

FICHA DE ASIGNATURA

Título: Diseño, desarrollo e implantación

Descripción: En esta asignatura vamos a profundizar en el concepto de Arquitectura de Seguridad, en su diseño y las posibles soluciones tecnológicas que deberemos conocer para poder implantar la seguridad adecuadamente en una organización.

Carácter: Obligatoria

Créditos ECTS: 3

Contextualización: Analizaremos qué elementos debemos de tener en cuenta a la hora de realizar un diseño de seguridad, contextualizando según los activos a proteger y las necesidades de seguridad. Presentaremos las principales soluciones tecnológicas existentes y destacaremos las lecciones aprendidas para poder implementarlas con éxito.

Modalidad: Online

Temario:

- Diseño de arquitecturas de seguridad en sistemas complejos y en redes, webservices y microservicios: protección pasiva, activa y aplicativa
- Entornos y metodologías (NIST Cybersecurity Framework, SDLC -Software developemnet life cycle-) de desarrollo: servicios, software y aplicaciones
- Entornos de producción e implantación de soluciones

Competencias Específicas:

CE2 – Diseñar el despliegue de sistemas de vigilancia, análisis y protección de sistemas complejos de tratamiento, almacenamiento y transmisión de datos.

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

CE13 – Aplicar metodologías que implementen soluciones de ciberseguridad en sistemas complejos de la información, servicios, software y aplicaciones.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	15	100%
Desarrollo de actividades del portafolio	12	0
Trabajo autónomo del alumno	48	0

Metodologías docentes

- Clases síncronas
- Vídeos con píldoras de conceptos teóricos
- Caso práctico
- Soporte a consultas

Sistema de Evaluación

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Examen	40%	60%
Trabajo individual	40%	60%

Normativa específica:

Bibliografía:

- ISO27001:2005 “Information Security Management- Specifications for an ISM”
- ISO/IEC 17799:2005 “Information Technology- Code of Practice for Information Security Management”
- Information Security Policy Templates
<https://www.sans.org/securityresources/policies/>
- Cyber security guidance for business:
<https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/>
- Open Security Architecture: <http://www.opensecurityarchitecture.org/>
- NIST: Cybersecurity Framework
- NIST: BigData Architecture
- NIST: Cloud Computing Security Reference Architecture
- Amazon - AWS Documentation: Standardized Architecture for NIST-based Assurance Frameworks on AWS
- Open Web Application Security Project (OWASP)
- ETSI: Security by Default (ETSI TR 103 309)
- ETSI - Security Controls for Effective Cyber Defense
- Sans: Critical Security Controls
- TOGAF: Open Enterprise Security Architecture (O-ESA)
- OpenSAMM: Software Assurance Maturity Model