IV. — ENSEÑANZA MILITAR

ENSEÑANZA DE PERFECCIONAMIENTO

Cursos

Resolución 220/07611/24

Cód. Informático: 2024010584.

Curso Avanzado de Ciberdefensa (4C002 2024 001)

Se convoca el presente Curso con la finalidad de proporcionar al personal designado las competencias que capaciten a los alumnos para continuar la formación en cursos específicos para funciones técnicas del plan FORCIBE.

De acuerdo con lo establecido en el Real Decreto 339/2015, de 30 de abril, por el que se ordenan las enseñanzas de perfeccionamiento y de Altos Estudios de la Defensa Nacional, artículo 4 apartado d) 3º, este curso tiene la consideración de curso militar, conjunto y, según lo señalado en el artículo 14, se trata de un curso de especialización.

Todo ello de acuerdo con las siguientes bases:

1. Centro responsable del desarrollo del curso

El curso se desarrollará en la Academia de Ingenieros del Ejército de Tierra, sita en Hoyo de Manzanares (Madrid), bajo la dirección del Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

El curso tiene una carga lectiva de 420 horas equivalente a 16,8 ECTS, de las que 50 serán en la fase no presencial (2 ECTS) y 370 en la fase de presente (14,8 ECTS).

La superación del curso se acreditará mediante el diploma correspondiente, que será entregado a su finalización.

2. Perfiles de ingreso y egreso

Perfil de ingreso. El Curso se dirige a oficiales y suboficiales de las FAS, con conocimientos de inglés técnico en la materia, y que dispongan de la habilitación de seguridad RESERVADO/NATO SECRET.

- Oficiales de empleos comprendidos entre Teniente Coronel/Capitán de Fragata a Teniente/Alférez de Navío de las Escalas de Oficiales de los Cuerpos Generales y de Especialistas del Ejército de Tierra, de la Armada y del Ejército del Aire y del Espacio, del Cuerpo de Infantería de Marina, así como de las Escalas de Oficiales y Técnicas del Cuerpo de Ingenieros Politécnicos del Ejército de Tierra, de la Armada y del Ejército del Aire y del Espacio.
- Suboficiales de empleos comprendidos entre Subteniente a Sargento de las Escalas de Suboficiales de los Cuerpos Generales y de Especialistas del Ejército de Tierra, de la Armada y del Ejército del Aire y del Espacio, así como del Cuerpo de Infantería de Marina.

Los alumnos, antes del inicio del curso, deberán tener 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 adecuada sobre seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (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 y las amenazas que se ciernen sobre ellos.

CVE: BOD-2024-098-13622
Verificable en https://sede.defensa.gob.es/acceda/bod

- 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, ...), 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 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.

Perfil de egreso. Los alumnos que completen el curso deberán alcanzar los siguientes resultados de aprendizaje:

- Aplicar mecanismos de cifrado y esteganografía pertinentes para proteger los datos residentes en un sistema o en tránsito en 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 mantenimientos 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.

- Describir de manera global los requisitos y el procedimiento de certificación de sistemas seguros.

- Utilizar de manera básica las herramientas de ciberseguridad, tanto Software como Hardware.

- 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 (Windows y Linux).

- Describir los aspectos básicos de configuración de seguridad de diversos Sistemas de Gestión de Bases de Datos.

CVE: BOD-2024-098-13623
Verificable en https://sede.defensa.gob.es/acceda/bod

- 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/ análisis de vulnerabilidades.

3. Calendario

El curso constará de dos fases:

- Fase no presencial del 2 de septiembre al 27 de septiembre (a. i.) de 2024, sin dedicar tiempo de la jornada laboral.
- Fase presencial del 30 de septiembre al 22 de noviembre (a. i.) de 2024, a desarrollar íntegramente en la Academia de Ingenieros del Ejército de Tierra de Hoyo de Manzanares (Madrid).

4. Organización del curso

De acuerdo con lo contemplado en el currículo, el curso está dividido en seis módulos:

- Módulo 1: Gestión STIC (FNP).
- Módulo 2: Especialidades criptográficas.
- Módulo 3: Fundamentos y análisis de vulnerabilidades (Pentesting).
- Módulo 4: Arquitecturas y redes seguras.
- Módulo 5: Seguridad en el software.
- Módulo 6: Ciberincidentes.

Para superar el módulo 1, impartido íntegramente en la Fase no presencial, será necesario haber cumplimentado dicha fase y superar una prueba escrita que tendrá lugar en la Academia de Ingenieros al comienzo de la Fase Presencial. Esta prueba supondrá el cien por cien (100%) de la nota de ese módulo. 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 o no cumplimenten la Fase no presencial, causarán baja del curso.

El resto de los módulos del curso se evaluará mediante un sistema que combinará:

- Evaluación continua mediante la observación, por parte del profesor de la resolución de problemas y trabajos prácticos realizados durante las sesiones prácticas. Esta nota supondrá el sesenta por ciento (60%) de la nota final de cada módulo.
- Pruebas objetivas. Exámenes de carácter teórico y teórico/práctico, cuya duración será de una sesión de clase y supondrá el cuarenta por ciento (40%) de cada módulo.

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) en la media ponderada de las observaciones y de las pruebas escritas.

5. Número de plazas

Veintiuna (21) plazas con la siguiente distribución:

- Órgano Central: Cuatro (4) plazas (3 para CESTIC, 1 para INTA).
- EMAD: Once (11) plazas.
- Ejército de Tierra: Dos (2) plazas.
- Armada: Dos (2) plazas.
- Ejército del Aire y del Espacio: Una (1) plaza.
- Presidencia de Gobierno: Una (1) plaza para DSN.

CVE: BOD-2024-098-13624
Verificable en https://sede.defensa.gob.es/acceda/bod

6. Prioridades para la designación de alumnos

Se establecen las siguientes prioridades:

1º- Personal que ocupa destinos en los que se desarrollan cometidos técnicos relacionados con ciberdefensa.
2º- Personal que está previsto que ocupe destinos en los que se desarrollan cometidos técnicos relacionados con ciberdefensa.
3º- Resto de personal.

La existencia de estas prioridades, en relación con el puesto desempeñado por el peticionario, deberá ser certificada expresamente por el Jefe de la UCO (certifico que el solicitante se encuentra en la prioridad indicada) en el lugar consignado a tal efecto en el apartado «observaciones» de las peticiones que se realicen mediante el módulo SOLCUR (en caso de no certificarlo, la prioridad indicada no tendrá validez).

7. Normas de carácter específico

El alumno presentará el primer día de la fase presencial del curso el certificado que demuestre estar en posesión de la habilitación de seguridad RESERVADO/NATO SECRET o que está en trámites de obtener la citada habilitación.

8. Solicitudes

El plazo de admisión de solicitudes será de ocho (8) días hábiles contados a partir del siguiente al de la publicación de la presente convocatoria en el «Boletín Oficial de Defensa».
Los solicitantes que no cumplan los requisitos y bases de esta convocatoria o las solicitudes que no se cumplimenten en todos sus apartados, no serán tenidos en consideración.

a) Las solicitudes para el personal de los Ejércitos, se gestionarán por el Órgano de Gestión de Personal de la UCO, mediante la grabación de las peticiones en el Módulo de Solicitud de Cursos (SOLCUR) del Sistema de Información de Personal de Defensa (SIPERDEF).

La citada grabación debe incluir:

- DNI y Nombre y Apellidos del solicitante.
- Curso que se solicita (4C002 2024 001).
- Observaciones del solicitante, en su caso.
- Impresión de dos ejemplares de comprobante/recibo de la solicitud, que firmará el interesado. Un ejemplar para archivo de la Unidad y otro para entregar al solicitante.
- Visado obligatorio del Jefe de Unidad y observaciones en su caso.

El Jefe de la UCO del solicitante deberá efectuar el visado correspondiente a la solicitud dentro del plazo máximo de cuatro (4) días hábiles, contados a partir de la finalización del plazo de admisión de solicitudes.

9. Selección de alumnos

Las Direcciones de Enseñanza de los Ejércitos y resto de organismos con plazas asignadas en el punto 5 de esta convocatoria, de acuerdo a las mismas y a las prioridades establecidas en el punto 6, realizarán sus propuestas de candidatos en SIPERDEF, dentro de los cuatro (4) días hábiles siguientes al de la finalización del plazo de visado de solicitudes, con la inclusión de un (1) suplente.
Las plazas que queden sin cubrir de las determinadas en el punto 5 podrán asignarse a los otros organismos.
No se seleccionarán peticionarios que hayan sido propuestos para otros cursos que coincidan en fechas con cualquier fase (a distancia o Presencial) de este curso.
La relación de alumnos del curso será publicada en el «Boletín Oficial de Defensa», atendiendo al orden facilitado por SIPERDEF, no siendo éste necesariamente el de antigüedad. Una vez publicada esta relación no se admitirán cambios de alumnos.

CVE: BOD-2024-098-13625
Verificable en https://sede.defensa.gob.es/acceda/bod

10. Reconocimientos, convalidaciones y homologaciones

Será de aplicación lo indicado en el capítulo VII de 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.

El procedimiento para el reconocimiento de créditos o convalidaciones de módulos, materias y asignaturas, se realizará mediante la solicitud que figura en el enlace que a continuación se indica en la página web de la Subdirección General de Enseñanza Militar, accediendo a Enseñanza de Perfeccionamiento/Convocatorias.

https://www.defensa.gob.es/ministerio/organigrama/subdef/digerem/sdgensenanza/

11. Régimen económico

A los alumnos que tengan que desplazarse de su destino les corresponderán las dietas de incorporación y regreso así como las indemnizaciones por residencia eventual (IRE), en la cuantía del cincuenta y cinco por ciento (55%) de la dieta entera, de acuerdo con lo previsto en el Real Decreto 462/2002, de 24 de mayo («Boletín Oficial del Estado» número 129), sobre indemnizaciones por razón del servicio.

Para el personal sin alojamiento en Residencia militar o Alojamiento logístico en el término municipal donde radique el centro, la cuantía se establecerá por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) conforme a sus normas internas. A efectos de percepción de esta indemnización, deberán aportar copia de la solicitud de alojamiento en dichas instalaciones y del documento de denegación de la citada solicitud.

Aquellos alumnos que por la proximidad geográfica de su residencia oficial puedan trasladarse diariamente a la localidad donde se realiza la fase de presente del curso, percibirán durante los días lectivos del mismo la indemnización que por gastos de viajes y manutención pudiera corresponderles, según lo regulado en el citado Real Decreto.

Estas indemnizaciones serán tramitadas y abonadas con cargo a los créditos del CESEDEN que para tal fin tiene asignado.

12. Ventajas y servidumbres

El curso está incluido entre los de categoría «A» (un año de servicios efectivos), conforme al artículo 5.2.c, del 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.

Este curso podrá ser considerado como preferencia o exigencia para poder desempeñar cometidos relacionados con la Ciberdefensa en cualquier puesto de la estructura operativa de las FAS.

13. Resarcimiento

En relación con el artículo 8 de la Orden DEF/1252/2021, de 11 de noviembre, por la que se determinan los supuestos y se establece el procedimiento para resarcir económicamente al Estado en caso de renuncia a la condición de militar, pase a determinadas situaciones administrativas o baja en las enseñanzas de formación, perfeccionamiento o Altos Estudios de la Defensa Nacional, podrá dar lugar al resarcimiento la baja a petición propia, con las prevenciones de lo recogido en el artículo 9 de la misma Orden DEF.

El coste individualizado por la formación recibida corresponderá a la cuantía de cinco euros con noventa y cinco céntimos (5,95 €) por día cursado en la fase online y de treinta y cuatro euros con cuarenta y cinco céntimos (34,45 €) por día cursado en la fase de presente.

14. Aplazamiento, renuncias y bajas

Los aplazamientos, renuncias y bajas se producirán por los motivos y con los efectos que se establecen en el capítulo VI de la Orden DEF/464/2017, de 19 de mayo.

15. Protección de la maternidad

CVE: BOD-2024-098-13626
Verificable en https://sede.defensa.gob.es/acceda/bod

Será de aplicación lo establecido en los artículos 3 y 4 del Real Decreto 293/2009, de 6 de marzo, por el que se aprueban las medidas de protección de la maternidad en el ámbito de la enseñanza en las Fuerzas Armadas, debiendo, según lo establecido en el artículo 5 del citado Real Decreto, acreditar ante el Director del curso, mediante la oportuna certificación médica oficial, la limitación para realizarlo.

Dicha protección se hará extensible al progenitor diferente de la madre biológica en aplicación a la Norma séptima del anexo I de la Orden DEF/253/2015 de 9 de febrero, por la que se regula el régimen de vacaciones, permisos, reducciones de jornada y licencias de los miembros de las Fuerzas Armadas, así mismo, tendrán la misma aplicación los casos de adopción, guarda con fines de adopción o acogimiento que se establecen en la citada Orden.

16. Protección de datos

Los datos de carácter personal de los interesados se obtendrán a través de consulta en el sistema de Información de Personal del MINISDEF.

El responsable del tratamiento es el Director General de Reclutamiento y Enseñanza Militar del MINISDEF, quien de conformidad con la base legitimadora 6.1.e) del Reglamento Europeo de protección de datos 679/2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales, lo realizará únicamente para la gestión administrativa, académica o docente de la actividad objeto de la presente convocatoria. No se cederán datos a terceros, salvo obligación legal.

El interesado podrá ejercitar los derechos recogidos en la normativa de protección de datos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad en aquellos casos que sea posible de acuerdo con la normativa vigente. El ejercicio de estos derechos podrá llevarse a cabo ante el responsable del tratamiento de forma online a través de la sede electrónica del Ministerio de Defensa.

https://www.defensa.gob.es/comun/politica-de-privacidad.html

Tiene derecho a interponer reclamaciones a su elección, con carácter previo ante el Delegado de Protección de Datos (DPD) del Ministerio de Defensa dpd@mde.es, o directamente ante la Autoridad de control de la Agencia Española de protección de datos. El interesado dispone de información adicional sobre el tratamiento de sus datos y el Registro de Actividades de Tratamiento en la página web de privacidad del Ministerio de Defensa accesible desde internet.

17. Igualdad de género

De acuerdo con el artículo 6.1 de la Ley 39/2007, de 19 de noviembre, la igualdad de trato de oportunidades es un principio que en las Fuerzas Armadas se aplicará de conformidad con lo previsto en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. Por ello el órgano de selección velará por el estricto cumplimiento del principio de igualdad de oportunidades entre los aspirantes de ambos sexos que participen en la convocatoria.

18. Lenguaje no sexista

De conformidad con el artículo 14.11 de la Ley Orgánica 3/2007, de 22 de marzo, todas las denominaciones que, en virtud del principio de economía del lenguaje, se hagan en género masculino inclusivo en esta convocatoria, referidas a titulares o miembros de órganos o a colectivos de personas, se entenderán realizadas tanto en género femenino como en masculino.

19. Base final

La presente convocatoria podrá ser anulada siembre que concurran circunstancias objetivas que así lo aconsejen.

CVE: BOD-2024-098-13627
Verificable en https://sede.defensa.gob.es/acceda/bod

La presente convocatoria y cuantos actos se deriven de ella, podrán ser impugnados en los casos y en la forma establecida en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Madrid, 10 de mayo de 2024.—El Subdirector General de Enseñanza Militar, Juan Manuel Sánchez Aldao.

CVE: BOD-2024-098-13628
Verificable en https://sede.defensa.gob.es/acceda/bod