Guía Docente				
Datos Identificativos				2023/24
Asignatura (*)	Seguridade en Centros de Datos		Código	614530113
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Optativa	3
Idioma	CastelánGalego			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da Información			
Coordinación	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			
Descrición xeral	A seguridade nun centro de procesamento de datos implica a implantación dunha variedade de medidas físicas e lóxicas para protexer a infraestrutura e os datos almacenados no CPD, co obxectivo de garantir a dispoñibilidade, confidencialidade e integridade da información e sistemas críticos para unha organización. Nesta materia farase unha introdución ás diferentes arquitecturas de centros de datos así como ás instalacións físicas auxiliares necesarias para o seu funcionamento. Traballaremos coas tecnoloxías de virtualización máis estendidas no mundo empresarial e confiaremos nelas para fortalecer o noso centro de procesamento de datos, os servizos que se ofrecen dende el e os datos que nel se aloxan.			

Competencias do título	
Código	Competencias do 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 da aprendizaxe			
Resultados de aprendizaxe	Competencias do título		
Adquirir os coñecementos necesarios sobre as diferentes arquitecturas dos Centros de Proceso de Datos (CPD) e os elementos auxiliares que o integran.		BP29	
Coñecer como a virtualización (informática, almacenamento e rede de comunicacións) facilita a mellora da seguridade no CPD e como o fai.	AP33		
Utilizar ferramentas para a virtualización de infraestruturas de computación, almacenamento e comunicacións	AP33		CP7
Saber fortalecer todos os elementos, tanto físicos como lóxicos, para que non supoñan un risco de seguridade			CP10 CP15
Saber protexer os datos da organización, o seu principal activo			CP10 CP15

Contidos	
Temas	Subtemas
Infraestruturas de centros de procesamento de datos (CPD)	Arquitectura do centro de datos: topoloxías físicas e lóxicas, supercomputadoras, hipervisores de virtualización e Computación na nube Instalacións físicas auxiliares: enerxía, accesos, climatización, extinción de incendios.
Virtualización	Introdución aos hipervisores Fortalecemento de infraestruturas físicas e hipervisores Virtualización de servizos: fortalecemento de máquinas virtuais e microservizos, redundancia e migración, escalado de servizos, seguridade como servizo (SECaaS), redes virtuais
Seguridade nos centros de procesamento de datos	Seguridade física e lóxica Seguridade dos datos: replicación e cifrado, almacenamento e cifrado de hardware. Estratexias e ferramentas de copia de seguridade
Xestión da seguridade	Xestión AAA, modelo de seguridade integral (ITIL, 27000,27002), auditorías e cumprimento legal Xestión de incidencias en centros de procesamento de datos

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Sesión maxistral	B29 C10 C15	10	20	30
Traballos tutelados	A33 C7 C10 C15	1	12	13
Proba obxectiva	A33 B29 C7 C10 C15	2	0	2
Prácticas de laboratorio	A33 C7 C10 C15	10	20	30
Atención personalizada		0		0
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	Descrición
Sesión maxistral	Docencia expositiva. Presentacións dos coñecementos teóricos dos temas da materia promovendo a interacción cos estudantes. NOTA: será posible utilizar algunha destas sesións para realizar algún obradoiro de empresa ou persoa colaboradora de recoñecida competencia.
Traballos tutelados	Traballo a desenvolver polo alumno sobre algunha das temáticas da materia a proposta do propio estudante ou do profesor. Este traballo terá seguimento por parte do profesorado e o estudante fará unha breve defensa presencial do mesmo
Proba obxectiva	Proba escrita para valorar os coñecementos adquiridos. Aínda que se centrará no material da docencia expositiva, poderá incorporar algunhas cuestións relacionadas coas sesións prácticas.
Prácticas de laboratorio	Sesións prácticas en computador asociadas a escenarios de virtualización, monitorización e fortificación/seguridade. O obxetivo é poñer en práctica os coñecementos das sesións maxistrais fomentando a aprendizaxe autónoma.

Atención personalizada	
Metodoloxías	Descrición

Prácticas de laboratorio Traballos tutelados	A atención persoalizada está enfocada a apoiar ó alumno na comprensión das diferentes técnicas mediante o apoio nas titorías e a resolución de dúbidas que podan xurdir nas clases maxistrais. Tamén se lle prestará axuda nas dúbidas que poidan xurdir durante a realización das prácticas e a aprendizaxe mediante traballos tutelados para un mellor aproveitamento e comprensión dos coñecementos acadados na clase.

Avaliación			
Metodoloxías	**Competencias**	**Descrición**	**Cualificación**
Prácticas de laboratorio	A33 C7 C10 C15	Sesións prácticas en computador asociadas a escenarios de virtualización, monitorización e fortificación/seguridade. O obxetivo é poñer en práctica os coñecementos das sesións maxistrais fomentando a aprendizaxe autónoma.. A avaliación será contínua perante as sesións. NOTA: Será posible utilizar algunha das sesións presenciais para realizar algún taller dunha entidade colaboradora.	40
Traballos tutelados	A33 C7 C10 C15	Traballo a desenvolver polo alumno sobre algunha das temáticas da materia a proposta do propio estudante ou do profesor. Este traballo terá seguimento por parte do profesorado e o estudante fará unha breve defensa presencial do mesmo.	20
Proba obxectiva	A33 B29 C7 C10 C15	Proba escrita para valorar os coñecementos adquiridos. Aínda que se centrará no material da docencia expositiva, poderá incorporar algunhas cuestións relacionadas coas sesións prácticas.	40

Observacións avaliación

Para superar a materia será necesario obter un mínimo de 4 sobre 10 tanto na proba obxectiva como no traballo práctico. En caso contrario, a nota máxima que se poderá acadar será de 4,5. A nota obtida na avaliación continua de prácticas de laboratorio e traballos tutelados conservarase ao longo do curso académico.

MODO DE TRABALLO

Tanto as prácticas de laboratorio como os traballos titorizados realizaranse en grupo, os tamaños dos grupos serán impostos polo profesorado mentres que os membros do mesmo serán de libre elección.

DATAS DE ENTREGA:

i) Prácticas de laboratorio: as memorias das prácticas de laboratorio entregaranse na plataforma virtual de docencia antes do remate do período lectivo e con tempo suficiente para ser avaliadas polo profesorado antes do inicio do período de exames. O número de entregas proporase a través da plataforma virtual de docencia.

ii) Traballos tutelados: deberán entregarse antes da última sesión práctica, que servirá para realizar as súas exposicións. A data definitiva de entrega proporase a través da plataforma virtual de docencia.

ESTUDANTADO QUE NON PARTICIPOU NA AVALIACIÓN CONTINUA DE PRÁCTICAS E TRABALLOS TITORIZADOS:

i) Cando o alumno compareza na primeira convocatoria de oportunidade, a súa cualificación será de 0 en ambas as metodoloxías.

ii) Cando o alumno/a concorra á convocatoria de segunda oportunidade ou convocatoria extraordinaria, sen participar no proceso de avaliación continua, mediante estas metodoloxías, poderá realizar as prácticas de forma individualizada co material dispoñible, na plataforma virtual docente. solicitando titorías cos profesores da materia.

ESTUDANTADO QUE NON PARTICIPA NA PROBA OBXECTIVO DE PRIMEIRA OPORTUNIDADE: Participa ou non no proceso de avaliación continua de prácticas e traballos titorizados, a súa cualificación será "Non Presentado".

PLAXIO: No caso de detectar plaxio en calquera proba ou material entregado, a cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos.

Fontes de información

Bibliografía 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
Bibliografía complementaria	

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións
Recoméndase ó estudante, para un aproveitamento óptimo da materia, un seguimento activo das clases así como participar nas distintas actividades e o uso da atención personalizada para a resolución das dúbidas ou cuestións que lle poidan xurdir.