Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: CONTROL DE ACCESO
Titulación: GRADO EN CIBERSEGURIDAD
Carácter: OBLIGATORIA.
Créditos ECTS: 6 ECTS
Curso: 1º
Distribución temporal: 2º SEMESTRE.
Idioma de impartición: CASTELLANO.
Equipo docente: Dr. Rufino Cabrera rufino.cabrera@euneiz.com
Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura esencial en el campo de la ciberseguridad, centrada en el estudio y la implementación de sistemas de control de accesos para la protección de información. A lo largo del curso, los estudiantes explorarán conceptos como identificación, autenticación, autorización y rendición de cuentas, y se enfrentarán a desafíos actuales como la seguridad en entornos cloud y el Internet de las Cosas (IoT). Mediante ejercicios prácticos y análisis de casos, adquirirán habilidades cruciales para diseñar y gestionar sistemas de control de accesos efectivos, adaptándose a las cambiantes necesidades de seguridad en el ámbito digital.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Conocimientos o contenidos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C3	Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	C4	Ejecutar técnicas de desarrollo y penetración analizando las mejoras técnicas, soluciones y buenas prácticas.
	C12	Conocer la nube, su seguridad y sus aplicaciones.
	C15	Utilizar la inteligencia artificial como herramienta necesaria para garantizar la seguridad.
Competencias (CO)	CO1	Usar y programar ordenadores, sistemas operativos, redes, bases de datos y el entorno de la nube para su aplicación en la ciberseguridad.
	CO3	Llevar a cabo distintos procesos de análisis en las diferentes áreas de la ciberseguridad.
	CO4	Realizar diseños de ingeniería aplicados a la ciberseguridad.
	CO5	Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.
	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO8	Analizar y ejecutar test de penetración en sistemas informáticos.
	CO11	Gestionar evidencias de vulnerabilidades.
	CO14	Comprender las vulnerabilidades de las nuevas tecnologías y aportar soluciones de ciberseguridad.
Habilidades o destrezas (H)	H2	Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H3	Ser hábil en la comunicación, tanto por escrito como oralmente, en inglés.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

• Módulo 1 - Introducción al Control de Accesos en Ciberseguridad

- Conceptos Básicos
  - Importancia del Control de Accesos
  - Componentes Clave
  - Tipos de Controles
  - Desafíos Actuales

- **Módulo 2 - Principios Básicos y Modelos de Control de Acceso**
    - Identificación, Autenticación y Autorización
    - Redención de Cuentas y Trazabilidad
    - Políticas y Procedimientos
    - Introducción a la Gestión de Identidades
    - Modelos de Control de Accesos
    - Contraste de Modelos
- **Módulo 3 - Sistemas de Identificación y Autenticación**
    - Fundamentos de la Identificación
    - Métodos de Autenticación
    - Autenticación Multifactor (MFA)
    - Sistemas Single Sign-On
- **Módulo 4 - Gestión de Privilegios y Administración de Cuentas**
    - Principios en la Gestión de Privilegios
    - Cuentas de Usuario y Grupos
    - Supervisión y Revisión de Privilegios
- **Módulo 5 - Auditoría y Monitoreo de Control de Accesos**
    - Fundamentos de la Auditoría en Control de Accesos
    - Herramientas y Técnicas de Monitoreo
    - Análisis y Correlación de Eventos
    - Auditoría en Diferentes Entornos
    - Gestión de Incidentes y Respuesta
    - Cumplimiento Normativo y Mejores Prácticas
- **Módulo 6 - Evaluación y Gestión de Riesgos en Control de Accesos**
    - Fundamentos de la Gestión de Riesgos
    - Evaluación de Riesgos
    - Mitigación y Contigencia
    - Monitoreo y Revisión Continua
- **Módulo 7 - Control de Accesos en Sistemas Operativos**
    - Logs en la Seguridad de diferentes Sistemas
    - Control de Accesos en Windows
    - Control de Accesos en Linux
    - Control de Accesos en MacOS
    - Estrategias de Seguridad de los diferentes SO
- **Módulo 8 - Seguridad en la Nube y Control de Accesos**
- **Módulo 9 - Implementación de Control de Accesos en Redes**
    - Control sw Accesos en Perímetros de Red
    - Seguridad de Red Inalámbrica

- Virtual Private Networks (VPN)
- Seguridad en la Capa de Transporte

• **Módulo 10 - Control de Accesos en Aplicaciones y Bases de Datos**

- Control de Accesos en Aplicaciones
- Gestión de Accesos en Bases de Datos
- API Security

• **Módulo 11 - Criptografía Aplicada al Control de Accesos**

- Introducción a la Criptografía
- Implementación del Cifrado Simétrico y Asimétrico
- Gestión de Claves
- Infraestructura de Clave Pública (PKI)
- Implementación de PKI en Control de Accesos
- Protocolos de Autenticación y Estándares de Criptografía
- Aplicaciones prácticas

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudios de caso.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	30	100
AF2: Clase prácticas.	16	100

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

AF3: Realización de trabajos (individuales y/o grupales).	6	50
AF3: Tutorías (individuales y/o grupales).	2,5	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	90,5	0
AF6: Pruebas de evaluación.	3	100
Total	**150**	**--**

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	10	35
SE3 Pruebas de evaluación y/o exámenes.	50	75

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).
- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el

profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.

- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)
Recursos audiovisuales
Material específico de la asignatura
Aula informatizada

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- "Access Control, Authentication, and Public Key Infrastructure" de Bill Ballad, Tricia Ballad, Erin Banks.
- "Access Control Systems: Security, Identity Management and Trust Models" de Messaoud Benantar.
- "Identity and Access Management: Business Performance Through Connected Intelligence" de Ertem Osmanoglu.

Bibliografía Complementaria

- "Digital Identity" de Phillip J. Windley.
- “El arte de la Invisibilidad” Kevin Mitnick.
- "Biometric Systems: Technology, Design and Performance Evaluation" por James L. Wayman, Anil K. Jain, Davide Maltoni, y Dario Maio.
- “El libro del Hacker. Edición 2022” De María Ángeles Caballero y Diego Cilleros Serrano.
- "Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations" de Morey J. Haber y Brad Hibbert.
- “Haz clic aquí para matarlos a todos” de Bruce Scheiner.

- "Operating System Security" de Trent Jaeger.

Otros Recursos de Aprendizaje Recomendados[3]

- https://www.nist.gov/
- https://www.shodan.io/
- https://www.wireshark.org/download.html
- https://www.first.org/cvss/
- https://attack.mitre.org/
- https://www.cisecurity.org/

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.