Proyecto docente

Asignatura	Fundamentos de ciberseguridad		
Materia	Seguridad de datos y ciberseguridad		
Titulación	Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros		
Plan	621	**Código**	
Periodo de impartición	Segundo semestre	**Tipo/Carácter**	Obligatoria
Nivel/Ciclo	Máster	**Curso**	1
Créditos ECTS	3		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Noemí de Castro García		
Datos de contacto (e-mail, teléfono…)	ncasg@unileon.es		
Horario de tutorías	Se propondrá el horario de tutorías al comienzo de la asignatura. Las mismas se realizarán previa petición por correo electrónico.		
Coordinador			
Departamento	Matemáticas		
Web			
Descripción General			

1. Situación / Sentido de la asignatura

1.1 Contextualización

En el marco de la materia de *Seguridad de datos y ciberseguridad*, es esencial que el alumnado comprenda los aspectos fundamentales, elementos y actores en el contexto de la ciberseguridad. Así mismo, la identificación de las principales amenazas a la seguridad en el ciberespacio y las direrentes casuísticas de cibercrimen así como de los mecanismos de defensa, resultan fundamentales para introducirse en los Sistemas de Gestión de Seguridad de la Información, en los que las herramientas de análisis de grandes volúmenes de datos cobran especial relevancia ante la notificación y gestión de eventos de ciberseguridad. Por último, se desarrollarán las nociones básicas de concienciación y buenas prácticas que son necesarias en la actual sociedad del conocimiento para poder cumplir requisitos mínimos de ciberseguridad en organizaciones y empresas.

1.2 Relación con otras asignaturas

- Tendencias emergentes en seguridad de datos
- Derecho en seguridad de datos
- Informática forense y auditoría de seguridad
- Tendencias emergentes en ciberseguridad

1.3 Prerrequisitos

Al tratarse de una asignatura básica no requiere ningún prerequisito específico más allá de los necesarios conocimientos de ofimática y de búsqueda de información por internet.

2. Competencias

2.1 Generales del título

CG2 - Capacidad de planificar y construir sistemas que permitan una gestión segura de los datos.

2.2 Específicas materia

- CSD1: Capacidad para utilizar los conceptos básicos de ciberseguridad en proyectos de Big Data.
- CSD3: Adquisición de competencias teóricas y prácticas sobre Sistemas de Gestión de la Seguridad de la Información.
- CSD4: Capacidad para acceder, analizar y aplicar la información generada en los Centros de Respuesta a Incidentes de Seguridad, así como conocer sus principios de funcionamiento y normativas.

3. Resultados de aprendizaje

Al finalizar la asignatura, el alumno será capaz de:

- Identificar los distintos elementos y actores en el contexto de la ciberseguridad.
- Comprender los aspectos esenciales relacionados con Big Data en sistemas de notificación y gestión de eventos de ciberseguridad.
- Llevar a cabo buenas prácticas de ciberseguridad en el entorno empresarial e institucional.

4. Contenido / Programa de la asignatura

Bloque 1: "Fundamentos de ciberseguridad"

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

En el marco de la materia de *Seguridad de datos y ciberseguridad*, es esencial que el alumnado comprenda los aspectos fundamentales, elementos y actores en el contexto de la ciberseguridad. Así mismo, la identificación de las principales amenazas a la seguridad en el ciberespacio y los principales tipos de cibercrimen así como de los mecanismos de defensa, resultan fundamentales para introducirse en los Sistemas de Gestión de Seguridad de la Información, en los que las herramientas de análisis de grandes volúmenes de datos cobran especial relevancia ante la notificación y gestión de eventos de ciberseguridad.

b. Objetivos de aprendizaje

Identificar los distintos elementos y actores en el contexto de la ciberseguridad

c. Contenidos y materiales de aprendizaje

- Introducción a la ciberseguridad.
- Conceptos clave.
- Introducción al estudio del cibercrimen y a los mecanismos de defensa.

d. Métodos docentes

La metodología docente se basa, principalmente, en la sesión magistral o exposición de contenidos que se complementa con diferentes materiales (documentación, enlaces web, etc). Así mismo, se pondrá a disposición del alumnado una sesión de tutoría grupal. Por otra parte, se resolverán las dudas individuales mediante tutorías, participación en foros y/o correo electrónico.

La evaluación se realizará a través de diferentes cuestionarios de evaluación.

e. Bibliografía básica

Andress, J., Cyber Warfare (2013). Techniques, Tactics and Tools for Security Practitioners.
Graham, J.. Howard, R., Olson, R. (2011). Cyber Security Essentials.
Stallings, W., Brown, L. (2018). Computer Security - Principles and Practice.

f. Bibliografía complementaria

Enlaces web a las guías y estándares de los organismos oficiales, así como a artículos científicos.

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros, emails
  - Sala videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
Bloque I - 1 ECTS	Semanas 1-4

Bloque 2: "Taxonomías"

Carga de trabajo en créditos ECTS: 1.4

a. Contextualización y justificación

En el marco de la materia de Seguridad de datos y ciberseguridad, es esencial que el alumnado identifique las principales amenazas a la seguridad en el ciberespacio y los principales tipos de cibercrimen, así como su efecto en los Sistemas de Gestión de Seguridad de la Información, en los que las herramientas de análisis de grandes volúmenes de datos cobran especial relevancia ante la notificación y gestión de eventos de ciberseguridad.

b. Objetivos de aprendizaje

Comprender los aspectos esenciales en sistemas de notificación y gestión de eventos de ciberseguridad.

c. Contenidos y materiales de aprendizaje

- Sistemas de Gestión de la Seguridad de la Información.
- Taxonomías de gestión de eventos de ciberseguridad.
- Taxonomías de soluciones en ciberseguridad

d. Métodos docentes

La metodología de este bloque es mixta:

- Sesión magistral o exposición de contenidos que se complementa con diferentes materiales (documentación, enlaces web, etc).
- Aprendizaje basado en proyectos y evidencias.
- Aprendizaje cooperativo.
- Así mismo, se pondrá a disposición del alumnado una sesión de tutoría grupal. Por otra parte, se resolverán las dudas individuales mediante tutorías, participación en foros y/o correo electrónico.

La evaluación se realizará a través de diferentes actividades individuales: elaboración y presentación/exposición de proyecto o carpeta de aprendizaje y evaluación de evidencias/proyectos.

e. Bibliografía básica

Andress, J., Cyber Warfare (2013). Techniques, Tactics and Tools for Security Practitioners.
Graham, J.. Howard, R., Olson, R. (2011). Cyber Security Essentials.
Stallings, W., Brown, L. (2018). Computer Security - Principles and Practice.

f. Bibliografía complementaria

Enlaces web a las guías y estándares de los organismos oficiales.

g. Recursos necesarios

- Plataforma docente
- Herramientas de grabación de vídeo con presentación.
- Cuenta de correo en repositorio en la nube o plataforma de vídeo (gratuito).
- Herramientas de comunicación:
  - Asíncronos: foros, emails
  - Sala videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
Bloque II - 1.4 ECTS	Semanas 3-7

Bloque 3: “Buenas prácticas”

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

En el marco de la materia de *Seguridad de datos y ciberseguridad*, es esencial que el alumnado comprenda los aspectos fundamentales, elementos y actores en el contexto de la ciberseguridad. Así mismo, la identificación de las principales amenazas a la seguridad en el ciberespacio y los principales tipos de cibercrimen así como de los mecanismos de defensa, resultan fundamentales para introducirse en los Sistemas de Gestión de Seguridad de la Información, en los que las herramientas de análisis de grandes volúmenes de datos cobran especial relevancia ante la notificación y gestión de eventos de ciberseguridad. Por último, se desarrollarán las nociones básicas de concienciación y buenas prácticas que son necesarias en la actual sociedad del conocimiento para poder cumplir requisitos mínimos de ciberseguridad en organizaciones y empresas.

b. Objetivos de aprendizaje

Llevar a cabo buenas prácticas de ciberseguridad en el entorno empresarial e institucional

c. Contenidos y materiales de aprendizaje

- Puntos clave para la gestión eficiente de la ciberseguridad: control de acceso, gestión de back-ups, etc.
- Dispositivos y sistemas involucrados: dispositivos móviles, redes, IOT.
- Buenas prácticas personales llevadas al entorno empresarial.
- Implementación de un Plan Director de Seguridad.

d. Métodos docentes

La metodología de este bloque es mixta:

- Sesión magistral o exposición de contenidos que se complementa con diferentes materiales (documentación, enlaces web, etc).
- Aula invertida.
- Así mismo, se pondrá a disposición del alumnado una sesión de tutoría grupal. Por otra parte, se resolverán las dudas individuales mediante tutorías, participación en foros y/o correo electrónico.

La evaluación se realizará a través de diferentes actividades individuales: elaboración y presentación de carpeta de aprendizaje y/o cuestionarios de evaluación.

e. Bibliografía básica

Andress, J., Cyber Warfare (2013). Techniques, Tactics and Tools for Security Practitioners.
Graham, J.. Howard, R., Olson, R. (2011). Cyber Security Essentials.
Stallings, W., Brown, L. (2018). Computer Security - Principles and Practice.

f. Bibliografía complementaria

Enlaces web a las guías y estándares de los organismos oficiales.

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros, emails
  - Sala videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
Bloque III – 0.5 ECTS	Semanas 6-7

5. Metodología de enseñanza y dedicación del estudiante a la asignatura

Actividad Formativa	Competencias relacionadas	Horas	Presencialidad (%)
Clases, conferencias y técnicas expositivas	CG2, CSD1, CSD3, CSD4	12	0
Actividades autónomas y en grupo (trabajos y lecturas dirigidas)	CSD1, CSD3, CSD4	45	0
Pruebas de seguimiento y presentación/ exposición de trabajos	CSD1, CSD3, CSD4	10	50
Tutoría individual, participación en foros y otros medios colaborativos	CG2, CSD1, CSD3, CSD4	8	0

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque I	1	Semanas 1-4
Bloque II	1.4	Semanas 3-7
Bloque III	0.6	Semanas 6-7

7. Evaluación

Instrumento / Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Evaluación sumativa, que incluye pruebas parciales individuales y prueba final	30%	30%
Realización de trabajos, proyectos, resolución de problemas y casos	50%	50%
Foros y participación	20%	20%

Criterios / Comentarios a la evaluación
• **Convocatoria ordinaria:** En cada prueba/actividad de evaluación se exigirá una calificación mínima para que la misma pueda formar parte de la evaluación continua. Este valor se fijará al comienzo del curso. Cualquier tarea copiada o plagiada obtendrá la calificación 0. Las actividades se han de entregar en tiempo y forma. La asignatura se supera sumando 50 puntos o más entre todas las actividades de evaluación computables en la evaluación continua. • **Convocatoria extraordinaria:** En la segunda convocatoria se realizará una prueba de evaluación que permita comprobar que se han adquirido las competencias desarrolladas en la asignatura, pudiendo conservar la calificación de algunas de las tareas incluidas en la carpeta de aprendizaje.

9. Consideraciones / Comentarios adicionales