de diversos Sistemas de Gestión de Bases de Datos (SGBD)
- Identificar los aspectos básicos de configuración de seguridad de todo tipo de aplicaciones web y escritorio y sus vulnerabilidades
- Describir las medidas para controlar los riesgos derivados del empleo de dispositivos personales (o de uso compartido) en un entorno profesional
- Aplicar las medidas de configuración segura de dispositivos móviles y dispositivos móviles corporativos
- Describir y aplicar los conceptos básicos relativos a los test de penetración y análisis de vulnerabilidades.

4. SISTEMA DE ADMISIÓN AL CURSO

4.1. Perfil de ingreso

4.1.1. Categoría y empleo militar

El curso se dirige a oficiales y suboficiales de los Ejércitos que tengan, o vayan a tener, cometidos técnicos relacionados con la Ciberdefensa.

4.1.2. Formación previa

- Conocimientos básicos de informática, en particular:

  - Entender la terminología y los conceptos básicos, tanto desde el punto de vista conceptual como técnico, en materia de ciberdefensa
  - Poseer una mentalización y concienciación adecuadas sobre seguridad de los Sistemas TIC y las amenazas y vulnerabilidades que representan las nuevas tecnologías
  - Conocimientos y habilidades básicos necesarios para poder evaluar el estado de seguridad de un sistema, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos
  - Conocimientos básicos necesarios para que sean capaces de comprobar, con una garantía suficiente, los aspectos de seguridad relativos a la infraestructura de red basada en elementos de comunicaciones (concentradores, enrutadores, etc.), dispositivos inalámbricos y redes privadas virtuales (VPN) introduciendo los conceptos de cortafuegos, sistemas de detección de intrusos (IDS) y dispositivos trampa (honeypots y honeynets)
  - Conocimientos necesarios para que sean capaces de comprobar, 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
- Gestión y administración de sistemas operativos Windows y Linux.

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

4.2. Sistema de selección

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

4.3. 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.

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 50 horas a desarrollar en 20 días hábiles y una fase presencial con una carga lectiva de 250 horas (200 de clase y 50 de estudio) a desarrollar en 40 días hábiles, en horario de mañana.

El curso está dividido en seis módulos:

- Módulo 1: Gestión STIC. (Fase no presencial)
- Módulo 2: Especialidades criptográficas
- Módulo 3: Fundamentos del análisis de vulnerabilidades (pentesting)
- Módulo 4: Arquitecturas y redes seguras
- Módulo 5: Seguridad en el software
- Módulo 6: Ciberincidentes.

El módulo 1 (fase no presencial) se evaluará mediante una prueba escrita. El resto de módulos se evaluarán mediante prueba escrita y evaluación continua en cada uno de ellos.

5.1.1. Fase no presencial

Módulo 1. Gestión STIC

Duración

50 horas, más una (1) sesión de una (1) hora para la prueba teórica en la fase presencial.

Contenido:

- Entorno socio-político de la ciberdefensa
- Aspectos legales del ciberespacio
- Normativa nacional de seguridad
- Introducción a la gestión de la seguridad
- Análisis de gestión de riesgos
- Estándares de seguridad de la información y certificación de sistemas seguros.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Aplicar los servicios, mecanismos y protocolos de seguridad para cada caso concreto
- Describir los procedimientos técnicos para la implantación, configuración y mantenimiento de redes de manera segura
- 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.
- Examinar los aspectos a contemplar en el diseño de una estrategia de seguridad
- Crear documentos, planes y proyectos técnicos de trabajo en el ámbito de la ciberseguridad
- Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la información (ISMS).

5.1.2. Fase presencial

Módulo 2. Especialidades criptográficas

Duración

33 horas durante la fase presencial. (28 teóricas, 4 prácticas y 1 para prueba escrita). 30 horas para trabajo del alumno (4 horas preparación examen, 18 lectura y estudio de materias y 8 horas de comprensión de problemas o casos reales).

Contenido:

- Servicios, amenazas y mecanismos de seguridad de la información
- Criptosistemas de clave simétrica
- Criptosistemas de clave asimétrica
- Autenticación: funciones HASH, MAC y firma digital. Protocolo de autenticación
- Gestión de equipamiento de cifra
- Criptografía en el mundo real.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Analizar mecanismos de cifrado y estenografía pertinentes para proteger los datos residentes en un sistema o en tránsito en red
- Aplicar la configuración y efectuar la carga de claves
- Explicar la administración de los equipos de cifra
- Aplicar los métodos y procedimientos en la gestión de equipos de cifra
- Explicar los procedimientos de gestión de claves (generación, distribución, almacenamiento y destrucción de claves).

Módulo 3. Fundamentos del análisis de vulnerabilidades (pentesting)

Duración

44 horas durante la fase presencial (19 teóricas, 24 prácticas y 1 para prueba escrita). 40 horas para trabajo del alumno (4 horas preparación examen, 16 de lectura y estudio de materias y 20 horas de compresión de problemas o casos reales).

Contenido:

- Planeamiento del pentesting. Fases
- Ingeniería social
- Reconocimiento, escaneos en profundidad
- Fundamentos de explotación y corrupción de memoria
- Ataque de credenciales
- Ataque de aplicaciones web
- Ataque Wireless.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Clasificar las principales anomalías y firmas de ataques en los sistemas y redes
- Distinguir las evidencias de ataques en los sistemas informáticos
- Describir los procedimientos que permitan preservar las evidencias y mantener la cadena de custodia de las mismas
- Aplicar las técnicas de investigación de ciberataques a un sistema específico
- Clasificar las técnicas de ocultación de ataques a sistemas y redes
- Aplicar los conceptos relativos a los test de penetración y análisis de vulnerabilidades.

Módulo 4. Arquitecturas y redes seguras

Duración

44 horas durante la fase presencial (19 teóricas, 24 prácticas y 1 de prueba escrita). 40 horas para trabajo del alumno (4 horas de preparación del examen, 16 de lectura y estudio de materias y 20 horas de comprensión de problemas o casos reales).

Contenido:

- Introducción en el diseño de arquitecturas y redes seguras
- Introducción a la seguridad de la información en redes: PKI, TLS e IPSEC
- Introducción a las arquitecturas AAA y control de acceso
- Introducción a la seguridad en redes inalámbricas
- Conceptos básicos de seguridad perimetral
- Cortafuegos: arquitecturas y configuración básica
- Sistema de detección de intrusiones: fundamentos y operación
- Introducción al análisis y monitorización de seguridad: SIEM
- Sistema señuelo: honeypots y honeynets.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Diferenciar los distintos tipos de tecnologías inalámbricas e identificar las amenazas y riesgos asociadas a las mismas, así como las medidas de protección
- Explicar los requisitos y el procedimiento de certificación de sistemas seguros
- Clasificar las herramientas de ciberseguridad, tanto SW como HW
- Explicar el procedimiento de análisis de vulnerabilidades.

Módulo 5. Seguridad en el software

Duración

34 horas durante la fase presencial (14 teóricas, 19 prácticas y 1 de prueba escrita). 30 horas para trabajo del alumno (4 horas de preparación del examen, 10 de lectura y estudio de materias y 16 horas de comprensión de problemas o casos reales).

Contenido:

- El problema de la seguridad en el software
- Seguridad en el ciclo de vida del software
- Configuración segura de aplicaciones, sistemas de gestión de bases de datos y sistemas operativos
- Seguridad de aplicaciones online y móviles.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Resaltar los mecanismos necesarios de prevención de fugas de información
- Explicar los aspectos de configuración de seguridad de los Sistemas Operativos (SO) Windows y Linux
- Describir los aspectos de configuración de seguridad de diversos Sistemas de Gestión de Bases de Datos (SGBD)
- Explicar los aspectos de configuración de seguridad de todo tipo de aplicaciones web y escritorio y sus vulnerabilidades
- Describir las medidas para controlar los riesgos derivados del empleo de dispositivos personales (o de uso compartido) en un entorno profesional
- Aplicar las medidas de configuración segura de dispositivos móviles y dispositivos móviles corporativos.

Módulo 6. Ciberincidentes

Duración

39 horas durante la fase presencial (14 teóricas, 24 prácticas y 1 de prueba escrita). 35 horas para trabajo del alumno (4 horas de preparación del examen, 13 de lectura y estudio de materias y 18 horas de comprensión de problemas o casos reales).

Contenido:

- Análisis y modelado de ciberataques
- Técnicas y patrones de ciberataques
- Introducción a la identificación y reacción ante ciberataques
- Fundamentos de análisis de malware

- Amenazas persistentes (APT)
- Introducción al análisis forense digital.

Resultado del módulo

Al finalizar el módulo el alumno será capaz de:

- Aplicar las estrategias de sensorización para distintos elementos de un sistema en red y analizar los eventos observados
- Aplicar las generalidades del procedimiento de gestión de incidentes de seguridad, diferenciando las fases
- Aplicar las capacidades y procedimientos de reacción frente a ciberataques. Describir y aplicar las generalidades del procedimiento y la gestión de incidentes de seguridad, diferenciando las fases.

5.2. Metodología de enseñanza-aprendizaje

El Curso se impartirá en formato semipresencial con una fase no presencial y otra presencial.

La fase no presencial se realizará compatibilizándose con los cometidos propios del destino que estén ocupando los alumnos designados. El trabajo autónomo del alumno en esta fase tiene una duración de 50 horas.

La fase presencial tendrá una duración de 200 horas, distribuidas en 8 semanas, a razón de 5 horas diarias.

Las exposiciones orales de los profesores cubren 94 horas. Se programarán sesiones con ejercicios prácticos que también servirán para comprobar que los alumnos alcanzan los resultados de aprendizaje. La duración total de estas prácticas será de 95 horas.

Adicionalmente a las horas lectivas, el curso comenzará con una ceremonia de inauguración y una conferencia dedicada a la exposición del desarrollo del curso, las instalaciones y servicios del Centro, la labor de tutoría y otros aspectos administrativos. El curso finalizará con una conferencia final y una ceremonia de clausura. Estas horas no lectivas de la fase presencial se han calculado en un total de 5 horas.

Se han asignado 175 horas para trabajo del alumno, teniendo en cuenta diferente carga en función de que cada módulo tenga un mayor o menor contenido en sesiones teóricas. Las sesiones correspondientes a las ceremonias de inauguración y clausura, exposición de temas administrativos y conferencia final no se han tenido en cuenta para computar la carga de trabajo del alumno pero sí para valorar la duración de la fase presencial.

5.3. Criterios de Evaluación

Para superar el módulo 1 (fase no presencial), será necesario superar una prueba escrita, cuya duración será de una sesión de clase y que tendrá lugar el primer día de la fase presencial. Esta prueba supondrá el 100% de la nota final del módulo. No cumplimentar la fase a distancia o no superar esta prueba supondrá la baja en el curso.

Los módulos de la fase presencial se evaluarán combinando:

- Un sistema de evaluación continua para cada uno de los módulos que componen esta fase que supondrá el 60% de la nota final del módulo

- Una prueba escrita de carácter teórico, teórico-práctico o práctico cuya duración será de una sesión de clase, 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 todos y cada uno de los módulos.

No superar cualquier módulo supondrá la no superación del Curso y provocará la baja del alumno en el mismo.

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

6. REQUISITOS DEL PROFESORADO Y DEL PERSONAL DE APOYO

Director

DICESEDEN nombrará un Director del Curso entre el personal a sus órdenes.

Coordinador

El centro donde se desarrolle el curso nombrará un Coordinador del mismo.

Personal docente

Durante la fase no presencial se contará con, al menos, dos profesores. En la fase presencial se contará con el número de profesores necesarios para impartir los diferentes módulos.

El centro responsable de la docencia podrá designar profesores de sus departamentos, con conocimientos y formación en Telecomunicaciones y Sistemas de Información.

Personal de apoyo

El centro docente facilitará los apoyos para administración, uso de los medios y servicios con personal propio del centro.

7. RECURSOS MATERIALES Y SERVICIOS

Fase no presencial

Los alumnos deberán disponer de conexión a internet para poder acceder a los contenidos. Las comunicaciones con el profesorado ser realizarán a través de la misma plataforma o del correo electrónico corporativo sobre la WAN PG del Ministerio del Ministerio de Defensa.

Fase presencial

El curso se impartirá en el centro que se determine, disponiendo de un aula con las características siguientes:

- Capacidad: 20 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.

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

Financiación: El curso será financiado por el Estado Mayor de la Defensa.

8. EFECTOS DE LA SUPERACIÓN DE LA ACTIVIDAD FORMATIVA

8.1. Ventajas 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 determinadas 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
- Acceder a cursos de mayor nivel tecnológico relacionados con la Ciberdefensa.

8.2. Resultados previstos

Los alumnos son personal profesional, con experiencia y conocimientos previos en el campo de la informática y las telecomunicaciones. 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. 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 de este Plan de Estudios.

9.2. Procedimientos de evaluación, mejora y análisis

El CESEDEN 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.

9.3. Procedimiento de recogida y análisis de sugerencias y reclamaciones

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.

De acuerdo con la norma decimoséptima de la Orden DEF/464/2017, se realizará una validación externa del curso con el objeto de comprobar que los alumnos, una vez incorporados a los puestos en los que desarrollan las aptitudes obtenidas, poseen las competencias previstas. Los resultados de esta validación serán utilizados por CESEDEN para la revisión y mejora del plan de estudios del curso.

9.4. 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.

Directora General de Reclutamiento y Enseñanza Militar

VALCARCE GARCIA MARIA AMPARO | 71497055Z

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Firmado digitalmente por VALCARCE GARCIA MARIA AMPARO |71497055Z
Nombre de reconocimiento (DN): c=ES, o=MINISTERIO DE DEFENSA, ou=PERSONAS, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, serialNumber=IDCES-71497055Z, sn=VALCARCE GARCIA |71497055Z, givenName=MARIA AMPARO, cn=VALCARCE GARCIA MARIA AMPARO |71497055Z
Fecha: 2019.06.11 13:37:04 +02'00'

- María Amparo Valcarce García -

ANEXOS:

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

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

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS

MODULO	HORAS	ORGANIZACIÓN TEMPORAL
1. Gestión STIC	51	Fase no presencial
2. Especialidades criptográficas	63	Fase presencial
3. Fundamentos del análisis de vulnerabilidades (pentesting)	84	Fase presencial
4. Arquitecturas y redes seguras.	84	Fase presencial
5. Seguridad en el software	65	Fase presencial
6. Ciberincidentes	74	Fases no presencial y presencial

DESCRIPCIÓN DE LOS MÓDULOS

MODULO	CONTENIDOS	No presencial	PRESENCIAL			
		Teórica	Teórica	Práctica	Prueba	Trabajo alumno
1. Gestión STIC	- Entorno socio-político de la ciberdefensa. - Aspectos legales del ciberespacio. - Normativa nacional de seguridad. - Introducción a la gestión de la seguridad. - Análisis de gestión de riesgos. - Estándares de seguridad de la información y certificación de sistemas seguros.	50			1	
2. Especialidades Criptográficas	- Servicios, amenazas y mecanismos de seguridad de la información. - Criptosistemas de clave simétrica. - Criptosistemas de clave asimétrica. - Autenticación: funciones hash, MAC y firma digital. Protocolo de autenticación. - Gestión de equipamiento de cifra. - Criptografía en el mundo real.		28	4	1	30
3. Fundamentos del análisis de vulnerabilidades (Pentesting)	- Planeamiento del pentesting. Fases Ingeniería social. - Reconocimiento, escaneos en profundidad.		19	24	1	40

	- Fundamentos de explotación y corrupción de memoria. - Ataque de credenciales. - Ataque de aplicaciones web. - Ataque Wireless.					
4. Arquitecturas y redes seguras	- Introducción en el diseño de arquitecturas y redes seguras. - Introducción a la seguridad de la información en redes PKI, TLS e IPSEC. - Introducción a las arquitecturas AAA y control de acceso. - Introducción a la seguridad en redes inalámbricas. - Conceptos básicos de seguridad perimetral. - Cortafuegos: arquitecturas y configuración básica. - Sistema de detección de intrusiones: fundamentos y operación. - Introducción al análisis y monitorización de seguridad: SIEM. - Sistema señuelo: honeypots y honeynets.		19	24	1	40
5. Seguridad en el software	- El problema de la seguridad en el software. - Seguridad en el ciclo de vida del software. - Configuración segura de aplicaciones, sistemas de gestión de bases de datos y sistemas operativos. - Seguridad de aplicaciones online y móviles.		14	19	1	30
6. Ciberincidentes	- Análisis y modelado de ciberataques. - Técnicas y patrones de ciberataques. - Introducción a la identificación y reacción ante ciberataques. - Fundamentos de análisis de malwares. - Amenazas persistentes (APT). - Introducción al análisis forense.		14	24	1	35
	Total	50	94	95	6	175