Guia docente				
Datos Identificativos				2023/24
Asignatura (*)	Seguridad en Centros de Datos		Código	614530113
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Optativa	3
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da Información			
Coordinador/a	López Rivas, Antonio Daniel	Correo electrónico	daniel.lopez@udc.es	
Profesorado	López Rivas, Antonio Daniel	Correo electrónico	daniel.lopez@udc.es	
Web	moovi.uvigo.es			
Descripción general	La seguridad en un centro de procesamiento de datos implica la implementación de una variedad de medidas físicas y lógicas para proteger la infraestructura y los datos almacenados en el CPD, con el objetivo de garantizar la disponibilidad, confidencialidad e integridad de la información y los sistemas críticos para una organización. En esta asignatura se realizará una introducción a las distintas arquitecturas de centros de datos así como a las instalaciones física auxiliares que son necesarias para su funcionamiento.			

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A33	HD-13 - Aplicar herramientas de virtualización de infraestructuras en Centros de Procesado de Datos, así como utilizar herramientas para la monitorización de sus infraestructuras y servicios
B29	K-13 - Interpretar los conceptos fundamentales, tipología y evolución de la arquitectura de los centros de procesos de datos (CPD) desde una visión centrada en la seguridad de la infraestructura física, así como las técnicas básicas de seguridad en CPD como son virtualización, fortificación de elementos físicos y lógicos y securización de datos
C7	C-02 - Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
C10	C-05 - Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Obtener el conocimiento necesario sobre las distintas arquitecturas de Centros de Proceso de Datos (CPD) y elementos auxiliares que lo conforman		BP29	
Conocer como la virtualización (computo, almacenamiento y red de comunicaciones) facilita la mejora de la seguridad en el CPD y como lo hace	AP33		
Utilizar herramientas para virtualización de infraestructuras de cómputo, almacenamiento y comunicaciones	AP33		CP7
Conocer como fortificar todos los elementos, tanto físicos como lógicos, para que no supongan un riesgo en la seguridad			CP10 CP15
Conocer como securizar los datos de la organización, principal activo de la misma			CP10 CP15

Contenidos

Tema	Subtema
Infraestructuras de centros de procesos de datos (CPD)	Arquitectura de los centros de datos: topologías físicas y lógicas, supercomputadores, hipervisores de virtualización y computación en la nube Instalaciones físicas auxiliares: energía, acceso, climatización, extinción de incendios.
Virtualización	Introducción a los hipervisores Fortificación de infraestructura física e hipervisores Virtualización de servicios: fortificación de máquinas virtuales y microservicios, redundancia y migración, escalado de servicios, seguridad como servicio (SECaaS), redes virtuales
Seguridad en centros de procesos de datos	Seguridad física y lógica Seguridad de los datos: replicación y codificación, almacenamiento y encriptación hardware. Estrategias y herramientas para copias de seguridad
Gestión de la seguridad	Gestión AAA, modelo integral de seguridad (ITIL, 27000,27002), auditorías y conformidad legal Gestión de incidentes en centros de procesos de datos

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	B29 C10 C15	10	20	30
Trabajos tutelados	A33 C7 C10 C15	1	12	13
Prueba objetiva	A33 B29 C7 C10 C15	2	0	2
Prácticas de laboratorio	A33 C7 C10 C15	10	20	30
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	Descripción
Sesión magistral	Docencia expositiva. Presentaciones de los conocimientos teóricos de las asignaturas fomentando la interacción con los alumnos. NOTA: será posible utilizar una de estas sesiones para realizar un taller para una empresa o persona colaboradora de reconocida competencia.
Trabajos tutelados	Trabajo a desarrollar por el alumno sobre uno de los temas de la asignatura a propuesta del alumno o del profesor. Este trabajo será supervisado por el profesorado y el alumno hará una breve defensa presencial del mismo.
Prueba objetiva	Prueba escrita para evaluar los conocimientos adquiridos. Aunque se centrará en la materia de la docencia expositiva, se podrán incorporar algunas cuestiones relacionadas con las sesiones prácticas.
Prácticas de laboratorio	Sesiones prácticas informáticas asociadas a escenarios de virtualización, monitorización y fortificación/seguridad. El objetivo es poner en práctica los conocimientos de las sesiones magistrales fomentando el aprendizaje autónomo.

Atención personalizada	
Metodologías	Descripción

Prácticas de laboratorio Trabajos tutelados	La atención personalizada se centra en apoyar al alumno en la comprensión de las diferentes técnicas mediante el apoyo en las tutorías y la resolución de dudas que puedan surgir en las clases magistrales. También se te ayudará en las dudas que te surjan durante la práctica y el aprendizaje mediante trabajos tutelados para un mejor aprovechamiento y comprensión de los conocimientos adquiridos en clase.

Evaluación			
Metodologías	Competencias / Resultados	Descripción	Calificación
Prácticas de laboratorio	A33 C7 C10 C15	Sesiones prácticas informáticas asociadas a escenarios de virtualización, monitorización y fortificación/seguridad. El objetivo es poner en práctica los conocimientos de las sesiones magistrales fomentando el aprendizaje autónomo. La evaluación será continua a través de las sesiones. NOTA: Será posible utilizar algunas de las sesiones presenciales para realizar un taller de una entidad colaboradora.	40
Trabajos tutelados	A33 C7 C10 C15	Prueba escrita para evaluar los conocimientos adquiridos. Aunque se centrará en el tema de la enseñanza expositiva, se podrán incorporar algunos temas relacionados con las sesiones prácticas.	20
Prueba objetiva	A33 B29 C7 C10 C15	Prueba escrita para evaluar los conocimientos adquiridos. Aunque se centrará en la materia de la docencia expositiva, se podrán incorporar algunas cuestiones relacionadas con las sesiones prácticas.	40

Observaciones evaluación

Para superar la materia, será preciso obtener un mínimo de 4 sobre 10 tanto en la prueba objetiva como en los trabajos prácticos. En caso contrario, la nota máxima que se podrá alcanzar será de 4.5. La nota obtenida en la evaluación continua de prácticas de laboratorio y trabajos tutelados será conservado durante todo el curso académico.

FORMA DE TRABAJO

Tanto las prácticas de laboratorio como los trabajos tutelados serán realizados en grupos, los tamaños de los grupos será impuestos por el profesorado mientras que los integrantes de los mismos serán de libre elección.

FECHAS DE ENTREGA:

i) Prácticas de laboratorio: las memorias de las prácticas de laboratorio serán entregadas en la plataforma virtual de docencia antes de finalizar el período de clases y con tiempo suficiente para ser evaluadas por los profesores antes del comienzo del período de examenes. El número de entregas será propuesto a través de la plataforma virtual de docencia.

ii) Trabajos tutelados: deberán ser entregado con anterioridad a la última sesión práctica, la cual será utilizada para hacer las exposiciones de los mismos. La fecha final de entrega será propuesta a través de la plataforma virtual de docencia.

ESTUDIANTADO QUE NO PARTICIPÓ EN LA EVALUACIÓN CONTÍNUA DE PRÁCTICAS Y TRABAJOS TUTELADOS:

i) Cuando el estudiante se presente en la convocatoria de primera oportunidad, su nota será de 0 en ambas metodologías.

ii) Cuando el estudiante se presente en la convocatoria de segunda oportunidad o convocatoria extraordinaria, sin participar en el proceso de evaluación continua, a través de estas metodologías, podrá realizar de forma individual las prácticas con el material disponible, en la plataforma virtual de docencia mediante la solicitud de tutorías con los profesores de la asignatura.

ESTUDIANTADO QUE NO PARTICIPA EN LA PRUEBA OBJETIVA EN LA PRIMERA OPORTUNIDAD: Participaran o no en el proceso de evaluación continua de prácticas y trabajo tutelado, su calificación será de "No Presentado".

Como ocurre en todos los aspectos docentes, queremos recordar que se cumplirá la normativa vigente de la UDC respecto a plagio, fraudes en la evaluación e igualdad.

Fuentes de información

Básica	- Maurizio Portolani (2003). Data Center Fundamentals. CiscoPress - Tom Clark (2003). Designing Storage Area Networks. A Practical Reference for Implementing Fibre Channel and Ip SANs. Addison-Wesley - Ulf Troppens (2009). Storage Networks Explained. Willey Publishing - Christopher Poelker, Alex Nikitin (2008). Storage Area Networks for dummies. Willey Publishing - Matthew Portnoy (2016). Virtualization Essentials. 2nd Edition. Sybex - José Luis Raya Cabrera et al (2009). Guía de campo [de] máquinas virtuales. Ra-ma - Marshall, Nick et al. (2019). Mastering VMware VSphere 6.7. Sybex - Luis Gómez, Ana Andrés (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Aenor
Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios
Se recomienda al alumno, para un aprovechamiento óptimo de la materia, el seguimiento activo de las clases así como la participación en las diferentes actividades y la utilización de una atención personalizada para resolver las dudas o cuestiones que puedan surgir.

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías