



Gonzalo de Francisco Rodríguez
presenta el resumen sobre

Arquitecto en Ciberseguridad

15 de febrero de 2025

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Arquitecto de Ciberseguridad, Certificaciones, Ciberataques, Estrategias de Ciberseguridad, Infraestructuras de Ciberseguridad

1. Definición y responsabilidades

Un **Arquitecto en Ciberseguridad** es un profesional encargado de diseñar, desarrollar e implementar infraestructuras de seguridad en una organización. Su trabajo es crucial para proteger los sistemas, redes y datos contra ataques cibernéticos. Para ello, debe planificar estrategias de seguridad, evaluar vulnerabilidades, diseñar soluciones seguras y supervisar su implementación.

1.1. Responsabilidades claves

■ Diseño de arquitectura segura:

- Definir marcos de seguridad para redes, sistemas y aplicaciones.
- Diseñar controles de acceso y segmentación de redes.
- Implementar principios de seguridad como “Zero Trust” y “Defense in Depth”.

■ Gestión de riesgos y cumplimiento:

- Evaluar amenazas y vulnerabilidades en la infraestructura de tecnología de la información TI.
- Garantizar el cumplimiento de normativas y estándares de seguridad (ISO 27001, NIST, GDPR, etc.).

- Desarrollar políticas y procedimientos de seguridad.

■ Implementación de tecnologías de seguridad:

- Seleccionar e integrar herramientas como firewalls, SIEMs, IDS/IPS, VPNs, etc.
- Definir estrategias de cifrado y gestión de claves.
- Proteger sistemas cloud, on-premise y entornos híbridos.

■ Supervisión y respuesta a incidentes:

- Coordinar equipos de seguridad en respuesta a incidentes.
- Implementar estrategias de detección y mitigación de ataques.
- Realizar pruebas de penetración y auditorías de seguridad.

■ Colaboración con otros equipos:

- Trabajar con equipos de desarrollo (DevSecOps) para integrar seguridad en el ciclo de vida del software.
- Coordinarse con administradores de red y sistemas.
- Formar y concienciar a empleados sobre mejores prácticas de seguridad.

2. Formación y lugares para estudiar

Para convertirse en arquitecto en ciberseguridad, es recomendable contar con una formación en **ingeniería informática, telecomunicaciones, ciberseguridad o áreas afines**, además de certificaciones especializadas.

2.1. Universidades y másteres

España:

- Universidad Politécnica de Madrid (UPM): Máster en Ciberseguridad.
- Universidad Carlos III de Madrid (UC3M): Máster en Ciberseguridad y Privacidad.
- Universitat Oberta de Catalunya (UOC): Máster en Seguridad de las TIC.
- Universidad de León (ULE): Máster de Investigación en Ciberseguridad.
- Universidad de Sevilla (US): Máster en Ciberseguridad.

Internacionales:

- Carnegie Mellon University (EE.UU.): MS in Information Security.
- ETH Zürich (Suiza): Máster en Seguridad de la Información.
- Royal Holloway, University of London (Reino Unido): MSc in Cyber Security.

2.2. Certificaciones clave

Además de la formación académica, muchas empresas exigen certificaciones especializadas:

- **CISSP** (Certified Information Systems Security Professional): enfoque en arquitectura de seguridad.
- **CCSP** (Certified Cloud Security Professional): seguridad en entornos cloud.
- **CEH** (Certified Ethical Hacker): seguridad ofensiva y hacking ético.
- **OSCP** (Offensive Security Certified Professional): pentesting avanzado.
- **CISM** (Certified Information Security Manager): gestión de seguridad y riesgos.

- **SABSA** (Sherwood Applied Business Security Architecture): especializada en arquitectura de seguridad.
- **SC-100**: diseño de soluciones y operaciones de ciberseguridad para infraestructuras que se alineen con los procedimientos recomendados y las prioridades de seguridad de una organización.

2.3. Plataformas de formación online

- **Coursera**: cursos de Stanford, Google, IBM sobre ciberseguridad.
- **Udemy**: cursos específicos de pentesting, firewalls, etc.
- **Cybrary**: cursos avanzados de seguridad ofensiva y defensiva.
- **INE Security**: formación práctica en ciberseguridad y hacking ético.

3. Salidas profesionales

Un arquitecto en ciberseguridad puede trabajar en diversos sectores, incluyendo:

- **Grandes empresas y corporaciones** (banca, telecomunicaciones, energía).
- **Empresas de tecnología y startups** (desarrollo de software, IA, cloud computing).
- **Consultoras de ciberseguridad** (Deloitte, PwC, Accenture, KPMG, IBM Security).
- **Sector gubernamental y defensa** (Ejército, ministerios de seguridad).
- **Organismos internacionales** (Interpol, ONU, Agencia Europea de Ciberseguridad - ENISA).

· Microsoft. *Microsoft Certified: Cybersecurity Architect Expert*. Disponible en: <https://learn.microsoft.com/es-es/credentials/certifications/cybersecurity-architect-expert>

· INCIBE. *Catálogo de Formación Reglada en Ciberseguridad en España*. Disponible en: <https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad>

· Augusta University. *Cybersecurity Architect: Salary, Job Description and Education*. Disponible en: https://www-augusta-edu.translate.google.com/blog/cybersecurity-architect-salary?_x_t

guridad/

- CAS Training. *Certificación SC-100: Microsoft Cybersecurity Architect*. Disponible en: <https://cas-training.com/formacion/tic/microsoft/certificacion-sc-100-microsoft-cybersecurity-architect/>