proconsi

experience+

Talento e Inserción Laboral para Jóvenes de Castilla y León

Ciberseguridad

PROCONSI.COM

fgulem | NOS IMPULSA | Ecyl | Junta de Castilla y León

Introducción

La Junta de Castilla y León, a través de la Consejería de Industria, Comercio y Empleo y las cuatro universidades públicas de la Comunidad, ha firmado su compromiso para el desarrollo del programa **Experience Plus, un proyecto estratégico que nace para intensificar la colaboración universidad-empresas a la hora impulsar la inserción laboral cualificada de los jóvenes recién titulados, favorecer la captación del talento y mejorar la competitividad de las empresas.**

Itinerario en Ciberseguridad Proconsi Experience Plus

CARACTERÍSTICAS

- Plazas ofertadas: 12.
- Duración total de itinerario: 800h.
- Horario: Jornada completa de lunes a viernes (40h semanales).
- Lunes a jueves 8:00-15:00 y 16:00-17:30h. Viernes 8:00-14:00h.
- Calendario: del 19 de enero al 11 de junio de 2026.
- Programa dual en 3 fases:
- Fase 1:

  Del 19 de enero al 27 de marzo 2026.
  Jornada semanal: 15h teóricas + 25h prácticas.
  Módulos: 1, 2, 3 y 4.
- Fase 2:

  Del 30 de marzo 14 de mayo 2026.
  Jornada semanal:10h teóricas+30h prácticas.
  Módulo: 5.
- Fase 3:

  Del 15 de mayo al 11 de junio 2026.
  Jornada semanal: 5h teóricas+35 horas prácticas.
  Módulos 5 y 6.

- Lugar de realización: SOC Proconsi, Ctra. De Santander km 5,5 Villarrodrigo de las Regueras, León.

CARACTERÍSTICAS

- Certificado de aprovechamiento de la formación recibida y las prácticas realizadas.

- Bolsa económica mensual desde el inicio del itinerario.

- El importe de la bolsa será proporcional al número de horas de prácticas realizadas.
  - Titulados universitarios: Máximo de 1.500,00€ brutos mensuales para una jornada completa de prácticas (40h/semanales).
  - Titulados FP: Máximo de 800,00€ brutos mensuales para una jornada completa de prácticas (40h/semanales).

- Contrato laboral para al menos el 50% de los participantes que finalicen con éxito el itinerario.

- Plazo de inscripción hasta el 8 de diciembre de 2025.

Itinerario en Ciberseguridad Proconsi Experience Plus

REQUISITOS PARTICIPANTES

• Residir en Castilla y León.

•Haber obtenido una Titulación Universitaria (Grado, Máster, Doctorado o Título Propio), o de Formación Profesional obtenida con posterioridad al 1 de septiembre de 2021 de alguna de estas titulaciones:

- Grado en Ingeniería Informática
- Grado en Ingeniería de Datos e IA
- Máster universitario en investigación en Ciberseguridad
- Grado Superior de Formación Profesional en Administración de Sistemas Informáticos en Red
- Grado Medio de Formación Profesional en Sistemas Microinformáticos y Redes

• No haber realizado prácticas formativas relacionadas con la titulación que accede al programa más de 184 días.

REQUISITOS PARTICIPANTES

• No haber trabajado por cuenta propia o ajena, acorde a la titulación con la que accede al Programa, durante un periodo superior a 184 días.

• Estar inscrito como demandante de empleo en el Servicio Público de Empleo de Castilla y León en situación laboral de “desempleado” y situación administrativa de “alta”.

• Permiso de conducir B1

• Inglés: Comprensión lectora.

• Plazo de inscripción hasta el 8 de diciembre de 2025.

Itinerario en Ciberseguridad Proconsi Experience Plus

¿POR QUÉ PARTICIPAR?

Recibirás formación técnica especializada que completa tu formación académica.

Realizarás prácticas no laborales en empresa con una ayuda económica mensual.

Recibirás asesoramiento individualizado durante el itinerario formativo.

Recibirás formación técnica y en competencias clave para mejorar tu empleabilidad.

Podrás poner en práctica los conocimientos adquiridos en un entorno empresarial real que mejorará tu CV.

Al finalizar el itinerario, posibilidad de recibir una oferta laboral para incorporarte a la empresa con un contrato laboral.

Formación especializada

El programa contempla, como novedad, el desarrollo de proyectos de formación especializada vinculada a la empresa que complementa **una experiencia práctica en las empresas participantes con itinerarios específicamente adaptados y diseñados para dar respuesta a sus necesidades productivas.**

Las 800 horas de formación, 230 horas de teoría y 570 horas de práctica se acreditarán mediante certificado de asistencia firmado por Proconsi y FGULEM.

Inserción laboral

Para los jóvenes titulados, **'Experience Plus' representa una oportunidad para su inserción laboral estable y desarrollo profesional en las empresas de Castilla y León**, fomentando, así, su arraigo en el territorio y evitando la fuga de talento. El programa les ofrece una oportunidad real de acceder a un entorno laboral estable con oportunidades de crecimiento.

Paralelamente, garantiza una mejor cualificación y una primera experiencia profesional en contacto directo con las empresas, mejorando su empleabilidad a través de un entrenamiento práctico e intensivo vinculado al desarrollo productivo en un entorno empresarial.

Los tutores y docentes cuentan con una amplia experiencia profesional y lectiva en el sector, lo que garantiza la calidad de la formación impartida.

Talento joven

El objetivo principal es impulsar la inserción laboral cualificada de jóvenes recién titulados, tanto universitarios como de formación profesional, en empresas de sectores estratégicos y áreas tecnológicas avanzadas de la comunidad. En este sentido, cabe destacar, que además de la alta cualificación que reciben los jóvenes participantes, otro aspecto fundamental y diferenciador del programa es el compromiso de contratación de, al menos, el 50 % de los participantes en las empresas, lo que garantiza una inserción laboral estable y de calidad.

Proconsi

Proconsi es un líder tecnológico que se encuentra en pleno proceso de expansión. Con un crecimiento anual sostenido en los últimos años y un incremento continuo en Investigación, Desarrollo e Innovación en Europa, África y Latinoamérica.

Somos una empresa de Tecnologías de la Información y la Comunicación especializada en el desarrollo e integración de soluciones informáticas para todo tipo de empresas. Más de tres décadas de experiencia avalan a una compañía tan flexible como responsable. Cuenta con un equipo multidisciplinar de más de 140 profesionales cualificados.

Proconsi es especialista en ciberseguridad, creación y desarrollo de software de gestión, consultoría tecnológica, dirección y gestión de proyectos I+D+i basados en TIC, soporte técnico, aplicaciones móviles, inteligencia artificial, robótica, visión artificial, machine learning y cloud computing.

Más de 5.500 clientes en el ámbito nacional e internacional garantizan la sólida experiencia de una empresa innovadora, acreedora de prestigiosos galardones y certificados de calidad, además de ser socialmente responsable.

Primer SOC para PYMEs

En el año 2017, Proconsi presentó el primer SOC para PYMEs de España, hasta entonces, este tipo de prevención estaba reservada a grandes corporaciones.

En el año 2024, Proconsi reforzó su posición como referente en innovación tecnológica y protección digital con la inauguración de su nuevo Centro de Operaciones de Seguridad (SOC), un espacio de 750 metros cuadrados, con más de 50 profesionales, equipado con la más avanzada tecnología para la vigilancia y defensa frente a amenazas cibernéticas. Esta instalación representó un paso decisivo en la expansión de sus servicios y en la consolidación de un ecosistema digital más seguro y resiliente, especialmente orientado a las pequeñas y medianas empresas (PYMEs).

Ciberseguridad

SERVICIOS DE CIBERSEGURIDAD DE PROCONSI:

- Auditorías de seguridad
- Pentesting y análisis de vulnerabilidades web
- Consultoría ENS y 27001 (implantación de un SGSI)
- Seguridad 24/7
- Servicio SIEM
- Análisis forense digital en Windows, Linux y redes
- Simulacros de phishing
- Formación y concienciación para empleados

COLABORACIONES CON PARTNERS:

•WATCHGUARD: Protección Endpoint (EPDR), Gestión de Parches, Seguridad Perimetral, Autenticación Multifactor (MFA)
•AREXDATA: Plataforma de seguridad del dato y tracking de rendimiento
•ACRONIS: BackUp y Disaster Recovery
•WALLIX: Gestión de acceso privilegiado (PAM)
•SYNETO: Infraestructura para gestión del dato, resiliencia y seguridad

La Formación como base de la Innovación

En Proconsi apostamos por el talento y el aprendizaje continuo como motores de innovación. Por ello, desarrollamos una amplia oferta de planes formativos y programas de prácticas dirigidos a estudiantes, recién titulados y profesionales que desean impulsar su carrera en el ámbito de la tecnología.

Nuestros programas se estructuran en dos ejes principales:

- **Formación práctica y personalizada**: Los participantes se incorporan a proyectos reales en áreas como desarrollo de software, ciberseguridad, sistemas, consultoría tecnológica o gestión de proyectos, contando con el acompañamiento de tutores especializados.

- **Itinerarios formativos adaptados**: Ofrecemos planes diseñados para reforzar competencias técnicas, metodológicas y transversales, combinando sesiones teóricas, talleres prácticos y aprendizaje colaborativo.

El objetivo es doble: facilitar la integración de los jóvenes talentos en el mercado laboral y, al mismo tiempo, promover la actualización constante de los conocimientos de quienes ya forman parte de nuestro equipo.

Ciberseguridad

Introducción a la Ciberseguridad (5h)

- Conceptos básicos: amenaza, vulnerabilidad, riesgo, impacto.
- Principios de seguridad: confidencialidad, integridad, disponibilidad, trazabilidad.
- Normativa y marcos de referencia (ISO 27001, ENS, NIST/2 CSF, PCI-DSS).
- Tipos de atacantes y motivaciones.
- Ciclo de vida de un ataque: kill chain, MITRE ATT&CK.

Hardening (20h)

Hardening de sistemas operativos

Windows
- Configuración segura inicial: políticas de contraseñas, UAC, BitLocker.
- Auditoría y logging (Event Viewer, Sysmon).
- Control de aplicaciones: AppLocker, WDAC.
- Actualizaciones y gestión de parches.

Linux
- Gestión de usuarios y permisos (sudo, PAM, SSH).
- Seguridad en procesos y servicios.
- Logs y auditoría (/var/log, journald, auditd).
- SELinux/AppArmor.
- Automatización de hardening (Lynis, OpenSCAP).

Hardening de servicios de red
- Copias de seguridad
- Estrategia 3-2-1 y backups offline.
- Cifrado y verificación de integridad.
- Pruebas periódicas de restauración.

Firewall
- Concepto de whitelisting vs blacklisting.
- Configuración de firewalls perimetrales (iptables, nftables, Windows Defender Firewall).
- Firewalls de nueva generación (NGFW).
- Segmentación de red y VLANs.

Hardening (20h)

EDR
- Diferencias: AV tradicional vs EDR/XDR.
- Funciones clave: detección de comportamiento, respuesta automatizada, IOC.
- Ejemplos prácticos: Ej. Microsoft Defender.

DNS
- DNS como vector de ataque (spoofing, tunneling).
- DNS seguro: DNSSEC, DoH/DoT.
- Filtrado de dominios maliciosos.
- Práctica: configuración segura de BIND/Unbound.

Web
- Hardening de servidores web (Apache, Nginx, IIS).
- TLS: certificados, versiones seguras, HSTS.
- Cabeceras de seguridad HTTP (CSP, X-Frame-Options, etc.).
- Protección contra DoS básico.

Correo electrónico
- Protocolos: SMTP, IMAP, POP3: riesgos y mitigaciones.
- Autenticación de correo: SPF, DKIM, DMARC.
- Filtros antispam y anti-phishing.
- Cifrado de correo (TLS, PGP, S/MIME).
- Análisis de cabeceras de correo

Respuesta ante incidentes (55h)

Introducción y marco conceptual

- Definición de incidente, evento y alerta
- Ciclo de vida de la respuesta ante incidentes
- Concepto y funciones de un SOC y un CSIRT

Preparación

- Plan de respuesta ante incidentes (IRP)
- Inventario de activos críticos y clasificación de la información
- Herramientas del SOC: SIEM, EDR/XDR, IDS/IPS, SOAR
- Playbooks de respuesta y casos de uso de detección

Operativa en un SOC

- Modelos de SOC: interno, externo, híbrido, MSSP
- Roles y niveles: analistas N1, N2, N3, Threat Hunter, Forense
- Flujos de trabajo: detección, escalado, análisis, cierre
- Gestión de tickets e integración con ITSM (Servicenow, TheHive)
- Coordinación con CERT/CSIRT nacionales e internacionales

Identificación y detección

- Fuentes de alertas: SIEM, EDR, IDS/IPS, usuarios
- Indicadores de compromiso e indicadores de ataque
- Uso de threat Intelligence (MISP, feeds de IoCs)
- Herramientas de análisis: Suricata, Zeek, Yara, OSQuery

Respuesta ante incidentes (55h)

Contención, Erradicación y Recuperación
- Estrategias de contención de red, endpoint y cloud
- Erradicación de malware y eliminación de persistencia
- Restauración segura de sistemas y datos
- Monitorización reforzada post-incidente

Análisis Forense

Windows
- Adquisición de evidencias
- Análisis de artefactos
- Persistencia y escalada de privilegios
- Herramientas: Volatility, FTK Imager, nirsoft, systinternals

Linux
- Adquisición de evidencias
- Análisis de logs
- Procesos, conexiones y rootkits
- Herramientas: Autopsy, chrootkit

Redes
- Captura y análisis de tráfico
- Detección de exfiltración de datos
- Reconstrucción de sesiones HTTP, DNS, SMTP

Análisis de Malware
- Análisis estático
- Análisis dinámico
- Análisis de comportamiento de red
- Ingeniería inversa básica
- Persistencia, evasión y ofuscación
- Firmas y reglas

Respuesta ante incidentes (55h)

Informe y Mejora continua
- Redacción de informe técnico y ejecutivo
- KPIs en IR: MTTD MTTR, nº de incidentes por tipología
- Actualización de playbooks tras el incidente
- Post-mortem y cultura de ciberseguridad

Pentest de Sistemas, perimetral, WiFi y Web (70h)

Introducción
- ¿Qué es un pentest? objetivos, alcance y límites.
- Diferencia entre pentest, red team, purple team y auditoría de seguridad.
- Ética, legalidad y autorización (scope, Rules of Engagement, get-out clauses).
- Tipologías de pruebas: caja blanca / gris / negra; pruebas internas vs externas.

Preparación y Gobernanza
- Definición del alcance y activos críticos.
- Acuerdos legales: contrato, autorización por escrito, horarios, comunicaciones de emergencia.
- Metodología y framework: OSSTMM, PTES, OWASP
- Gestión de riesgos durante el test (impacto en producción, backups, POC safe).
- Herramientas de gestión de pruebas y evidencias (tickets, repositorios, captura de resultados).

Pentest de Sistemas, perimetral, WiFi y Web (70h)

Metodología común al pentest

- Fases del pentest: reconocimiento, enumeración, explotación, post-explotación, pivoting, limpieza, reporting.
- Recolección de información: pasiva y activa.
- Automatización vs análisis manual: cuándo usar cada uno.
- Bullding de playbooks y reutilización de técnicas/artefactos.
- Control de evidencias y reproducibilidad (logs, capturas, timestamps).

Pentest a Sistemas Windows y Linux

- Reconocimiento: mapeo de servicios, escaneo de puertos y versiones (nmap, masscan).
- Enumeración detallada: shares, users, servicios, horarios, cron, SUDOers.
- Explotación local y remota: vulnerabilidades conocidas (CVE), explotación de servicios, RCE, LPE.
- Post-explotación: recolección de credenciales, lateral movement (Pass-the-Hash, SSH keys), exfiltración controlada, limpieza.
- Hardening checks: políticas de contraseñas, actualizaciones, configuraciones de servicios.
- Herramientas: Metasploit, Empire, NetExec, BloodHound, Mimikatz, Responder, LinEnum, PowerUp/PowerSploit.

Pentest de Sistemas, perimetral, WiFi y Web (70h)

Seguridad perimetral

- Reconocimiento externo: subdominios, DNS, OSINT, fingerprinting de dispositivos (Shodan, crt.sh, dnsenum).
- Scanning a perímetro: puertos, servicios, banners, fingerprinting de FW/IDS (nmap + scripts, taniwha-esque techniques).
- Testing de firewalls y ACLs: bypasses, NAT traversal, fragmented packets, tunneling.
- VPNs y acceso remoto: bruteforce/credentials stuffing, split tunneling, MisConfigurations.
- IDS/IPS evasion basics (fragmentation, obfuscation) — ética y límites.
- Testing de appliances (load balancers, proxies, proxies inversos).
- Herramientas: nmap NSE, masscan, nikto, curl, sslyze, hydra, hping3, burp (extensions de red).

Pentest WiFi

- Fundamentos: modos (AP/Infrastructure, Ad-hoc), estándares (WEP/WPA/WPA2/WPA3), EAP types.
- Reconocimiento: identificación de SSID, BSSIDs, canales, capacidades (aireplay, airodump).
- Ataques a capa de enlace: WEP cracking, WPA/WPA2 handshake capture + offline cracking, PMKID attack.
- Ataques a clientes: Evil-Twin, rogue AP, Karma, MITM, ARP spoofing, captive portals.

Pentest de Sistemas, perimetral, WiFi y Web (70h)

- Ataques de autenticación empresarial (EAP-PEAP, EAP-TTLS) y targeting of misconfigured 802.1X.
- Auditoría de segmentación: acceso entre VLANs, client isolation bypass.
- Herramientas: aircrack-ng suite, hcxdumptool + hcxtools, wifite, hostapd-wpe, bettercap, Wireshark, cowpatty, hashcat.
- Seguridad operacional: uso de adaptadores, antenas, legalidad y alcance/permissions.

Pentest Web

- Reconocimiento web: descubrimiento de subdominios, endpoints, fingerprinting, y mapeo de URLs (ffuf, dirbuster).
- Análisis de top 10 OWASP: Injection, Auth flaws, XSS, CSRF, Insecure Deserialization, Broken Access Control, Security Misconfigurations, etc.
- Testing de APIs: autenticación, authorización, rate limits, input validation, abuse cases.
- Automatización y fuzzing: Burp Suite (Scanner, Intruder, Repeater), OWASP ZAP, SQLMap, wfuzz.
- Business logic flaws y chained vulnerabilities.
- Testing de autenticación multifactor, SSO, JWT and token handling.
- Deserialización y RCE en frameworks (Java, PHP, .NET, Node).
- Generación de payloads y explotación segura (no destructive).

	• Output: PoC reproducible, captura de request/response. • Herramientas: Burp Suite Pro/Community, Burp extensions, sqlmap, nmap, ffuf, Nikto, Metasploit web modules, OWASP ZAP, Postman.
Pentest de Sistemas, perimetral, WiFi y Web (70h)	Informe y mitigaciones • Estructura del informe técnico y ejecutivo (impacto, reproducciones, PoC, mitigaciones prioritarias). • Priorización de hallazgos: riesgo, explotabilidad, impacto empresarial. • Recomendaciones técnicas (fixes, configuraciones, parches) y estratégicas (compensating controls). • Revisión post-fix y pruebas de verificación (re-test).
Instalación de laboratorio y fundamentos teóricos para las prácticas (60 h)	
Formación básica en la empresa (20 h)	• Prevención de Riesgos Laborales, Sensibilización en Igualdad de Oportunidades y Sensibilización en Violencia Laboral.
Práctica en empresa (570 h)	• Configuración de dispositivos UTM con distintos niveles de protección • Configuración y securización de sistemas operativos y servicios de red (DNS, Web, Correo electrónico • Implementación de planes de recuperación ante desastres • Análisis forense sobre estaciones de trabajo y entornos de red • Realización de análisis de vulnerabilidades • Realización de pentest

Proconsi S.L.
Parque Tecnológico de León,
C/ Andrés Suárez 5, 24009.
León (España).

+34 **902 214 010** / **987 281 906**
info@proconsi.com
proconsi.com

proconsi

fgulem | NOS IMPULSA | ecyl | Junta de Castilla y León