PLAN DOCENTE DE LA ASIGNATURA

Curso académico: 2026/2027

Identificación y características de la asignatura					
Código	402420				
Denominación (español)	**Seguridad en Sistemas Distribuidos y HPC**				
Denominación (inglés)	**Security in Distributed Systems and HPC**				
Titulaciones	**Máster en Ingeniería Informática**				
Centro	Escuela Politécnica				
Módulo	Sistemas Distribuidos y Cloud Computing				
Materia	Sistemas Distribuidos y Cloud Computing				
Carácter	Obligatoria	ECTS	6	Semestre	2º

Profesorado		
Nombre	Despacho	Correo-e
Lorenzo M. Martínez Bravo	Despacho 7, Edificio de Informática	lorenzom@unex.es
Área de conocimiento	Ingeniería Telemática	
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos	
Nombre	Despacho	Correo-e
David Rodríguez Lozano	Despacho 3 Edificio de Investigación	drlozano@unex.es
Área de conocimiento	Arquitectura y Tecnología de los Computadores	
Departamento	Tecnología de los Computadores y de las Comunicaciones	
Coordinador	Lorenzo M. Martínez Bravo	

Competencias / Resultados de aprendizaje

- C02 - Al finalizar el aprendizaje, el o la estudiante será capaz de determinar los conceptos, arquitecturas y modelos informáticos, matemáticos, estadísticos y de ingeniería más apropiados para la resolución de problemas de comunicaciones y servicios distribuidos

complejos. TIPO: Conocimientos o contenidos.

- COM09 - Al finalizar el aprendizaje, el o la estudiante será capaz de evaluar las necesidades de un producto, sistema o infraestructura para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen su ejecución y comunicación efectiva y segura en un sistema local, distribuido o en nube. TIPO: Competencias.
- COM10 - Al finalizar el aprendizaje, el o la estudiante será capaz de diseñar modelos, sistemas, soluciones, protocolos y algoritmos en un entorno complejo de sistemas distribuidos conectados en red. TIPO: Competencias.
- HB06 - Al finalizar el aprendizaje, el o la estudiante será capaz de aplicar las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario, así como los servicios necesarios para la comunicación local, distribuida y en nube en la resolución de problemas que usen sistemas. informáticos en organizaciones de cualquier tipo y sector. TIPO: Habilidades o destrezas.
- HB07 - Al finalizar el aprendizaje, el o la estudiante será capaz de implementar, configurar e integrar sistemas de comunicaciones por cable, línea y satélite en entornos fijos y móviles, así como de seleccionar y aplicar los protocolos de red y de aplicación adecuados a cada medio para la implementación de soluciones IoT. TIPO: Habilidades o destrezas.
- COM11 - Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo. TIPO: Competencias

Contenidos

Descripción general del contenido: Se abordará la seguridad integral en arquitecturas distribuidas y entornos de alto rendimiento (HPC), analizando desde la protección de componentes como APIs, contenedores y microservicios hasta la gestión avanzada de identidades federadas y mecanismos de autenticación para grandes volúmenes de usuarios.

Se profundizará en estrategias de resiliencia y recuperación ante desastres, así como en la mitigación de vulnerabilidades específicas de clústeres y supercomputadores, garantizando la confidencialidad de datos sensibles mediante cifrado, así como nuevas tecnologías para asegurar la seguridad en escenarios post-cuánticos.

Temario

Tema 1: Fundamentos de ciberseguridad en arquitecturas distribuidas yHPC.

Contenidos: Visión general de la seguridad integral en sistemas distribuidos y supercomputación. La tríada CIA en entornos de alta concurrencia. Modelos de riesgo, cumplimiento normativo y adaptación de marcos de control de

seguridad (alineados con NIST) para grandes infraestructuras científicas y empresariales.

Actividad teórica: Análisis de incidentes de seguridad reales en infraestructuras distribuidas y grandes clústeres, evaluando fallos en el diseño inicial y su correlación con los controles de riesgo estándar.

Actividad práctica: Elaboración de una matriz de riesgos y análisis de impacto orientada a una arquitectura distribuida heterogénea.

Tema 2: Seguridad en componentes: APIs, contenedores y microservicios.

Contenidos: Protección y control de puntos de entrada mediante APIs seguras en sistemas distribuidos. Aislamiento de aplicaciones, gestión de riesgos en imágenes base y orquestación segura de microservicios y contenedores en entornos de alto rendimiento.

Actividad teórica: Estudio de los vectores de ataque más comunes en APIs distribuidas y vulnerabilidades críticas asociadas al aislamiento de microservicios.

Actividad práctica: Auditoría de seguridad y escaneo de vulnerabilidades en un despliegue de microservicios contenerizados, aplicando restricciones de red y políticas de privilegios mínimos.

Tema 3: Gestión avanzada de Identidades federadas y autenticación a gran escala.

Contenidos: Mecanismos de autenticación y autorización para grandes volúmenes de usuarios concurrentes. Protocolos de identidad federada (SAML, OAuth 2.0, OIDC), gestión de accesos basados en atributos (ABAC) y control de credenciales en clústeres distribuidos.

Actividad teórica: Comparativa analítica entre los modelos de federación de identidades tradicionales y los esquemas descentralizados aptos para comunidades científicas globales.

Actividad práctica: Configuración de un proveedor de identidad federada simulado para la autenticación centralizada de usuarios en un clúster de computación distribuida.

Tema 4: Mitigación de vulnerabilidades en clústeres y supercomputadores.

Contenidos: Identificación y mitigación de vulnerabilidades específicas a nivel de nodo de cálculo y supercomputador. Seguridad en redes de interconexión de baja latencia, prevención de ataques de denegación de servicio y control de ejecuciones maliciosas de código.

Actividad teórica: Estudio técnico sobre el impacto de brechas de seguridad físicas y lógicas en la infraestructura base de un supercomputador.

Actividad práctica: Simulación de políticas de control de acceso obligatorio y segmentación de tráfico en redes de interconexión para blindar nodos de cálculo compartidos.

Tema 5: Confidencialidad de datos sensibles y cifrado en entornos distribuidos.

Contenidos: Estrategias avanzadas para garantizar la confidencialidad de datos sensibles tanto en tránsito como en reposo. Sistemas de almacenamiento paralelo seguro y técnicas de procesamiento de datos cifrados en arquitecturas distribuidas masivas.

Actividad teórica: Revisión de normativas y estándares tecnológicos para el cifrado de volúmenes de almacenamiento masivo y bases de datos distribuidas.

Actividad práctica: Implementación de un flujo de cifrado extremo a extremo y gestión de claves criptográficas para proteger conjuntos de datos sensibles en un entorno distribuido.

Tema 6: Resiliencia, continuidad de negocio y recuperación de desastres.

Contenidos: Estrategias de resiliencia frente a fallos sistémicos o ataques dirigidos en infraestructuras distribuidas. Mecanismos de tolerancia a fallos, replicación de estados, alta disponibilidad y planes estructurados de recuperación ante desastres.

Actividad teórica: Diseño de arquitecturas tolerantes a fallos y análisis de métricas de recuperación (RTO y RPO) aplicadas a supercomputación y sistemas distribuidos críticos.

Actividad práctica: Simulación de un escenario de caída catastrófica de un nodo coordinador en un sistema distribuido y ejecución del protocolo de conmutación por error y restauración de datos.

Tema 7: Criptografía Post-Cuántica en infraestructuras críticas y HPC.

Contenidos: Amenazas de la computación cuántica sobre los algoritmos criptográficos actuales (RSA, ECC). Nuevas tecnologías, algoritmos resistentes a la computación cuántica estandarizados por el NIST y su impacto en la seguridad a largo plazo de sistemas distribuidos y HPC.

Actividad teórica: Estudio de las vulnerabilidades del cifrado asimétrico clásico frente al algoritmo de Shor y evaluación de los nuevos estándares criptográficos post-cuánticos.

Actividad práctica: Evaluación e integración experimental de primitivas o algoritmos criptográficos post-cuánticos en un canal de comunicación simulado de una arquitectura distribuida.

Tema 8: Gobernanza, auditoría y nuevos paradigmas de seguridad integral.

Contenidos: Supervisión continua, monitorización de eventos a gran escala, detección de anomalías y auditorías de cumplimiento normativo. Gobernanza de la seguridad en infraestructuras federadas complejas y superfacilidades.

Actividad teórica: Desarrollo de marcos de respuesta a incidentes de seguridad adaptados a entornos de computación distribuida de gran escala.

Actividad práctica: Proyecto integrador final: Auditoría integral de seguridad de una arquitectura distribuida y HPC simulada, evaluando componentes, identidades, cifrado y resiliencia, con su respectiva propuesta de mejora.

Actividades formativas

		Actividades Presenciales (AP)					Actividades Virtuales (AV)					
TEMA	**TOTAL**	**GG**	**CH**	**L**	**O**	**S**	**CST**	**CSP**	**CAT**	**CAP**	**TP**	**TA**
1	15	2			1				2	2		8
2	18	2			2				2	2		10
3	19	2			2				2	2		11
4	19	2			2				2	2		11
5	19	2			2				2	2		11
6	19	2			2				2	2		11
7	15	1			2				2	2		8
8	11	1			1				1	1		7
Evaluación	15	1			1							13
Totales	**150**	15			15				15	15		90
		% Presencialidad					% Virtualidad					

Actividades Presenciales (AP)

Actividades que se desarrollan en un único espacio físico y que implican interacción física entre estudiante y docente:

- GG: Grupo Grande (85 estudiantes).
- CH: Actividades de prácticas clínicas hospitalarias (7 estudiantes)
- L: Actividades de laboratorio o prácticas de campo (15 estudiantes)
- O: Actividades en sala de ordenadores o laboratorio de idiomas (20 estudiantes)
- S: Actividades de seminario o de problemas en clase (40 estudiantes).

Actividades Virtuales (AV)

Actividades que no se desarrollan en un espacio físico común. Pueden ser síncronas (implican interacción estudiante / docente) o asíncronas:

- CST: Clase síncrona teórica.
- CSP: Clase síncrona práctica.
- CAT: Clase asíncrona teórica.
- CAP: Clase asíncrona práctica.

- TP: Tutorías Programadas (seguimiento docente, tutorías ECTS).
- TA: Trabajo autónomo del estudiante.

Metodologías docentes

1. Docencia basada en clases expositivas para la presentación de los contenidos de la asignatura.
2. Actividades prácticas, sesiones de laboratorio guiadas, seminarios de resolución de problemas, etc. en grupos bajo la dirección de un profesor.
3. Seguimiento síncrono del aprendizaje del estudiante.
4. Realización de actividades, trabajos y estudio por parte del estudiante.
5. Metodologías centradas en el alumnado como el Aprendizaje basado en Proyectos (ABP), Aprendizaje basado en Equipos (TBL), Aula Invertida, Aprendizaje Cooperativo, Gamificación, etc.

Sistemas de evaluación

De acuerdo con la normativa de la UEx, la asignatura puede evaluarse mediante modalidad de evaluación continua o mediante la modalidad de evaluación global. El estudiante elegirá una de ellas al inicio del periodo de docencia de la asignatura. En el caso de no elegirla, se entiende que opta por la modalidad de evaluación continua.

Mecanismos de evaluación:

1. Examen: pruebas objetivas, semi-objetivas, de desarrollo escrito u oral y resolución de problemas sobre los conocimientos adquiridos en la asignatura. Estos instrumentos de evaluación se realizarán de forma presencial en las instalaciones del centro.
2. Evaluación de trabajos dirigidos y evidencias: corrección, y/o pruebas objetivas o semi-objetivas, de desarrollo escrito u oral, sobre los trabajos dirigidos, cuadernos de prácticas, memorias técnicas y trabajos realizados en los proyectos.

Criterios de evaluación:

1. **Examen final de la asignatura (ET):** Examen escrito teórico/práctico de los contenidos y actividades teóricas de la asignatura.
2. **Actividades teórico/prácticas (ATP):** Media ponderada de las calificaciones obtenidas en las diferentes actividades teórico/prácticas desarrolladas en la asignatura.

Nota final = 40% ET +60% ATP

Se deben superar ambas partes por separado (nota mayor o igual a 5), aunque se establece la posibilidad de compensar (siempre para notas mayores o iguales a 4).

Cualquier comportamiento fraudulento en cualquiera de las pruebas y/o actividades, supondrá una calificación de Suspenso (0), amén de las acciones que se establecen en la normativa de evaluación de la UEx.

Bibliografía (básica y complementaria)

- Cybersecurity and High-Performance Computing Environments, Kuan-Ching Li, Nitin Sukhija, Elizabeth Bautista, Jean-Luc Gaudiot, CRC Press, 2022.
- Patni, J. C. & Bahadure, N. B. (Eds.). High-Performance Computing and Sustainability Through Artificial Intelligence. Bentham Books, 2026.
- Rice, L. Container Security, 2ª ed. O'Reilly, 2025.
- Paar, C., Pelzl, J. & Güneysu, T. Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, 2ª ed. Springer, 2024.
- Saarinen, M.-J. & Smith-Tone, D. (Eds.). Post-Quantum Cryptography-PQCrypto 2024 (LNCS 14771/14772). Springer, 2024.
- Sarker, I. H. (Ed.). AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. Springer, 2024.
- Cybersecurity and Human Capabilities Through Symbiotic Artificial

Intelligence, ICGS3 2024, Springer.

- Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
- Tanenbaum, Andrew S., & Van Steen, Maarten. Distributed Systems: Principles and Paradigms. Pearson, 2020.
- Security in network functions virtualization, Zhang, Zonghua; Meddahi, Ahmed, 2017.
- NIST Special Publication 800 NIST SP 800-234 High-Performance Computing (HPC) Security Overlay, 2026.
- NIST Special Publication 800 NIST SP 800-223 High-Performance Computing Security, 2024.
- NIST Special Publication 800 NIST SP 800-190 Application Container Security Guide.

Otros recursos y materiales docentes complementarios

Material disponible en el aula virtual del Campus Virtual de la UEX.