



© 2026 CS³ Group – Todos los derechos reservados

16 de enero de 2026 | Master UA · Alicante (España)

El cuento de la lechera en una escalera...

Tipo de documento: Presentación

Autor del documento: CS³ Group (Pedro C. aka s4ur0n)

Código del Documento: GRC.pdf

Versión: 1.0

Categoría: PÚBLICO

Fecha de elaboración: 10/01/2026

Nº de Páginas: 105



Universitat d'Alacant

Whoami

```
class PedroC:
```

```
    def __init__(self):
```

```
        self.name = 'Pedro Candel'
```

```
        self.email = 's4ur0n@s4ur0n.com'
```

```
        self.web = 'https://www.s4ur0n.com'
```

```
        self.nick = '@NN2ed_s4ur0n'
```

```
        self.company = 'CS3 Group'
```

```
        self.webcorp = 'https://cs3group.com'
```

```
        self.role = 'Security Researcher'
```

```
        self.work = [ 'Reversing', 'Malware', 'Offensive Security', '...' ]
```

```
        self.groups = [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```



Universitat d'Alacant
Universidad de Alicante

CS³ Group (<https://cs3group.com>)

Formación en Seguridad

Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Ingeniería Inversa

Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Hardware Hacking

Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Forense

Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

SIGINT

Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

ATM

Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

Hacking Ético

Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Exploiting

Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Seguridad en dispositivos móviles

Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

DevSecOps

Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

T.S.C.M.

Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

PoS/TPV

Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

Análisis de Malware

Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Desarrollo Seguro

Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Respuesta ante incidentes

Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Intelligence

Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

Telecom

Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

LOPD/GPDR/Cumplimiento

LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

Contenido

- **Módulo I**
 - El cuento de la lechera en una escalera (2 h.)
- **Módulo II**
 - Ejercicio práctico (1:30 h.)
- **Conclusiones**

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

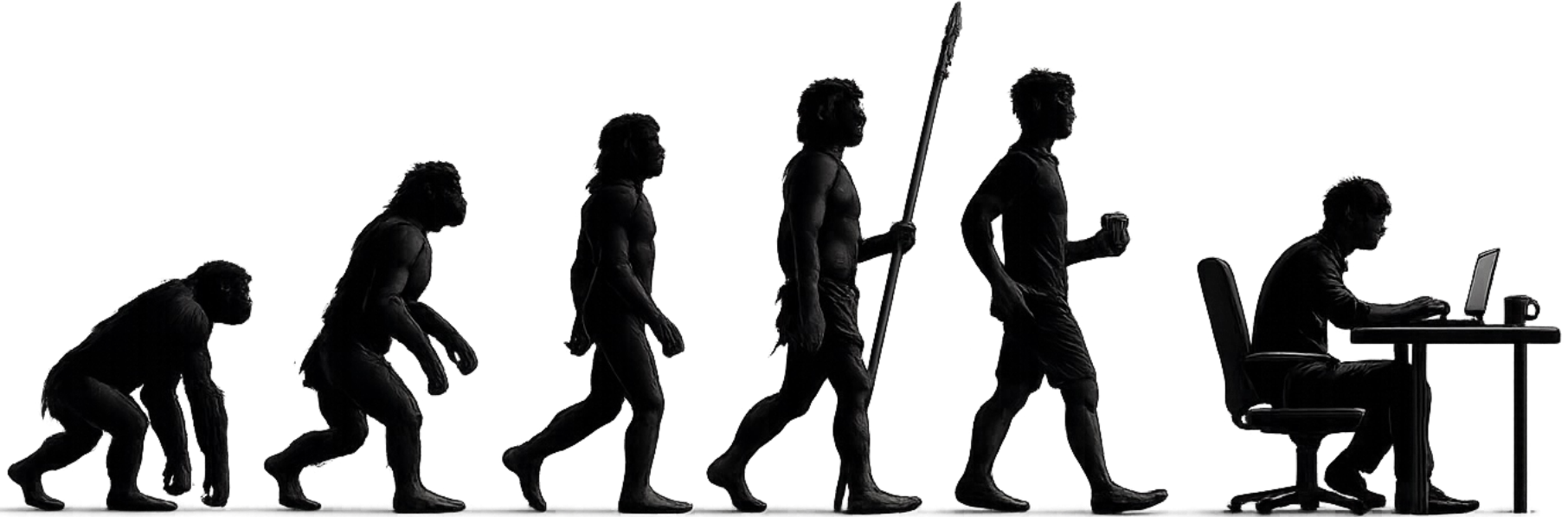
Ciberseguridad 360

Evolución

Evolución



Evolución



Evolución

Análisis y diagnóstico del talento de ciberseguridad en España (Marzo 2022)



Source:

<https://www.observaciber.es/sites/observaciber/files/media/documents/EstudioDiagnosticoTalento2022.pdf>

Evolución

¿Cómo ha adquirido los conocimientos y competencias en seguridad?



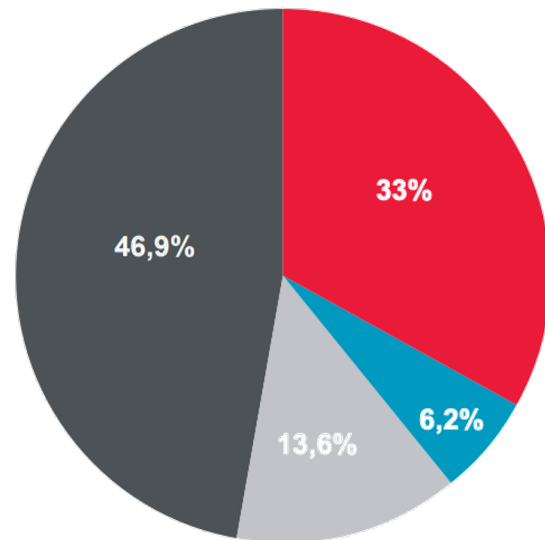
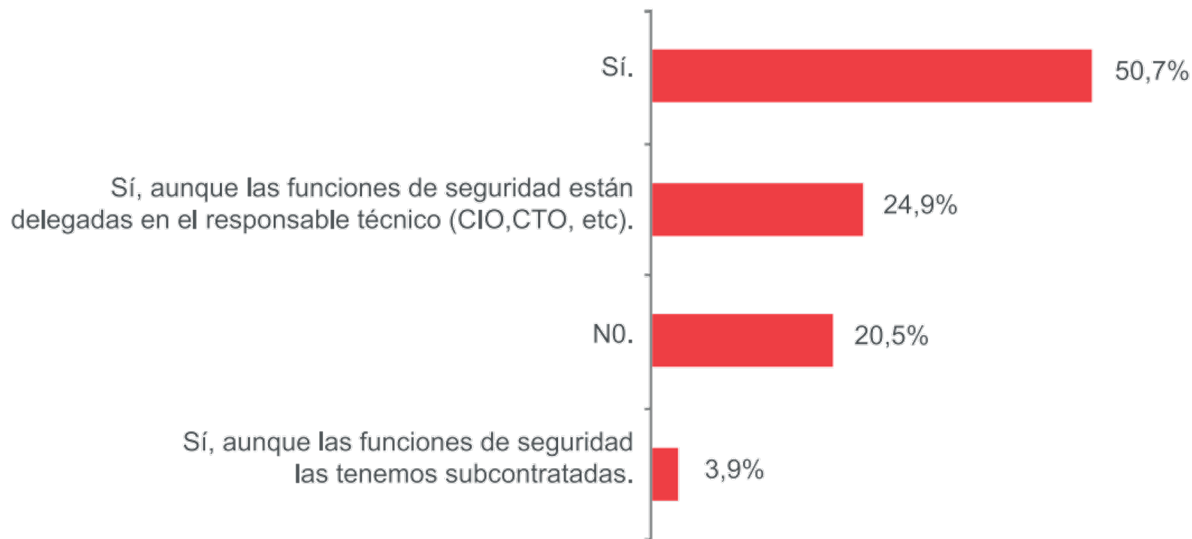
Evolución

Opciones preferidas para desarrollar competencias y conocimientos de manera autodidacta



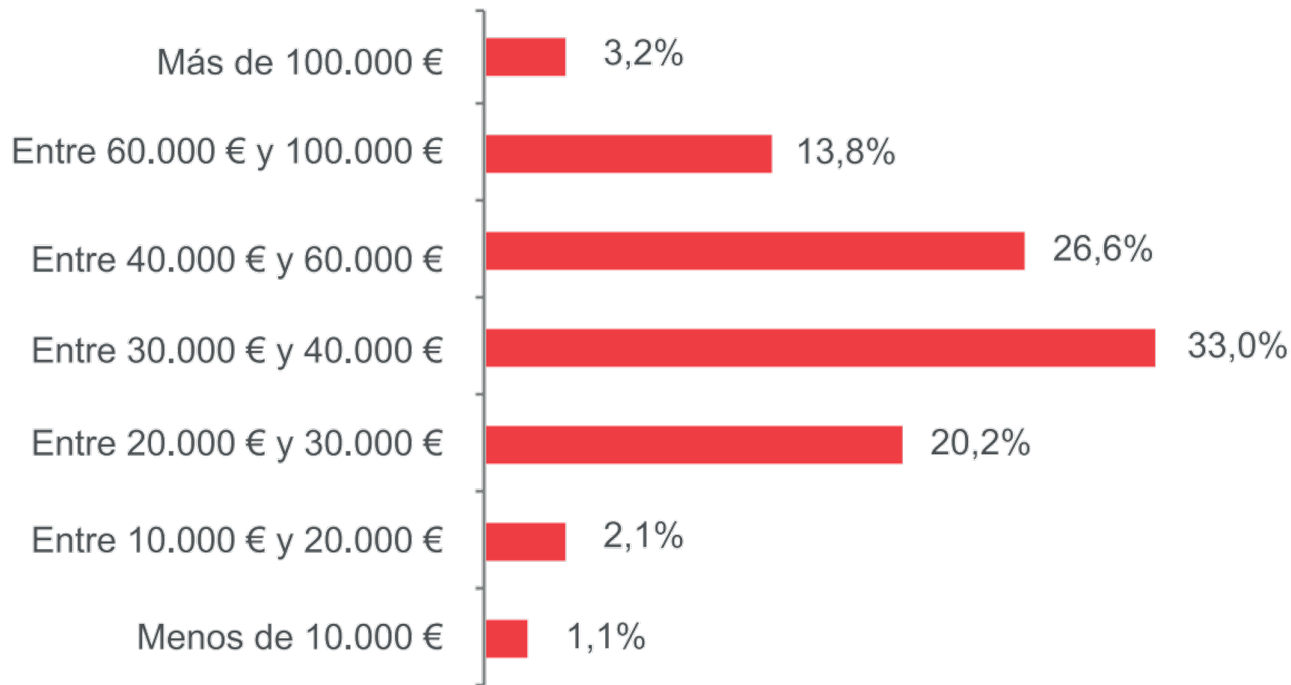
Evolución

Existencia de departamentos de seguridad en las organizaciones

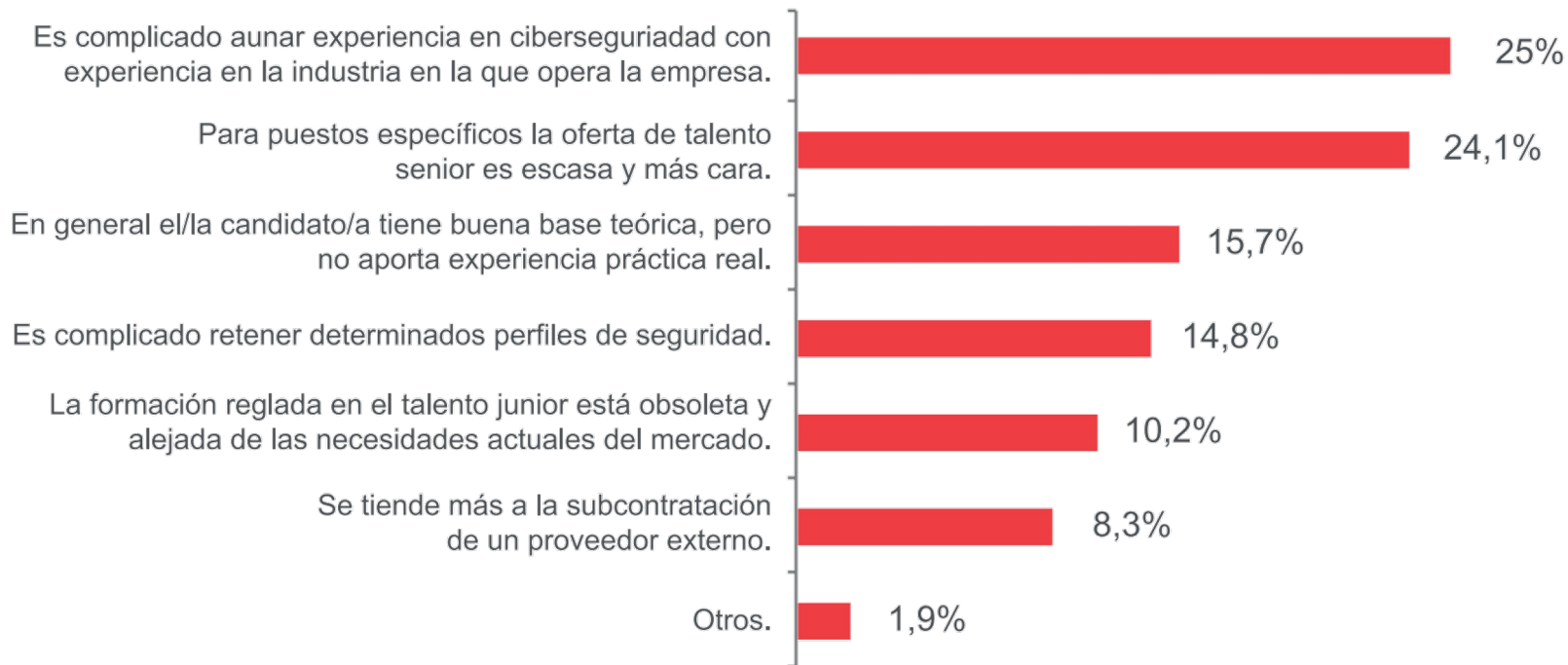


Evolución

Escala salarial en la que se distribuye la muestra consultada



Principales barreras encontradas en el proceso de recruiting



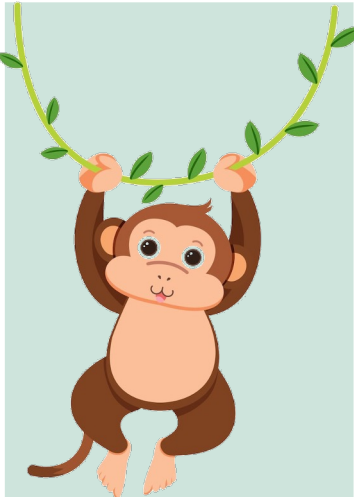
Evolución

¿Un nuevo “big bang”?

CS³ SECURITY SERVICES
<https://cs3group.com>



Evolución

Puesto	Trabajo	Salario	Resultados	Wanna be
		Base:  Extras: 		 HACKER!!!

Evolución



UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

Perfiles y posiciones

Perfiles y posiciones

ENISA - European Cybersecurity Skills Framework (ECSF) (2022)



Chief Information
Security Officer (CISO)



Cyber Incident
Responder



Cyber Legal, Policy and
Compliance Officer



Cybersecurity Risk
Manager



Digital Forensics
Investigator



Penetration
Tester



Cybersecurity
Educator



Cybersecurity
Implementer



Cybersecurity
Researcher



Cyber Threat
Intelligence Specialist



Cybersecurity
Architect



Cybersecurity
Auditor

Source:

<https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf>



Perfiles y posiciones

Digital Forensics

- Threat Hunter (Threat/Warning Analyst)
- Digital Forensic (Cyber Defense Forensics Analyst)
- Malware Analyst
- Cyber Defense Incident Responder/Law Enforcement Counterintelligence Forensics Analyst
- Media Exploitation Analyst (Cyber Crime Investigator)

Perfiles y posiciones

Cyber Defense

- Blue Teamer – All-Around Defender (Cyber Defense Analyst)
- Security Architect (NICE) and Engineer
- Cybersecurity Analyst/Engineer (Systems Security Analyst)
- OSINT Investigator/Analyst
- Intrusion Detection/SOC Analyst (Cyber Defense Analyst)

Perfiles y posiciones

Cloud Security

- Cloud Security Analyst
- DevSecOps Engineer (Information Systems Security Developer)

Perfiles y posiciones

Industrial Control Systems

- ICS/OT Security Assessment Consultant (ICS/SCADA Security Engineer)

Perfiles y posiciones

Offensive Operations

- Red Teamer (Adversary Emulation Specialist)
- Vulnerability Researcher & Exploit Developer (Vulnerability Assessment Analyst)
- Application Pen Tester (Secure Software Accessor)

Perfiles y posiciones

Purple Team

- Purple Teamer

Perfiles y posiciones

Cybersecurity Leadership

- Chief Information Security Officer (CISO) (Executive Cyber Leadership)
- Technical Director (Information Systems Security Manager)
- Security Awareness Officer (Security Awareness & Communications Manager)

Perfiles y posiciones

2025

Application

- Application Security Specialist
- DevSecOps
- Security Code Auditor
- Security Software Developer



Architecture

- Cyber Security Architect
- Enterprise Security Architect
- Senior Security Architect



Audit

- Security Auditor



Investigation

- Cyber Crime Analyst
- Cyber Crime Investigator
- Cyber Security Researcher
- Incident & Intrusion Analyst
- Malware Analyst
- Senior Malware Analyst



Networking

- Network Security
- Network Security Engineer & Administrator
- Senior Network Security Engineer



Perfiles y posiciones

Cloud

- Cloud Security Architect
- Cloud Security Engineer
- Senior Cloud Security Architect
- Senior Cloud Security Engineer



Compliance

- Cyber Security Compliance Manager
- Cyber Security Compliance Officer



Education

- Cyber Security Lecturer
- Cyber Security Professor
- Cyber Security Awareness Trainer
- Cyber Security Educator



Offensive

- Junior Penetration Tester
- Penetration Tester
- Team Lead Penetration Tester
- Vulnerability Tester



Operations

- Cyber Security Administrator
- Cyber Security Analyst
- Senior Security Administrator
- Senior Security Analyst
- Senior SOC Analyst
- SOC Analyst



Privacy

- Data Protection Officer
- Privacy Analyst



Perfiles y posiciones

2025

Engineering



- Cryptographer
- Security Engineer

Generalist



- Cyber Security Consultant
- Cyber Security Specialist
- Senior Security Consultant

Governance



- Chief Information Security Officer
- Chief Privacy Officer
- Cyber Security Lawyer
- Cyber Security Manager
- Cyber Security Risk Manager

Sales



- Cyber Security Sales
- Senior Cyber Security Sales

Threat



- Cyber Threat Intelligence Specialist
- Senior Cyber Threat Intelligence Specialist
- Senior Threat Hunter
- Threat Hunter



Stage 3



Stage 4



Stage 5

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

Certificaciones y especializaciones

Certificaciones y especializaciones

ANECA (Agencia Nacional de Evaluación de la Calidad y Acreditación)

BUSCADOR

LISTADO DE TÍTULOS

Titulación

Inteligencia

Ciclo

Máster

Rama

Ingeniería y Arquitectura

Universidad

- Cualquiera -



Titulación actual

Universidad

Máster Universitario en Inteligencia Computacional e Internet de las Cosas

Universidad de Córdoba

Máster Universitario en Ciberseguridad e Inteligencia de Datos

Universidad de La Laguna

Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros / Business Intelligence And Big Data In Cyber-secure Environments

Universidad de Valladolid

Máster Universitario en Inteligencia Artificial

Universidad Internacional de La Rioja

Máster Universitario en Investigación en Inteligencia Artificial

Universidad Internacional Menéndez Pelayo

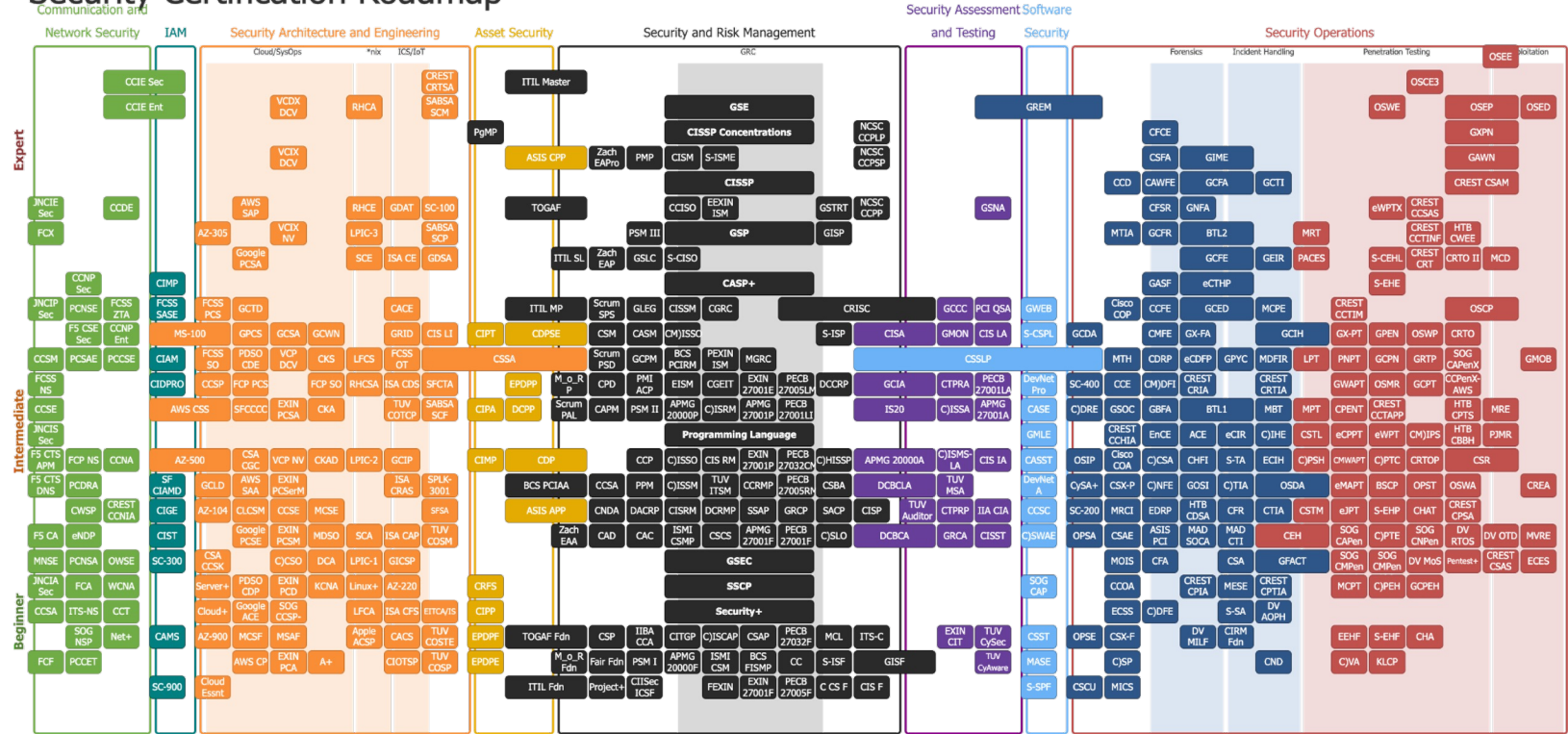
Máster Universitario en Seguridad Vial y Tráfico

Universidad Carlos III de Madrid

Source: <https://srv.aneca.es/ListadoTitulos/busqueda-titulaciones>

Certificaciones y especializaciones

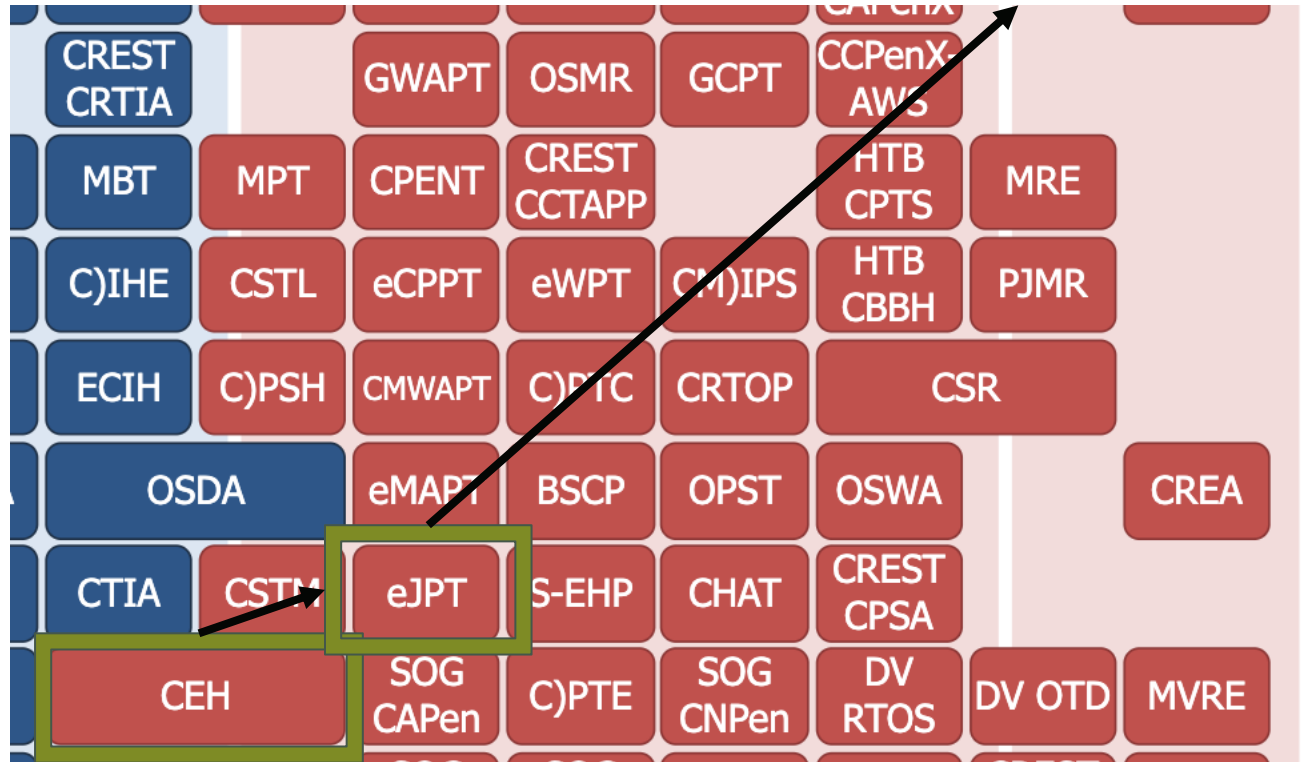
Security Certification Roadmap



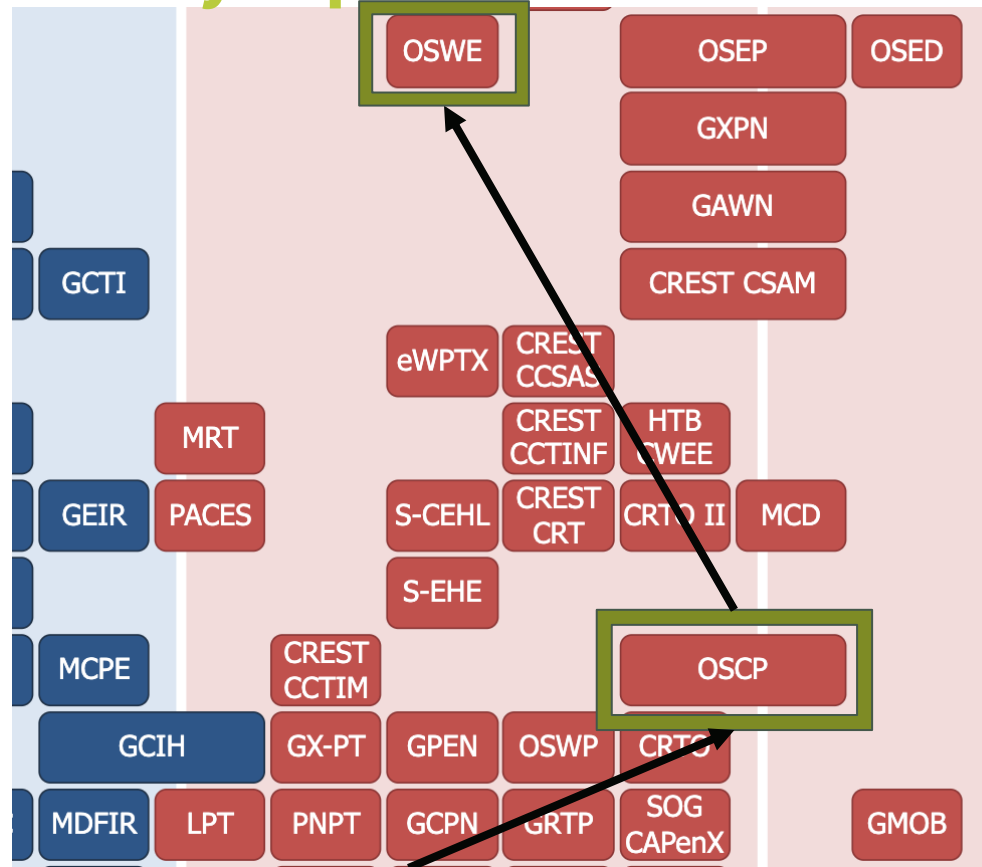
481 certifications listed | March 2025, FireShark Technologies

Source: <https://fireshark.in/security-certification-roadmap.html>

Certificaciones y especializaciones



Certificaciones y especializaciones



Certificaciones y especializaciones



UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

Salarios

Salarios

Manfred 2026 (Agencia de Recruiting IT & Estrategia de HR)

Backend Engineer salary in Spain



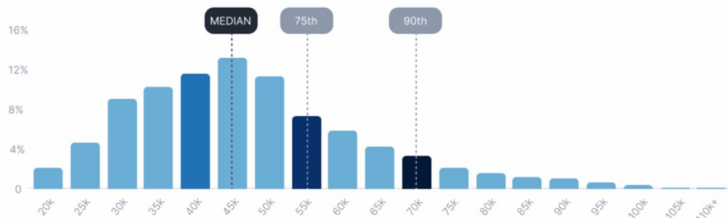
MOST FREQUENT SALARY (MEDIAN)

45.654 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Frontend Engineer salary in Spain



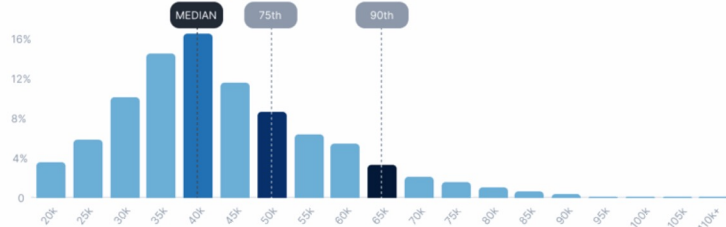
MOST FREQUENT SALARY (MEDIAN)

42.570 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Source: <https://www.getmanfred.com/blog/guia-salarial-2026-salarios-en-tecnologia-espana-manfred>

Salarios

Desarrollo & QA

Full-Stack Engineer salary in Spain



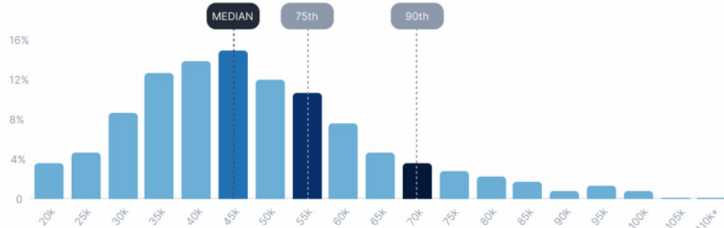
MOST FREQUENT SALARY (MEDIAN)

47.450 €



Compensation distribution

TOTAL ANUAL COMPENSATION (€)



getmanfred.com

QA & Testing salary in Spain



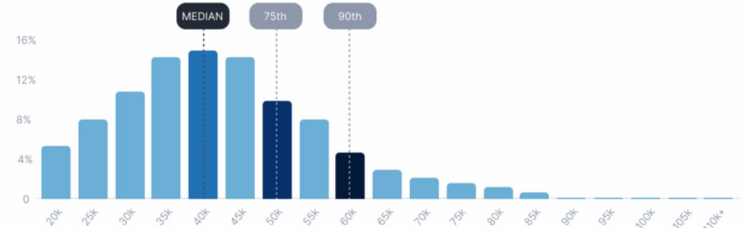
MOST FREQUENT SALARY (MEDIAN)

37.256 €



Compensation distribution

TOTAL ANUAL COMPENSATION (€)



getmanfred.com

Mobile Engineer salary in Spain



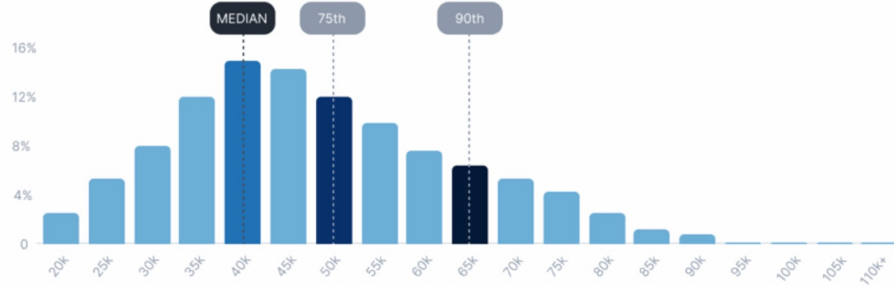
MOST FREQUENT SALARY (MEDIAN)

40.500 €



Compensation distribution

TOTAL ANUAL COMPENSATION (€)



getmanfred.com

Salarios

Emergente (AI)

AI Engineer salary in Spain



MOST FREQUENT SALARY (MEDIAN)

52.250 €



40.5K €

25TH%



52.2K €

50TH%

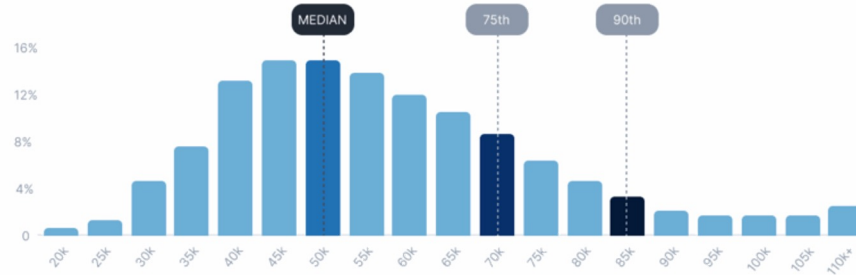


68.5K €

75TH%

Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

Sistema e Infraestructura

SysAdmin salary in Spain



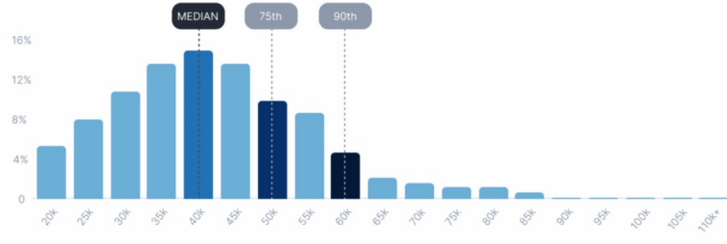
MOST FREQUENT SALARY (MEDIAN)

40.656 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

SRE/DevOps salary in Spain



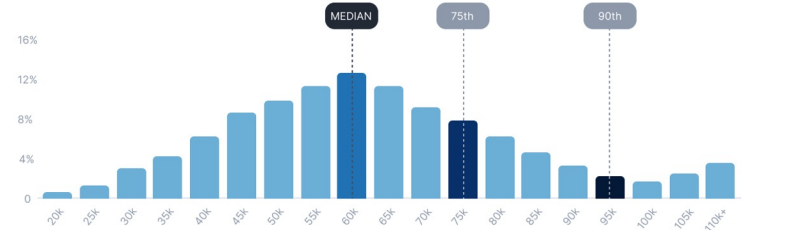
MOST FREQUENT SALARY (MEDIAN)

58.500 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

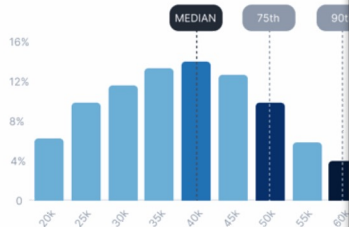
Data Engineer

Data Analyst salary in Spain

MOST FREQUENT SALARY (MEDIAN)
37.545 €

32.7K € 25TH% 37.5K € 50TH%

Compensation distribution

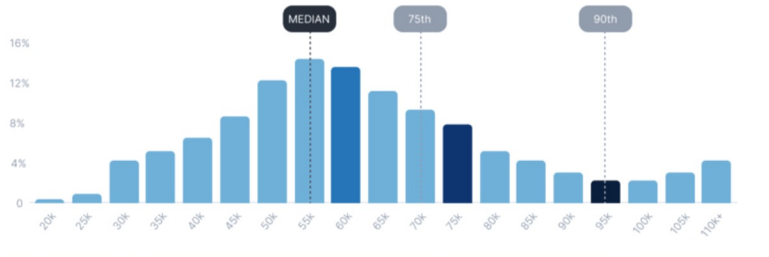


Data Scientist salary in Spain

MOST FREQUENT SALARY (MEDIAN)
55.400 €

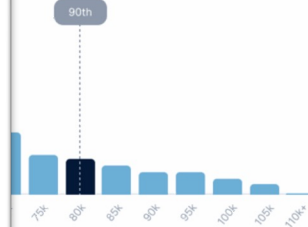
45.0K € 25TH% 55.4K € 50TH% 68.8K € 75TH%

Compensation distribution



getmanfred.com

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

MLOPS / Data architect

MLOps salary in Spain



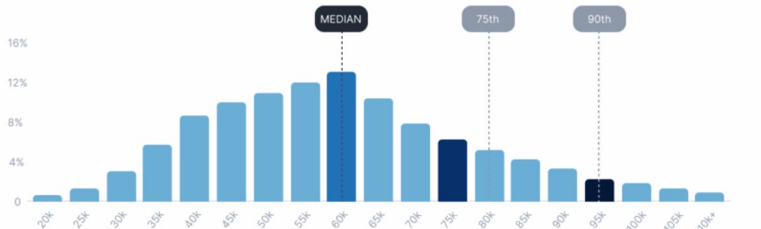
MOST FREQUENT SALARY (MEDIAN)

60.125 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Data Architect salary in Spain



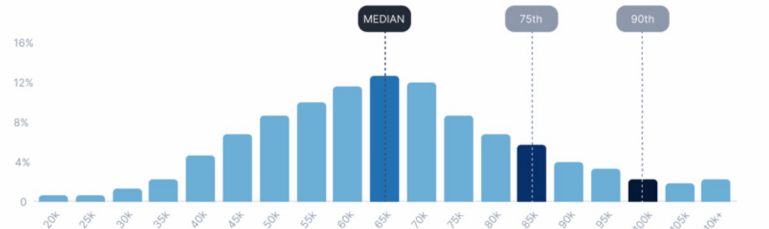
MOST FREQUENT SALARY (MEDIAN)

67.455 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

Liderazgo técnico

Tech Lead salary in Spain



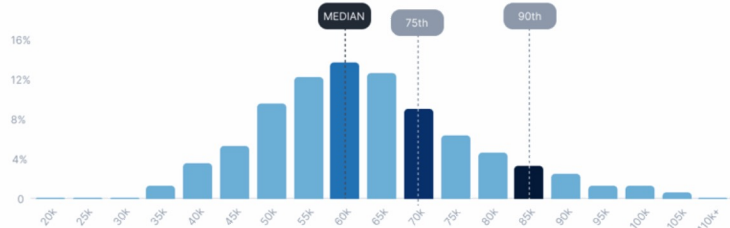
MOST FREQUENT SALARY (MEDIAN)

58.755 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Software Architect salary in Spain



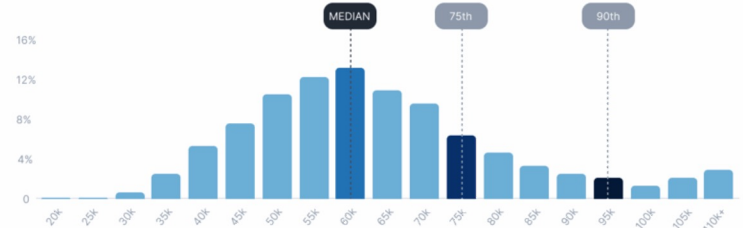
MOST FREQUENT SALARY (MEDIAN)

62.420 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

Liderazgo técnico

Engineering Manager salary in Spain

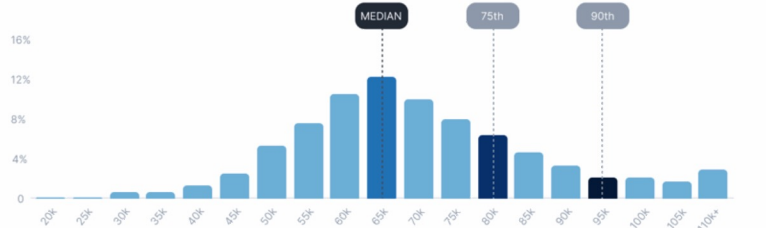


MOST FREQUENT SALARY (MEDIAN)
65.700 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Staff Engineer salary in Spain

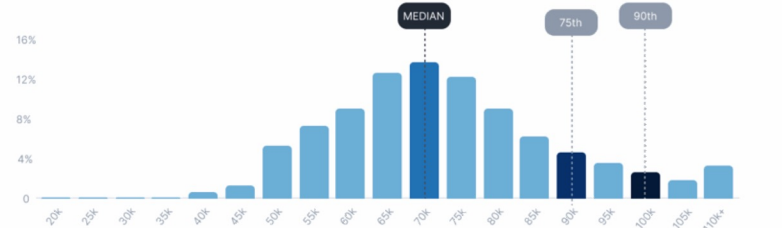


MOST FREQUENT SALARY (MEDIAN)
70.720 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

Liderazgo técnico

VP of Engineering salary in Spain



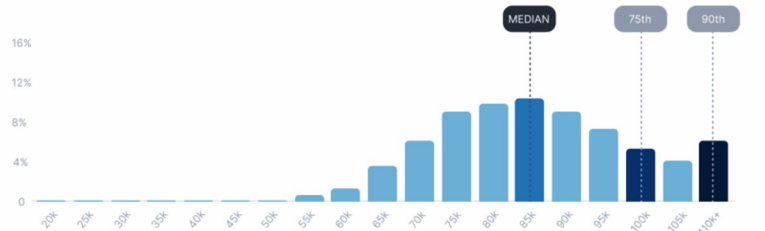
MOST FREQUENT SALARY (MEDIAN)

85.650 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

CTO/ Head of Engineering salary in Spain



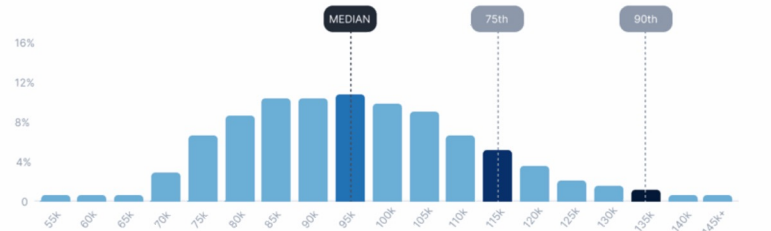
MOST FREQUENT SALARY (MEDIAN)

94.280 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Salarios

Producto

Product Designer salary in Spain



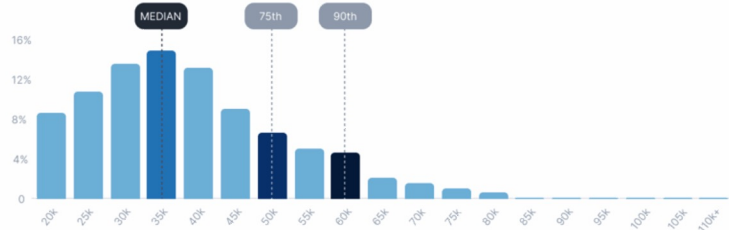
MOST FREQUENT SALARY (MEDIAN)

35.575 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com

Product Manager salary in Spain



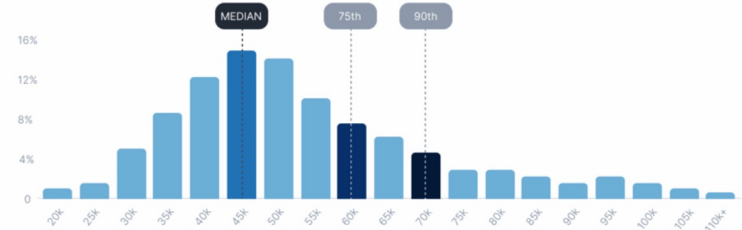
MOST FREQUENT SALARY (MEDIAN)

47.500 €



Compensation distribution

TOTAL ANNUAL COMPENSATION (€)



getmanfred.com



MOST FREQUENT SALARY (MEDIAN)

56.670 €

Experiencia

Salarios

<2 años

€25-30K

2-5 años

€31-40K

5-10 años

€41-55K

>10 años

€56-80K



getmanfred.com

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

Regulación, conformidad y certificación

Regulación, conformidad y certificación

Necesario distinguir estos conceptos. Obligados por controles de la norma UNE-EN ISO/IEC 27001:2023

- **A.5.31 - Identificación de requisitos legales, reglamentarios y contractuales**
- A.5.32 - Derechos de propiedad intelectual (DPI)
- A.5.34 - Privacidad y protección de datos de carácter personal (DCP)
- A.5.36 - Cumplimiento de las políticas y normas de seguridad de la información

Regulación, conformidad y certificación

Regulación (Regulatory Compliance)

Regulación es el conjunto de leyes, reglamentos y disposiciones legales obligatorias emitidas por autoridades competentes (UE, Estado, reguladores sectoriales) que una organización **debe cumplir por imperativo legal**.

Es de obligado cumplimiento. *Su incumplimiento conlleva sanciones administrativas, penales o civiles.*

No es opcional ni certificable.

Regulación, conformidad y certificación

Ejemplos: RGPD, NIS2, ENS, DORA, LOPDGDD.

En GRC:

La regulación define el **marco mínimo legal** sobre el que se construyen los controles de gobierno y gestión del riesgo.

Regulación, conformidad y certificación

Conformidad (Compliance)

Conformidad es el **grado en que una organización cumple** con requisitos definidos, ya sean:

- Legales (regulación)
- Normativos (ISO, ENS)
- Contractuales
- o Internos (políticas, procedimientos).

Es una condición, no un sello.

Regulación, conformidad y certificación

Puede evaluarse *interna* o *externamente*.

- Aplica tanto a leyes como a normas voluntarias.
- Se demuestra mediante **evidencias** y **controles**.

En GRC:

La conformidad es el estado operativo que conecta regulación, riesgos y controles: “¿estamos cumpliendo y podemos demostrarlo?”

Regulación, conformidad y certificación

Certificación

Certificación es el proceso formal mediante el cual ***un tercero independiente y acreditado verifica y declara que un sistema, proceso u organización cumple con los requisitos de una norma*** concreta.

Es **voluntaria**, salvo exigencia contractual.

Aplica **solo a normas certificables**, no a leyes.

Regulación, conformidad y certificación

Tiene **alcance, vigencia y auditorías periódicas.**

No exime de responsabilidad legal.

En GRC:

La certificación es un ***mecanismo de confianza y evidencia***, útil para clientes, reguladores y comités, pero no sustituye al cumplimiento real.

Regulación

Protección de datos y privacidad (inevitables)

- **RGPD (Reglamento UE 2016/679)** – La madre de todas las conversaciones incómodas.
- **LOPDGDD (Ley Orgánica 3/2018)** – Aterrizaje español del RGPD.
- **ePrivacy** (Directiva 2002/58/CE, en transición eterna) – Cookies, comunicaciones electrónicas, consentimiento.

Regulación

Ciberseguridad y servicios esenciales

- **Directiva NIS2 (UE 2022/2555)** – Obligatoria: gestión de riesgos, reporting, responsabilidad del management.
- **Ley 8/2011 y RD 43/2021** – Protección de infraestructuras críticas (si aplica).
- **ENS (Esquema Nacional de Seguridad)** – Obligatorio para sector público y proveedores.
- **Ley 34/2002 (LSSI-CE)** – Servicios de la sociedad de la información y comercio electrónico.

Regulación

Continuidad, resiliencia y operación

- **DORA (Reglamento UE 2022/2554)** – Para sector financiero: resiliencia operativa digital.
- **Ley 10/2010 PBC/FT** – Prevención de blanqueo de capitales (si aplica).
- **Ley 11/2018** – Información no financiera y gobierno corporativo (riesgos, controles, compliance).

Regulación

Penal, responsabilidad y “cuando todo sale mal”

- **Código Penal (art. 31 bis)** – Responsabilidad penal de la persona jurídica.
- **Ley 1/2019 de Secretos Empresariales** – Protección de información sensible.
- **Ley 1/2025** (transposición NIS2 en España, en curso) – Para no llevarse sorpresas regulatorias.

Regulación

Sectoriales (solo si aplica al sector)

- **PSD2 / PSD3** – Pagos y autenticación fuerte.
- **HIPAA / similares** – Salud (si hay datos sanitarios).
- **PCI DSS** – No es ley, pero actúa como tal si tocas tarjetas.
- **SOX** – Si cotiza o depende de empresas US.

Certificación

Las “tres” marías

- **ISO 9001** – Gestión de la calidad
- **ISO 14001** – Medio ambiente
- **ISO 45000** – Sistemas de Gestión de Seguridad y Salud en el Trabajo

Operación y calidad (según madurez)

- **ISO/IEC 20000-1** – Gestión de servicios TI.

Certificación

Seguridad de la información y ciberseguridad (núcleo)

- **ISO/IEC 27001** – Sistema de Gestión de Seguridad de la Información (la imprescindible).
- **ISO/IEC 27002** – Controles de seguridad (el “cómo” del 27001).
- **ISO/IEC 27005** – Gestión del riesgo de seguridad de la información.
- **ISO/IEC 27004** – Métricas y medición de la seguridad (KPIs “oficiales”).

Certificación

- **ISO/IEC 27035** – Gestión de incidentes de seguridad.
- **ISO/IEC 27006** – Requisitos para organismos de certificación (útil para entender al auditor).
- **ISO/IEC 27031** – Continuidad de las TIC.

Continuidad y resiliencia

- **ISO 22301** – Continuidad de negocio (BCMS).
- **ISO 22316** – Resiliencia organizacional (más estratégica, menos técnica).

Certificación

Privacidad y protección de datos

- **ISO/IEC 27701** – Sistema de gestión de la privacidad (extensión natural de 27001, muy alineada con RGPD).
- **ISO/IEC 27018** – Protección de datos personales en la nube.
- **ISO/IEC 29134** – Evaluaciones de impacto en privacidad (PIA/DPIA).

Certificación

Cloud y terceros

- **ISO/IEC 27017** – Controles de seguridad para servicios cloud.
- **ISO/IEC 27036** – Seguridad en relaciones con proveedores.
- **ISO/IEC 27040** – Seguridad en almacenamiento de la información.

Certificación

Riesgo, gobierno y gestión

- **ISO 31000** – Gestión del riesgo corporativo (ERM).
- **ISO/IEC 38500** – Gobierno corporativo de las TI.
- **ISO 37301** – Sistemas de gestión de compliance.

UA

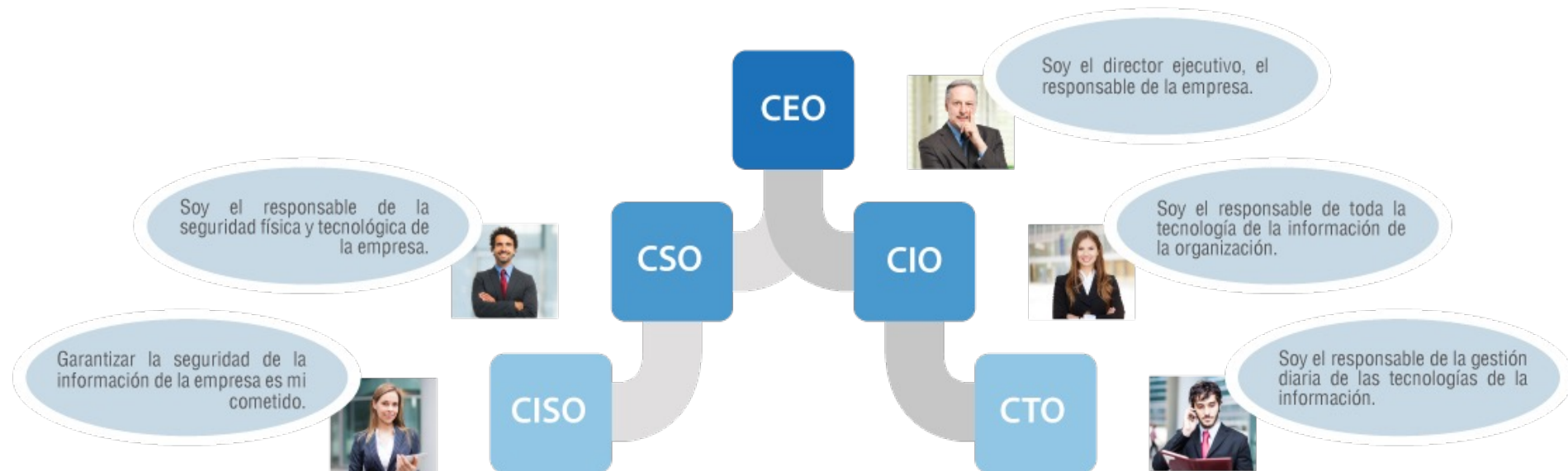
UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

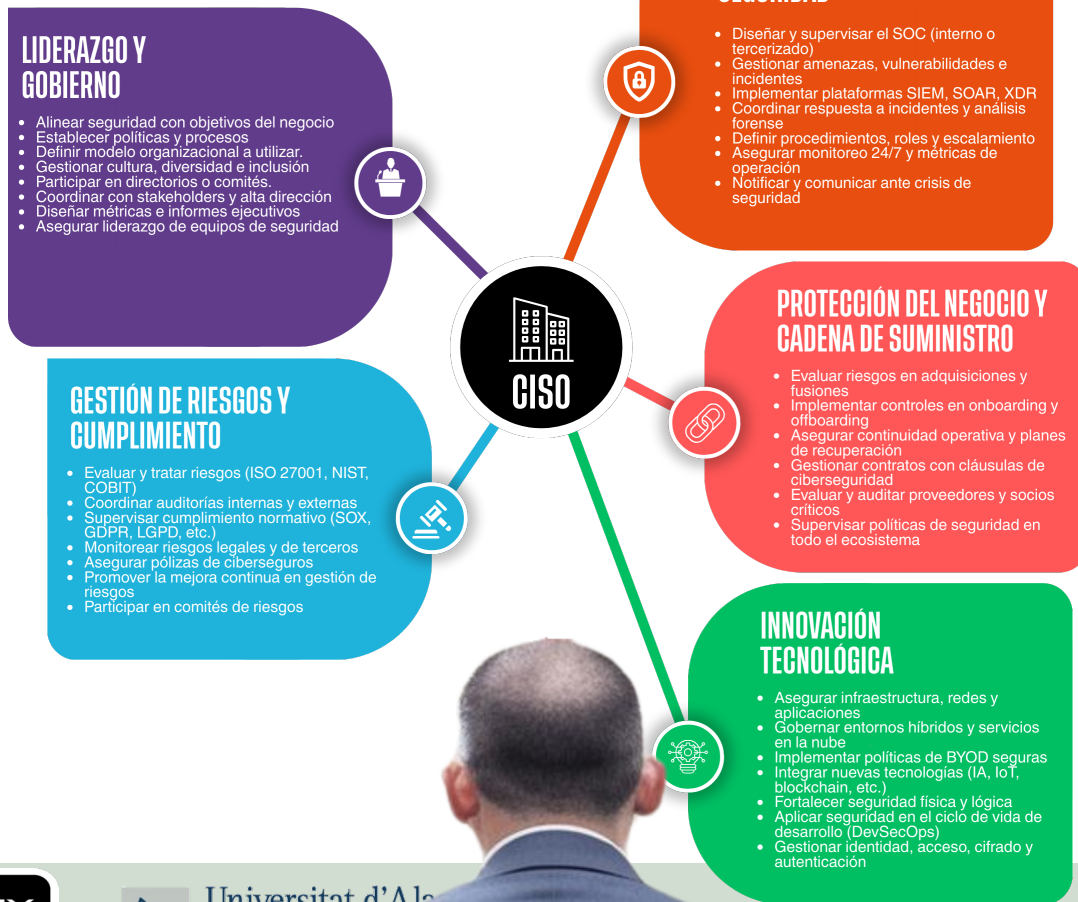
Ciberseguridad 360

El rol del Ciso: cuando todo funciona, nadie pregunta por ti

El rol del Ciso



El rol del Ciso



El rol del Ciso

El peso de proteger lo intangible

Una de las grandes dificultades que enfrenta el CISO es comunicar el valor de su trabajo a audiencias que no siempre comprenden el riesgo.

Convencer al **CFO** de invertir en algo que todavía no ocurrió, o al **CEO** de que un dato mal protegido puede costar millones.

El rol del Ciso

Y mientras tanto:

- Las amenazas se transforman
- Los marcos legales se actualizan
- Los entornos tecnológicos se diversifican

Y el almuerzo, muchas veces, llega frente al teclado...

El rol del Ciso

Hoja de ruta para los 100 primeros días

- La planificación comienza antes del primer día
- Evaluar el estado de madurez de la seguridad
- Definir prioridades estratégicas y métricas claras
- Comunicar con claridad y liderar con visión
- Ejecutar acciones visibles y generar impacto
- Medir, ajustar y evolucionar

El rol del Ciso

Enfermedades/Problemas Relacionados con el Rol (Estrés y Carga Laboral):

- **Estrés y Ansiedad:** alta presión por prevenir ciberataques, gestionar crisis y la responsabilidad sobre la seguridad de la organización.
- **Impotencia:** sentimiento de no poder controlar todas las amenazas, especialmente las que involucran error humano o amenazas internas.

El rol del Ciso

- Agotamiento (B) y cambiante de l

La empresa empieza a tener perdidas, hay que despedir a Paco.



aturaleza constante de recursos.



El rol del Ciso

50 preguntas para una entrevista como CISO

<https://www.adaface.com/es/blog/preguntas-entrevista-chief-information-security-officer/>

- ¿Cómo se mantiene al día con las últimas amenazas y tendencias de ciberseguridad?
- Describa una situación en la que tuvo que lidiar con una violación de seguridad. ¿Qué medidas tomó?
- ¿Cómo prioriza las iniciativas de seguridad cuando los recursos son limitados?

El rol del Ciso

- ¿Cómo equilibra la necesidad de seguridad con la eficiencia empresarial?
- ¿Qué estrategias emplea para fomentar una cultura de seguridad primero dentro de una organización?
- ¿Cuál es su estrategia para garantizar el cumplimiento de las regulaciones de protección de datos en múltiples jurisdicciones?
- ¿Cómo prioriza los riesgos cuando se identifican múltiples problemas de alta prioridad simultáneamente?

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

ENAC y la auditora

ENAC y la auditora

Auditora: empresa acreditada en ENAC.

ENAC (Entidad Nacional de Acreditación y Conformidad)

<https://www.enac.es/>

- **Designación Gubernamental:** es el organismo oficial en España, designado por el Estado, para la acreditación.
- **Adhesión a Normas Internacionales:** Se basa en normas como el Reglamento (CE) 765/2008 y aplica requisitos de normas técnicas internacionales para evaluar a otras entidades.

Tarifas 2026

TABLA II	
Inspección Certificación de Sistemas de Gestión Certificación de Producto Certificación de Personas Verificadores Medioambientales⁹ Organismos de Validación y Verificación Proveedores de Ensayos de Aptitud Productores de Materiales de Referencia	
1. Tarifa de gestión	
Inicial	1.557 €
Inicial consecutiva	525 €
Ampliación	525 €
Visita de Control/ Evaluación complementaria <i>in situ</i> ⁽¹⁾	1.469 €
Extraordinaria ⁽¹⁾	1.557 €
Acreditación transfronteriza	1.269 €
2. Coste de la evaluación	
Auditor	1.203 €/día
3. Certificado de acreditación	
Certificado de Acreditación	948 €
Copia certificado acreditación o anexos técnicos	70 €
4. Cuota anual de mantenimiento de la acreditación	
Cuota base:	
Primera acreditación por esquema de acreditación	1.223 €
Segunda acreditación (y siguientes) para el mismo esquema	1.011 €
Complementos ⁽²⁾ :	
Área del alcance (a partir de la segunda)	859 €
Campo acreditado (a partir del segundo)	158 €
Emplazamiento (a partir del segundo)	100 €

Source: <https://www.enac.es/documents/7020/c3bfb09c-6ce8-4568-83e5-396e488d312f>

ENAC y la auditora

Empresas auditoras acreditadas (UNE-EN ISO/IEC 27001:2022)

- LABORATORIO DE SAÚDE PÚBLICA DE GALICIA
- LGAI TECHNOLOGICAL CENTER, S.A. (APPLUS)
- AENOR CONFÍA, S.A.
- BUREAU VERITAS IBERIA, S.L.
- OCA Instituto de Certificación, S.L.
- IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
- IGC CERTIFICACIÓN GLOBAL, S.L.
- CÁMARA CERTIFICA
- SGS INTERNATIONAL CERTIFICATION SERVICES IBÉRICA, S.A.
- EQA European Quality Assurance
- SISTEMAS Y PROCESOS DE GESTIÓN, CERTIFICACIÓN, S.L.
- CERTIFICACIONES CERTHIA, S.L.
- ADOK CERTIFICACIÓN, S.L.

ENAC y la auditora

Empresas auditoras acreditadas (ENS RD 311/2022)

- COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE CASTELLÓN. LABORATORIO "SEBASTIÁN CARPI"
- BIOCARBURANTES DE CASTILLA Y LEÓN, S.A.
- AENOR CONFÍA, S.A.
- AUDERTIS AUDIT SERVICES, S.L.
- LEET SECURITY, S.L.
- BDO AUDITORES, S.L.P.
- LGAI TECHNOLOGICAL CENTER, S.A. (APPLUS)
- CERTIFICACIÓN Y CONFIANZA CÁMARA, S.L.
- SGS INSPECCIONES REGLAMENTARIAS, S.A.
- IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
- OCA Instituto de Certificación, S.L.
- EUROPEAN QUALITY ASSURANCE SPAIN, S.L. (EQA European Quality Assurance)
- BUREAU VERITAS IBERIA, S.L.
- DNV BUSINESS ASSURANCE SPAIN, S.L.
- IMQ IBÉRICA, S.L.
- SGS BRIGHTSIGHT BARCELONA, S.L.
- SGS INTERNATIONAL CERTIFICATION SERVICES IBÉRICA, S.A.
- ADOK CERTIFICACIÓN, S.L.
- IGC CERTIFICACIÓN GLOBAL, S.L.
- ICDQ, INSTITUTO DE CERTIFICACIÓN, S.L.
- AGENCIA PARA LA CERTIFICACIÓN DE LA CALIDAD Y EL MEDIO AMBIENTE, S.L. (ACCM)

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

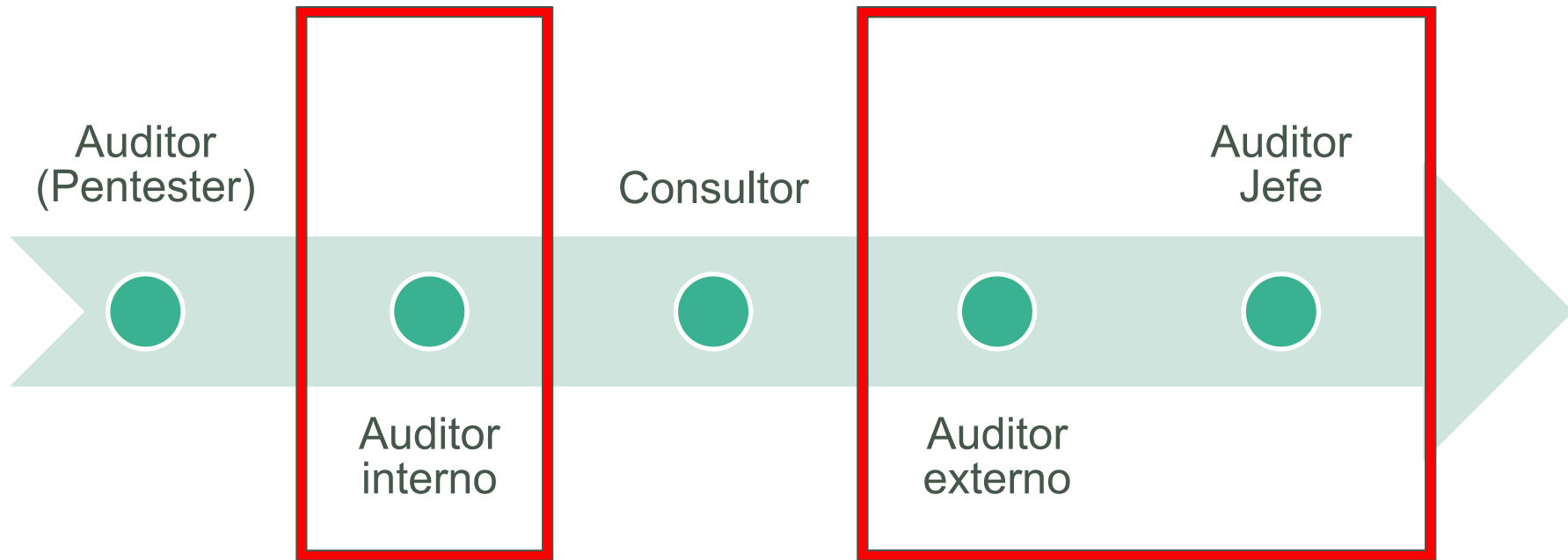
Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

¡Quiero ser auditor!

¡Quiero ser auditor!

Varios “trajes y disfraces” que existen:



¡Quiero ser auditor!

Auditor interno

- Profesión **no regulada**
- **Cumplimiento de requisitos** básicos
- Emite informe de **auditoría interna**

¡Quiero ser auditor!

Auditor externo

<https://www.aenor.com/web/mex/formacion/tecnologias-de-la-informacion/certificacion-leadmaster-auditor-lider-iso-27001>

- Principio de “independencia”
- Formación específica (40 horas online/presencial)
- Registro y seguimiento del auditor
- Aproximadamente 1063€ (bonificables por Fundae)

¡Quiero ser auditor!

- Introducción al proceso de auditoría de los SGSI
- Revisión de los requisitos de la Norma UNE-EN ISO 27001:2023.
- La Norma ISO 19011:2018. Directrices para la auditoría de los Sistemas de Gestión.
- Objetivo y tipos de auditoría.
- Normas aplicables a la realización de auditorías.
- Términos y definiciones.
- Principios de auditoría.
- Gestión del programa de auditoría.

¡Quiero ser auditor!

- Planificación y realización de las auditorías:
 - Preparación de la auditoría.
 - Desarrollo de la auditoría.
 - Las herramientas del auditor.
 - Comportamiento del auditor.
 - Recogida y verificación de información.
 - Redacción y clasificación de no conformidades.
 - Elaboración del informe de auditoría.
 - Finalización de la auditoría y seguimiento.

¡Quiero ser auditor!

- Role-playing (simulación en la ejecución de una auditoría).
- Recomendaciones en la ejecución de una auditoría
- Competencia y evaluación de las personas implicadas en la auditoría.

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Ciberseguridad 360

Proceso de auditoría

Proceso de auditoría

Tipos de auditoría

Auditoría interna: es realizada por la propia organización o un auditor externo contratado. Identifican las no conformidades antes de la auditoría de certificación y evalúan si los controles de seguridad funcionan correctamente.

Auditoría de certificación: es llevada a cabo por un organismo certificador acreditado la cual se realiza en dos fases.

Proceso de auditoría

- **Fase 1:** Revisión documental del SGSI.
- **Fase 2:** Evaluación práctica de la implementación de los controles.

Si la empresa cumple los requisitos, recibe la certificación ISO 27001.

Auditorías de seguimiento y recertificación: se realizan periódicamente (generalmente cada año) para mantener la certificación y, a su vez, cada tres años, se requiere una auditoría de recertificación para renovar la validez del certificado.

Proceso de auditoría

Tipo de Auditoría	Quién la realiza	Frecuencia
Auditoría Interna	Audidores internos o auditores externos contratados	Al menos 1 vez al año
Auditoría de Certificación	Organismo Certificador Acreditado	Una vez para obtener la certificación
Auditoría de Seguimiento	Organismo Certificador Acreditado	1 vez al año (después de la certificación)
Auditoría de Recertificación	Organismo Certificador Acreditado	Cada 3 años



Coffee Break (20 m.)

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Parte II

Ejercicio práctico (Ciso Assistant)

Ciso Assistant Community Edition

INUITEM (Ciso Assistant)

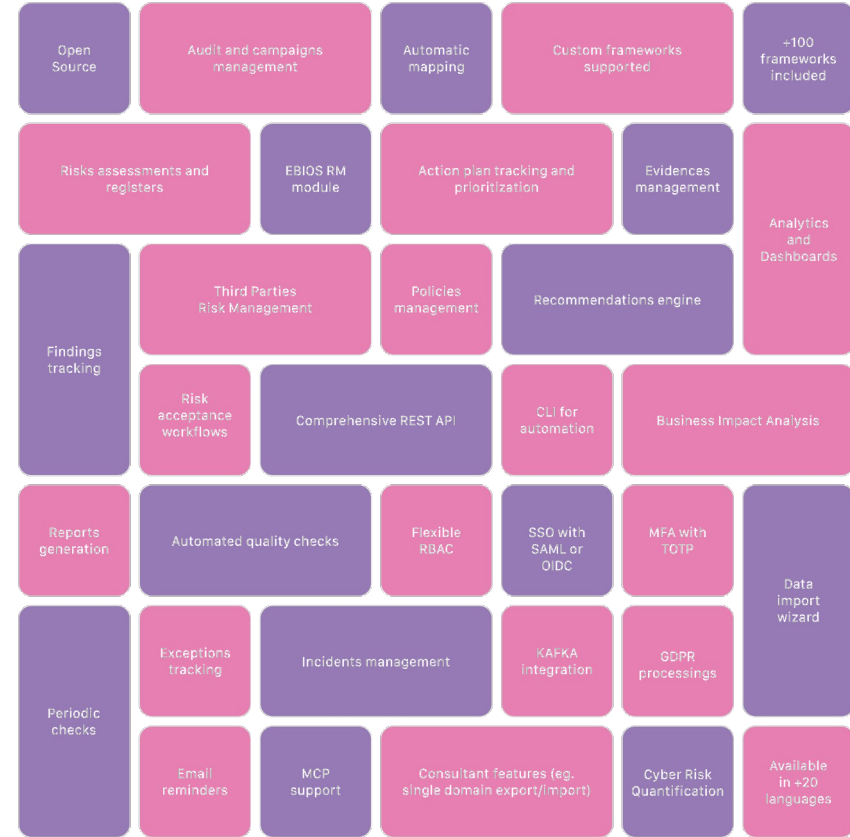
<https://github.com/intuitem/ciso-assistant-community>



CISO Assistant

**Extra arms for your
cyber security program**

Ciso Assistant Community Edition



Ciso Assistant Community Edition

INSTALACIÓN:

```
git clone --single-branch -b main  
https://github.com/intuitem/ciso-assistant-  
community.git
```

```
cd ciso-assistant-community
```

```
./docker-compose-build.sh
```

Acceder a **<https://localhost:8443/>**

Ciso Assistant Community Edition

EJECUCIÓN POSTERIOR:

```
docker compose up
```

Problemas (Contraseña usuario):

```
docker compose exec backend poetry run python  
manage.py changepassword <user_email>
```

Ciso Assistant Community Edition

MARCOS PERSONALIZADOS (<https://intuitem.gitbook.io/ciso-assistant/customization/getting-your-custom-framework>)

```
cd tools
```

```
pip3 install -r requirements.txt --break-system-packages
```

```
python3 convert_library_v1.py custom-framework.xlsx
```

Genera archivo de importación `custom-framework.yaml`

UA

UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE

Escola Politècnica Superior
Escuela Politécnica Superior

Conclusiones

Conclusiones

«El GRC es aburrido, para corbatas y con ánimo de lucro: vivir para el riesgo, el compliance, auditorías infinitas, los KPIs que nadie mira, los frameworks que nadie cumple y los engaños de los “quick wins”; así que dejo el teclado, salvo para PowerPoints, comités estériles y justificar presupuestos que nunca llegan.»

CISO Anónimo

¿Preguntas?



Muchas gracias



© 2026 CS³ GROUP. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.