FACULTAD DE INGENIERÍA Y ARQUITECTURA
SECCIÓN POSGRADO: MAESTRÍA

SÍLABO
SEGURIDAD DE INFORMACIÓN

I. DATOS GENERALES

1.1 Facultad	:	Ingeniería y Arquitectura
1.2 Escuela	:	Post Grado
1.3 Semestre Académico	:	2019 – II
1.4 Código	:	091101
1.5 Ciclo	:	I
1.6 Créditos	:	04
1.7 Horas Semanales	:	04
1.8 Carácter	:	Obligatorio
1.9 Pre – requisitos	:	091081
1.10 Profesor Responsable	:	Mg. Ing. Jorge Martin Figueroa Revilla

II. SUMILLA

Se crea competencia y habilidades para entender el valor de los activos tangibles e intangibles de Hardware, software, comunicaciones y recursos humanos, así como sus vulnerabilidades. Así como para el diseño de procesos de monitoreo y evaluación de los activos, documentar los riesgos, amenazas, áreas de impacto, que permitan anticiparse a los cambio y amenazas relacionados al medioambiente y el uso de las TIC. Se crean competencias para identificar los conceptos fundamentales de un SGSI según las normas ISO y otras normas internacionales relacionadas, y su implementación progresiva en las organizaciones. Del mismo modo el estudio de las técnicas de auditoría y control orientados hacia los sistemas informáticos de una organización. La auditoría de los sistemas de gobierno corporativo y gestión / administración de las Tecnologías de la Información en la empresa; la auditoría de las funciones, procesos y actividades ligadas a la adquisición, el desarrollo y la puesta en funcionamiento de los Sistemas de Información en la empresa; la auditoría de las funciones, procesos y actividades ligadas a la operación, mantenimiento y soporte de los Sistemas de Información en la empresa.

III. COMPETENCIAS Y SUS COMPONENTES COMPRENDIDOS EN LA ASIGNATURA

3.1 Competencias

- Adquiere un conocimiento amplio de las metodologías y herramientas necesarias para realizar la evaluación de riesgos como el diseño e implementación de un SGSI (Sistema de Gestión de Seguridad de Información).
- Obtiene el conocimiento necesario para evaluar las vulnerabilidades como los riesgos existentes con el fin de identifica los controles necesarios para implementar un sistema de gestión de seguridad de información para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Reconoce los fundamentos para realizar un diagnóstico de seguridad de información, diseñar un

Sistema de Gestión de Seguridad de información y cumplir con lo requerido en los 14 dominios exigidos por la ISO de seguridad de Información.

- Gerencia efectivamente de la gestión de seguridad de información.

3.2 Componentes

- **Capacidades**

- Desarrolla las habilidades necesarias para identificar y evaluar las debilidades propias de la organización gestión de la seguridad de información.
- Desarrolla la capacidad para participar y dar conceptos en el proceso de planeación estratégica de TI aportando el elemento de control.
- Planifica el desarrollo de una Auditoría de Sistemas.
- Supervisa las funciones de Seguridad de Información.

- **Contenidos actitudinales**

- Propone las recomendaciones de valor para el negocio.
- Comprende el proceso de Seguridad de la Información.
- Proporciona las herramientas necesarias para diseñar, planear y ejecutar un Sistemas de Gestión de Seguridad.
- Comprende el Sistema de Gestión de Seguridad de Información SGSI.
- Comprende los 14 procesos que exige la Norma Internacional que soportan la entrega y la administración de los sistemas de información dentro de un entorno específico.

IV. PROGRAMACIÓN DE CONTENIDOS

UNIDAD I: Gestión de la Seguridad de Información					
CAPACIDAD: Desarrolla las habilidades necesarias para Gestionar el Gobierno y Gestión de la Seguridad de Información.					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
1	Presentación del curso. Conceptos y lineamientos metodológicos para el gobierno y gestión de la Seguridad de Información.	Conocer los estándares y marco de referencia, lineamientos metodológicos para la Gestión de Seguridad de la Información. - Conocer las buenas prácticas para su implementación. Definir los grupos para los talleres y planteamiento de casos.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
2	Definición e implementación de estrategias con enfoque de gobierno seguridad de Información.	Analizar los fundamentos de la gestión de seguridad de información.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
3	Evaluación y gestión de Riegos en Seguridad de Información	Aplicar la Gestión de Riesgos de seguridad de información y como se reduce el nivel de vulnerabilidad.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
4	Gestión de un programa y portafolio de la seguridad de información: caso de negocio, roles y responsabilidad.	Conocer los estándares y marco de referencia, lineamientos metodológicos para definir un programa y portafolio de proyectos de Gestión de Seguridad de la Información. -	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4

UNIDAD II: Definición de Estrategias, Procesos de las Gestión de seguridad de información					
CAPACIDAD: Desarrolla la capacidad para participar y dar conceptos en el proceso de seguridad de información y aportando al gobierno de gestión de seguridad de información					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
5	Gestión de los procesos de la seguridad de información; activos de información, proveedores, cultura, incidentes, continuidad y cumplimiento.	Conocer los procesos de la seguridad de información, definir los activos de información, continuidad y cumplimiento.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
6	Principios de ciberseguridad bajo la ISO 27032 y criterios de implantación de criterios.	Conocer los fundamentos y procesos de Ciberseguridad.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
7	Desarrollo de un Sistemas de Gestión de Ciberseguridad	Definir y desarrollar un SGCS con trabajo de investigación.	**De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
8	Examen Parcial	Estudiar los temas hasta la Unidad II.	**De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	

UNIDAD III: Desarrollo de un Sistema de Gestión de Seguridad de Información, sus dominios y procesos.					
CAPACIDAD: Planifica el desarrollo de un Sistema de Gestión de Seguridad de Información					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
9	Desarrollo de objetivos, necesidades y Requisitos de seguridad de información.	Desarrollar y evaluar los requisitos de seguridad de información.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
10	Definición dl Alcance y Políticas de seguridad de Información	Metodología de análisis de riesgos y activos de información.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
11	Inventarios de Activos, identificar amenazas y vulnerabilidades, identificar impacto, análisis y evaluación de riesgos, selección de controles.	Analizar e implementar cada una de las actividades relacionadas al análisis de vulnerabilidades, riesgos, y selección de controles.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
12	Definir plan de tratamiento de riesgos, controles, operación del SGSI.	Realizar cada una de las actividades para operar un SGSI.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas	4	4

			· Trabajo grupal: 1 hora		

UNIDAD IV: GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS DE TI					
CAPACIDAD: Diseñar y gestionar la continuidad de los servicios de T.I.					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
13	BIA (Recursos Mínimos, RTO's y RPO's), Análisis de Riesgos, Estrategias Operativas, Administración de Crisis, Mecanismos de Comunicación, Divulgación y Capacitación, Cronogramas de Pruebas	Desarrollar el análisis del impacto, análisis de riesgos.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
14	Plan de Recuperación de desastres Plan de contingencia de T.I.	Desarrollar de los planes de Recuperación de desastre y Plan de continuidad de tecnología. Desarrollar y evaluar los procesos para la de Continuidad de Negocio.	**Lectivas (L):** · Introducción al tema: 1 hora · Desarrollo del tema: 2 horas · Ejercicios en aula: 1 hora **De trabajo Independiente (T.I):** · Resolución tareas: 1 hora · Trabajo de investigación: 2 horas · Trabajo grupal: 1 hora	4	4
15	Sustentación del trabajo final	Sustentación de los trabajos finales.	**Lectivas (L):** · Conclusiones del curso: 1 hora · Sustentación de los trabajos finales: 3 horas	4	
16	Examen Final	Estudiar los temas de todas las unidades.			

V. CONTENIDO

ESTRATEGIAS METODOLÓGICAS

- Método Expositivo – Interactivo. Disertación docente, exposición del estudiante.
- Método de Discusión Guiada. Conducción del grupo para abordar situaciones y llegar a conclusiones y recomendaciones.
- Método de Demostración – Ejecución. El docente ejecuta para demostrar cómo y con que se hace y el estudiante ejecuta, para demostrar que aprendió.

RECURSOS DIDÁCTICOS

Equipos: computadora, ecran, proyector de multimedia.
Materiales: Separatas, pizarra, plumones.

EVALUACIÓN DEL APRENDIZAJE

El promedio final de la asignatura se obtiene mediante la fórmula siguiente:

PF = (PE+EP+EF)/3

PE= (P1+P2+P3+P4+P5)/5

Dónde:

PF	: Promedio Final
PE	: Promedio de evaluación
EF	: Examen final
P1 - P5	: Prácticas calificadas (escrito)

VI. FUENTES DE CONSULTA:

Bibliográficas

- Modelo para el gobierno de las TIC basado en las normas ISO, Carlos Manuel y Mario Piattini Velthuis ***Aenor Ediciones,*** *2014*
- *Seguridad de la Información, Redes, Informática y sistemas de Información; Javier Areitio; 2014*

Electrónicas

- Los Objetivos de Control para la Información y la Tecnología relacionada / IT Governance based on CobiT4.1: *http:// www.itri.org/ Cobit 4.1.pdf*
- Los Objetivos de Control para la Información y la Tecnología relacionada / IT Governance based on (COBIT @ 5.0)*: http:// www.itri.org/ Cobit 5.0.pdf*
- Internacional Organization for Standardization (2014): *ISO/IEC 27000:2014 – Information Teclmology :* http://webstore.iec.ch/preview/info_isoiec27000.pdf
- Internacional Organization for Standardization (2014): *ISO/IEC 27001:2014 – Tecnología de la informacion. Técnica de seguridad. Sistemas de Gestión de la Seguridad de la información(SGSI) Requisitos*
  http://webstore.iec.ch/preview/info_isoiec27001.pdf
- Internacional Organization for Standardization (2014): *ISO/IEC 27002:2014 – Tecnología de la información- Técnica de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.*
  http://webstore.iec.ch/preview/info_isoiec27002.pdf

- Internacional Organization for Standardization (2018): *ISO/IEC 27005:2018 – Tecnología de la información- Gestión de Riesgos de Seguridad de Información.* http://webstore.iec.ch/preview/info_isoiec27002.pdf

Libros Texto:

- Information Security Management Handbook, 4th Ed. by Harold F. Tipton and Micki Krause
  CISSP Certified Information Systems Security Professional Study Guide