CURSO ESPECIALIZACIÓN CIBERSEGURIDAD Y HACKING ÉTICO

Convocatoria 2025

BASES DE LA FORMACIÓN

DATOS PROGRAMA FORMATIVO CIBERSEGURIDAD

Fecha Inicio: 3 de marzo 2025

Fecha Fin: 31 de mayo 2025

Horario: 9h a 14h de lunes a viernes, siendo todos los miércoles **formación Agile**, de 09:00 a 12:00 y **formación en orientación laboral** de 12:00 a 14:00.

Formato: On line (necesaria la asistencia virtual de lunes a viernes de 9 a 14)

BENEFICIARIOS

Podrán solicitar la formación personas que cuente con un certificado de discapacidad igual o superior al 33% emitido por una Comunidad Autónoma española, que tenga nacionalidad española o extranjero con permiso de trabajo en el reino de España y que reúna los requisitos exigidos en los apartados siguientes.

REQUISITOS

Requisitos Generales:

- Tener un conocimiento general en informática e interés pro los sistemas informáticos y redes.
- Tener disponibilidad en el horario establecido para la formación (de 9:00 a 14:00 de lunes a viernes)
- Compromiso de participación y finalización del curso
- Superar el proceso de selección

Requisitos ordenador personal:

• RAM: mínimo 4 GB. Recomendable de 8 GB en adelante.

• Procesador: recomendable Intel i5 en adelante.

• Disco: al menos 30 GB libres para instalación de programas, bases de datos y entornos de desarrollo.

• Posibilidad de instalar nuevos programas.

Requisitos competenciales

- Implicación, compromiso y responsabilidad
- Planificación y Organización
- Orientación a Resultados
- Motivación, Optimismo y Energía

DOCUMENTACION A PRESENTAR

- Copia del certificado de discapacidad o tarjeta en vigor expedido en España.
- Copia DNI.
- El CV es necesario que esté registrado en la web de la Fundación Adecco: www.fundacionadecco.org.
- Anexo III: Aceptación de las Bases de la Formación Firmado
- Cesión de imágenes firmada para la grabación de las clases, que se almacenarán en la plataforma para repaso de los alumnos.

PLAZO Y FORMA DE PRESENTACIÓN.

El plazo para hacer llegar a la Fundación Adecco la solicitud y documentación requerida será desde el 10 de febrero al 2025 al 27 de febrero de 2025.

SELECCIÓN DE BENEFICIARIOS

El proceso de admisión contará con las siguientes fases que se desarrollarán entre los meses de abril y mayo:

1. **Entrevista de valoración con Fundación Adecco.**
   - Entrevista de motivación y competencias.
   - Pruebas psicotécnicas: competencias laborales, test mecanografía y de código.

La Fundación Adecco comunicará a los participantes la superación o no del proceso a la finalización del mismo.

RESOLUCIÓN

Una vez finalizado el proceso de admisión completo se comunicará por correo electrónico a todos los participantes la admisión al curso de Especialización en Ciberseguridad y Hacking ético.

PROTECCION DE DATOS

La Fundación Adecco establecerá todos los mecanismos legales para salvaguardar la privacidad de la documentación presentada en la solicitud de curso de formación de Fundación Adecco. Todos los datos de carácter personal que el usuario nos proporcione pasarán a formar parte de un fichero automatizado de carácter personal del que la Fundación Adecco es responsable.

La persona beneficiaria al presentar sus datos se compromete a que los mismos sean fidedignos, correctos y actuales. Se informa que la solicitud podrá ser rechazada si se detectase cualquier dato falso o engañoso facilitado por el usuario o que no cumplan los requisitos, procediéndose a su eliminación sin necesidad de previo aviso.

El tratamiento de los datos de carácter personal de los usuarios realizado por la Fundación Adecco, así como el envío de comunicaciones comerciales

realizadas por medios electrónicos son acordes, respectivamente, con la normativa general vigente: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de Protección de Datos Personales, la Ley Orgánica de Protección de Datos de Carácter Personal y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Usted podrá, en cualquier momento, ejercer los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento o portabilidad de los datos enviando un correo electrónico a la dirección proteccion.datos@adecco.com. Le informamos, como destinatario de este mensaje, que las comunicaciones por medios electrónicos no permiten asegurar, ni garantizar la confidencialidad, integridad o correcta recepción del mensaje, declinando cualquier responsabilidad por la concurrencia de tales incidencias. Puede dejar de recibir esta información en su cuenta de e-mail accediendo con sus claves personales a "Mi sitio Adecco" (apartado "Mis opciones") a través del siguiente link: https://4dec.co/index.php/syn.candidate/do._displayLogin

OBLIGACIONES

- **Compromiso de asistencia:** El curso se desarrolla de lunes a viernes en horario de 9 a 14h. Se admitirán un máximo de 3 faltas debidamente justificadas. Superadas las 3 faltas se considera falta de aprovechamiento del curso y se anulará la inscripción al curso.

- **Compromiso de aprovechamiento:** Además de la conexión a las clases, para el correcto aprovechamiento del curso diariamente es necesario un tiempo estimado de 2 horas de trabajo personal para completar tareas complementarias.

El incumplimiento de los compromisos de asistencia y/o de aprovechamiento por parte del alumno conllevarán la expulsión del curso. En caso contrario, cuando se supere la formación se emitirá un diploma acreditativo de superación del curso por parte de Fundación Adecco.

Las personas que superen el curso con calificación APTA, serán becados con una certificación oficial de cisco (formación más examen)

La participación en esta convocatoria implica la aceptación de las presentes bases.

ANEXO I: Contenidos del programa formativo.

FUNDACIÓN ADECCO

Temario Ciberseguridad y Hacking Ético

1 REDES y SISTEMAS OPERATIVOS

- **Introducción a las Redes Informáticas**
1.1. Introducción 1.2. Tipos de redes 1.3. Sistemas operativos de red

- **Ethernet y Canales de Comunicación**
2.1. Canales de comunicación 2.2. Cableado 2.3. Instalaciones

- **Direccionamiento IP**
3.1. Fundamentos3.2. Subredes3.3. Redes privadas3.4. IPv6

- **Modelo OSI y TCP/IP**
4.1. Modelo OSI y sus capas4.2. Modelo TCP/IP y sus capas

- **Utilidades TCP/IP**
5.1. NET5.2. PING5.3. NETstat5.4. ARP5.5. Telnet

- **Windows Server**
6.1. Instalación de diferentes versiones (2003-2016)

- **Sistemas Linux**
7.1. Características 7.2. Sistemas de ficheros 7.3. Fundamentos 7.4. Usuarios y grupos 7.5. Configuración de red

- **Modos de Acceso a Internet**
8.1. Modulación digital 8.2. Digital Subscriber Line (DSL)

- **Redes WAN**
9.1. Arquitectura 9.2. Dispositivos 9.3. Políticas 9.4. Servidores

- **Packet Tracer**
10.1. Instalación y uso

FUNDACIÓN ADECCO

2 Introducción a la Ciberseguridad

- **Entorno Linux**
12.1. Distribuciones (Distros)12.2. Sistemas12.3. Sistemas de ficheros12.4. Rutas y formato de archivos

- **Tipos de Auditorías**
13.1. Por tipo13.2. Por ámbito

- **Pentesting**
14.1. Fases explicadas

- **Virtualización e Instalación de Laboratorios**
15.1. Tipos de hypervisores15.2. Tipos de archivos de instalación

- **Bash Scripting**
16.1. Completo básico

- **Herramientas Básicas**
17.1. Whois17.2. Ping17.3. Tracert17.4. Nslookup17.5. Dig17.6. Google

- **Metadatos**
18.1. Tipos18.2. FOCA18.3. ExifTool

- **OSINT (Open Source Intelligence)**
19.1. Maltego 19.2. TheHarvester 19.3. Dmitry 19.4. Dorks 19.5. CEWL 19.6. Redes sociales 19.7. Filtraciones 19.8. IoT

- **Descubrimiento de Máquinas**

- **Análisis de Puertos**
21.1. Herramientas21.2. Tipos de escaneo

- **Análisis de Vulnerabilidades**
22.1. Clasificación de vulnerabilidades22.2. Herramientas de escaneo

- **Metasploit**
23.1. Websploit23.2. Searchsploit

- **CMS (Content Management Systems)**
24.1. JoomScan24.2. WPScan

- **Ataques a Servicios**
25.1. SSH25.2. VNC25.3. SMB25.4. FTP

- **Autenticación**
26.1. LM26.2. NTLM26.3. Linux

FUNDACIÓN ADECCO

- **Diccionarios Disponibles**
27.1. RockYou 27.2. Big WPA List 27.3. CrackStation 27.4. Diccionarios por idiomas

- **Generación de Diccionarios**
28.1. Crunch 28.2. CEWL 28.3. CUPP

- **Ataques por Fuerza Bruta**
29.1. Hydra 29.2. Medusa 29.3. Hashcat 29.4. John the Ripper

- **Ataques DoS y DDoS**

- **Red Tor**
31.1. Arquitectura 31.2. Tor 31.3. HexChat 31.4. ProxyChains 31.5. TorGhost

- **Red I2P**

- **Cuentas de Correo Temporales**

- **VPN**

- **Métodos de Evasión**
35.1. Shellter 35.2. MSFvenom 35.3. TheFatRat 35.4. Evasión manual

- **Ataques WiFi**
36.1. Conceptos básicos 36.2. Funcionamiento 36.3. Tipos de ataques 36.4. Automatización 36.5. Portales cautivos

- **Análisis de Tráfico**
37.1. Wireshark 37.2. Ettercap 37.3. Tshark

- **Envenenamiento de Tráfico**
38.1. MITM6 38.2. EvilFOCA

- **Ingeniería Social**
39.1. Psicología 39.2. Manipulación 39.3. Contacto humano real 39.4. Técnicas de ingeniería social 39.5. Contramedidas

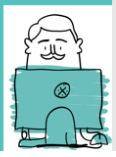
- **Hacking Web**
40.1. Ejecución de código remoto 40.2. Inyección SQL40.3. XSS40.4. LFI/RFI40.5. Webshells

- **Pentesting en Dispositivos Móviles**
41.1. Técnicas 41.2. Pasos básicos 41.3. Creación de APK maliciosa 41.4. Análisis de APKs

- **Postexplotación**
42.1. Métodos pasivos y activos 42.2. Escalada de privilegios 42.3. Persistencia 42.4. Pivoting

- **Ataques a Active Directory**
43.1. NetExec

- **Documentación en Auditorías**
44.1. Contrato 44.2. Tipos de informes



EVALUACIÓN DEL CURSO:

1. Casos prácticos y ejercicios. Es necesario aprobar el 50% de los casos prácticos para la superación del curso.
2. Presentación de proyecto transversal. Tiene que obtenerse como mínimo un 5 en la nota media para la superación del curso.
3. Valoración continua de la aptitud y motivación en el desarrollo diario.
4. Se entregará un diploma acreditativo de superación del curso a aquellas personas que terminen la formación de manera satisfactoria.

ANEXO II: Criterios de Selección

* CV completo subido a través de la página web de Fundación Adecco

* Presentación del Certificado o tarjeta de discapacidad igual o superior al 33% en vigor y emitido por una Comunidad Autónoma española.

* Resultado de test de Competencias Laborales:

  - Implicación, compromiso y responsabilidad: mínimo nivel 4.

    - Constancia y perseverancia
    - Implicación con los objetivos propuestos
    - Sentimiento de responsabilidad hacia la tarea y sus resultados

  - Planificación y Organización: mínimo nivel 3.

    - Organización de recursos
    - Priorización de objetivos y tareas
    - Gestión del tiempo y el orden

  - Orientación a Resultados: mínimo nivel 4

    - Consecución de resultados conforme a objetivos
    - Maximización Rentabilidad y eficiencia en el uso de los recursos y ahorro de costes
    - Actitud y perseverancia respecto a los resultados

  - Motivación, Optimismo y Energía: mínimo nivel 3.

    - Actitud ante el trabajo.
    - Actitud ante las dificultades.

* Resultado del test Mecanografía: 30 wpm

* Resultado test de código: 10 wpm

ANEXO III Aceptación Bases de la Formación

SOLICITUD CURSO CIBERSEGURIDAD Y HACKING ÉTICO FUNDACION ADECCO.

DATOS PERSONALES

NOMBRE Y APELLIDOS	
DNI	
TELEFONO	
MAIL	
DIRECCION (Ciudad, Provincia, CP)	
FECHA NACIMIENTO	

Con la firma del este documento acepto los compromisos reflejados en las Bases de la Convocatoria:

- **Compromiso de asistencia:** El curso se desarrolla de lunes a viernes en horario de 9 a 14h. Se admitirán un máximo de 3 faltas debidamente justificadas. Superadas las 3 faltas se considera falta de aprovechamiento del curso y se anulará la inscripción al curso.

- **Compromiso de aprovechamiento:** Además de la conexión a las clases, para el correcto aprovechamiento del curso diariamente es necesario un tiempo estimado de 2 horas de trabajo personal para completar tareas complementarias.

El incumplimiento de los compromisos de asistencia y/o de aprovechamiento por parte del alumno conllevarán la expulsión del curso.

Conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de Protección de Datos Personales y a la Ley Orgánica de Protección de Datos de Carácter Personal, la información facilitada en este documento será tratada confidencialmente, teniendo como exclusiva finalidad el cumplimiento de los objetivos de los beneficiarios con el fin último de lograr la integración laboral. La cumplimentación de todos los datos tiene carácter obligatorio e implica aceptar y consentir expresamente el tratamiento de los mismos. Vd. podrá, en cualquier momento, ejercer los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento o portabilidad de los datos enviando un correo electrónico a la dirección proteccion.datos@adecco.com. El responsable del fichero es Fundación Adecco CIF: G-82382987, con domicilio social en la calle Príncipe de Vergara 110, en Madrid.

Con la firma de esta solicitud acepto las Bases de la Convocatoria así como los compromisos aquí reflejados.

……., …….de …… 2025

Nombre solicitante:

Firma solicitante: