Maestría en seguridad informática

Asignatura		Fundamentos en Seguridad de la Información					
Área		Especializadas					
Código	SIFS14	**Créditos**	**4**	**TIT**	**144**	**TPT**	**48**

1. DESCRIPCIÓN

Los riesgos de seguridad de la información son variables a lo largo del tiempo y dependen de numerosas variables que pueden afectar la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de los activos de información.

Cuando estos riesgos se materializan, hablamos de la ocurrencia de incidentes de seguridad de la información con el correspondiente impacto para la compañía. Con el fin de minimizar dichos impactos, es fundamental realizar todas las tareas necesarias de prevención, en donde se realice una adecuada gestión de los riesgos de seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información con sus respectivos modelos de seguridad, en donde se establezcan los activos de información, la valoración de los mismos, los riesgos asociados, los controles a implementar, el modelo de medición para la eficiencia de dichos controles y el modelo de verificación y mejora continua para elevar de forma sostenida el nivel de seguridad de la información a lo largo del tiempo.

De igual manera, entender las redes de computadores y las TIC en general es fundamental, toda vez que la seguridad se fortalece en la medida que los procesos técnicos tengan niveles y modelos de seguridad acordes a las organizaciones.

2. CONTENIDO

Contenido detallado	**Tiempo**
Descripción del contenido de la asignatura especificando cada ítem.	***Número de horas presenciales dedicadas al contenido específico.***

Conceptos básicos de redes de computadores:
• Introducción a las redes de computadores
• Modelo OSI: Protocolos y servicios de red.
  ○ Tecnologías alámbricas e inalámbricas.
  ○ Router, Sw, AccessPoint.
	10

○ MPLS, ARP, TCP, UDP, DHCP, DNS, SMB, etc. ○ Direccionamiento IP (Versión 4 y 6) ○ Sistemas de almacenamiento NAS, SAN, CAS. ○ IoT: conceptos básicos. • Sistemas operativos. ○ Windows ○ Linux / Unix ○ Smartphone • Bases de datos ○ Relacionales ○ NoSQL • Arquitecturas de aplicaciones: 2 niveles, 3 niveles, n niveles.	
Conceptos básicos de seguridad de la información: Confidencialidad, disponibilidad e integridad.	**3**
Conceptos básicos de riesgo, amenaza, impacto y vulnerabilidades.	**3**
Objetivo de seguridad de la información. • ¿Por qué es necesaria la seguridad de la información en las organizaciones y el país? • Características a proteger en la seguridad de la información. Retos y desafíos de la seguridad.	**3**
Modelos de Seguridad de la Información. • Descripción y componentes de un framework. • Estándares y modelos de seguridad de la información: ISO, NIST, • Análisis y comparación de los diferentes modelos de seguridad. • Control del flujo de información.	**8**
Aspectos técnicos de un modelo de seguridad de la información. • Aspectos básicos de tipos de ataques a la Infraestructura tecnológica. • Metodología de Ethical Hacking • Controles técnicos de un modelo de seguridad: Firewall, IPS, IDS, DLP, balanceadores de carga, Antispam. • Certificados digitales.	**12**

• Control de acceso, Usuarios y roles. • Criptografía. • Seguridad en aplicaciones. • Detección de intrusos.	
Aspectos administrativos de un modelo de seguridad de la Información: • Gobernabilidad de seguridad de la Información • Políticas de seguridad de la información. • Auditoría de seguridad de la información. • Proceso de control de vulnerabilidades. • Proceso de gestión de incidentes. • Medición de un modelo de seguridad.	**9**

3. EVALUACION

Actividades de evaluación		
Actividad	%	Fecha
Práctica: Sistemas operativos y servicios de red.	20%	Semana 3
Ensayo: Seguridad de la información en las organizaciones	20%	Semana 5
Presentación y exposición: Amenazas	20%	Semana 6
Presentación y exposición: Modelos, metodologías y marcos	20%	Semana 8
Trabajo final: Implementación del SGSI	20%	Semana 11

4. BIBLIOGRAFÍA

- Tanenbaum, Andrew S. (2009). Sistemas operativos modernos. Pearson Educación. México.
- Stallings, William (2004). Comunicaciones y redes de computadores. Editorial Pearson. México.
- Baca Urbina, Gabriel (2016). Introducción a la Seguridad Informática. Grupo Editorial Patria. México.

- ISO/IEC, (2013). ISO/IEC 27001:2013 Information technology -- Security techniques -- Specification for an Information Security Management System. Geneva, Switzerland: ISO/IEC.
- ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación). (2006). Gestión de riesgo, NTC 5254 - Norma Técnica Colombiana
- National Institute of Standards and Technology (2003). 800-53 Guide to Information Technology Security Services.

Cibergrafía.

- Ministerio TIC (2019). Sistema de gestión de la seguridad de la información – SGSI. Consultado el 1 de agosto de 2019 en http://www.mintic.gov.co/gestionti/615/w3-article-5482.html
- LACNIC (2019). Taller Amparo – CSIRTs. Consultado el 1 de agosto de 2019 en: https://warp.lacnic.net/csirts#colombia
- OWASP Security Operations Center (SOC) Framework Project. consultado el 1 de agosto de 2019 en: https://www.owasp.org/index.php/OWASP_Security_Operations_Center_(SOC)_Framework_Project
- National Institute of Standards and Technology (2019). Cybersecurity Framework. consultado el 1 de agosto de 2019 en: https://www.nist.gov/cyberframework
- Open Source Security Testing Methodology Manual -OSSTMM (2019). consultado en línea el 1 de agosto de 2019 en: http://www.isecom.org/research/

Elaborado por:	Héctor Fernando Vargas Montoya		
Revisado por	Juan Fernando Hurtado Rivera		
Aprobado por:	Comité curricular	**Fecha:**	Julio 26 de 2018