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	*3*	*Horas*		*Semanas*	*16*	
Distribución créditos	*HTD*	64	*HTC*	32	*HTA*	48
Metodología	Virtual					

PROGRAMACIÓN DEL CONTENIDO
CONOCIMIENTOS PREVIOS
Tecnologías de la Información, Seguridad de la Información, Ciberseguridad, Riesgos de Seguridad de la Información y Ciberseguridad
DESCRIPCIÓN DEL CURSO
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: confidencialidad, integridad y disponibilidad de la información; riesgos de seguridad de la información y temas relacionados con los sistemas de gestión de la seguridad de la información, mejor conocidos como SGSI. 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.
ÁREAS DE CONOCIMIENTO
Seguridad de la Información.

Riesgos de seguridad de la información.

COMPETENCIAS EN FORMACIÓN

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.

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.

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, 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. Gobierno de Seguridad de la Información

OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Conocer los conceptos básicos de Seguridad de la Información y	1.1 Introducción y conceptos de seguridad de la información
	1.2 Modelos de seguridad de la información

recursos de un gobierno de Seguridad de la Información.	1.3 Recursos del Programa de Seguridad de la Información
	1.4 Desarrollo y Evaluación del Programa de Seguridad de la Información
UNIDAD 2. Gestión de Riesgos de Seguridad de la Información	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Identificar y proponer una metodología de gestión de activos y riesgos de seguridad de la información.	2.1 Gestión de activos de información
	2.2 Metodologías de gestión de riesgos de seguridad de la información
	2.3 Metodologías de valoración de riesgos
	2.4 Tratamiento de riesgos y controles
UNIDAD 3. Continuidad del Negocio y Marco Legal	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
- Comprender los conceptos de continuidad del negocio y su impacto en la gestión de Seguridad de la Información en una organización. - Identificar los aspectos legales que se deben tener en cuenta en la gestión de Seguridad de la Información en una organización.	3.1 Seguridad y Gestión de Continuidad del Negocio
	3.2 Plan de recuperación de desastres
	3.3 Gestión de Incidentes de seguridad de la información
	3.4 Marco legal
UNIDAD 4. Sistema de Gestión de Seguridad de la Información	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Conocer, entender e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO 27001.	4.1 Planeación SGSI
	4.2 Controles ISO 27002
	4.3 Hacer, Verificar y Actuar

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**
Unidad 1: Foro	Actividad Inicial: Seguridad de la Información Vs. Seguridad Informática	10%
Unidad 1: Trabajo	Actividad: Políticas, Estándares y Procedimientos de Seguridad de la información	10%
Unidad 2: Trabajo	Actividad: Construcción de Escenarios de Riesgos	15%
Unidad 2: Trabajo Final	Actividad: Primera Entrega Proyecto Asignatura: Contexto de la organización	10%
Unidad 3: Trabajo	Actividad: Gestión de Incidentes de Seguridad de la información	10%
Unidad 3: Cuestionario	Actividad: Evaluación Conceptos Unidad 3	10%
Unidad 3: Trabajo Final	Actividad: Segunda Entrega Proyecto Asignatura: Controles de Seguridad de la Información	10%
Unidad 4: Trabajo	Actividad: ISO 27002 y otros estándares	15%
Unidad 4: Trabajo Final	Actividad: Entrega Final Proyecto Asignatura: Declaración de Aplicabilidad	10%
		100 %

BIBLIOGRAFÍA	
1	Consejo Superior de Administración Electrónica. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I Método.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

2	International Organization for Standardization. (Otrubre de 2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.* Obtenido de https://www.iso.org/standard/75106.html
3	International Organization for Standardization. (Febrero de 2022). *ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security controls.* Obtenido de https://www.iso.org/standard/75652.html
4	International Organization for Standardization. (Octubre de 2022). *ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Obtenido de https://www.iso.org/standard/27001
5	International Organization for Standardization. (Octubre de 2022). *ISO 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* Obtenido de https://www.iso.org/standard/80585.html
6	International Organization for Standarization. (Noviembre de 2016). *ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management.* Obtenido de https://www.iso.org/standard/60803.html
7	International Organization for Standarization. (Febrero de 2018). *ISO 31000:2018 Risk management — Guidelines.* Obtenido de https://www.iso.org/standard/65694.html
8	International Organization for Standarization. (Febrero de 2018). *ISO/IEC 27000:2018 Information security management systems - Overview and vocabulary.* Obtenido de https://www.iso.org/standard/73906.html
9	ISACA. (27 de Julio de 2020). Risk IT Framework, 2nd Edition. Obtenido de www.isaca.org
10	ISACA. (28 de Febrero de 2022). CISM REview Manual, 16th Edition. Obtenido de https://www.isaca.org/

ORGANIZACIÓN / TIEMPOS																
PROGRAMA SINTÉTICO		**SEMANAS ACADÉMICAS**														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1.	Gobierno de Seguridad de la Información															
	1.1 Introducción y conceptos de Seguridad de la Información															
	1.2 Modelos de seguridad de la información.															

	1.3 Recursos del Programa de Seguridad de la Información															
	1.4 Desarrollo y Evaluación del Programa de Seguridad de la Información															
2.	Gestión de Riesgos de Seguridad de la Información															
	2.1 Gestión de activos de información															
	2.2 Metodologías de Gestión de Riesgos de Seguridad de la Información															
	2.3 Metodologías de Valoración de Riesgos															
	2.4 Tratamiento de riesgos y Controles															
3.	Continuidad del Negocio y Marco Legal															
	3.1 Seguridad y Gestión de Continuidad del Negocio															
	3.2 Plan de Recuperación de Desastres															
	3.3 Gestión de Incidentes de Seguridad de la Información															
	3.4 Marco Legal															
4.	Sistema de Gestión de Seguridad de la Información															
	4.1 Planeación SGSI															
	4.2 Controles ISO 27002															

	4.3 Hacer, Verificar y Actuar															

ELABORÓ: Yesid Alberto Tibaquira Cortes
09/07/2024