CONTENIDO DEL CURSO:

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

Objetivo:

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

Objetivo:

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

Objetivo:

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)

Objetivo:

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

Objetivo:

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

Objetivo:

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)

RECURSOS, METODOLOGÍA Y TUTORIZACIÓN

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 a implantar para garantizar que el alumno 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.

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.