INFORMACIÓN ESPACIO ACADÉMICO						
Nombre de asignatura	**CIBERSEGURIDAD**					
Código	11501003					
Definición de asignatura	***Obligatorio***	***X***	***Básico***		***Complementario***	
	Electivo		***Intrínseco***	***X***	***Extrínseco***	
Número de créditos	*3*	***Horas***	*144*	***Semanas***	*16*	
Distribución créditos	***HTD***	*64*	***HTC***	*32*	***HTA***	48
	Hora de trabajo cooperativo					
Metodología	Virtual					

PROGRAMACIÓN DEL CONTENIDO
CONOCIMIENTOS PREVIOS
• Tecnologías de la Información (TI) • Seguridad de la Información (SI)
DESCRIPCIÓN DEL CURSO
Esta asignatura aporta el conocimiento tecnológico y de gestión para la implementación de un programa de gobierno de ciberseguridad en sectores tanto públicos como privados, soportado en los lineamentos estratégicos de la maestría, en el desarrollo de la asignatura se cubrirán modelos de gestión de ciberseguridad, aspectos tecnológicos que deben ser cubiertos por esos modelos y finalmente metodologías para identificar el nivel de madurez de un modelo de gestión. Lo anterior se encuentra basado en estándares y marcos de trabajo para la ciberseguridad independiente del sector industrial.
ÁREAS DE CONOCIMIENTO
• Gestión de Riesgos • Arquitectura de Seguridad • Seguridad en Cloud • Gestión Tecnológica
COMPETENCIAS EN FORMACIÓN
Al final de la asignatura el estudiante podrá contar con las siguientes competencias: • Identificar y desarrollar un programa de gestión de ciberseguridad según las necesidades del negocio • Habilidades para la gestión de ciber-riesgos • Conocimiento técnico para el gobierno e implementación asertiva de medidas de mitigación o controles • Habilidades para la implementación de un modelo de madurez que identifique el estado actual y el estado objetivo de un programa de gestión de ciberseguridad

ESTRUCTURA DEL MÓDULO	
UNIDAD 1. Gobierno de Ciberseguridad	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
• Fundamentos de Gobierno de Ciberseguridad y la Gestión de riesgos.	1.1 Fundamentos
	1.2 Gestión de Riesgos
	1.3 Marcos de Trabajo de Ciberseguridad
	1.4 Modelos de Madurez
	1.5 Gestión de Incidentes de Seguridad de la Información
UNIDAD 2. Seguridad en Sistemas de Información	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
• Evaluar los Sistemas operativos, las bases de datos, los Hipervisores y contenedores.	2.1 Sistemas Operativos y Bases de Datos
	2.2 Hipervisores y contenedores
	2.3 Criptografía
	2.4 Aplicaciones Web y de Escritorio
	2.5 DevSecOps
	2.6 Equipo de Usuario Final
UNIDAD 3. Seguridad en Infraestructuras de Red	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
• Describir los componentes de una red, además identificar la defensa perimetral y la defensa en profundidad	3.1 Componentes de Red
	3.2 Defensa Perimetral
	3.3 Defensa en profundidad
UNIDAD 4. Seguridad en Redes Inalámbricas	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
• Conocer la seguridad en redes inalámbricas, sus componentes, como también, identificar los protocolos de seguridad y los controles de acceso.	4.1 Protocolos de Seguridad
	4.2 Control de Acceso
	4.3 Componentes en Redes Inalámbricas

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**
Continua	Actividad Inicial (Foro), Cuadro comparativo de Metodologías de Gestión	35%

	de Riesgos de Ciberseguridad, Fase 1 Proyecto Final.	
Formativa	Parcial virtual Unidad 1, mapa conceptual controles sistemas de información, fase 2 proyecto final	35%
Formativa	Fase 3 Proyecto Final. Presentación completa del Proyecto Final incluyendo, nivel de madurez, controles a implementar y planeación de la implementación	30%
	Total del curso	**100 %**

BIBLIOGRAFÍA	
1	Chapple, M., Stewart, J. M., & Gibson, D. (2018). (ISC)2 CISSP® Certified Information Systems Security Professional: Official Study Guide, Eighth Edition. Indianapolis: John Wiley & Sons, Inc.
2	Deloitte. (Marzo de 2019). Cyber Strategy Framework. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/es/Documents/riesgos/Deloitte-ES-RA-CyberStrategyFram ework.pdf
3	Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity - Attack and Defenses Strategies. Birmingham: Packt Publishing.
4	Garbis, J., & Chapman, J. (2021). Zero Trust Security: An Enterprise Guide. Atlanta: Apress. doi:https://doi.org/10.1007/978-1-4842-6702-8
5	Harkins, M. (2013). Managing Risk and Information Security. Apress Media, LLC.
6	NIST - National Institute of Standards and Technology. (16 de Abril de 2018). Framework for Improving Critical Infrastructure Cybersecurity. Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
7	Salmon, A., Levesque, W., & McLafferty, M. (2017). Applied Network Security. Birmingham: Packt Publishing.
8	Siriwardena, P. (2020). Advanced API Security. Berkeley: Apress. doi:https://doi.org/10.1007/978-1-4842- 2050-4_1
9	Stallings, W. (2017). Cryptography and Network Security. Harlow: Pearson. U.S. Department of Energy. (Julio de 2021). Cybersecurity Capability Maturity Model (C2M2). Obtenido de https://c2m2.doe.gov/C2M2%20Version%202.0%20July%202021.pdf

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 Ciberseguridad	**X**	**X**	**X**	**X**												
2.	Seguridad en Sistemas de Información					**X**	**X**	**X**	**X**	**X**							
3.	Seguridad en Infraestructuras de Red										**X**	**X**	**X**				

4.	Seguridad en Redes Inalámbricas												**X**	**X**	**X**	**X**

ELABORÓ: Yesid Alberto Tibaquira Cortes