Cámara Madrid

Curso Superior en Ciberseguridad de la Empresa

PRESENTACIÓN

Las nuevas amenazas para la empresas, provenientes de un entorno virtual en permanente cambio, suponen un alto riesgo para el que se debe estar prevenido y protegido. Existe una obligación, cada vez más necesaria, de establecer dentro de las empresas, protocolos de seguridad contra la delincuencia cibernética.

La implantación de planes de Seguridad, que incluyan las tecnologías, procesos y el conocimiento de los usuarios implicados, así como la protección de la red interna y externa de la empresa y el control de las aplicaciones, debe realizarse sin influir en la productividad de los usuarios y el eficiente funcionamiento de los sistema informáticos.

Para ello, las empresa deben buscar especialistas en Ciberseguridad para anticiparse a los riesgos y encargarse de la privacidad y proyección de sus sistemas informáticos y datos.

Según del Consejo Nacional de Ciberseguridad **para 2025 se requerirán cerca de 825.000 profesionales de Ciberseguridad** de todos los ámbitos. Este Curso supone el primer paso para una especialización con gran proyección y trayectoria profesional.

DIRIGIDO A:

Para este curso no es necesario disponer de conocimientos informáticos avanzados. Se trata de formar expertos en la detección, análisis y creación de Planes de Ciberseguridad en la Empresa, para su posterior ejecución tecnológica y normativa.

- Cuadros medios y directivos que tengan que organizar Planes de Ciberseguridad.
- Administradores que quieran integrar la Ciberseguridad como valor añadido a su negocio de necesiten conocer los métodos y procedimiento y tecnologías.
- Licenciados-graduados que quieran iniciarse, mejorar o consolidad su desarrollo profesional en el ámbito de la gestión y administración de la Cibersegridad en empresas.
- Gestiones de proyectos donde sea necesario integrar la Ciberseguridad como valor añadido al negocio o deban implementar medidas impuestas por su organización.

OBJETIVOS

El objetivo principal del Curso es capacitar al alumno en los procesos de toma de decisiones estratégicas empresariales en materia de Cibersdeguridad. Asimismo:

. Adquirir una base de conocimiento profundo en las amenazas y riesgos cibernéticos y cómo defenderse ante ellos desde el punto de vista empresarial.

. Desarrollar competencias profesionales para establecer protocolo de Ciberseguridad interna y externa en las empresas, utilizando herramientas y procesos de prevención y detección y actuación específicos.

. Conocer el procedimiento de análisis forense y ciclo de vida la información en la empresas para su mejor protección ante ciberataque e insiders.

. Aprender los principales conceptos de Ciberinteligencia empresarial y sus herramientas

PROGRAMA

1. CIBERSEGURIDAD: CONCEPTOS Y ESTRATEGIA GENERAL DE LA DEFENSA. CIBERAMENAZAS

- Internet y su evolución.
- ¿ Qué es la ciberseguridad?.
- ¿Cómo podemos lograr la ciberseguridad?.
- Factores de inseguridad.
- Ciberamenazas
- Estrategia nacional y europea (introducción).
- Implantación de la Seguridad en la Empresa
  - Organización de la Seguridad
  - Políticas y marco normativo
  - Controles Técnicos y Humanos

2. TALLER DE MÁQUINAS VIRTUALES

- Utilizad de la máquinas virtuales..
- Aplicación de las máquinas virtuales de la Ciberseguridad.

3. SEGURIDAD EN LA RED Y ANONIMIZACIÓN

- Criptografía Básica.
- Cifrado en las comunicaciones.
- Certificados y firmas digitales.
- Prevención y detección en la red.
- Anonimatos a diferentes niveles
- Virtualización y prevención de riesgos.

4. ANÁLISIS FORENSE

- Fundamentos.
- Ejemplos de casos reales.
- Esquema de actuación y preservación de evidencias.ISO27037
- Artefactos
- Valor de la prueba.

5. SEGURIDAD PERIMETRAL DE LA EMPRESA

- Detección y prevención de ataques
- Firewalls
- Antispam, antivirus
- VPN/ UTM

6. SERVICIOS EN LA NUBE Y EXTERNALIZACIÓN

- Tipos de Servicios (IasaS, PaaS, SaaS)
- Externalización y subcontratación
- Riesgos y controles

7. INCIDENTES DE SEGURIDAD Y NOTIFICACIÓN

- Eventos, ficheros de logs, monitorización y detección
- Valoración e investigación de incidentes
- Notificación a las autoridades de control y la Alta Dirección

8. CONCIENCIACIÓN EN LAS EMPRESAS

- Vulnerabilidades
- Plan de acción
- Seguimiento y actualización
- Formación

9. RIESGO INTERNO: FUGA DE INFORMACIÓN E INSIDERS.

- Naturaleza de las amenazas de insiders.
- Tipologías de los ataques realizados por insiders..
- Detección de nodos de influencia en la organización.
- Análisis de redes sociales..

10. INGENIERIA SOCIAL E INFLUENCIA

- Dirección de tácticas de perfilado de objetivos.
- Ataques basados en la sobreexposición de información en las redes sociales.
- Metodologías de acercamiento a los objetivos.

11. GESTIÓN DE CRISIS

- Estrategias y coordinación de la defensa
- Continuidad del negocio
- Planes de contingencia
- Planes de cooperación ante desastres

12. REPUTACION Y VIGILANCIA DE MARCA.GUERRAS DE INFORMACIÓN

- Reputación
- Gestión de la Reputación online
- Definiciones y tipos de Redes Sociales
- Marca personal Vs Marca de Empresa
- Gestión de Perfiles personales/Gestión de perfiles de empresa en al principales RRSS (Facebook, LinKedin, Twitter, Telegram e Instagram)
- Herramientas de análisis y gestión de RRSS
- Vigilancia competitiva, vigilancia tecnológica.
- Guerra de información, Inteligencia Económica

13. CIBERDERECHO

- Reputación
- Gestión de la Reputación online
- Definiciones y tipos de Redes Sociales
- Gestión de Perfiles personales/Gestión de perfiles de empresa

14. DESARROLLO DE PLANES DE SEGURIDAD

- Determinación de las necesidades financieras y ayudas económicas para la empresa.
- Clasificación de los productos y servicios financieros.
- Valoración de productos y servicios financieros.
- Tipología de las operaciones de seguros.
- Selección de inversiones en activos financieros y económicos.
- Integración de presupuestos.

CLAUSTRO

- Álvaro Ortigosa. Director del ICFS y profesor Doctor en Ingenería Informática
- Elena Ortega, colsultor técnico en Ciberseguridad en el Banco Santander
- Miriam Tendero, Organizadora del grupo de hacking ético de la Facultad de Informática de la Universidad Complutense
- Daniel García : Trainee en Guardia Civil estudiante de ingeniería Informática en la UCM. Fundador y organizador del evento de ciberseguridad CryptoParty Madrid. Fundador y organizador del grupo de hacking de la Universidad Complutense de Madrid. Cibercooperante
- Carlota Urruela: Proyect Manager & Reseacher ICFS. Trainee en Guardia Civil
- Casimiro Nevado: Inspector Policía Nacional . Profesor Escuela Nacional de Policia
- Sandra Vázquez: responsable de Comunicación y Relaciones Institucionales del ICFS, Docente y Directora del curso Homicidios sin Resolver en sus respectivas ediciones. Docente del curso Big Data para Community Managers de la Fundación Uned y docente en el curso Gestión de Estrategias de Defensa en Ciberseguridad
- Araceli Bailón: Gerente de ICFS
- Fénix Ávila: Experto en Derecho de Ciberseguridad

Duración: 180 horas

1ª Convocatoria: 25 febrero al 20 de junio de 2019

2ª Convocatoria: 28 octubre 2019 al 27 de febrero de 2020

Modalidad: Presencial de Lunes a Jueves , 19:00 a 22:00 horas

Precio Total: 2800 €. Matrícula: 1000 € / Mensualidades: 600 € (tres mensualidades de marzo a mayo de 2019)

La realización del curso incluye el derecho a presentarse al examen para obtener la Certificación de Gestión en Ciberseguridad otorgada por la ACC (Agencia de Cibercertificaciones del ICFS/UAM). El coste de la presentación será de 80 €

Centro de Formación de la Cámara Oficial de Comercio, Industria y Servicios de Madrid -IFE-
Calle Pedro Salinas, 11 -28043 Madrid
camara@camaramadrid.es

Información e inscripciones
91 538 38 24
91 538 38 38
91 538 35 00