INFORMACIÓN ESPACIO ACADÉMICO						
Nombre de asignatura	**SEGURIDAD CLOUD**					
Código	11503004 - Electiva III					
Definición de asignatura	***Obligatorio***		***Básico***		***Complementario***	
	Electivo	***X***	***Intrínseco***		***Extrínseco***	***X***
Número de créditos	*2*	*Horas*	4	*Semanas*	*16*	
Distribución créditos	*HTD*	*64*	*HTC*	*32*	*HTA*	48
	Horas de trabajo cooperativo					
Metodología	• Metodología Pedagógica y Didáctica • Modelo virtual con la plataforma de aprendizaje Interactiva Moodle • Foros en la plataforma virtual • Lecturas (artículos, fragmentos de libros) • Trabajo colaborativo mediante la herramienta Moodle. • Se debe procurar incentivar el trabajo de grupo más que el trabajo individual. (Se recomienda trabajar en grupos de cuatro a cinco estudiantes).					

PROGRAMACIÓN DEL CONTENIDO
CONOCIMIENTOS PREVIOS
• Tecnologías de la información • Seguridad de la Información • Ciberseguridad
DESCRIPCIÓN DEL CURSO
La asignatura Seguridad Cloud brindará, en un primer momento, los conceptos fundamentales que permitirán comprender a qué hace referencia el término de computación en la nube, la gestión de los riesgos de seguridad de la información a los que está expuesta la información y las soluciones tecnológicas que son implementadas en nube. Asimismo, permitirá los diferentes mecanismos de protección de la información en las diferentes fases del ciclo de vida de seguridad de los datos en la nube en los diferentes modelos de servicio y de despliegue, teniendo en cuenta las necesidades organizacionales, legales, regulatorias y de cumplimiento aplicables según los sectores industriales de las organizaciones.
ÁREAS DE CONOCIMIENTO
En el desarrollo de la asignatura se cubrirán los siguientes temas: • Computación en la nube. • Riesgos de seguridad de la información y de ciberseguridad • Controles de seguridad en la nube
COMPETENCIAS EN FORMACIÓN

Al final de la asignatura el estudiante podrá contar con las siguientes competencias:

- Comprender los conceptos fundamentales de la computación en la nube.
- Identificar y gestionar los riesgos de seguridad de la información y ciberseguridad de la implementación de una solución en la nube.
- Desarrollar las habilidades requeridas para implementar y soportar la implementación de soluciones en la nube desde una perspectiva basada en seguridad de la información.

ESTRUCTURA DEL MÓDULO	
UNIDAD 1. Conceptos y Arquitectura.	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Conocer los conceptos básicos, riesgos, amenazas y marcos de seguridad para la computación en la nube.	1.1 Conceptos y arquitectura
	1.2 Conceptos de seguridad.
	1.3 Riesgos y marcos de trabajo de seguridad.
	1.4 Evaluación de proveedores.
UNIDAD 2. Seguridad de los datos.	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Identificar y proponer los controles de seguridad en el ciclo de vida de la seguridad de los datos en la computación en la nube.	2.1 Ciclo de vida de la seguridad de datos y arquitecturas de almacenamiento.
	2.2 Descubrimiento y clasificación.
	2.3 IRM y protección.
	2.4 Retención, eliminación y gestión de registros de auditoría.
UNIDAD 3. Seguridad de la infraestructura y Aplicaciones.	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Identificar la estructura de la nube y de los centros de cómputo, como también, el plan de recuperación de desastres (DRP) y el plan de continuidad de negocio (BCP)	3.1 Infraestructura en nube y centros de cómputo.
	3.2 Seguridad en infraestructura, DRP & BCP.
	3.3. Concientización y ciclo de vida de desarrollo seguro.
	4.4 Validación de aplicaciones, controles y gestión de identidades.
UNIDAD 4. Seguridad en las operaciones y Marco legal.	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
• Identificar y proponer los controles de seguridad a nivel de infraestructura y aplicación en una solución desplegada en la nube. • Establecer las necesidades y restricciones legales, de privacidad y de auditoría que tiene la implementación de una solución en la nube.	4.1 Seguridad física y lógica en infraestructura.
	4.2 Gestión de procesos de TI, Forense y SOC.

	4.3 Requerimientos legales y privacidad.
	4.4 Riesgo empresarial y proveedores.

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**
Formativa	Foro: actividad inicial	0%
Evaluativa	**Unidad 1.** Modelos de despliegue y servicio. **Unidad 1**. Conceptos y arquitectura	16%
	Unidad 2. Ciclo de vida de seguridad en los datos. **Unidad 2.** Descubrimiento digital vs. eDiscovery	17.5%
	Unidad 3. Seleccionando un caso de estudio en la nube. **Unidad 3.** Los servicios de seguridad en la nube.	17.5%
	Unidad 4. Análisis de seguridad de caso de estudio.	35%
	Total del curso	**100 %**

BIBLIOGRAFÍA	
1	**(ISC)². (2023)**. *The official (ISC)²CCSP CBK Reference (4th ed.).* New Jersey: John Wiley & Sons.
2	**Cloud Security Alliance. (2019).** *Top Threats to Cloud Computing: Egregious Eleven.* https://cloudsecurityalliance.org/artifacts/top-threats-to-cloudcomputing-egregious-eleven/

3	**Cloud Security Alliance. (2021).** *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0.* https://cloudsecurityalliance.org/download/securityguidance-v4.
4	**Dotson, C. (2019).** *Practical Cloud Security: A Guide for Secure Design and Deployment.* Sebastopol: O'Reilly Media.
5	**ENISA. (2009).** *Cloud Computing Risk Assessment.* Obtenido de https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
6	**Joyanes Aguilar, L. (2012).** *Computación en la nube. Estrategias de Cloud Computing en las Empresas.* México: Alfaomega.
7	**NIST -** National Institute of Standards and Technology. (September de 2011). *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

ORGANIZACIÓN / TIEMPOS																
PROGRAMA SINTÉTICO		**SEMANAS ACADÉMICAS**														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1.	**Unidad 1.** Conceptos y Arquitectura.	**X**	**X**	**X**	**X**												
2.	**Unidad 2.** Seguridad de los datos.					**X**	**X**	**X**	**X**								
3.	**Unidad 3.** Seguridad de la Infraestructura y Aplicaciones.									**X**	**X**	**X**	**X**				
4.	**Unidad 4.** Seguridad en las Operaciones y Marco Legal.													**X**	**X**	**X**	**X**

ELABORÓ: Yesid Tibáquira
15/06/2023