



INFORMACIÓN ESPACIO ACADÉMICO						
Nombre de asignatura	SEGURIDAD DE LA INFORMACIÓN					
Código	11501002					
Definición de asignatura	Obligatorio	X	Básico		Complementario	
	Electivo		Intrínseco		Extrínseco	
Número de créditos		Horas		Semanas	16	
Distribución créditos	HTD	64	HTC	32	HTA	48
	Horas de trabajo cooperativo					
Metodología	Virtual					

PROGRAMACIÓN DEL CONTENIDO
<b>CONOCIMIENTOS PREVIOS</b>
<p>El estudiante del curso de Seguridad de la Información de la Maestría en Gestión y Seguridad de la Información debe contar con ciertos conocimientos previos en cuanto a las siguientes temáticas:</p> <ul style="list-style-type: none"> <li>• Sistemas de información</li> <li>• Bases de datos relacionales</li> <li>• Fundamentos de redes de computadores</li> </ul>
<b>DESCRIPCIÓN DEL CURSO</b>
<p>El curso de Seguridad de la Información de la Maestría en Gestión y Seguridad de la Información está estructurado en torno a conceptos básicos de seguridad de la información: seguridad física y lógica de la información; <i>software</i> de seguridad y seguridad en redes; técnicas criptográficas y modelos de seguridad; y temas relacionados con los sistemas de gestión de la seguridad de la información, mejor conocidos como SGSI.</p> <p>A partir del curso, se busca que el estudiante comprenda y maneje conceptos básicos y necesarios relacionados con la seguridad de la información. Estos conceptos son fundamentales para el desarrollo de la maestría y todas las asignaturas que la componen.</p>
<b>ÁREAS DE CONOCIMIENTO</b>
<ul style="list-style-type: none"> <li>• Gestión de proyectos</li> <li>• Sistemas de información</li> </ul>
<b>COMPETENCIAS EN FORMACIÓN</b>
<p>El curso Seguridad de la Información de la Maestría en Gestión y Seguridad de la Información busca que los estudiantes se formen en competencias relacionadas con la adquisición y el desarrollo de aptitudes empresariales, y en el manejo de las tecnologías de la información y las comunicaciones (TIC), con el fin de conocer los principios y elementos fundamentales de la seguridad de la información aplicables a entornos empresariales, entre otros.</p> <p>Se busca fomentar en los estudiantes la capacidad de resolver problemas en el ámbito empresarial y en el manejo de las TIC, en relación con los procesos de seguridad que ameritan tenerse en cuenta en dichos ámbitos; además, el estudiante tendrá la competencia y la capacidad de identificar, analizar y definir elementos que sean significativos en cuanto a la seguridad de la información.</p>





En ese sentido, el estudiante estará en capacidad de resolver problemas que se presenten en el ámbito de la seguridad de la información y en el uso de diferentes entornos relacionados con las tecnologías de la información y las comunicaciones, promoviendo la capacidad para la utilización y la integración de tecnologías de la información, aplicaciones y sistemas de información en contextos organizativos y empresariales; además, el estudiante podrá adoptar las medidas de seguridad apropiadas y oportunas.

Se busca desarrollar competencias específicas como la relacionada con el análisis de necesidades de información, procesos, sistemas de información y seguridad sobre estos mismos en procesos una organización

Los estudiantes estarán en capacidad de generar y comunicar conclusiones y aportar sus conocimientos en la solución de situaciones relacionadas con la seguridad de la información.

### ESTRUCTURA DEL MÓDULO

#### UNIDAD 1. Fundamentos de seguridad física y lógica

OBJETIVO DE APRENDIZAJE	TÍTULO DE TEMA
Conocer e identificar las características que debe cumplir la información para que sea confiable y segura.	1.1. Introducción a la seguridad de la información
Adquirir destrezas en la identificación y gestión de riesgos en la infraestructura física y lógica de un sistema informático.	1.2. Conceptos fundamentales de la seguridad de la información
Conocer los mecanismos para realizar el aseguramiento físico y lógico de los recursos informáticos de un sistema de comunicaciones.	1.3. Servicios y mecanismos de seguridad
	1.4. Tipos de redes de comunicaciones

#### UNIDAD 2. *Software* de seguridad y seguridad en redes

OBJETIVO DE APRENDIZAJE	TÍTULO DE TEMA
Identificar plenamente el <i>software</i> existente para vulnerar la seguridad en una red de computadores.	2.1. Introducción
Identificar plenamente el <i>hardware</i> y el <i>software</i> existentes para garantizar la seguridad en una red de comunicaciones.	2.2. Generalidades de la seguridad en redes
Identificar aspectos y conceptos propios de la seguridad en una red wifi.	2.3. Delitos informáticos
	2.4. Tipos de ataques informáticos

#### UNIDAD 3. Modelos de seguridad y técnicas criptográficas

OBJETIVO DE APRENDIZAJE	TÍTULO DE TEMA
Conocer los modelos existentes para el aseguramiento de la información en ambientes locales o distribuidos.	3.1. Modelos de seguridad de la información
Adquirir destreza en la implementación de modelos de seguridad de la información en	3.2. Técnicas criptográficas



ambientes empresariales públicos y privados.	
Identificar los principales algoritmos y técnicas de encriptación de información.	3.3. Cifrado y algoritmos de cifrado
<b>UNIDAD 4. Sistemas de gestión de seguridad de la información (SGSI)</b>	
<b>OBJETIVO DE APRENDIZAJE</b>	<b>TÍTULO DE TEMA</b>
Conocer, entender y aplicar la norma 27000, a partir de la cual se establecen los mecanismos y servicios de seguridad en un sistema telemático.	4.1. Introducción
Identificar los aspectos generales a tener en cuenta en el aseguramiento de un sistema informático.	4.2. ¿Qué es un SGSI?
Aplicar los conocimientos adquiridos en el curso para diseñar e implementar controles que garanticen la privacidad, la autenticidad, la confiabilidad y la disponibilidad de los datos y de la información.	4.3. Norma ISO 27000

Tenga en cuenta las siguientes **estrategias de aprendizaje** para el planteamiento de las actividades de evaluación:

- **Estudio autónomo:** lectura y revisión de las unidades, de los recursos tales como videos, lecturas, hipervínculos, investigación, exploración en redes académicas
- **Tutoría:** revisión de clases magistrales virtuales, asistencia a tutoría virtuales presenciales, comunicación con el tutor y aclaración de dudas.
- **Autoevaluaciones:** cuestionarios de evaluación en línea
- **Prácticas:** actividades durante el desarrollo del curso de diferente índole, orientadas a proyectos, problemas, investigación, estudio de caso, entre otras
- **Trabajo final:** elaboración de una actividad que integra lo desarrollado durante el curso, la cual se debe entregar la última semana del curso.
- **Notas:** las actividades se pueden desarrollar tanto individual como grupal, según criterio del docente.

EVALUACIÓN		
TIPO	EVALUACIÓN/ACTIVIDAD	PORCENTAJE
Evaluativa	Evaluar bajo los principios planteados por los modelos CIA y AAA la seguridad de la información de la empresa donde el estudiante trabaja u otra empresa real de su preferencia.	10%





Evaluativa	Elaborar el plan para la seguridad física y el plan para la recuperación de desastres, con el objetivo garantizar la seguridad de la información de la empresa en la que el estudiante trabaja u otra empresa real de su preferencia.	10%
Formativa	Elaborar un artículo científico cuya temática sea la autenticación multifactor, con énfasis en el análisis de sus ventajas con respecto a otros esquemas.	5%
Evaluativa	Desarrollar una guía práctica para la configuración del <i>firewall</i> de Windows o del sistema operativo de su preferencia (ejemplo: Kali Linux).	10%
Evaluativa	Desarrollar una guía práctica para gestionar la seguridad en una red corporativa que incluya equipos, aplicaciones, sistemas operativos y usuarios.	10%
Evaluativa	Tomar como ejemplo mínimo tres virus, identificar su forma de propagación y su finalidad; realizar un plan para la prevención, desinfección y recuperación del sistema si este ya fue infectado.	5%
Evaluativa	Dar a conocer en detalle o plantear la creación de un modelo de seguridad de la información para la empresa donde el estudiante trabaja u otra empresa real de su preferencia.	25%
Evaluativa	Plantear la manera de implementar un SGSI integrándolo con otros sistemas de la organización para la empresa en la que el estudiante trabaja u otra empresa real de su preferencia	15%
Formativa	Hacer un análisis de la aplicación de la norma ISO 27000 para la empresa en la que el estudiante trabaja u otra empresa real de su preferencia.	10%
<b>Total, del curso</b>		<b>100 %</b>

**BIBLIOGRAFÍA**

1	ANDREW, FERNANDO; PELLEREJO, IZASKUN, LESTA, Amaia. (2006) Fundamentos y Aplicaciones de Seguridad en Redes WLAN. Marcombo S. A.
2	Areitio, Javier. (2008) Seguridad de la información: Redes informáticas y sistemas de información. Paraninfo.
3	Ariganelo, Ernesto, et al. (2010). Redes CISCO CCNP a Fondo. México: Alfaomega.





4	Forouzan, Behrouz. (2001). Transmisión de datos y redes de comunicaciones. Madrid: McGrawHill.
5	García, Juan Luis, et al. (s.f.). Esquema Nacional de Seguridad con Microsoft, OXWord.2014.
6	Joyanes A., Luis. (2015). Sistemas de información en la empresa. México: Alfaomega.
7	Muñoz Muñoz, Alfonso. (2014). Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA. OXword
8	Santos de los, Sergio. (2013). Una al día, 16 años de seguridad informática. HispasecSistemas
9	Stallings, William. (2005) Fundamentos de seguridad en redes, aplicaciones y estándares. Editorial Pearson, Prentice Hall.

PROGRAMA SINTÉTICO		ORGANIZACIÓN / TIEMPOS															
		SEMANAS ACADÉMICAS															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.	Fundamentos de seguridad física y lógica	X	X	X	X												
2.	Software de seguridad y seguridad en redes					X	X	X	X								
3.	Modelos de seguridad y técnicas criptográficas									X	X	X	X				
4.	Sistemas de Gestión de Seguridad de la Información (SGSI)													X	X	X	X

ELABORÓ: Miguel Ángel Leguizamón Páez

