CURSO ONLINE DE CIBERSEGURIDAD PARA PROFESIONALES Y EMPRESAS

La **ciberseguridad** ya no es sólo una cuestión tecnológica: es una necesidad para proteger **información sensible**, documentación técnica, datos personales, cuentas corporativas y accesos remotos. Hoy cualquier profesional o empresa puede ser objetivo de ataques que afecten a la actividad diaria y generen pérdidas económicas o legales.

En este curso online de **4 semanas (40 horas)**, los participantes aprenderán a **identificar amenazas reales** (phishing, malware, intrusiones y fraudes), aplicar medidas prácticas de **prevención y protección**, y reforzar la seguridad del puesto de trabajo y la organización. Además, se abordará el **marco normativo**, la privacidad y las responsabilidades asociadas (RGPD, teletrabajo seguro y buenas prácticas).

NOTA: Para repaso de contenidos, tras la finalización, este curso incluye **2 semanas extra de libre acceso** a los materiales, una vez concluida la fase de tutorización y evaluación.

RECURSOS, METODOLOGÍA Y TUTORIZACIÓN

En RBC INGENIEROS, estamos dedicados a ofrecer una **experiencia educativa completa y accesible**. Hemos desarrollado un programa basado en tres pilares esenciales: contenidos y accesibilidad, interacción tutor-alumno, y evaluación con acreditación. A continuación, te mostramos un resumen de los recursos y métodos que implementaremos para garantizar que cada participante logre sus metas de aprendizaje de manera efectiva.

Contenidos y accesibilidad

Material pedagógico en formato multimedia.
Aula 100% responsive (accesible desde PC, tablets o móviles).
Más de 20 videos explicativos.
Ejemplos prácticos desarrollados en vídeos.
Acceso a la plataforma 24 horas/día.

Interacción tutores y alumnos

Sesiones semanales de Tutorías online mediante chat (2 sesiones/semana).
Foros de discusión atendidos a diario por los tutores.
Tutor virtual LEONARDO (atención inmediata 24 horas/día).
Mensajería interna.

Evaluación y acreditación

Evaluación mediante cuestionarios tipo test.
Diploma acreditativo.

IMPORTANTE:

Los **contenidos y actividades del curso** están diseñados en formato multimedia SCORM, accesibles únicamente desde el aula virtual, por lo que **no se pueden descargar** y requieren el uso de la plataforma para su funcionamiento.

EQUIPO DOCENTE

En nuestro curso, los participantes cuentan con la guía experta de Rafael Blanco Ocaña, Ingeniero Técnico Industrial con extensa experiencia, Alberto Millares Prats, arquitecto con una dilatada carrera profesional y Leonardo, un tutor virtual que ofrece soporte 24/7, combinando conocimiento profesional con asistencia tecnológica inmediata.

Rafael Blanco Ocaña, *Ingeniero Técnico Industrial*
Con más de 25 años de experiencia en diseño y cálculo de estructuras, instalaciones industriales y en edificios, eficiencia energética, y como formador en el ámbito de la ingeniería, las nuevas tecnologías y la inteligencia artificial.

Laura Aranda Barrera, *Ingeniera Informática*
Amplia experiencia en desarrollo y entornos tecnológicos. Docente de Ciberseguridad, IA y nuevas tecnologías.

Leonardo, tutor virtual mediante *Inteligencia Artificial*.
Esta innovadora herramienta está diseñada para ofrecer asistencia inmediata a las consultas, 24 horas al día, 7 días a la semana, proporcionando recursos adicionales y guiando a los participantes a través de su proceso de aprendizaje de manera eficiente, interactiva y personalizada.

FECHAS Y DURACIÓN DEL CURSO:

El curso tiene una duración de 4 semanas, equivalente a 40 horas lectivas de formación, y cuenta a la finalización de **2 semanas adicionales** sin tutorización, para repaso de contenido.

Fecha de inicio: 13 de abril de 2026.
Fecha de finalización: 10 de mayo de 2026.

El plazo de inscripción estará abierto hasta el viernes 17 de abril a las 12.00 horas.

MATRICULACIÓN Y PRECIOS:

La inscripción se realizará mediante este **formulario**. Además, si solicitan la bonificación de FUNDAE también deberán cumplimentar la inscripción en este formulario para recibir información y forma de abono.

https://forms.gle/kreB8TPLeEib4LU58

Si desea más información puede contactar en el siguiente email: administracion@rbcingenieros.com en el teléfono: 955 382 831.

PRECIOS DE MATRICULACIÓN:

- COLEGIADOS DESEMPLEADOS / JUBILADOS / PREJUBILADOS: **176,00 €**
- COLEGIADOS: **185,00 €**
- NO COLEGIADOS: **280,00 €**

Esta actividad de formación es **bonificable** por **FUNDAE** (antigua Fundación Tripartita) para **trabajadores por cuenta ajena**. RBC Ingenieros, como Empresa Organizadora de FUNDAE puede gestionar la bonificación. Para ello es necesario formalizar la tramitación **con 5 días hábiles** de antelación al inicio del curso**. El coste de la tramitación es de 55€, también subvencionable.**

CONTENIDO DEL CURSO

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

Al finalizar la unidad, el alumnado será capaz de identificar los principales conceptos en los sistemas de información, la clasificación de medidas de seguridad y los requisitos de seguridad de los sistemas informáticos.

Contenido:

- Introducción
- Mapa conceptual
- Conceptos de seguridad en los sistemas
- La ingeniería social
- Clasificación de las medidas de seguridad en los sistemas
  - Seguridad lógica
  - Seguridad física
- Requerimientos de seguridad en los sistemas de información
  - Principales características
    - Confidencialidad
      - ¿Qué sabe Google o Facebook de nosotros?
      - Nos vigilan
    - Integridad
    - Disponibilidad
    - Otras características
- Los “Hacker”
- ¿Y los ataques de países del Este?
- Tipos de ataques
  - Ingeniería social
  - Malware
  - Ataque de “denegación de servicio”
  - Ataques de “día cero”
  - Fallos de seguridad
- Hemos aprendido

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD

Al finalizar esta unidad, el alumnado sabrá distinguir las distintas formas de ataques que se pueden realizar. También podrá ver cómo afectan las vulnerabilidades de los programas y conocerá tecnologías de seguridad y estrategias para publicar información hacia el exterior.

Contenido:

- Concepto de ciberseguridad
- Vulnerabilidades
- OWASP
- Amenazas más frecuentes
- Ataques de fuerza bruta y diccionario
- Inyección de sentencias
- Obtención de contraseñas

.

- Tecnologías de seguridad
  - Cortafuegos
  - Seguridad en conexiones inalámbricas (WiFi)
  - IDS
  - SIEM
- Análisis forense
- Monitorización activa externa
- Copias de seguridad
- Hemos aprendido

UNIDAD DIDÁCTICA 3. SOFTWARE PELIGROSO

Al finalizar esta unidad, el alumnado será capaz de identificar las distintas categorías de software malicioso que puede dañar la información, reconocer amenazas según sus efectos o manifestación y comprender riesgos como el robo, destrucción o secuestro de datos.

Contenido:

- Conceptos sobre software dañino
- Clasificación y tipos de amenazas
  - Virus
    - Residentes
    - Macros
    - Scripts
  - Troyanos
  - Gusanos
  - Bombas lógicas
  - Spyware y keylogger
  - Adware
  - Backdoor
  - Ransomware
- Phishing
- Hoax y noticias falsas
- Mensajes SMS y llamadas falsas
- Estafas por redes sociales
- Spam
- Amenazas persistentes y avanzadas
- La mayor vulnerabilidad: nosotros
- Cómo nos protegemos
- Hemos aprendido

UNIDAD DIDÁCTICA 4. SEGURIDAD EN REDES INALÁMBRICAS (WIFI)

Al finalizar esta unidad, el alumnado sabrá identificar las partes de la configuración de una red inalámbrica, clasificar protocolos de comunicaciones y seguridad aplicados y elegir la forma más segura de conexión.

Contenido:

- El entorno inalámbrico
- Conceptos y tecnologías de redes inalámbricas

- Zonas domésticas y zonas de empresa
- Protocolos de emisión WiFi
- Protocolos de seguridad
- Canales
- SSID o identificador
- Protocolos actuales
- Ruido en la conexión
- Cómo identificar la seguridad de una red
- Configuración de seguridad del router o punto WiFi
- Portales web de identificación
- Intrusión en redes WiFi
- WiFi profesional: 802.1x
- NFC
- Hemos aprendido

UNIDAD DIDÁCTICA 5. HERRAMIENTAS DE SEGURIDAD

Al finalizar la unidad, el alumnado será capaz de distinguir las herramientas y tecnologías que ayudan a proteger equipos e instalaciones, tanto a nivel de usuario como en organizaciones, con un enfoque preventivo.

Contenido:

- Antivirus / antimalware
- Programas de protección
- Actualización del equipo y aplicaciones
- Amenazas en navegadores web
- SmartScreen
- DLP (Prevención de pérdida de datos)
- Control de acceso y permisos de usuarios
- Autentificación y contraseñas
- Doble autenticación
- Seguridad en móviles
- Puertos USB
- Control de acceso a Internet
- Hemos aprendido
- Conclusiones finales
    - Recomendaciones a nivel de usuario
    - Recomendaciones para empresas
    - En el entorno familiar

UNIDAD DIDÁCTICA 6. REGLAMENTOS Y ASPECTOS LEGALES

En esta unidad se abordarán reglamentos y aspectos legales, con situaciones reales relacionadas con la seguridad y qué hacer ante estafas en Internet.

Contenido:

- Situaciones de crisis, nuevas amenazas y teletrabajo
- Espionaje industrial
- Ingeniería social
- Teletrabajo seguro

.

  - VPN
  - Escritorio remoto
- RGPD
- Videovigilancia
- ISO 27001. Seguridad de la información
- Supuestos legales y jurisprudencia
  - Difusión de vídeos privados
  - Acceso de la empresa al correo
  - Control parental: “controlar sí, espiar no”
- Delitos asociados a acceso a WiFi
- Compras y fraude en Internet
- Qué hacer ante una estafa
- Reportar fraude
- Derecho al olvido
- Hemos aprendido

Nota: El contenido del curso está sujeto a cambios a criterio del equipo docente.

RCB INGENIERIA ARQUITECTURA Y FORMACIÓN, S.L. es miembro de la Asociación Nacional de Centros y Proveedores de E-learning (ANCYPEL)

ANCYPEL
ASOCIACIÓN NACIONAL DE CENTROS Y PROVEEDORES DE E-LEARNING
Desde 1977 al servicio de la formación