MAPA DE COMPETENCIAS

MAP OF COMPETENCES

1. **TABLAS/TABLES** (Ver descripción abajo/Description below)

MATERIA Y ASIGNATURAS subjects	COMPETENCIAS BÁSICAS Basic Competences	COMPETENCIAS GENERALES General Competences	COMPETENCIAS ESPECÍFICAS Specific Competences
PRIMER CURSO- FIRST YEAR			
MATERIA 1 "Técnicas de Ciberataque"			
- Explotación de Sistemas Software - Técnicas de Ciberataque - Amenazas persistentes y Fugas de Información - Análisis e Ingeniería de Malware - Ciberdelitos, Ciberterrorismo y Ciberguerra	CB6, CB7, CB8, CB9, CB10	CG1, CG3, CG4	CE1, CE2, CE3, CE7
MATERIA 2 "Técnicas de Ciberdefensa y Comunicaciones Seguras"			
- Comunicaciones Seguras - Identificación y Autenticación - Protección de Datos - Sistemas de Ciberdefensa - Análisis Forense de Sistemas Informáticos - Arquitecturas Seguras - Ingeniería de Sistemas Seguros - Seguridad en Sistemas y Comunicaciones Móviles	CB6, CB7, CB8, CB9, CB10	CG2, CG3, CG4	CE4, CE5, CE6, CE7, CE8
MATERIA 3 "Gestión de la Ciberseguridad"			
- Gestión y Administración de la Ciberseguridad - Análisis de Riesgos en Ciberseguridad	CB8, CB9, CB10	CG4, CG5	CE9
MATERIA 4 "Trabajo Fin de Máster"			
- Trabajo Fin de Máster	CB6, CB7, CB8, CB9, CB10	CG1, CG2, CG3, CG4, CG5	
MATERIA 5 "Seminarios"			
- Seminario 1 - Seminario 2	CB6, CB7, CB8, CB10	CG1, CG2, CG4	CE3, CE5, CE8

2. DESCRIPCIÓN DE RESULTADOS DE APRENDIZAJE Y COMPETENCIAS/DESCRIPTION OF LEARNING OUTCOMES AND COMPETENCES

○ COMPETENCIAS BÁSICAS/BASIC COMPETENCES:

- CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

○ COMPETENCIAS GENERALES/GENERAL COMPETENCES:

- CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.
- CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido.
- CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.
- CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.
- CG5 Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS).

○ COMPETENCIAS ESPECÍFICAS/SPECIFIC COMPETENCES:

- CE1 Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.
- CE2 Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.
- CE3 Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.
- CE4 Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
- CE5 Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.
- CE6 Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.
- CE7 Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.
- CE8 Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.
- CE9 Capacidad para aplicar las metodologías existentes al análisis de riesgos, transmitir los resultados y proponer las medidas para disminuir los riesgos de acuerdo con el caso concreto de la organización, partiendo del inventario de activos de una organización