MINISTERIO
DE
DEFENSA

ESTADO MAYOR
DE LA DEFENSA

CENTRO SUPERIOR
DE ESTUDIOS DE LA
DEFENSA NACIONAL

CURRÍCULO DEL CURSO DE "ADMINISTRADOR DE SEGURIDAD DE CIBERDEFENSA"

Mayo 2020

INTENCIONADAMENTE EN BLANCO

ÍNDICE

ANEXOS

CURRICULO DEL CURSO DE

"ADMINISTRADOR DE SEGURIDAD DE CIBERDEFENSA"

1. DESCRIPCIÓN GENERAL DEL CURSO

1.1. Denominación del curso.

Curso de Administrador de Seguridad 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 y 13, este curso tiene la consideración de curso militar conjunto, de especialización e indistinto.

1.3. Objetivos del curso.

Proporcionar a los alumnos los conocimientos necesarios en el ámbito de la administración de seguridad de los sistemas TIC usados en el Ministerio de Defensa.

1.4. Categoría a la que pertenece.

Categoría «A», según la Orden DEF/1407/2018, de 14 de diciembre, por la que se establecen las categorías en las que quedan comprendidos los cursos de perfeccionamiento y de Altos Estudios de la Defensa Nacional.

1.5. Duración.

El curso presenta una carga lectiva de 186,5 horas (equivalente a 7,46 ECTS).

1.6. Idioma.

Español.

1.7. Centro docente militar responsable del desarrollo del curso.

El responsable del curso es el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), impartiéndose en la Escuela de Técnicas de Mando, Control y Telecomunicaciones del Ejército del Aire (EMACOT).

1.8. Modalidad de enseñanza.

Semipresencial.

1.9. Número mínimo y máximo de alumnos por curso.

Mínimo ocho (8) y máximo veinte (20) alumnos.

2. 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.

En la actualidad ya existen en el MINISDEF cursos que cubren las necesidades de formación expresadas en el Plan FORCIBE y, siguiendo esta tendencia, se implementó este curso, el cual, proporciona la aptitud necesaria para capacitar al alumno en el desempeño de las funciones de administrador de seguridad de las TIC, incluyendo tanto a los administradores de red como a los de sistemas.

Para cubrir los puestos en los distintos Centros de Operaciones de Seguridad (COS) de los Ejércitos y la Armada, en el Centro de Apoyo Técnico Avanzado (CATA) del Ejército del Aire y en el MCCD, es necesario impartir un curso de estas características que permitan la formación y actualización del personal en dichos puestos.

2.1. Referentes internos y externos

Como refleja el Real Decreto-ley 12/2018, de 7 de septiembre, sobre la seguridad de las redes y sistemas de información, la evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.

El carácter transversal e interconectado de las tecnologías de la información y de la comunicación, que también caracteriza a sus amenazas y riesgos, limita la eficacia de las medidas que se emplean para contrarrestarlos cuando se toman de modo aislado. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos sectoriales afectados.
Por tanto, es oportuno establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

3. PERFIL DE EGRESO

El objetivo general del curso es proporcionar las competencias necesarias para el desempeño de las funciones de los administradores de seguridad en materia de ciberdefensa, en aplicación del Plan FORCIBE del Ministerio de Defensa.
Los alumnos que completen el curso deberán alcanzar las siguientes competencias generales y específicas:

- **Competencias generales:**

1. Desarrollar y realizar tareas sencillas en el área de la securización de sistemas informáticos relativos a las redes de área local, sistemas operativos Windows y GNU/Linux y dispositivos móviles.
2. Poseer la capacidad de resolver problemas a situaciones predecibles dentro del campo de la administración de seguridad de sistemas de ciberdefensa.

- **Competencias específicas:**

1. Administrar e implementar medidas de seguridad en dispositivos e infraestructuras de red, servidores, estaciones de trabajo y dispositivos móviles.

2. Comprobar la seguridad de los sistemas de información relativos a redes digitales, sistemas operativos Windows y GNU/Linux, y dispositivos móviles y, en caso necesario, desarrollar soluciones sencillas que permitan asegurar los mismos.

4. SISTEMA DE ADMISIÓN DE ALUMNOS

4.1. Perfil de ingreso.

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 función de administrador de seguridad en materia de ciberdefensa.

Los alumnos deberán acreditar antes del inicio del curso que tienen las competencias básicas de informática que comprendan:

- Describir los sistemas operativos Windows y Linux a nivel administrador.
- Identificar los aspectos básicos de configuración de seguridad de los sistemas operativos (SO) (Windows y Linux).
- Describir, a nivel administrador, las comunicaciones y redes TCP/IP.
- Describir, a nivel administrador, los principios de la seguridad informática.
- Describir los procedimientos técnicos para la implantación, configuración y mantenimientos de redes.
- Diferenciar los distintos tipos de tecnologías inalámbricas.
- Identificar los aspectos básicos de configuración de seguridad de todo tipo de aplicaciones 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 de dispositivos móviles y dispositivos móviles corporativos.

Además, los alumnos deberán tener conocimientos de inglés técnico en la materia.

4.2. Sistema de selección

El sistema de selección será por concurso-oposición. Los aspirantes al curso deberán realizar un examen inicial de conocimientos previos conforme a lo señalado en el punto anterior.

Los aspirantes con mejor nota de cada Unidad solicitante serán seleccionados para cubrir sus plazas asignadas por BOD y realizar la Fase No Presencial del curso.

La relación de seleccionados será publicada en el BOD, pudiendo adelantarse mediante mensaje oficial.

El primer día de la Fase Presencial se realizará un examen sobre los contenidos de la Fase No Presencial. Aquellos alumnos que no superen esta prueba con una nota igual o superior a cinco (5) puntos, sobre una escala de cero (0) a diez (10) puntos, causarán baja en el curso.

4.3. 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 de:

- Estructura, Director y Coordinador del Curso.
- Dirección (postal, telefónica y correo electrónico) a efectos de trámites administrativos.
- Lugar, fecha y hora de presentación para la realización del curso, cómo llegar y medios de transporte posibles, requisitos de acceso al centro docente y procedimiento para acceder con vehículo propio.
- Ubicación del aparcamiento, vestuarios, cafetería, comedor y apoyos logísticos accesibles.
- Ficha de filiación del alumno (que debe ser cumplimentada y remitida por los aspirantes antes del inicio del curso).
- Enlace de intranet donde puede consultar información relativa al curso que va a realizar (currículo del curso, guías didácticas del curso, sistema de evaluación, procedimiento operativo sobre régimen interno para cursos de perfeccionamiento, etc.), así como de los demás cursos que se imparten en el centro.
- Cronograma del curso.
- Datos de contacto del coordinador del curso, pues éste será el responsable de asistir a los alumnos sobre todas las cuestiones que surjan durante la fase online.

4.4. Reconocimiento o convalidaciones y homologaciones

Se realizará de acuerdo con la orden DEF/464/2017.

Se podrán convalidad los módulos obtenidos en otras enseñanzas realizadas siempre que coincidan los objetivos expresados como resultados de aprendizaje. Los módulos convalidados se calificarán con un 5, a efectos de la obtención de la nota media.

Quienes no superen todos los módulos profesionales específicos podrán solicitar un certificado académico en el que consten los módulos profesionales superados, así como las unidades de competencia acreditadas del Catálogo Nacional de Cualificaciones Profesionales.

5. PLAN DE ESTUDIOS

5.1. Estructura general del plan de estudios

El Curso está dividido en dos fases:

- **Fase No Presencial**

  Tiene asignada una duración de cuatro (4) semanas, correspondiéndole una carga de trabajo de 74 horas.

  En esta fase el alumno deberá emplear 2 horas diarias de dedicación en horario laboral y 1 hora de trabajo autónomo fuera de dicho horario, además, se contabiliza una dedicación de 3,5 horas de trabajo autónomo durante cada fin de semana. Total de 18,5 horas a la semana.

  Un Profesor-Tutor designado al efecto orientará al alumno sobre las materias objeto de estudio y le hará un seguimiento para comprobar su aplicación.

- **Fase Presencial**

  Tiene asignada una duración de 3 semanas, con una carga de trabajo de 112,5 horas.

  En esta fase el alumno deberá dedicar cada día laborable 6 horas en clase presencial y 1,5 horas de trabajo autónomo. Total de 37,5 horas a la semana.

  Se desarrollará mediante la impartición de una serie de contenidos teóricos y teórico-prácticos.

MÓDULOS	HORAS (ETCS)	ORGANIZACIÓN TEMPORAL
MÓDULO 1	88 (3,52)	- No presencial: 44 horas. - Presencial: 44 horas.
MÓDULO 2	82 (3,28)	- No presencial: 43 horas. - Presencial: 39 horas.
MÓDULO 3	16,5 (0,66)	- No presencial: 11 horas. - Presencial: 5,5 horas.

5.2. Descripción de los módulos

Módulo 1: Seguridad de la Administración de red

Módulo	Seguridad de la Administración de red
Horas (ECTS)	88 (3,52)
Competencias generales: 1 Competencias específicas: 1,2	
Resultados de aprendizaje: ▪ Emplea medidas básicas de redes.	**Criterios de evaluación:** CE1: Distingue las distintas capas del modelo OSI, y describe la arquitectura del modelo TCP/IP, y las distintas topologías de red. CE2: Explica los principios básicos del funcionamiento de las redes TCP/IP. CE3: Compara los distintos dispositivos de red más idóneos que podrían utilizarse para fortalecer una red de carácter militar. CE4: Hace uso del entorno de simulación GNS3 para el desarrollo de entornos de pruebas previos a un despliegue. CE5: Reconoce distintas fuentes de relevancia para mantenerse al día de las últimas vulnerabilidades, actualizaciones disponibles, tendencias y ataques frecuentes a las redes LAN, así como sus salvaguardas.
▪ Comprueba y soluciona ataques detectados, y esboza medidas efectivas de salvaguardas.	CE1: Recuerda los conceptos que apuntan a la necesidad de *hardering* y monitorización de los equipos de red. CE2: Resuelve los ataques más frecuentes a las redes de área local (LAN). CE3: Selecciona en un supuesto práctico distintas salvaguardas encaminadas a evitar o mitigar el efecto de los

	ataques más comunes a redes como: Ataques MAC/CAM, VLAN *hopping*, y *spoofing* a los protocolos DHCP y ARP.
▪ Aplica segmentación de la red.	CE1: Demuestra la necesidad de segmentar la red para permitir un mejor flujo de datos, así como para aumentar la seguridad de la organización, dividiéndola en subredes más pequeñas que facilitan su gestión y protección.
▪ Usa herramientas y dispositivos de seguridad de red.	CE1: Usa y configura las herramientas más comunes de uso por los administradores de redes locales.
▪ Manipula la administración de Firewall de red.	CE1: Escoge las reglas de configuración adecuadas a implementar en dispositivos firewalls de red.
▪ Opera el enrutamiento y cifrado de las comunicaciones.	CE1: Selecciona el uso de los protocolos de red adecuados según la necesidad del flujo de datos en las comunicaciones y sabe cómo cifrar las comunicaciones en los mismos.
Contenidos:	- Conceptos básicos de redes, ataques y salvaguardas, segmentación, herramientas y dispositivos de seguridad de red. - Métodos de administración de un Firewall. - Planificación de enrutamiento y cifrado de las comunicaciones.
Metodología de enseñanza-aprendizaje	
Fase online	- Aprendizaje a través del aula virtual (incluyendo actividades en línea, como video conferencias, video tutoriales y autoevaluaciones) - Tutoría individualizada.
Fase presencial	- Clases teórico-prácticas y coloquios en grupos. - Prácticas profesionales en entornos simulados. - Tutorías grupales.

Módulo 2: Seguridad de la Administración de sistemas

Módulo	Seguridad de la Administración de sistemas.
Horas (ECTS)	82 (3,28)
Competencias generales: 1 Competencias específicas: 1,2	
Resultados de aprendizaje:	**Criterios de evaluación:**
▪ Aplica los fundamentos de securización (hardering) de sistemas.	CE1: Identifica los distintos sistemas operativos y se manejan a nivel de administrador los dos utilizados en el Ministerio de Defensa (Windows y GNU/Linux) CE2: Hace uso de hipervisores de tipo 2 (Virtual Box) para el desarrollo de entornos de pruebas previos a un despliegue. CE3: En un supuesto práctico de intentos de intrusión a los sistemas, sabe escoger las medidas adecuadas para impedir o dificultar que éstos puedan llevarse a cabo. CE4: Reconoce que la formación de los usuarios finales es tan importante como la correcta configuración y securización de sistemas, pudiendo ser partícipe a la hora de informar sobre buenas prácticas en el uso de los sistemas de la organización. CE5: Comprende que, por encontrarse en un campo que sufre de evolución constante, su proceso de formación debe ser constante y mantenerse en el tiempo.
▪ Contrasta las diferentes formas de autenticación.	CE1: Sabe utilizar distingas formas de autenticación para el acceso local y remoto en los distintos sistemas operativos.
▪ Desarrolla implementaciones de seguridad en estaciones de trabajo.	CE1: Cita distintos motivos que ejemplifican la necesidad de securiación (*hardering)* y monitorización de logs y eventos de las estaciones de trabajo y servidores de la organización. CE2: Lista distintas fuentes relevantes para mantenerse al día de las últimas vulnerabilidades, actualizaciones

▪ Construye medidas de protección en servidores Windows. ▪ Construye medidas de protección en servidores Linux	disponibles, tendencias y ataques frecuentes a los distintos sistemas operativos y sus posibles salvaguardas. CE1: Hace uso de las guías CCN-STIC de la serie 500 para la configuración segura de servidores y puestos de trabajo del sistema operativo Windows. CE1: Hace uso de las guías CCN-STIC de la serie 600 para la configuración segura de servidores y puestos de trabajo del sistema operativo GNU/Linux.
Contenidos:	- Conceptos básicos de securización de sistemas Windows y Linux - Métodos de autenticación de sistemas. - Planificación de protección de servidores Windows Server y GNU/Linux.
Metodología de enseñanza-aprendizaje	
Fase online	- Aprendizaje a través del aula virtual (incluyendo actividades en línea, como video conferencias, video tutoriales y autoevaluaciones) - Tutoría individualizada.
Fase presencial	- Clases teórico-prácticas y coloquios en grupos. - Prácticas profesionales en entornos simulados. - Tutorías grupales.

Módulo 3: Seguridad de dispositivos móviles

Módulo	Seguridad de dispositivos móviles
Horas (ECTS)	16,5 (0,66)
Competencias generales: 1 Competencias específicas: 1,2	

Resultados de aprendizaje:	**Criterios de evaluación:**
▪ Emplea actualizaciones del sistema operativo Android.	CE1: Discute la opción óptima a la hora de utilizar mecanismos de actualización del sistema operativo del dispositivo y utiliza distintos métodos para llevarlo a cabo, como son las actualizaciones automáticas y *seamless update*.
▪ Usa el modelo y arquitectura de seguridad Android.	CE1: Aplica medidas de seguridad en el sistema operativo, en las aplicaciones y en el arranque del dispositivo.
▪ Relata las opciones disponibles de gestión empresarial de dispositivos móviles basados en Android.	CE1: Cita distintos entornos de gestión empresarial para la configuración remota de dispositivos móviles.
▪ Ejemplifica cómo es el acceso físico al dispositivo.	CE1: Identifica las distintas formas de acceso no autorizado a un dispositivo móvil.
▪ Aplica el cifrado de datos.	CE1: Usa el cifrado en medios de almacenamiento del dispositivo y de las comunicaciones de datos.
▪ Hace uso de los protocolos de comunicaciones.	CE1: Memoriza el funcionamiento básico de los protocolos de comunicaciones que suelen utilizar los dispositivos más modernos.
Contenidos:	- Conceptos básicos: actualizaciones del sistema operativo, modelos y arquitectura de seguridad Android. - Planificación de la gestión remota. - Métodos de acceso físico al dispositivo, cifrado de datos y comunicaciones.
Metodología de enseñanza-aprendizaje	

Fase online	- Aprendizaje a través del aula virtual (incluyendo actividades en línea, como video conferencias, video tutoriales y autoevaluaciones) - Tutoría individualizada.
Fase presencial	- Clases teóricas y coloquios en grupos. - Tutorías grupales.

Sistema de evaluación del curso

Fase No Presencial

La evaluación de esta fase consistirá en la ejecución de una serie de ejercicios y respuestas a preguntas de tipo test que versarán sobre los contenidos de los módulos. Para superarla será necesario obtener una calificación igual o superior a cinco puntos en cada una de las pruebas indicadas de cada módulo.

Fase Presencial

La evaluación de esta fase consistirá en la realización de una serie de actividades que versarán sobre los contenidos de los distintos módulos, a base de exámenes, trabajos didácticos, exposiciones, o una combinación de ellos.

Evaluación final del curso

Para la superación del curso será necesario haber superado la evaluación de todos los módulos en sus dos fases.

El sistema de calificación será el previsto en la legislación vigente. Se tendrán en cuenta los siguientes procedimientos generales:

1. Evaluación durante la fase online del rendimiento de los alumnos en cada uno de los módulos del curso, por medio de autoevaluaciones en línea, asistencia y participación en las Webinar, foros, etc., y la elaboración de los trabajos académicos correspondientes.
2. Evaluación del rendimiento de los alumnos mediante una prueba escrita.
3. Evaluación durante la fase presencial de diferentes prácticas, que permitan la evaluación de las distintas competencias del curso.

4. El porcentaje de calificación del curso será de un 40% para la fase *online* y de un 60% de la fase presencial.

El sistema de calificación del curso seguirá la siguiente escala:

0,0-4,9: Suspenso

5,0-6,9: Aprobado

7,0-8,9: Notable

9,0-10: Sobresaliente

6. REQUISITOS DEL PROFESORADO Y PERSONAL DE APOYO.

6.1. Personal académico

- **Director**: El CESEDEN nombrará un Director del Curso.
- **Coordinador**: El centro docente nombrará un Coordinador del Curso.
- **Personal docente**: Profesores con experiencia en la formación semipresencial y con conocimientos y/o experiencia acreditada en la administración segura de servidores (Windows y GNU/Linux), redes, y dispositivos móviles.

  La escuela cuenta con personal que reúne dichas condiciones. El número ideal de profesores sería de cinco (5), que se repartirían las tareas de formación en sus respectivas asignaturas, elaboración del temario y la creación de laboratorios para las prácticas (2 para administración segura de servidores, 2 para administración segura de redes y 1 para la administración segura de dispositivos móviles).

  El mínimo sería de dos (2), los cuales, deberían disponer casi de exclusividad completa en su puesto de trabajo para dedicarse a este curso, con capacidad, además, de impartir el curso por completo cada uno de ellos, con objeto de cubrir las posibles bajas o destinos del otro.

6.2. Personal de apoyo

El personal de apoyo está compuesto por, al menos, los 5 componentes del área de administración y servicios de la EMACOT, todos ellos con experiencia en la gestión y administración de cursos.

- Tutor.
- Administración.

- Informática.
- Fotografía.
- Protocolo.
- Riesgos laborales.

7. RECURSOS MATERIALES Y SERVICIOS

El curso se impartirá en un aula equipada con ordenadores y conexión a red e internet, con las siguientes características:

- Capacidad máxima: 24 puestos + 1 puesto profesor, PC con procesador i5 o superior y 16 o más 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 del centro en el mismo horario que el resto de profesores y alumnos.

8. EFECTOS DE LA SUPERACIÓN DE LA ACTIVIDAD FORMATIVA

8.1. Ventajas y servidumbres

De conformidad con lo establecido en el anexo de la Orden DEF/1407/2018, de 14 de diciembre, por la que se establecen las categorías en las que quedan comprendidos los cursos de perfeccionamiento y de Altos Estudios de la Defensa Nacional, este curso se considera categoría A y por tanto los alumnos estarán sujetos a unos tiempos mínimos de servicios efectivos de un año desde la finalización de los cursos.

La superación del curso facultará al personal para:

- Desempeñar cometidos en los puestos de ciberdefensa de la estructura del Ministerio de Defensa que requieran los conocimientos impartidos en ente curso.

- Realizar algunas funciones relacionadas con la administración de 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.

8.2. Resultados previstos

Los datos que se proporcionan a continuación se fundamentan en la experiencia de los años anteriores en los que se ha impartido este curso. Los alumnos deberían ser personal profesional, con experiencia y conocimientos previos en las materias, que ya están trabajando o pronto trabajarán en este ámbito administrando los sistemas mencionados.

La comprobación de los resultados del aprendizaje se realizará según se detalla en el punto 5 (apartado “criterios de evaluación”).

- Tasa de éxito (TE) prevista: superior al 86%. Al ser un curso complejo, que requiere que los aspirantes cuenten previamente con conocimientos de disciplinas tan distintas y complejas, como son la administración de servidores y la administración de dispositivos de red, entre otros, es poco probable que la totalidad de los alumnos cuenten con ese conocimiento previo básico, que será de suma importancia para la adecuada comprensión del curso. Por dicho motivo y, en consonancia con el nivel de esfuerzo que exigirá la EMACOT (mucho mayor que en su edición anterior), se estima que la tasa de aprobados no sería lógico que estuviera por encima del 86%.
- Tasa de Bajas Académicas (TBA) prevista: inferior al 10%
- Tasa de Bajas a Petición Propia (TBPS) prevista: 4%
- Tasa de Abandono (TA) prevista: 0%.

La TBPS está basada en la experiencia de petición de bajas de cursos similares y, la TBA sería el resultado de la diferencia entre la TE – TBPS.

9. SISTEMA DE GARANTÍA INTERNA DE LA CALIDAD

9.1. Sistema de garantía de calidad del Plan de Estudios

El Director y el 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, con el apoyo del centro docente, 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 del centro implicado en la realización del curso.

9.3. Procedimiento de autoevaluación y análisis de sugerencias y reclamaciones.

Al año de haber finalizado el curso, los egresados que estén ocupando una vacante en con exigencia del título de Administrador de Seguridad en 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 currículo del curso.

Las sugerencias, quejas y/o reclamaciones, pueden surgir en cualquier momento de la realización del curso por parte de cualquier alumno, planteadas a través del coordinador de curso, que será el responsable de la gestión de las mismas y posteriores entregas al Director 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 al mismo a través de la intranet del Ministerio de Defensa, en la página correspondiente al CESEDEN y en la del centro docente.
A la convocatoria del curso se le dará difusión a través de los canales de comunicación de las OFAP de los Ejércitos/Armada.

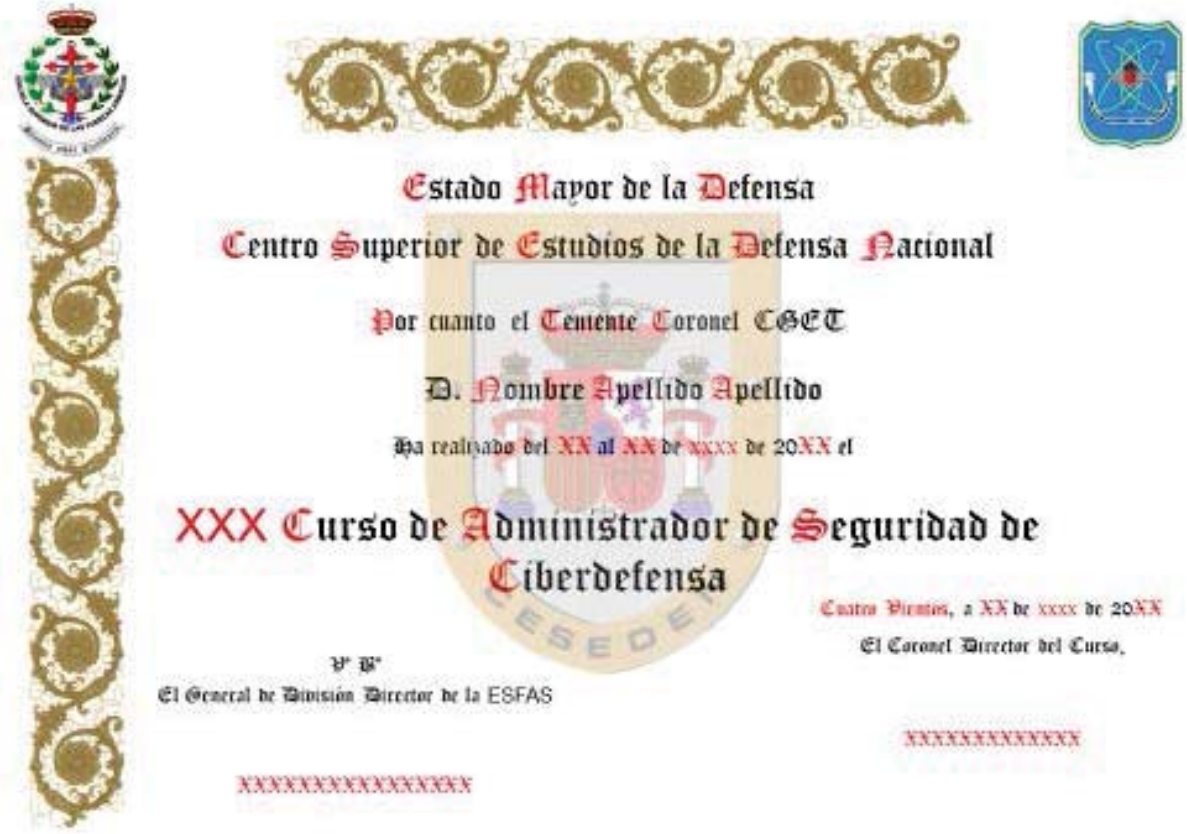
10. CALENDARIO DE IMPLANTACIÓN

Se desarrollará un curso al año, comenzando en 2020.

11. MODELO DE DOCUMENTO ACREDITATIVO DE SUPERACIÓN DEL CURSO

El documento acreditativo de superación del curso especialización, según la Orden DEF/464/2017, de 19 de mayo, será un Diploma.

Modelo de diploma de superación del curso (anverso)



Madrid, a de septiembre del 2020

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

FIRMA ELECTRÓNICA MINISDEF-EC-WPG-PKI:
DICESEDEN
Francisco de Paula Bisbal Pons
FECHA DE LA FIRMA: 07/09/2020

- Francisco de Paula Bisbal Pons –

ANEXOS:

ANEXO I: DESCRIPCIÓN DE LOS MÓDULOS

ANEXO II: ANÁLISIS DE VIGENCIA

ANEXO I
DESCRIPCIÓN DE LOS MÓDULOS

MÓDULO	UNIDADES DIDÁCTICAS	UNIDADES DE APRENDIZAJE				RESULTADOS DE APRENDIZAJE
		Teoría distancia	Práctica distancia	Teoría presencial	Práctica presencial	
1. SEGURIDAD DE LA ADMINISTRACIÓN DE RED	FUNDAMENTOS DE REDES Y CONFIGURACIONES SEGURAS	28	16	13	19	• RA1: Conoce los conceptos básicos de redes ◦ Introducción a las redes de ordenadores ◦ Topologías de red ◦ Arquitectura TCP/IP • RA2: Monitoriza y detecta ataques, y elabora salvaguardas ◦ Ataques MAC/CAM ◦ Vlan hopping ◦ DHCP ◦ ARP ◦ Spoofing. • RA3: Implementa segmentación de la red ◦ Segregación de una infraestructura de red ◦ Separación de redes, servicios y sistemas ◦ Protección de las infraestructuras • RA4: Usa herramientas y dispositivos de seguridad de red ◦ Ping ◦ Traceroute/Tracert ◦ Nmap ◦ NetStat ◦ Hostname ◦ IDS/IPS ◦ Firewall ◦ Servidores Radius ◦ Wireshark

						◦ Securización de Switch ◦ Enrutamiento en Vlan ◦ EthernetChannel. • RA5: Diseña la administración de Firewall de red ◦ Configuración inicial ◦ Reglas ◦ Filtrado de puertos ◦ Activación de logs ◦ Registros de acciones en el FW • RA6: Implementa el enrutamiento y cifrado de las comunicaciones ◦ Enrutamiento estático ◦ Enrutamiento dinámico ◦ OSPF y OSPF segura ◦ SSH ◦ Listas de acceso (ACL) ◦ VPN ◦ IPSEC
	TOTAL HORAS	28	16	13	19	
	TOTAL HORAS EVALUACIÓN			1		
	TOTAL HORAS DE ESTUDIO AUTÓNOMO			11		
	TOTAL HORAS MÓDULO	88				

MÓDULO	UNIDADES DIDÁCTICAS			UNIDADES DE APRENDIZAJE		RESULTADOS DE APRENDIZAJE
		Teoría distancial	Práctica distancia	Teoría presencial	Práctica presencial	
2. SEGURIDAD DE LA ADMINISTRACIÓN DE SISTEMAS	CONFIGURACIONES SEGURAS PARA LOS SISTEMAS OPERATIVOS	23	20	8	19	• RA7: Conoce los fundamentos de securización (hardering) de sistemas ◦ Introducción al concepto de hardering de sistemas • RA8: Explica las diferentes formas de autenticación ◦ Tipos de sistemas de autenticación ◦ Protección de autenticación local ◦ Protección de autenticación en red ◦ Protocolos y algoritmos • RA9: Construye implementaciones de seguridad en estaciones de trabajo ◦ Seguridad en sistemas Windows ◦ Seguridad en sistemas Linux • RA10: Aplica protección en servidores Windows ◦ Objetos de Directivas de Grupo (GPO) ◦ Permisos de usuario ◦ Directiva de auditoría ◦ Device Guard ◦ Protección de identidades ◦ Credential Guard ◦ Creacción de grupos restringidos ◦ Correo electrónico: SMTP, antispam, SPF, DKIM y DMARC ◦ Directivas de restricción del software, Applocker ◦ Firewall de Windows con seguridad avanzada

						◦ Cifrado de datos con Bitlocker ◦ Windows Server Backup • RA11: Aplica protección sobre servidores Linux ◦ Protección del arranque ◦ Cifrado de disco duro y ficheros ◦ Iptables ◦ Minimizar los servicios del sistema ◦ Permisos y control de accesos a ficheros y directorios ◦ Cuentas de usuario y entorno ◦ Fortificación y seguridad en SSH ◦ Tunneling y SOCKS ◦ Port-Knocking ◦ Configuración syslog, trypwire, cron, AT y copias de seguridad
	TOTAL HORAS	23	20	8	19	
	TOTAL HORAS EVALUACIÓN			1		
	TOTAL HORAS DE ESTUDIO AUTÓNOMO			11		
	TOTAL HORAS MÓDULO	82				

MODULO	UNIDADES DIDÁCTICAS	UNIDADES DE APRENDIZAJE				RESULTADOS DE APRENDIZAJE
		Teoría distnacia	Práctica distancia	Teoria presencial	Práctica presencial	
3. SEGURIDAD EN DISPOSITIVOS MÓVILES	SECURIZACIÓN DE DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID	10		5		• RA12: Implementa actualizaciones del sistema operativo Android ◦ Actualizaciones automáticas ◦ Actualizaciones seamless update • RA13: Conoce el modelo y arquitectura de seguridad Android ◦ Modelo de permisos ◦ Arranque seguro: Verified Boot y Safe Mode ◦ Configuración por defecto del dispositivo • RA14: Explica la gestión empresarial de dispositivos móviles basados en Android ◦ Gestión remota (MDM) ◦ Android for work • RA15: Describe cómo es acceso físico al dispositivo ◦ Métodos de acceso ◦ Múltiples perfiles de usuario • RA16: Conoce el cifrado de datos ◦ Cifrado del dispositivo móviles • RA17: Reconoce y explica los protocolos de comunicaciones ◦ USB ◦ NFC ◦ Bluetooth ◦ WI-FI ◦ Mensajes de Texto (SMS) ◦ Voz y Datos
	TOTAL HORAS TEÓRICAS	10		5		
	TOTAL HORAS EVALUACIÓN	1		0		

	TOTAL HORAS DE ESTUDIO AUTÓNOMO		0,5	
	TOTAL HORAS MÓDULO	16		

ANEXO II
ANÁLISIS DE VIGENCIA

Se anexa en archivo adjunto