1. DATOS BÁSICOS

Asignatura	Seguridad en Bases de Datos
Titulación	Grado en Ingeniería de la Ciberseguridad
Escuela/ Facultad	Ingeniería y Arquitectura
Curso	Tercero
ECTS	6 ECTS
Carácter	Obligatoria
Idioma/s	Español
Modalidad	Online
Semestre	S6
Curso académico	2024-2025
Docente coordinador	Álvaro Manuel Rodríguez Rodríguez
Docente	Álvaro Manuel Rodríguez Rodríguez

2. PRESENTACIÓN

La asignatura Seguridad en Bases de Datos proporciona al estudiante un conocimiento especializado sobre las técnicas, tecnologías y estrategias necesarias para garantizar la protección de la información almacenada en bases de datos. Se abordan aspectos clave como la confidencialidad, integridad y disponibilidad (la tríada CIA), el control de accesos, el cifrado, las auditorías, la gestión de usuarios y roles, y la recuperación ante desastres. Además, se estudian herramientas actuales como Sqlmap, Sleuth o Wapiti, fundamentales para el análisis y refuerzo de la seguridad en entornos reales. La asignatura tiene un enfoque práctico y aplicado, con ejemplos de ataques y soluciones adoptadas en la industria.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CB1: Que los estudiantes hayan demostrado poseer y comprender conocimientos en el área de la ciberseguridad, incluidos los relacionados con la seguridad de bases de datos.
- CB2: Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de forma profesional.
- CB3: Que los estudiantes puedan reunir e interpretar datos relevantes para emitir juicios en materia de seguridad informática.

Competencias transversales:

- CT1: Uso avanzado de las TIC para la búsqueda, análisis y gestión de la información.
- CT2: Adaptación a situaciones imprevistas o estresantes, transformándolas en oportunidades de mejora.
- CT3: Comunicación eficaz de problemas, soluciones y resultados, tanto oralmente como por escrito, en contextos técnicos.

Competencias específicas:

- CP05. Diseñar, desarrollar y mantener técnicas y soluciones para la protección de los datos (almacenados, procesados o en tránsito), considerando en todo momento la privacidad de éstos.
- CP10. Aplicar y analizar los principios y técnicas basadas en la criptografía que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de la información, así como la autenticación y autorización de sus entidades.
- CP14. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.
- CP18. Adaptarse a situaciones adversas, inesperadas, que causen estrés, ya sean personales o profesionales, superándolas e incluso convirtiéndolas en oportunidades de cambio positivo.
- CP19. Mostrar comportamientos éticos y compromiso social en el desempeño de las actividades de una profesión, así como sensibilidad a la desigualdad y a la diversidad.

Resultados de aprendizaje:

- RA1. Describir los fundamentos de la seguridad en bases de datos y su evolución.
- RA2. Aplicar técnicas de control de acceso, cifrado, auditoría y respaldo de la información.
- RA3. Reconocer las implicaciones legales y éticas asociadas a la protección de datos.
- RA4. Implementar soluciones seguras frente a amenazas internas y externas en sistemas de gestión de bases de datos.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CB1, CP05, CP10	RA1, RA2
CB2, CT1, CP05, CP14	RA2, RA4
CB3, CT2, CP19	RA3, RA4
CT3, CP05, CP10, CP18	RA1, RA4

4. CONTENIDOS

La asignatura se estructura en seis unidades que cubren de forma integral los aspectos fundamentales y avanzados de la seguridad en bases de datos. En la Unidad 1, se abordan los principios avanzados de la seguridad en entornos de bases de datos, con especial atención a la triada CIA (confidencialidad, integridad y disponibilidad) y a los modelos de control de acceso como DAC, MAC y RBAC. En la Unidad 2, se profundiza en los mecanismos de control de acceso y las prácticas de autenticación segura, incluyendo la autenticación multifactor y la gestión de sesiones.

La Unidad 3 está dedicada a las técnicas de encriptación, enmascaramiento y protección de datos, con un enfoque práctico sobre algoritmos, gestión de claves y estrategias de protección en tránsito y en reposo. La Unidad 4 explora los procesos de auditoría, monitoreo y detección de anomalías mediante el uso de inteligencia artificial y aprendizaje automático. En la Unidad 5, se examinan los marcos legales y éticos vinculados a la protección de datos, así como el cumplimiento normativo. Finalmente, la Unidad 6 se centra en la planificación y respuesta ante incidentes de seguridad y en los procedimientos de recuperación de desastres que garanticen la resiliencia de los sistemas de bases de datos.

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

Las metodologías empleadas se basan en el aprendizaje activo y aplicado, incluyendo:

- Clases teóricas expositivas para introducir conceptos clave.
- Sesiones prácticas con herramientas reales del sector.
- Análisis de casos y resolución de problemas reales.
- Aprendizaje colaborativo mediante trabajos en grupo y simulaciones.
- Evaluación mediante prueba de conocimientos y actividades prácticas entregables.

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad virtual:

Actividad formativa	Número de horas
Clases magistrales	8
Seminarios de aplicación práctica	26
Elaboración de informes y escritos	10
Investigaciones y proyectos	38
Actividades en talleres/ laboratorios	12
Trabajo autónomo	50
Debates y coloquios	4
Pruebas presenciales de conocimiento	2
Total Actividades:	**150**

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad virtual:

Sistema de evaluación	%Min	%Max
Pruebas de evaluación virtuales	60%	60%
Informes y escritos	5%	10%
Observación del desempeño	0%	5%
Investigaciones y proyectos	10%	15%
Cuaderno de prácticas de laboratorio	10%	25%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Actividades evaluables	Fecha
Actividad 1.	Semana 18
Actividad 2.	Semana 18
Actividad 3.	Semana 18

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

La obra de referencia para el seguimiento de la asignatura es:

Doug N. (2020). Introduction to Database Security: Security Basics You Need to Know. Disponible en: https://www.poweradmin.com/blog/introduction-to-database-security-security-basics-you-need-to-know/

Lee J. (2023) Role-Based Access Control vs. Discretionary Access Control: A Comparison. Disponible en: https://www.secureidentityhub.com/access-control-vs-discretionary-access/

Alghawazi, M, et al. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. Journal of Cybersecurity and Privacy 2, no. 4: 764-777. https://doi.org/10.3390/jcp2040039

Atef M. (2023). How to Conduct a Vulnerability Assessment: A Step-by-Step Guide. Disponible en: https://medium.com/@m.atef_72234/how-to-conduct-a-vulnerability-assessment-a-step-by-step-guide-392200dc1786

Lee Jamie (2023). Role-Based Access Control vs. Discretionary Access Control: A Comparison. Disponible en: https://www.secureidentityhub.com/access-control-vs-discretionary-access/

MS-Learn (2024). What is Azure attribute-based access control (Azure ABAC)? Disponible en: https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

Nyakundi , H. (2023). Secure User Authentication Methods – 2FA, Biometric, and Passwordless Login Explained. Disponible en: https://www.freecodecamp.org/news/user-authentication-methods-explained/

Rennolds , N. (2024). 6 Best Multi-Factor Authentication (MFA) Solutions for 2024. Disponible en: https://www.techrepublic.com/article/best-multi-factor-authentication-solutions/

OWASP Top 10:2021(2024). A07:2021 – Identification and Authentication Failures.Disponible en: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

Palacios Katarina (2023). Session management best practices: what you need to know. Disponible en: https://screenconnect.connectwise.com/blog/remote-support-access/session-management-best-practices

Pius Okoth (2023). Session management security: Best practices for protecting user sessions. Disponible en: https://snyk.io/blog/session-management-security/

Entrust (2024). Everything You Need to Know About Encryption. Disponible en: https://www.entrust.com/resources/learn/encryption

European Commission (2022). Protection of databases. Digital Strategy - European Commission1. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/protection-databases

Jignesh J, (2023). Types of Database Encryption: Best Practices for Securing Your Data. Disponible en: https://www.redswitches.com/blog/encrypted-database/

Christiano, P. (2023). Top 8 Data Masking Techniques: Best Practices & Use Cases. Disponible en: https://expertbeacon.com/data-masking/

Satori Cyber (2021). Data Masking: 8 Techniques and How to Implement Them Successfully. Disponible en: https://satoricyber.com/data-masking/data-masking-8-techniques-and-how-to-implement-them-successfully/

Fortinet (2024). What Is Public Key Infrastructure (PKI)? Disponible en: https://www.fortinet.com/uk/resources/cyberglossary/public-key-infrastructure

Thales group (2024). What is the Encryption Key Management Lifecycle? Disponible en: https://cpl.thalesgroup.com/faq/key-secrets-management/what-encryption-key-management-lifecycle

Caldwell Ronald (2023). What is a Database Audit? Disponible en: https://www.liquidweb.com/kb/database-audit/

Codingdrills (2024). Database Auditing and Compliance. Disponible en: https://www.codingdrills.com/tutorial/database-tutorial/sec-auditing

Logic Monitor (2024). What Is Database Monitoring, and Why Is It Still Important? Disponible en: https://www.logicmonitor.com/blog/what-is-database-monitoring-and-why-is-it-still-important

Gardini Paulo (2024). 12 Best Database Monitoring Tools Reviewed For 2024. Disponible en: https://thectoclub.com/tools/best-database-monitoring-tools/

Chavan, V.D.; Yalagi, P.S. (2023). A Review of Machine Learning Tools and Techniques for Anomaly Detection. Disponible en: https://doi.org/10.1007/978-981-99-3982-4_34

Harshini (2023). Role of AI and ML in Transforming Database Security. Disponible en: https://www.analyticsinsight.net/role-of-ai-and-machine-learning-in-transforming-database-security/

Hewitt Nik (2023). A Predictive Future for Cybersecurity Analytics. Disponible en: https://truefort.com/predictive-cybersecurity-analytics/

Kime, C. (2023). 7 Database Security Best Practices: Database Security Guide. Disponible en: https://www.esecurityplanet.com/networks/database-security-best-practices/

Thompson, K. (2024). 10 Database Security Best Practices You Should Know. Disponible en: https://www.tripwire.com/state-of-security/database-security-best-practices-you-should-know

Lord Nate (2023). What is NIST SP 800-53? (Definition & Compliance Tips) - Digital Guardian. Disponible en: https://www.digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance

CyberInsight (2023). Exploring GRC: The Intersection of Governance, Risk, and Compliance in Cybersecurity. Disponible en: https://cyberinsight.co/what-is-grc-in-cyber-security/

Dalao, K. (2023). Understanding IT security frameworks: Types and examples. Disponible en: https://www.onetrust.com/blog/security-framework-types/

Fayayola, O. y Olorunfemi, O. (2024). Ethical decision-making in IT governance: A review of models and frameworks. International Journal of Scientific Research in Information Systems. Disponible en: https://mail.ijsra.net/sites/default/files/IJSRA-2024-0373.pdf

Hardin, G. y Roth, P. (2023). The ethics of managing people's data. Harvard Business Review. Disponible en: https://hbr.org/2023/07/the-ethics-of-managing-peoples-data

Informatica (n.d.). What is data stewardship. Informática. Disponible en: https://www.informatica.com/resources/articles/what-is-data-stewardship.html

Howell, D. (2023). How to choose the right storage medium for your organization's backup strategy. ITPro. Disponible en: https://www.itpro.com/infrastructure/backup/how-to-choose-the-right-storage-medium-for-your-organizations-backup-strategy

Kamat, S. (2023). Best practices for a comprehensive backup strategy. ConnectWise. Disponible en: https://www.connectwise.com/blog/business-continuity/backup-strategy-best-practices

Kost, E. (2023). How to create an incident response plan (detailed guide). Disponible en: https://www.upguard.com/blog/creating-a-cyber-security-incident-response-plan

OWASP (2024). Database security - OWASP cheat sheet series. Disponible en: https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html

Patida, A. (2024). Incident response vs. disaster recovery: What's the difference? Disponible en: https://www.loginradius.com/blog/identity/difference-between-incident-response-disaster-recovery/

Mather, D. (2023). Cracking the code: A deep dive into forensic analysis. Security Gladiators. Disponible en: https://securitygladiators.com/security/forensic-analysis/

National Institute of Standards and Technology (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). Disponible en: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

ReasonLabs (2024). What are forensic analysis? Cybersecurity investigation & analysis. Disponible en: https://cyberpedia.reasonlabs.com/EN/forensic%20analysis.html

Salvation DATA (2022). What is database forensics? Salvation DATA. Disponible en: https://www.salvationdata.com/knowledge/what-is-database-forensics/

10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.

Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tu opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.