PROYECTO EMPRESARIAL: HUB DE FORMACIÓN AVANZADA EN CIBERSEGURIDAD EN EXTREMADURA

GUÍA INFORMATIVA DE CURSOS DE CCI - EX

Índice

1. **Nombre del curso**

De acuerdo con los cursos de formación ofrecidos por el Centro de Ciberseguridad e Innovación en Extremadura (en adelante CCI-EX), se impartirá la primera edición del programa de ***Cybersecurity Auditor*** y ***Pentester - Auditor Técnico***.

2. **Objetivo del curso**

El curso se divide en 4 asignaturas, cada uno tiene un objetivo concreto:

- **Trabajo en proyectos:** Instruir al alumno en el uso de herramientas indispensables para el correcto entendimiento del curso, así como también, la adquisición de habilidades técnicas necesarias para la inserción en el mundo laboral asociadas al trabajo en equipo, presentaciones y trabajo en proyectos que le permita ser más eficiente.

- **Fundamentos de ciberseguridad:** Capacitar al alumno en el área de la ciberseguridad informática proporcionando conocimientos sobre la gestión y gobierno de las operaciones de la ciberseguridad en las empresas y una visión global de los principales servicios de ciberseguridad.

- **Especialidad:** Formar al alumno para trabajar en una de las áreas con más futuro en Ciberseguridad en un entorno de trabajo eminentemente práctico para afianzar las competencias asociadas y que el alumno pueda ser productivo desde el primer día en el sector competitivo.
  - **Pentester - Auditor técnico**: Facultar al alumno a evaluar la eficiencia de los controles de seguridad, revelar y utilizar las vulnerabilidades de ciberseguridad, evaluando su criticidad explotación por actores de amenaza. También, orientado a aportar al candidato conceptos fundamentales en los test de intuición de aplicaciones webs.
  - **Cybersecurity Auditor:** Habilitar al candidato a auditar riesgos en un sistema de información e implementar medidas de seguridad adaptadas a las organizaciones empresariales. Del mismo modo, elaborar un plan de continuidad de negocio y preparar al sistema ante eventualidades que afecten al servicio de las compañías.

- **Empleabilidad y marca personal:** Adecuar al alumno con metodología, técnicas y herramientas que aporten a la puesta en valor de su marca y perfil en el mercado laboral, facilitando su orientación al empleo con éxito.

3. **Datos de interés**

a. **Fechas de inicio y finalización de los cursos de formación**

Inicio: **16 de octubre**

Vacaciones: **22 de diciembre al 7 de enero**
Finalización: **19 de febrero**

b. Horario

Curso de Pentester - Auditor técnico: **9:00** a **14:00**.
Curso de Cybersecurity Auditor: **15:00** a **20:00**.

c. Modalidad

Se ha diseñado un formato curricular **Presencial** y **Presencial *On Line***, dotando al mismo tanto de clases **presenciales en el Aula** como ***On-Line* síncronas**. Además, el alumnado dispondrá de materiales de apoyo, tutorizaciones y soporte técnico on-line que le permitirán avanzar en determinadas materias en el momento que mejor se adapte a sus necesidades, mientras que las clases presenciales y *on-line* síncronas serán guiadas por el profesor para garantizar la consecución de ciertos objetivos académicos clave y la resolución de dudas a la hora de hacer los ejercicios prácticos.

La **metodología de trabajo será eminentemente práctica** (70% del total de horas por curso), con simulación de casos reales en formato ***"Learning by doing"***. Los alumnos trabajarán en proyectos similares a las situaciones en las que se van a ver en sus trabajos futuros, lo que permitirá que sean autónomos cuando se incorporen a los mismos.

d. Duración

Los contenidos formativos propuestos para la primera tanda de cursos a desarrollar corresponden a **400 horas lectivas cada uno**. A continuación, se incluye su distribución de horas y la planificación prevista el primer año para cada una de las acciones formativas.

e. Plazas

Curso de Pentester - Auditor técnico: **20 alumnos.**
Curso de Cybersecurity Auditor: **20 alumnos.**

f. Lugar de impartición

Av/ Virgen de Guadalupe 7, Planta 1, Local 6, Cáceres (España).

g. Precio

Gratuito.

4. Estructura del curso

En primer lugar, se impartirá el programa de ***Cybersecurity Auditor*** y ***Pentester - Auditor técnico*** bajo la impartición de cursos presenciales que, estarán conformados por las siguientes **asignaturas**:

Cybersecurity Auditor:

Trabajo en proyectos	
☑ **Presencial** ☑ **On-line sincrono**	15 horas
Descripción	
Este módulo de "Trabajo en proyectos" instruirá a los alumnos en herramientas indispensables para el correcto entendimiento del curso, así como la adquisición de ciertas habilidades técnicas necesarias para la inserción en el mundo laboral como por ejemplo el manejo de Google Workspace.	
Objetivos	
• Dotar a los participantes de las herramientas y metodología necesarias para que el aprovechamiento del programa sea el máximo. • Adquirir un nivel adecuado en el uso de herramientas digitales para el correcto desarrollo de los siguientes bloques formativos.	
Capacidades desarrolladas	
Conocer las formas y los medios de comunicación disponibles durante el desarrollo del curso. • Visión general sobre las herramientas digitales colaborativas del mundo digital actual. • Nivel medio - avanzado en el uso de las herramientas más relevantes de Google Workspace.	
Contenidos	

- Formas y canales de comunicación durante el curso.
- Herramientas digitales – Overview.
- Generación de equipos
- Gestión de proyectos
- Google Workspace.
  - ➢ Gmail
  - ➢ Calendar
  - ➢ Drive
  - ➢ Meet
  - ➢ Forms
  - ➢ Datastudio

Fundamentos de ciberseguridad	
☑ **Presencial** ☑ **On-line sincrono**	40 horas

Descripción

Con este módulo se pretende profundizar en el área de la Ciberseguridad informática proporcionando conocimientos sobre la gestión y gobierno de las operaciones de ciberseguridad en las empresas y una visión global de los principales servicios de ciberseguridad.

Objetivos

Dotar a los participantes de una visión general de la Ciberseguridad, riesgos a tener en cuenta, conceptos de cibercrimen y delitos informáticos y la importancia de la Ciberseguridad personal.

Capacidades desarrolladas

- Comunicación y colaboración con todas las áreas de la organización para servir de puente entre las necesidades de los equipos y los riesgos potenciales en seguridad.
- Comprensión del comportamiento humano.
- Investigación, reporting y documentación.
- Capacidad de adaptación y aprendizaje, dados los continuos cambios, deben ser capaces de ofrecer soluciones cada vez más creativas para repeler los ciberataques.
- Pensamiento analítico.

Contenidos

- Ciberseguridad: Conceptos
- Ciberespacio y ciberseguridad. Visión, alcance, historia.
  - ➢ Conceptos fundamentales. Seguridad de información, activo, amenaza y vulnerabilidad, principales amenazas y vulnerabilidades, el factor humano, riesgo, control, ciberataque.
  - ➢ Introducción al cibercrimen. Cibercrimen, brechas y actores.
  - ➢ Delitos informáticos. Tipología, casos por tipo.
  - ➢ Ciberseguridad personal.
- Ciberseguridad: Operaciones
  - ➢ Gestión integral de la ciberseguridad.
  - ➢ Gobierno de la ciberseguridad.
  - ➢ Threat Intelligence.
  - ➢ Blue Team – Seguridad defensiva.
  - ➢ Red Team – Seguridad ofensiva.
  - ➢ Tecnologías de ciberseguridad.
- Ciberseguridad: Servicios
  - ➢ Visión valor añadido aportado por los servicios.
  - ➢ Servicios de Ciberseguridad.
  - ➢ Awareness.
  - ➢ Governance, Risk & Compliance.
  - ➢ Inteligencia Corporativa.
  - ➢ Defense & Response.
  - ➢ Attack Surface Reduction.
  - ➢ Platform. Infraestructura y seguridad.
  - ➢ IAM. Gestión de identidades.
  - ➢ Cloud Security.
  - ➢ CSIRT.
  - ➢ Servicios a sectores industriales.

Auditor en Seguridad de la Información	
☑ **Presencial** ☑ **On-line sincrono**	170 horas
Descripción	
Este módulo capacita al alumno en la tarea de auditar los riesgos en un sistema de información e implementar un plan de medidas de seguridad adaptadas a la organización.	
Objetivos	
Dotar al alumno de la capacidad para realizar revisiones independientes para evaluar la eficacia de los procesos y controles, así como el	

cumplimiento general de las políticas de los marcos legales y reglamentarios de la organización en materia de seguridad de la información. El alumno será capaz de evaluar, probar y verificar los productos relacionados con la ciberseguridad (sistemas, hardware, software y servicios), las funciones y las políticas garantizando el cumplimiento de las directrices, las normas y los reglamentos relacionados.

Mediante la realización de este módulo, el alumno dispondrá de los conocimientos básicos de la seguridad de la información, permitiéndole de este modo realizar diversas tareas dentro de las organizaciones:

- Dar asesoramiento a empresas en cuanto a la Seguridad de la Información,
- Llevar a cabo proyectos de implantación de la ISO2700 y de evaluación de implantación de la misma.
- Definir marcos de control tecnológicos y revisar su nivel de implantación y eficacia.
- Implementar análisis de riesgos y definir planes de acción que permitan incrementar su nivel de madurez.
- Definir e implantar un plan de concienciación y formación para los empleados de las organizaciones.

Capacidades desarrolladas

Organizar y trabajar de forma sistemática y determinista basándose en pruebas.

- Seguir y practicar marcos, normas y metodologías de auditoría.
- Aplicar herramientas y técnicas de auditoría.
- Analizar los procesos empresariales, así como evaluar y revisar los controles técnicos y organizativos.
- Comunicar, explicar y adaptar los requisitos legales y reglamentarios y las necesidades empresariales.
- Planificar y realizar entrevistas de forma sistemática y determinista.
- Recoger, evaluar, mantener y proteger la información de auditoría.
- Auditar con integridad, siendo imparcial e independiente.

Contenidos

- Introducción SEGINFO
  - ➢ Principios fundamentales de seguridad de la información
  - ➢ Introducción a los sistemas de gestión y enfoque de procesos
  - ➢ Presentación de los marcos regulatorios
  - ➢ Introducción a la normativa de referencia de la seguridad de la información
  - ➢ Sistemas de Gestión de Seguridad de la Información

Estructura del sistema de gestión de seguridad de la información

- Contexto de la organización y liderazgo
  - ➢ Comprender la organización y su contexto
  - ➢ Comprender las necesidades y expectativas de las partes interesadas
  - ➢ Determinar el alcance del sistema de gestión de seguridad de la información
  - ➢ Sistema de gestión de seguridad de la información
  - ➢ Liderazgo y compromiso
  - ➢ Política de seguridad de la información
  - ➢ Funciones organizativas, roles y responsabilidades

- Planificación
  - ➢ Definición del ámbito de aplicación del sistema de gestión de seguridad de la información
  - ➢ Análisis de riesgos: identificación, análisis y tratamiento del riesgo
  - ➢ Metodología de análisis de riesgos
  - ➢ Objetivos de seguridad de la información
  - ➢ Declaración de aplicabilidad
  - ➢ Plan de tratamiento de riesgos
  - ➢ Taller de análisis y plan de tratamiento del riesgo

- Operación
  - ➢ Recursos y competencias
  - ➢ Desarrollo de un programa de formación, concienciación y comunicación
  - ➢ Información documentada

- Evaluación del desempeño
  - ➢ Seguimiento, medición, análisis y evaluación
  - ➢ Auditoría interna de un SGSI
  - ➢ Revisión por la dirección
  - ➢ Mejora continua
  - ➢ Preparación para una auditoría de certificación

- Proyecto de implementación de un SGSI
  - ➢ Fases de implantación de un SGSI

- ➢ Liderazgo
- ➢ Riesgos
- ➢ Obtener un sponsor y el compromiso de la dirección

- Caso práctico

El caso práctico se plantea como un mecanismo de demostración de los conocimientos que se van adquiriendo a través de los distintos módulos que componen el curso y englobará en gran medida todos los grandes dominios de la ISO:27.001.

El alumno llevará a cabo una simulación de un caso real en el que tendrá que plantear para una entidad ficticia los siguientes puntos:

- Análisis de contexto
- Descripción del alcance
- Desarrollo de la Política de Seguridad de la Información
- Análisis de riesgos
- Plan de Tratamiento del Riesgo
- Plan de formación
- Plan de concienciación
- Exposición del caso práctico

Conocimientos adquiridos con este módulo:

Este curso se centra en la formación a los alumnos para alcanzar un nivel básico para que, posteriormente, estén capacitados y continuar su formación en los distintos dominios de seguridad:

- Conocer qué es un Sistema de Gestión de Seguridad de la Información, qué procesos lo conforman y la normativa que lo regula.
- Comprender qué ha de disponer una entidad de cara a lograr tener implantado un SGSI. Definir un marco normativo de Seguridad acorde a lo que se establece en un SGSI.
- Llevar a cabo Análisis de Riesgos, basándose en una metodología previamente definida y aplicación de los planes de acción para completar los controles implantados.
- Dotar de las capacidades pertinentes a los recursos de la empresa en cuanto a la seguridad de la información, además de ser capaces de administrar la misma a través de los distintos recursos disponibles.
- Capacitar al SGSI de una revisión continua del sistema y proponer mejoras sobre el mismo.
- Tener las capacidades de gestión de proyectos, como pudiera ser un SGSI.

Continuidad y resiliencia	
☑ Presencial ☑ On-line sincrono	125 horas
Descripción	
Este módulo capacita al alumno para elaborar un plan de continuidad del negocio y preparar al sistema ante eventualidades que afecten al servicio de la organización.	
Objetivos	
Dotar al alumno de los conocimientos básicos para la gestión de la Continuidad de Negocio de una entidad. Una correcta gestión del Sistema de Continuidad de Negocio permitirá a la entidad impactar lo menos posible a su negocio y ser capaces de que sus actividades recuperen lo antes posible. En esta situación, el alumno habrá diseñado las actividades y elementos necesarios para que esa circunstancia sea posible.	
Capacidades desarrolladas	
• Dar asesoramiento a empresas en cuanto a la Continuidad de Negocio. • Llevar a cabo proyectos de implantación de un SGCN y de evaluación de implantación del mismo. • Conocer la documentación necesaria, los roles y responsabilidades que han de existir en un SGCN. • Desarrollar análisis de impacto en el Negocio y definir planes de acción que permitan incrementar su nivel de madurez. • Diseñar las pruebas pertinentes de los distintos escenarios que se puedan plantear. • Definir e implantar un plan de concienciación y formación para los empleados de las organizaciones.	
Contenidos	

- Introducción a los sistemas de gestión de continuidad de negocio (SGCN)
  - ➢ Principios fundamentales de continuidad de negocio y resiliencia
  - ➢ Enfoque a procesos
  - ➢ Introducción a los sistemas de gestión y anexo SL
  - ➢ Introducción al marco regulatorio
  - ➢ Antecedentes de ISO 22301
  - ➢ Beneficios de un SGCN
  - ➢ Estructura del sistema de gestión de continuidad de negocio
  - ➢ Ejercicios y caso práctico

- Contexto de la organización y liderazgo
  - ➢ Comprender la organización y su contexto
  - ➢ Comprender las necesidades y expectativas de las partes interesadas
  - ➢ Determinar el alcance del SGCN
  - ➢ Orientación a procesos del SGCN
  - ➢ Liderazgo y compromiso
  - ➢ Política
  - ➢ Roles, responsabilidades y autoridades
  - ➢ Ejercicios y caso práctico

- Planificación de un sistema de gestión de continuidad de negocio
  - ➢ Medidas para abordar los riesgos y oportunidades
  - ➢ Objetivos de continuidad de negocio y planificación para alcanzarlos
  - ➢ Gestión de cambios del SGCN
  - ➢ Formación y concienciación
  - ➢ Comunicación
  - ➢ Control de la información documentada
  - ➢ Ejercicios y caso práctico

- Operación de un sistema de gestión de continuidad de negocio
  - ➢ Planificación y control operacional
  - ➢ Evaluación de riesgos disruptivos
  - ➢ Evaluación de impacto en el negocio (BIA)
  - ➢ Estrategias y soluciones
  - ➢ Plan de Gestión de Incidentes
  - ➢ Plan de Continuidad de Negocio
  - ➢ Pruebas y ejercicios
  - ➢ Evaluación de continuidad de negocio
  - ➢ Riesgos y estrategias en un centro de datos
  - ➢ Ejercicios y caso práctico

- Continuidad y Resiliencia. Monitoreo, medición, revisión, auditoría y mejora de un SGCN

- ➢ Monitoreo y medición de procesos de continuidad de negocio
- ➢ Auditoría interna de un SGCN
- ➢ Revisión de una dirección de un SGCN
- ➢ Mejora continua
- ➢ Proceso de certificación de un SGCN
- ➢ Ejercicios y caso práctico

- Proyecto de implantación de un SGCN
  - ➢ Fases de implantación de un SGCN
  - ➢ Liderazgo
  - ➢ Riesgos del proyecto y resolución de problemas
  - ➢ Ejercicios y caso práctico

Conocimientos adquiridos con este módulo:

Este módulo se centra en la formación a los alumnos para alcanzar un nivel básico para que, posteriormente, estén capacitados y continuar su formación en el ámbito de la Continuidad de Negocio.

- Conocer qué es un Sistema de Gestión de la Continuidad de Negocio, qué procesos lo conforman y la normativa que lo regula.
- Comprender qué ha de disponer una entidad de cara a lograr implantar un SGCN. Definir un marco normativo de Continuidad de Negocio y sus documentos de soporte (procedimientos, procesos, instrucciones técnicas, etc.)
- Llevar a cabo BIAs, basándose en una metodología previamente definida para las pruebas pertinentes, realizar ejercicios prácticos y definir estrategias que minimicen las afectaciones en caso de incidentes.
- Dotar de las capacidades pertinentes a los recursos de la empresa en cuanto a gestión de la continuidad de negocio, además de ser capaces de administrar la misma a través de los distintos recursos disponibles.
- Capacitar al SGCN de una revisión continua del sistema y proponer mejoras sobre el mismo.
- Tener las capacidades de gestión de proyectos, como pudiera ser un SGCN.

Empleabilidad y marca personal	
☑ Presencial ☑ On-line sincrono	40 horas
Descripción	
Este módulo de Talleres prácticos prepara al alumno en las herramientas y	

técnicas para poner en valor su Marca (CV y "Elevator Pitch") en el mercado laboral facilitando su orientación al empleo con éxito.
Objetivos
Dotar a los participantes de las herramientas y metodología para facilitar el poner en valor su Marca Personal en el mercado laboral al que quieren dirigirse con éxito.
Capacidades desarrolladas
Autoconfianza, Autocontrol, orientación a objetivos, Marca personal, Comunicación oral y escrita, venta.
Contenidos
Taller de Grow-Marca Personal - Dotar a los participantes de metodología, Dafo. Preparación del "*elevator pitch*". • Taller de CVs - Dotar a los participantes de herramientas para hacer un buen CV adaptado al puesto objetivo y realización del CV. • Taller de Linkedin - Dotar a los participantes de las claves para hacer un CV atractivo en Linkedin, que se realizará en el mismo taller. • Taller de entrevistas - Dotar a los participantes de las técnicas de entrevistas por competencias e incidentes críticos. Ensayo de preguntas difíciles y entrevistas. • Taller de Canales de empleo - Mostrar los canales de empleo y su uso, incluido el contacto. Ensayar. • Tutorización individual durante - Horas de tutoría de preparación de CVs y entrevistas **Conocimientos adquiridos con este módulo:** Mediante el empleo de la metodología de coaching GROW contrastada y adaptada a orientación, con un porcentaje del 100% de inserciones laborales en menos de 3 meses, se trabaja con el alumno la preparación del CV, el CV en linkedin, el elevator pitch, las entrevista y el uso de los canales de empleo, además de su propia autoconfianza y empowerment para tener éxito en la búsqueda de empleo.

Pentester - Auditor Técnico:

Trabajo en proyectos

☑ **Presencial** ☑ **On-line sincrono**	15 horas

Descripción
Este módulo de "Trabajo en proyectos" instruirá a los alumnos en herramientas indispensables para el correcto entendimiento del curso, así como la adquisición de ciertas habilidades técnicas necesarias para la inserción en el mundo laboral como por ejemplo el manejo de Google Workspace.
Objetivos
• Dotar a los participantes de las herramientas y metodología necesarias para que el aprovechamiento del programa sea el máximo. • Adquirir un nivel adecuado en el uso de herramientas digitales para el correcto desarrollo de los siguientes bloques formativos.
Capacidades desarrolladas
Conocer las formas y los medios de comunicación disponibles durante el desarrollo del curso. • Visión general sobre las herramientas digitales colaborativas del mundo digital actual. • Nivel medio - avanzado en el uso de las herramientas más relevantes de Google Workspace.
Contenidos
• Formas y canales de comunicación durante el curso. • Herramientas digitales – Overview. • Generación de equipos • Gestión de proyectos • Google Workspace. ➢ Gmail ➢ Calendar ➢ Drive ➢ Meet ➢ Forms ➢ Datastudio

Fundamentos de ciberseguridad

☑ **Presencial** ☑ **On-line sincrono**	40 horas

Descripción
Con este módulo se pretende profundizar en el área de la Ciberseguridad informática proporcionando conocimientos sobre la gestión y gobierno de las operaciones de ciberseguridad en las empresas y una visión global de los principales servicios de ciberseguridad.

Objetivos
Dotar a los participantes de una visión general de la Ciberseguridad, riesgos a tener en cuenta, conceptos de cibercrimen y delitos informáticos y la importancia de la Ciberseguridad personal.

Capacidades desarrolladas
• Comunicación y colaboración con todas las áreas de la organización para servir de puente entre las necesidades de los equipos y los riesgos potenciales en seguridad. • Comprensión del comportamiento humano. • Investigación, reporting y documentación. • Capacidad de adaptación y aprendizaje, dados los continuos cambios, deben ser capaces de ofrecer soluciones cada vez más creativas para repeler los ciberataques. • Pensamiento analítico.

Contenidos
• Ciberseguridad: Conceptos • Ciberespacio y ciberseguridad. Visión, alcance, historia. ➢ Conceptos fundamentales. Seguridad de información, activo, amenaza y vulnerabilidad, principales amenazas y vulnerabilidades, el factor humano, riesgo, control, ciberataque. ➢ Introducción al cibercrimen. Cibercrimen, brechas y actores. ➢ Delitos informáticos. Tipología, casos por tipo. ➢ Ciberseguridad personal. • Ciberseguridad: Operaciones ➢ Gestión integral de la ciberseguridad. ➢ Gobierno de la ciberseguridad. ➢ Threat Intelligence. ➢ Blue Team – Seguridad defensiva. ➢ Red Team – Seguridad ofensiva. ➢ Tecnologías de ciberseguridad.

- Ciberseguridad: Servicios
  - ➢ Visión valor añadido aportado por los servicios.
  - ➢ Servicios de Ciberseguridad.
  - ➢ Awareness.
  - ➢ Governance, Risk & Compliance.
  - ➢ Inteligencia Corporativa.
  - ➢ Defense & Response.
  - ➢ Attack Surface Reduction.
  - ➢ Platform. Infraestructura y seguridad.
  - ➢ IAM. Gestión de identidades.
  - ➢ Cloud Security.
  - ➢ CSIRT.
  - ➢ Servicios a sectores industriales.

Hacking Ético de Sistemas y Redes	
☑ Presencial ☑ On-line sincrono	185 horas
Descripción	
El módulo está orientado a evaluar la eficacia de los controles de seguridad, revelar y utilizar las vulnerabilidades de ciberseguridad, evaluando su criticidad si son explotadas por los actores de la amenaza.	
Objetivos	
Este módulo enseña a los participantes a planificar, diseñar, implementar y ejecutar tests de intrusión y escenarios de ataque para evaluar la eficacia de las medidas de seguridad desplegadas o planificadas. Se pretende Identificar vulnerabilidades o fallos en los controles técnicos y organizativos que afectan a la confidencialidad, la integridad y la disponibilidad de los productos de TIC (por ejemplo, sistemas, hardware, software y servicios). En este módulo se contempla la formación para realizar unas buenas prácticas las cuales son necesarias para ejecutar tests de intrusión con éxito. Se tendrá material teórico como práctico junto a laboratorios donde se podrán explotar vulnerabilidades en un entorno controlado. La protección de los sistemas de red requiere de una comprensión amplia de las estrategias de ataque y de un conocimiento profundo de los procesos y herramientas que se utilizan en una auditoría de seguridad. Se trabajarán los fundamentos del hacking profundizando en las etapas que existen para la realización de las pruebas de intrusión. Pasando por las	

fases de reconocimiento, enumeración, explotación, postexplotación e informes. También entrará en materia otras modalidades importantes como pueden ser los aspectos éticos y legales, y la criptografía.

Capacidades desarrolladas

- Desarrollar códigos, scripts y programas.
- Realizar ingeniería social.
- Identificar y explotar vulnerabilidades.
- Pensar de forma creativa y original.
- Resolver y solucionar problemas.
- Comunicar e informar.
- Utilizar eficazmente las herramientas de pruebas de penetración.
- Adaptar y personalizar las herramientas y técnicas de pruebas de penetración.

Contenidos

- Fundamentos de Hacking
  - ➢ Elementos de seguridad de la información
  - ➢ El triángulo de la seguridad, la funcionalidad y la usabilidad
  - ➢ Tipos de Hackers
  - ➢ Hacking Ético
  - ➢ Vulnerabilidades
  - ➢ Divulgación ética de vulnerabilidades

- Aspectos éticos y legales
  - ➢ Aspectos legales de un hacking ético
  - ➢ Normatividad

- Metodologías y estándares
  - ➢ Metodologías
  - ➢ Estándares
  - ➢ Buenas prácticas

- Levantamiento de huellas y reconocimiento
  - ➢ Conceptos básicos
  - ➢ Herramientas
  - ➢ Google Hacking
  - ➢ Técnicas del footprinting
  - ➢ OSINT

- Escaneo de redes y dispositivos
  - ➢ Definición y tipos de escaneo
  - ➢ Metodología de exploración de CEH
  - ➢ Técnicas y herramientas

- Banner fingerprinting, acaparamiento y OS
- Proxies y anonimizadores

- Enumeración de activos
  - Conceptos básicos
  - Técnicas y tipos de enumeración
  - Contramedidas

- Análisis de vulnerabilidades
  - Herramientas de detección de vulnerabilidades
  - Gestión de falsos positivos

- Escalamiento de privilegios
  - Escalamiento horizontal
  - Escalamiento vertical
  - Contramedidas

- Ataques a dispositivos
  - Conceptos básicos
  - Herramientas y técnicas de ataque
  - Contramedidas

- Ataques a redes cableadas
  - Conceptos básicos
  - Modelo OSI
  - Herramientas y técnicas de ataque
  - Contramedidas

- Ataques a redes cableadas
  - Introducción al malware
  - Etapas de vida del malware
  - Tipos de malware
  - Troyanos
  - Gusano
  - Sheep Dip
  - Contramedidas

- Evasión de antivirus
  - Técnicas y herramientas de evasión

- Ingeniería social
  - Fases de un ataque de ingeniería social
  - Tipos de ingeniería social
  - Redes sociales, suplantación y riesgos
  - Robo de identidad
  - Pruebas de penetración de la ingeniería social

- Denegación de servicio
  - ➢ Definición y explicación de DoS - DDoS
  - ➢ Internet Relay Chat - IRC
  - ➢ Técnicas de ataque DoS
  - ➢ Botnets
  - ➢ Herramientas de ataque
  - ➢ Contramedidas

- Detección y evasión de IDS, Firewalls y honeypots
  - ➢ Sistema de detección de intrusos y cómo detectar intrusos.
  - ➢ Tipos de IDS
  - ➢ Firewall y tipos de firewall.
  - ➢ Honeypot y tipos de honeypot
  - ➢ Sistema IDS, firewall y honeypot
  - ➢ Evasión de IDS y firewalls
  - ➢ Contramedidas

- Criptografía
  - ➢ Tipos de criptografia
  - ➢ Cifrados
  - ➢ Herramientas de criptografía
  - ➢ Firma digital
  - ➢ Cifrado y herramientas de cifrado de disco duro
  - ➢ Herramientas de criptoanálisis

- Reportes
  - ➢ Tipos de reportes
  - ➢ Detalles de un reporte
  - ➢ Declaraciones

Conocimientos adquiridos con este módulo:

- Se estudiarán las etapas necesarias para un pentesting.
- Se aprenderá a utilizar herramientas de búsqueda y explotación de vulnerabilidades.
- Se conocerán las leyes que prevalecen en el mundo del pentesting
- Se podrán realizar explotaciones con Escalado de privilegios
- Se aprenderá a evadir antivirus, Firewalls, IDS para poder conseguir una explotación satisfactoria
- Se adquirirán conocimientos de criptografía como pueden ser algoritmos de cifrados y ataques criptográficos.
- Se tendrá una buena base para la realización informes ya que son el único resultado tangible de los tests de intrusión.

Aplicaciones web y sistemas

☑ Presencial ☑ On-line sincrono	110 horas

Descripción
El módulo está orientado al conocimiento de los conceptos más importantes en los tests de intrusión de aplicaciones webs.

Objetivos
Este curso enseña a los participantes a planificar, diseñar, implementar y ejecutar tests de intrusión y escenarios de ataque para evaluar la eficacia de las medidas de seguridad desplegadas o planificadas. Se pretende Identificar vulnerabilidades o fallos en los controles técnicos y organizativos que afectan a la confidencialidad, la integridad y la disponibilidad de aplicaciones web y sistemas. Se estudiarán las vulnerabilidades más conocidas y críticas para estos entornos y el cómo explotarlas correctamente. Principalmente se tratarán los ataques de inyección del tipo XSS, SQL y se realizarán prácticas de laboratorio con ataques más avanzados.

Capacidades desarrolladas
• Desarrollar códigos, scripts y programas. • Realizar ingeniería social. • Identificar y explotar vulnerabilidades. • Pensar de forma creativa y original. • Resolver y solucionar problemas. • Comunicar e informar. • Utilizar eficazmente las herramientas de pruebas de penetración. • Adaptar y personalizar las herramientas y técnicas de pruebas de penetración.

Contenidos
• Homologación de conceptos ➢ Fundamentos de seguridad en aplicaciones web ➢ Vulnerabilidades comunes en aplicaciones web ➢ Vectores de ataque adicionales • Configuración de entornos y laboratorios • Injection • Command execution • Ataques Web Avanzados • Web Application Firewalls

Conocimientos adquiridos con este módulo:

- Se estudiarán las etapas necesarias para realizar un pentest web
- Se aprenderá a utilizar herramientas que se utilizan para la realización de los pentests we
- Se conocerán los conceptos a bajo nivel de las vulnerabilidades mas conocidas en entornos we
- Se realizará la explotación de vulnerabilidades de inyección del tipo XSS y SQL
- Se crearán laboratorios para la realización de pruebas web avanzadas en entornos controlados.

Empleabilidad y marca personal	
☑ Presencial ☑ On-line sincrono	40 horas
Descripción	
Este módulo de Talleres prácticos prepara al alumno en las herramientas y técnicas para poner en valor su Marca (CV y "Elevator Pitch") en el mercado laboral facilitando su orientación al empleo con éxito.	
Objetivos	
Dotar a los participantes de las herramientas y metodología para facilitar el poner en valor su Marca Personal en el mercado laboral al que quieren dirigirse con éxito.	
Capacidades desarrolladas	
Autoconfianza, Autocontrol, orientación a objetivos, Marca personal, Comunicación oral y escrita, venta.	
Contenidos	

Taller de Grow-Marca Personal - Dotar a los participantes de metodología, Dafo.

Preparación del "*elevator pitch*".

- Taller de CVs - Dotar a los participantes de herramientas para hacer un buen CV adaptado al puesto objetivo y realización del CV.
- Taller de Linkedin - Dotar a los participantes de las claves para hacer un CV atractivo en Linkedin, que se realizará en el mismo taller.
- Taller de entrevistas - Dotar a los participantes de las técnicas de entrevistas por competencias e incidentes críticos. Ensayo de preguntas difíciles y entrevistas.
- Taller de Canales de empleo - Mostrar los canales de empleo y su uso, incluido el contacto. Ensayar.
- Tutorización individual durante - Horas de tutoría de preparación de CVs y entrevistas

Conocimientos adquiridos con este módulo:

Mediante el empleo de la metodología de coaching GROW contrastada y adaptada a orientación, con un porcentaje del 100% de inserciones laborales en menos de 3 meses, se trabaja con el alumno la preparación del CV, el CV en linkedin, el elevator pitch, las entrevista y el uso de los canales de empleo, además de su propia autoconfianza y empowerment para tener éxito en la búsqueda de empleo.

5. Perfil del alumno

El curso de formación en ***Cybersecurity Auditor*** está dirigido a recién titulados en Ciencias Sociales y/o Jurídicas, titulados o profesionales de auditoría y/o calidad que quieran desarrollar su carrera en Ciberseguridad, donde se capacitarán para ser Auditores de Riesgos de Seguridad de la información y Continuidad del Negocio.

El curso de formación de ***Pentester - Auditor Técnico*** está dirigido a recién graduados en estudios de formación profesional o grados universitarios técnicos (informática, sistemas, desarrollo, comunicaciones o ingenierías), o profesionales con experiencia laboral en el área técnica. Esto capacitará a los candidatos a ser Pentesters - Auditores Técnicos de Ciberseguridad (Hackers éticos)

Nota importante: Será necesario haber cursado algún tipo de formación técnica (mínimo Formación Profesional de Grado Superior) o disponer de experiencia demostrable de ámbito técnico relacionada con el perfil de cada especialidad

formativa. Para el proceso de selección de participantes se seguirá el procedimiento que determine la normativa reguladora de la convocatoria.

6. ¿Por qué CCI-EX?

El *"Centro de Ciberseguridad e Innovación, S.L. "CCI-Ex"* es una nueva compañía ubicada en Don Benito – Villanueva de la Serena (Badajoz), que tiene como propósito el ofrecer servicios industrializados de operación, **formación, consultoría, desarrollo y cooperación en innovación tecnológica y ciberseguridad a PYMEs y entidades públicas locales, regionales o gremiales, en modalidad de Centro de Servicios Compartidos (CSC).**

CCI-EX tiene como valor diferencial el permitir, a través de metodologías contrastadas durante más de veinte años y tecnologías de primer nivel tanto propias como de mercado, por economía de escala y delegación de responsabilidades por parte de las organizaciones receptoras del servicio, la **prestación de servicios tecnológicamente avanzados y de alta complejidad técnica** que de otra forma no serían accesibles para la mayor parte de las organizaciones públicas y privadas. Adicionalmente, CCI-Ex se constituirá como un **centro formativo de primer nivel en materia de ciberseguridad** que convertirá a Extremadura en un polo de generación y atracción de talento en el sur de Europa y que beneficiará a su entorno al evitar la fuga de talento, combatir la despoblación rural y fomentar la digitalización de empresas locales.