UNIVERSIDAD INTERNACIONAL DE LA RIOJA unir

Asignatura: Gestión de la Seguridad

Cuatrimestre: 2º

ECTS: 3

Carácter: OB

Contenidos:

ID	Descripción
C1	Seguridad de la información en las organizaciones.
C2	Certificaciones, modelos de madurez y buenas prácticas en seguridad de la información.
C3	Control de accesos.
C4	Programas, procesos y políticas de seguridad de la información.

Competencias[1]:

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7- Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- CG1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en el ámbito de la Ingeniería de Software.
- CG2 - Capacidad para dirigir, planificar y supervisar equipos multidisciplinares.

[1] CB: Competencia básica; CG: Competencia general; CE: Competencia específica ; CT: Competencia transversal

- CG3 - Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería de Software siguiendo criterios de calidad.
- CG4 - Capacidad para la dirección general, dirección técnica y dirección de proyectos de I+D+I, en empresas y centros tecnológicos, en el ámbito de la Ingeniería de Software.
- CG5 - Capacidad para la puesta en marcha, dirección y gestión de procesos de diseño y desarrollo de sistemas informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
- CG6 - Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.
- CE16- Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración entre todos los departamentos de una empresa o entidad.
- CE17 - Analizar la infraestructura de red y los entornos de seguridad para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas.
- CE21 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, seguridad en centros financieros, seguridad en infraestructuras de defensa y principales conceptos de auditoría de sistemas.
- CE22 - Realizar un asesoramiento integral que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
- CE24 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
- CT1 -Analizar de forma reflexiva y crítica las cuestiones más relevantes de la sociedad actual para una toma de decisiones coherente.
- CT2 -Identificar las nuevas tecnologías como herramientas didácticas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje grupal.
- CT3 - Aplicar los conocimientos y capacidades aportados por los estudios a casos reales y en un entorno de grupos de trabajo en empresas u organizaciones.
- CT4 - Adquirir la capacidad de trabajo independiente, impulsando la organización y favoreciendo el aprendizaje autónomo.

Metodologías docentes:

ID	Denominación	Descripción
MD1	Lección magistral	Presentación de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada.
MD2	Estudios de casos	Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

ID	Denominación	Descripción
MD3	Resolución de ejercicios y problemas	Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral.
MD4	Aprendizaje Basado en Problemas (ABP)	A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas.
MD5	Contrato de Aprendizaje	Acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con la supervisión del profesor.

Temario:

Tema 1. **La seguridad de la información en las organizaciones**

1.1. Confidencialidad integridad y disponibilidad

1.2. La seguridad es un proceso y un asunto económico

1.3. Clasificación de la información

1.4. La seguridad implica gestión de riesgos

1.5. Controles de Seguridad

1.6. Seguridad física y lógica

Tema 2. **El profesional de la seguridad de la información**

2.1. La seguridad de la información como profesión

2.2. Las certificaciones (ISC)2

2.3. El estándar ISO 27001

2.4. Buenas prácticas de seguridad en la gestión de servicios de TI

2.5. Modelos de madurez para la seguridad de la información

2.6. Otras certificaciones y estándares.

Tema 3. **Control de accesos**

3.1. Requisitos del control de acceso

3.2. Mecanismos de autenticación

3.3. Métodos de autorización

3.4. Contabilidad y auditoría de accesos

3.5. Tecnologías “Triple A”

Tema 4. **Programas, procesos y políticas de seguridad de la información**

4.1. Programas de gestión de la seguridad

4.2. La gestión de riesgos

4.3. Diseño de políticas de seguridad

Tema 5. **Planes de continuidad de negocio**

5.1. Introducción a los PCN 1

5.2. Fase I y II

5.3. Fase III y IV

5.4. Mantenimiento del PCN

Tema 6. Protejamos nuestra empresa

6.1. Redes DMZ

6.2. Sistemas de detección de intrusos

6.3. Listas de control de accesos

6.4. Aprender del atacante: Honeypot

Bibliografía básica:

Asignatura basada exclusivamente en los apuntes del profesor.