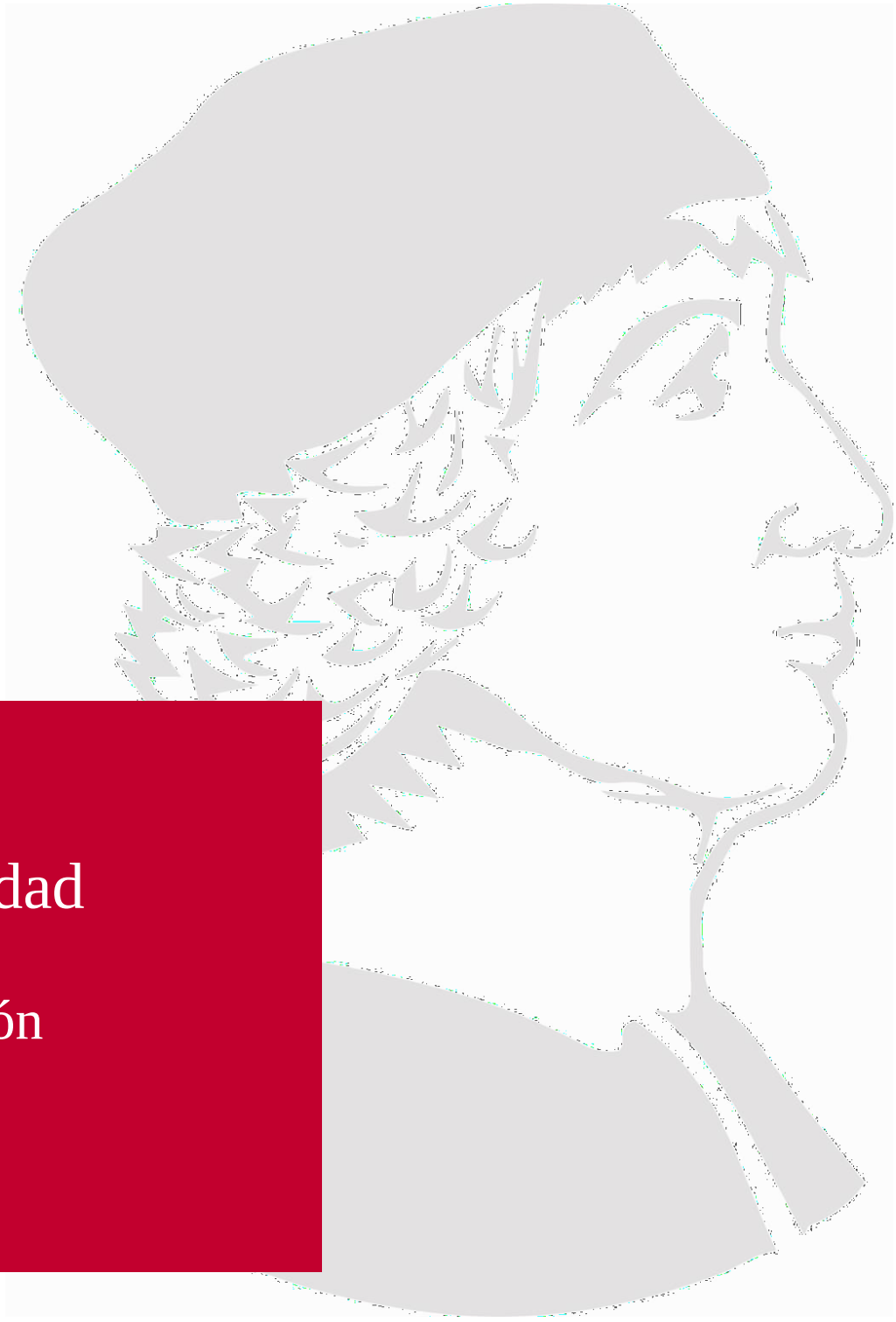

Ciberseguridad

Diploma en Transformación Digital

UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Ciberseguridad

Titulación: Diploma en transformación Digital

Carácter: Obligatoria

Idioma: Castellano.

Modalidad: On Line

Créditos: 6

Curso: 3º

Semestre: 2º

Profesores/Equipo Docente: Paloma Romera García

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

La asignatura contribuye a adquirir las siguientes competencias:

Competencias específicas:

CEB04. Aplicar los conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.

CG01/CG21 - Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.

CG11/12/20 - Capacidad para tomar iniciativas y espíritu emprendedor, el liderazgo, la dirección la gestión de equipos y proyectos.

CE19/20 - Conocimiento de los tipos apropiados de soluciones, y comprensión de la complejidad de los problemas informáticos y la viabilidad de su solución.

CE42 - Combinar la teoría y la práctica para realizar tareas informáticas.

CE06 - Comprender intelectualmente el papel central que tienen los algoritmos y las estructuras de datos, así como una apreciación del mismo.

CEC13. Conocer y aplicar las herramientas necesarias para el almacenamiento, procesamiento y acceso a los Sistemas de información.

Competencias generales:

CGT1. Analizar y sintetizar la información necesaria para realizar su trabajo plasmando los resultados en informes o en la toma de decisiones en proyectos del ámbito de la ingeniería informática.

CGT2. Organizar y planificar los recursos e ideas necesarias para realizar su trabajo ideando acciones e hitos en proyectos del ámbito de la ingeniería informática.

CGT3. Comunicar de forma oral y escrita en la lengua nativa pudiendo expresar sus opiniones de forma clara para transmitir conceptos y soluciones dentro del ámbito de la ingeniería informática.

CGT5. Aplicar conocimientos de informática relativos al ámbito de estudio al trabajar en proyectos del ámbito de la ingeniería informática.

CGT6. Gestionar la información, conociendo su importancia y la forma de procesarla generando los recursos necesarios para facilitar su acceso y provisión en el ámbito de la ingeniería informática.

CGT7. Resolver problemas en el entorno de trabajo, dentro del ámbito de la ingeniería informática, enfrentándose a situaciones complejas en cuanto a problemas técnicos y a las relaciones personales y profesionales.

CGT8. Tomar decisiones basadas en la información disponible en el ámbito de la ingeniería informática.

CGS1. Aplicar la motivación por la calidad en el desarrollo de su actividad profesional poniendo el máximo cuidado en el desarrollo de los entregables dentro de proyectos de ingeniería informática.

CGS2. Razonar de forma crítica ante los problemas que surjan en el ámbito de la ingeniería informática, contando con la información disponible, y explicar dicho razonamiento.

CGS4. Aprender de forma autónoma conceptos relativos a la profesión ingenieril para facilitar la mejora continua ya sea mediante el acceso a información disponible o cualquier otro medio.

CGS5. Adaptarse a nuevas situaciones en el entorno de la ingeniería informática, reconociendo dichas situaciones y expresando formas de afrontarlas.

CGS6. Aplicar la creatividad ante las diferentes circunstancias generando soluciones novedosas dentro del ámbito de la ingeniería informática.

CGP1. Trabajar en equipo contribuyendo de forma activa al resultado de los proyectos u operaciones del ámbito de la ingeniería informática.

1.2. Resultados de aprendizaje

La asignatura contribuye a los siguientes resultados de aprendizaje:

- Capacitar con las habilidades necesarias para la dirección y la gestión del entorno de la seguridad de sistemas y redes de información.
- Capacitar en la respuesta a las obligaciones legales que la empresa tiene frente a la seguridad de los datos que se manejan.
- Adquirir el conocimiento técnico necesario para una correcta gestión del entorno de ciberseguridad, con las actividades de diseño, planificación, operación y gestión de incidentes.
- Adquirir las habilidades necesarias para interactuar y desarrollar en proyectos nuevos de Ciberseguridad como parte del proceso empresaria
- Adquirir competencias relacionadas con la arquitectura de la seguridad, el análisis de riesgos, la auditoría y Forensic.
- Aprender lo necesario para acometer la gestión de vulnerabilidades y la detección, análisis y respuesta frente a todo tipo de amenazas.

2. CONTENIDOS

2.1. Requisitos previos

Es conveniente, aunque no imprescindible haber cursado asignaturas o tener conocimientos de programación, arquitectura de computadores .

2.2. Descripción de los contenidos

- Comprender y gestionar la Seguridad Informática y la Ciberseguridad de las empresas
- Conocer las arquitecturas de densa y respuesta ante Ciberataques
- Comprender el rol de CISO (Chief Information Security Officer) y RSI (Responsable de

Seguridad de la Información)

2.3. Contenido detallado

El objetivo de este libro es dar a conocer las técnicas y herramientas en diferentes campos de la ciberseguridad, aportando los conocimientos necesarios para desarrollar, evaluar y auditar la seguridad de los sistemas informáticos, en general, y aplicaciones, en particular

El temario del curso es el siguiente:

Tema 1. Principios de la Seguridad de la Información

Tema 2. Tipos de Amenazas

Tema 3. Hacking ético, Malware y Forensic

Tema 4. Cifrado

Tema 5. Ciso

Tema 6. Legislación

Tema 7. Seguridad en la Nube

Tema 8. Arquitectura de Seguridad: Prevención

Tema 9. Arquitectura de Seguridad: Detección

Tema 10. Arquitectura de Seguridad: Reacción

Tema 11. Arquitectura de Seguridad: Recuperación

Como actividad dirigida, los alumnos han de desarrollar una práctica en grupo que consistirá en la realización de una política de seguridad para una empresa

Esta práctica es unitaria, es decir, se extiende de forma progresiva a medida que el temario va cubriendo los distintos módulos de la parte teórica, de manera que el alumno empiece ya desde el primer tema y termine al final del curso.

El contenido de las prácticas podrá modificarse con el fin de afianzar aquellos aspectos para los que se detecte una mayor dificultad de aprendizaje.

2.4. Actividades formativas

Código	Actividades formativas	Descripción
AF1	Clases de teoría, evaluación y problemas	Las clases de teoría utilizan la metodología de Lección Magistral que se desarrollará en el aula empleando la pizarra y/o el cañón de proyección. Las clases de problemas se podrán impartir en aula informática utilizando la pizarra y/o el ordenador. En función de la asignatura se dará un mayor peso a unas u otras.
AF2	Tutorías	Consulta al profesor por parte de los alumnos sobre la materia en los horarios de tutorías o empleando mecanismos de tutoría telemática (correo electrónico, uso del campus virtual de la Universidad o herramientas de telepresencialidad como Blackboard Collaborate)
AF3	Prácticas	Se desarrollarán en los ordenadores propios. El profesor enseñará a los alumnos a utilizar programas informáticos o herramientas electrónicas para la asignatura indicada en cada caso. Los alumnos realizarán las prácticas aplicando los conocimientos adquiridos en las clases de teoría y problemas, ayudándoles a afianzarlos.
AF4	Estudio individual	Trabajo individual del alumno utilizando los apuntes de clase, libros de la biblioteca, o apuntes del profesor disponibles en el campus virtual. Se le encargarán al alumno la realización y entrega de trabajos individuales o en grupo. Algunos de ellos se expondrán oralmente a lo largo del curso por parte de los alumnos, lo que facilitará alcanzar la competencia comunicativa en mayor grado. Algunos trabajos requerirán el manejo de programas informáticos que estarán disponibles en los ordenadores de la universidad. Otros requerirán un trabajo de investigación sobre los contenidos de la materia o similares y aplicaciones.

CÓDIGO	ACTIVIDAD FORMATIVA	HORAS	PORCENTAJE DE PRESENCIALIDAD
AF1	Clases de teoría, evaluación y problemas	45	100
AF2	Tutorías	12,5	100
AF3	Prácticas	15	100
AF4	Estudio individual	77,5	0

3. SISTEMA DE EVALUACIÓN

3.1. Sistema de calificaciones

El sistema de calificaciones finales se expresará numéricamente del siguiente modo:

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 que hayan obtenido una calificación igual o superior a 9,0.

3.2. Criterios de evaluación

Se evaluará una práctica en grupo que si se supera con más de un 6 a nivel global e individual, exime de la prueba escrita.
En caso contrario, se aplican la puntuación de la Convocatoria ordinaria

Convocatoria ordinaria

Sistemas de evaluación	Porcentaje
Evaluación de la participación del alumno	10%
Actividades dirigidas, prácticas y memorias de prácticas, trabajos (obligatorios y voluntarios) y proyectos a realizar.	45%
Prueba escrita final	45%

Convocatoria extraordinaria

Sistemas de evaluación	Porcentaje
Actividades dirigidas, prácticas y memorias de prácticas, trabajos (obligatorios y voluntarios) y proyectos a realizar.	50%
Prueba escrita final	50%

3.3. Restricciones

Calificación mínima
La ponderación tanto del examen parcial como de los conceptos de participación y trabajos escritos/prácticas, solo se aplicará si el alumno obtiene al menos un 5,0 en el examen final. Esta ponderación también se aplica solo en el caso de que el alumno obtenga al menos un 5,0 en este examen final extraordinario.

La no superación de las prácticas supone el suspenso automático de la asignatura en la convocatoria ordinaria y extraordinaria. Se conservará la nota de prácticas aprobadas para posteriores convocatorias.

Las prácticas que no hayan sido aprobadas pueden, en su caso, ser entregadas de nuevo para ser evaluadas en la convocatoria extraordinaria, previa consulta al profesor y siempre antes del examen de la convocatoria ordinaria.

Asistencia
El alumno que, injustificadamente, deje de asistir a más de un 25% de las clases presenciales podrá verse privado del derecho a examinarse en la convocatoria ordinaria.

Normas de escritura
Se prestará especial atención en los trabajos, prácticas y proyectos escritos, así como en los exámenes tanto a la presentación como al contenido, cuidando los aspectos gramaticales y ortográficos. El no cumplimiento de los mínimos aceptables puede ocasionar que se resten puntos en dicho trabajo.

3.4. Advertencia sobre plagio

La Universidad Antonio de Nebrija no tolerará en ningún caso el plagio o copia. Se considerará plagio la reproducción de párrafos a partir de textos de auditoría distinta a la del estudiante (Internet, libros, artículos, trabajos de compañeros…), cuando no se cite la fuente original de la que provienen. El uso de las citas no puede ser indiscriminado. El plagio es un delito.

En caso de detectarse este tipo de prácticas, se considerará Falta Grave y se podrá aplicar la sanción prevista en el Reglamento del Alumno.

4. BIBLIOGRAFÍA

Bibliografía recomendada

- Gestión De Incidentes De Ciberseguridad
  Maite Moreno Garcia

- Ciberseguridad. Manual Práctico
  Jose Manuel Ortega Candel