

GUÍA DOCENTE

**SEGURIDAD INFORMÁTICA Y
CIBERSEGURIDAD EN LA EMPRESA**

Seguridad Informática Y Ciberseguridad En La Empresa

Número total de créditos ECTS		6
Tipología		Obligatoria
Organización temporal		Curso 3; Semestre 5
Modalidad		Presencial y Virtual
Idioma		Español
Contenidos		<p>Introducción a la Seguridad Lógica y Ciberseguridad Análisis del ecosistema de Seguridad Componentes de Seguridad a contemplar en el diseño de redes de Computación Roles asociados a la Seguridad Y Ciberseguridad Encriptación de Mensajes Introducción a la ISO27000 Ciber-Seguridad en la Red. Centro de Operaciones de Seguridad. Estrategias de Protección Gestión de Identidades y Accesos. Seguridad por diseño en la creación de Aplicaciones Seguridad en Aplicaciones Móviles y Web Seguridad en Entornos de Nube Herramientas para la Gestión de la Seguridad</p>
Resultados de aprendizaje TÍTULO	Conocimientos y contenidos	<p>CC01 Conocer las herramientas básicas de gestión de la información en el contexto empresarial y de negocio CC02 Conocer herramientas para el desarrollo de proyectos de emprendimiento innovadores y diferenciales. CC04 Identificar las características de los diferentes tipos de organizaciones, tipos de contratos en la prestación de servicios de TI y el papel que juegan las TIC en las mismas</p>
	Habilidades y destrezas	<p>HD01 Aplicar técnicas de gestión de personas, liderazgo y negociación en el contexto empresarial y de negocio HD02 Elaborar propuestas de proyectos tecnológicos teniendo en cuenta los recursos, las alternativas y tendencias disponibles, la seguridad requerida y las condiciones de mercado HD06 Tomar decisiones empresariales y de negocio con una perspectiva de estrategia corporativa global HD10 Defender ideas y argumentos propios en un contexto profesional HD11 Proyectar enfoques alternativos, buscar soluciones y generar valor en contextos complejos y cambiantes HD12 Trabajar en entornos multiculturales e internacionales en base al reconocimiento y el respeto a la diversidad HD13 Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional</p>
	Competencias	<p>CP07 Planificar proyectos y departamentos técnicos en el entorno de las TIC tanto con recursos propios como con recursos del Ecosistema existente tanto nacional como internacional.</p>

Resultados de aprendizaje ASIGNATURA				
<ul style="list-style-type: none"> • Entender las amenazas y riesgos de seguridad de los sistemas informáticos • Entender las ideas generales de las implicaciones legales de la seguridad informática • Conocer las problemáticas de seguridad en las redes de computadores y ser capaz de encontrar soluciones para protegerlas • Diseñar mecanismos de protección para las aplicaciones distribuidas. • Entender la necesidad y funcionamiento de mecanismos forenses a la seguridad informática • Utilizar mecanismos criptográficos para la protección de recursos informáticos • Entender, aplicar y diseñar infraestructuras de clave pública (PKI) • Entender los mecanismos de protección y las políticas de seguridad. 				
Modalidad Presencial	Actividades formativas		Horas totales	
	Clases Expositivas		28	
	Seminarios		2	
	Clases prácticas		28	
	Tutorías		12	
	Trabajo autónomo		76	
	Prueba de evaluación final		4	
	Total		150	
	Sistemas de evaluación		MÍNIMO	MÁXIMO
	Evaluación final: prueba o examen		50	50
	Resolución problemas		10	30
	Estudio casos - Proyectos		10	30
	Otras actividades de evaluación continua		0	10
	Total		70	120
Observaciones				
Modalidad Virtual	Actividades formativas		Horas totales	
	Clases Expositivas		13	
	Seminarios		2	
	Clases prácticas		13	
	Actividades Dirigidas Asíncronas		30	
	Tutorías		12	
	Trabajo autónomo		76	
	Prueba de evaluación final		4	
	Total		150	
	Sistemas de evaluación		MÍNIMO	MÁXIMO
	Evaluación final: prueba o examen		50	50
	Resolución problemas		10	30
	Estudio casos - Proyectos		10	30
	Otras actividades de evaluación continua		0	10
Total		70	120	
Observaciones				