



# Ciberseguridad, redes y sistemas

Programa de  
especialización  
inicial.

Este programa te proporciona  
una **comprensión profunda**  
**de los conceptos y técnicas**  
**fundamentales en sistemas y**  
**redes informáticas en línea.**

# Sobre el programa

Aprenderás **en qué consiste la ciberseguridad y los conceptos básicos sobre la tecnología, los principales peligros de internet, ciberataques, configuración y seguridad en redes**, entre otros. Tendrás una base sólida para **comprender los sistemas informáticos y cómo protegerlos**.

Además te introduciremos a la **programación y algorítmica**, lo que te servirá para comprender los fundamentos de los sistemas y aplicaciones informáticas.



**Fechas**  
Septiembre 2024



**Duración**  
600 hs



**Modalidad**  
Presencial



**Prácticas 100% aseguradas** en empresas de 1er nivel



**Becas y financiación** disponibles

**Este programa ha sido validado por las siguientes empresas de nuestro Consejo Asesor Empresarial:**



**¡SIN REQUISITOS PREVIOS!**

## Qué aprenderás

- Una base de conocimientos digitales en todos los ámbitos.
- Conocimientos de ciberseguridad que permita desarrollar soluciones seguras y adecuadas medidas de protección.
- Acciones a realizar ante un ciberataque
- Capacidad de liderazgo para tomar decisiones en situaciones complicadas.

## Este programa es para ti si...

...tengas la formación que tengas, quieres desarrollarte profesionalmente en el área de las ciberseguridad, cada vez más demandada por las empresas.

## Cómo lo aprenderás

Mediante **clases presenciales participativas, trabajo en equipo, realización de proyectos y contenido multimedia.**

Con **team building y team work**, fomentado desde el primer día de clase.

# Salidas profesionales

- **Técnico/a en Ciberseguridad junior:** tareas técnicas específicas, como monitorear la red, realizar análisis de vulnerabilidades y aplicar parches y actualizaciones de seguridad.
- **Administrador de sistemas junior:** configuración y mantenimiento de sistemas y herramientas de seguridad.
- **Analista de seguridad junior:** asiste en la identificación y análisis de problemas de seguridad y en la implementación de soluciones de seguridad.
- **Soporte técnico en seguridad de la información:** para la resolución de problemas básicos de seguridad y la implementación de medidas de seguridad.



## Por qué este programa



### **Totalmente práctico**

Contenido totalmente práctico con casos reales, enfocado a lo que pide el mercado. Retorno inversión único.



### **Salidas profesionales**

Preparación para trabajar en una profesión en alta demanda.



### **Mentoring**

Orientación profesional en soft skills y seguimiento de la asimilación del programa.



# Módulos del programa

## 1. Introducción a la Ciberseguridad

- T-1: Introducción: principales peligros de internet.
- T-2: Antivirus. Comparativa antivirus AV-Test. Windows Defender. Malware bytes. Virus Total e Hybrid Analysis.
- T-3: Contraseñas. Importancia. Leaks. Hashes. Ataques diccionario. Crackeo de contraseñas. KeePass. Gestores de contraseñas.
- T-4: Anonimato en internet. Anonimato en internet. Emails temporales. Tutanota y Protonmail. HTTP/HTTPS (SSL/TLS). Thispersondoesnotexist.
- T-5: Navegadores y proyecto ToR. Navegadores y proyecto ToR. Chrome. Duckduckgo. Brave. Opera. Onion Routing. ToR y HTTPS.
- T-6: Ciberataques. APTs. Phishing. Man in the middle. Ransomware. Spyware. Botnet. DoS y DDoS. Ataques de inyección (SQLi y XSS). Seguridad en RRSS.

## 2. Redes informáticas

- T-1: Introducción a las redes informáticas. Definición de red informática. Tipos de redes informáticas. Componentes de una red informática.
- T-2: Modelo OSI y TCP/IP. Funciones de las capas del modelo OSI. Introducción al modelo TCP/IP. Relación entre el modelo OSI y TCP/IP.
- T-3: Ethernet y topologías de red. Tipos de cableado de red. Tipos de conectores. Topologías de red (bus, estrella, anillo, malla).
- T-4: Protocolos de red. Protocolos de comunicación de datos. Protocolos de transporte. Protocolos de aplicación. El protocolo Spanning Tree.
- T-5: Direcciones IP y subredes. Introducción a las direcciones IP. Tipos de direcciones IP (IPv4, IPv6). Subredes y máscaras de red.
- T-6: Configuración de redes. Configuración de dispositivos de red (routers, switches). La conmutación de capa 2. Configuración de servidores y clientes. Configuración de protocolos de red. VLAN.
- T-7: Seguridad en redes. Amenazas y vulnerabilidades de red. Métodos de autenticación y autorización. Técnicas de seguridad de red (firewalls, VPN, IDS/IPS).
- T-8: Servicios de red. Servicios de red comunes (DNS, DHCP, FTP, HTTP, SMTP). Configuración de servicios de red.

## 3. Programación y fundamentos de algorítmica

- T-1: Estructuras de control.
- T-2: Programación Modular o Estructurada.
- T-3 Archivos.
- T-4: Introducción a la POO.
- T-5: POO.
- T-6. Principales lenguajes de programación.



#### 4. Sistemas operativos y terminales

- T-1: Introducción.
- T-2: Seguridad y gestión de recursos.
- T-3: Windows
- T-4: LINUX.
- T-5: SO de servidores.
- T-6. Virtualización.

#### 5. Principios básicos de Ciberseguridad

- T-1: Metadatos. Foca. Exiftool. Metagoofil
- T-2: Información básica y geolocalización. GeolIPTool. Georecon. Whois. Información empresarial.
- T-3 Herramientas básicas y plugins. Osint-Spy. TheHarvester. Maltego. Final- Recon. Flightradar. Ghunt. Wpscan. Huron – Spiderfoot. Wayback Machine. IPinfo. Wappalyzer. Blackbird. Instantusername.
- T-4: Hacking y filtración de datos RSS. Dorks. Shodan. Webcamhopper y Skylinewebcams. Haveibeenpwned. Phonia. – Motores de búsqueda. imágenes en google y bing (Ingeniería inversa).

#### 6. Ingeniería social

- T-1: Introducción. ¿Qué es la Ingeniería social? Personajes reseñables. Tipos de ataques
- T-2: Técnicas de suplantación. Suplantación de identidad. Phishing. Vishing. Spoofing mail. Smishing. Spear fishing
- T-3: Otros ataques. Trashing. Baiting. Qrishing. Pharming. Fraude del CEO. Estafa nigeriana. Fraudes
- T-4: Gophish. ¿Qué es Gophish? Instalación y acceso. Campaña de envío de correos. Lanzamiento de campaña
- T-5: Herramientas de Ingeniería Social. Zphisher. Ngrok. BlackPhish. Hiddeneye. Evilurl. Modificación de links
- T-6: SET. SET 1345. Mass Mailer Attack. SET QRishing. SET Arduino. Powershell Attack Vectors. Website Attack Vectors
- T-7: Psicología. Elicitación. Técnicas de manipulación. Detección de mentiras. Operaciones Psicológicas. Programación neurolingüística. Psicología social
- T-8: Contramedidas y mitigaciones.. Sentido común. Prevención y respuesta Test de phishing

**Con esas bases estarías listo para profundizar ya sea en Red o Blue Team, pentesting, en computación forense, en hardening, análisis de malware, entre otras rutas.**

# Sobre IMPELIA.

Somos un **Campus Profesional de Especialización Tecnológica**. Formamos a los **perfiles profesionales que las empresas nos piden**. Trabajamos con ellas en la definición de nuestros programas, para asegurar que responden a lo que el mercado pide, tanto en las **capacidades hard** (técnicas) como **soft** (interpersonales), creando una **formación real**, la que de verdad se necesita.



IA & Data Science



Ciberseguridad



Industria 4.0

## ¿Con qué empresas validamos los programas?

Forman parte de nuestro Consejo Asesor Empresarial un grupo de empresas con las que trabajamos de manera activa para reducir la brecha competencial. **Nos mueve que tu trabajo sea el que sueñas y que las empresas encuentren el profesional que esperan.**

MANGO

Nestlé



Agbar

FLUIDRA

cellnex  
foundation



matholding



BASF  
The Chemical Company

Schneider  
Electric

CEMENTOS  
MOLINS

verfen

FICOSA

## Qué nos diferencia.

**Primero de todo, ellas.** La relación activa con las empresas crea una formación real y flexible, con empleabilidad alta. ¿Y qué más?:



**Metodología propia para las soft skills:**  
las trabajamos y certificamos.



**Mentor personal.**  
Te acompaña y se asegura de que aprendas bien.



**Life long learning.**  
Aquí siempre encontrarás formación adaptada a tu etapa profesional.



**Método activo.**  
Aprende haciendo. Totalmente práctico.



## Formación **adaptada a ti.** Tanto si sabes mucho como si no tienes todavía conocimientos.

### PEI - Programas Especialización Inicial

Si **no tienes experiencia o conocimientos** previos, empieza desde la base.

*¡Ya eres un profesional del campo! Sigue formándote o/y empieza a trabajar.*

### PEA - Programas Especialización Avanzada

Si eres profesional **con experiencia o conocimientos** previos en el área de formación.

*¡Eres un especialista! Solo te faltará reciclarte de vez en cuando.*

### Bootcamps de especialización

Programas intensivos para profesionales que quieren reciclarse o actualizarse.

Carrera profesional



## ¿Cómo te podemos **ayudar?**

Para PEI y PEA

Becas

**IMPELIA**  
CAMPUS PROFESIONAL

Financiación

 **Bcas**

No pagues hasta  
que trabajes (ISA)

**tokey**

Pregúntanos :)

Para PEI, PEA y Bootcamps

Para empresas: bonifica el curso



**Fundación Estatal**  
PARA LA FORMACIÓN EN EL EMPLEO



931 94 16 91  
[www.impelia.org](http://www.impelia.org)