



FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Gobierno, Riesgo y Cumplimiento de la Seguridad
Código	DTC-MCS-513
Impartido en	Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Anual
Créditos	6,0 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Juan Francisco Cornago Baratech
Horario	Jueves y Viernes de 15:00 a 17:00
Horario de tutorías	Por petición previa a través de correo
Descriptor	<p>Descripción El propósito de esta asignatura es proporcionar a los alumnos una amplia visión de las metodologías, normativas, procesos y actividades necesarias para dirigir una organización de seguridad. Esta asignatura se impartirá por profesionales de prestigio que trabajan día a día en los diferentes ámbitos de la ciberseguridad en empresas privadas. La asignatura está organizada en formato continuo de clases, sobre un temario determinado, distribuidas en 4 horas a la semana durante el primer semestre. En este periodo 3 profesores impartirán los temas necesarios para que el alumno entienda cómo se organizan los procesos de seguridad necesarios para establecer una defensa proporcionada a los riesgos en materia de Ciberseguridad. Las clases se orientarán hacia tres líneas de actuación:</p> <ul style="list-style-type: none">• Introducción a la Ciberseguridad. En esta primera parte haremos una comprensión de los desafíos y estrategias en la gestión del riesgo de ciberseguridad a través de ejemplos prácticos enfocados al sec

Datos del profesorado	
Profesor	
Nombre	David Estévez Maestre
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	destevez@icai.comillas.edu
Profesor	
Nombre	Juan Francisco Cornago Baratech
Departamento / Área	Departamento de Telemática y Computación
Despacho	Cualquier duda o aclaración por correo electrónico
Correo electrónico	jfcornago@icai.comillas.edu
Profesor	
Nombre	Valentín López Sotomayor
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	vlisotomayor@icai.comillas.edu



DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Competencias - Objetivos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Índice de contenido

- TEMA INTRO 1. Entorno de amenaza
 - Conceptos básicos y autoevaluación
 - Cibercrimen y actores
 - Riesgos más importantes para el negocio
 - Estrategias de seguridad
- TEMA INTRO 2. Gobierno
 - Cumplimiento regulatorio en el sector financiero
 - Gestión del Riesgo en la cadena de suministro
 - Diseño y ejecución de una estrategia de ciberseguridad en 100 días.
- TEMA INTRO 2. Identificar vulnerabilidades
 - Superficie de ataque
 - Tipos de análisis de seguridad
- TEMA INTRO 3. Proteger, Detectar y Responder ante ciberataques
 - Controles clave para prevención de ataques.
 - Controles clave para la detección de posibles eventos de seguridad
 - Respuesta ante incidentes.
- TEMA INTRO 4. Recuperación de la actividad
 - Implementación de un Plan de Continuidad de Negocio

- TEMA GRC 0. el profesional de ciberseguridad
 - Consejos básicos para iniciarse al mundo de la ciberseguridad
- TEMA GRC 1. La Ciberseguridad en España
 - Qué es la seguridad
 - Principales amenazas: Dónde va el mundo, Directivos, Tecnología, seguridad.
 - Cómo se estructura la ciberseguridad en España: DSN, INCIBE, FCCSSEE, CNPIC, CCNCERT, MCCD, AEPD.
 - Ciberseguridad dentro de las organizaciones
- TEMA GRC 2. Normativas, estándares, buenas prácticas...
 - En Europa, España, EE. UU., Otras
 - Cómo entender una normativa: alcances, estructura, objetivos, etc.
 - Cómo crear una normativa
- TEMA GRC 3. ISO 27001, ISO27002



- Sistemas de Gestión de Seguridad de la Información
 - Controles derivados
- TEMA GRC 4. ENS
 - Qué es el Esquema Nacional de Seguridad de la Información
 - Cómo adecuarse
- TEMA GRC 5. Ley PIC, LOPDGDD, Directiva NIS
 - Infraestructuras críticas, Servicios esenciales y Privacidad
- TEMA GRC 6. Sistema Integrado de Gestión.
 - Qué es. Por qué es necesario. Qué va a controlar. Quien es el responsable. Cómo se construye. Cómo se mantiene.
- TEMA GRC 7. Cuadro de mando de la ciberseguridad.
 - medir. A quién reporto. Cada cuánto tiempo. Cómo lo divulgo.
- TEMA GRC 8. Auditoría.
 - Metodología
 - Caso práctico. Auditando una Organización.
- TEMA GRC 9: CÓMO GESTIONAR EL RIESGO EN LAS ORGANIZACIONES
 - Análisis de riesgo mediante la metodología MAGERIT
 - Tratamiento de los riesgos.
 - Herramientas: PILAR, MOSLER
 - Otras metodologías de análisis de riesgo.
 - Caso práctico. Realización de un análisis de riesgo real en una organización.
- TEMA GRC 10: CULTURA DE LA CIBERSEGURIDAD
 - El usuario final, principal actor en materia de ciberseguridad.
 - Cómo atraer la atención del usuario.
- Persuasión frente a la simple comunicación.

- TEMA C1. Introducción a GID
 - ¿Qué es la Gestión de Identidades?
 - Áreas de la Gestión de Identidades y Accesos
 - Identidad Digital
- TEMA C2. Control de Acceso
 - Componentes del Control de Acceso
 - Modelos de Control de Acceso
 - Técnicas y Administración de Control de Acceso
 - Inicio de sesión único (single sign on)
 - Directorios
- TEMA C3. Access Manager
 - Federación de Identidades
 - SAML
 - Cl@ve
 - OAUTH
 - FIDO
 - CIAM
- TEMA C4. Gobierno de la Identidad
 - Gobierno de la Identidad
 - Ciclo de Vida JML
 - Segregación Funcional (SoD)



- Recertificación de Accesos.
- RBAC y ABAC
- Perfilado
- TEMA C5 Cuentas Privilegiadas
 - Importancia de las cuentas privilegiadas
 - Controles adicionales
 - Soluciones dedicadas.
- TEMA C6. Cloud Access
 - La nube: nuevas amenazas
 - ¿Qué es diferente entre Gobierno de Cloud vs IGA?
 - Gobierno Cloud

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Prerrequisitos

Aunque no es estrictamente necesario, ayuda a la comprensión de la asignatura el disponer de conocimientos de conceptos básicos de ciberseguridad, tanto tecnológicos como normativos, que por otra parte se adquirirán a lo largo del curso.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Método de evaluación

- Pruebas intermedias: 20%
 - Comprensión de los conceptos teóricos.
 - Aplicación de dichos conceptos para la resolución de problemas.
 - Análisis e interpretación crítica de los resultados obtenidos en la resolución de problemas.
- Examen Final: 60%
 - Comprensión de los conceptos teóricos.
 - Aplicación de dichos conceptos para la resolución de problemas.
 - Análisis e interpretación crítica de los resultados obtenidos en la resolución de problemas.
- Proactividad, Actitud y esfuerzo: 20%
 - Iniciativa y proactividad en el trabajo, y colaboración en el trabajo en equipo.
 - Habilidades de comunicación en la escritura y en las presentaciones verbales.

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Bibliografía

- Directiva NIS
- ENISA
- Serie ISO 27000



COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

GUÍA DOCENTE
2024 - 2025

- ENS
- Ley PIC
- LOPDGDD
- NIST
- SOX