VICERRECTORÍA DE DOCENCIA DE PREGRADO – DIRECCIÓN DE PREGRADO
Proceso de EVALUACIÓN FORMATIVA DE SYLLABUS

NOMBRE DEL MODULO	*SEGURIDAD Y AUDITORIA INFORMATICA*
Nº CRÉDITOS ECTS	*Clases: 2 Horas* *Ayudantía: 1 Hora* *Laboratorio: 1 Hora* *Estudio Autónomo: 3,5* *Total Semanal: 7,5 Horas* *Total Módulo: 135 Horas → 5 créditos ECTS*
NIVEL	*9 (Noveno Semestre)*
REQUISITOS	*SISTEMAS OPERATIVOS Y REDES*
RESPONSABLE(S) DE LA CONSTRUCCIÓN DEL SYLLABUS	*INGENIERÍA INFORMÁTICA EMPRESARIAL*

CONTRIBUCIÓN DE ESTE MÓDULO A LA FORMACIÓN	*El Modulo de Seguridad y auditoría Informática, está orientada a introducir a los alumnos en la teoría y mejores prácticas que sustentan las necesidades críticas de la industria de proporcionar una formación profesional que permita asegurar que la Tecnología de Información en la Organización se lleve a cabo de manera responsable, y bajo los controles de seguridad apropiados según el actual estado de cosas en la materia. Que puedan identificar, entender y evaluar los principales riesgos que puede generar el uso de Tecnologías de Información (TI) en las Empresas y determinar, mejorar y evaluar los controles computacionales que puedan minimizar dichos riesgos.* *Deberán ser capaces de entender en la practica la naturaleza y alcance de los problemas y soluciones que se encuentran en el campo de aplicación.* *Los estudiantes deberán ser capaces de enfrentar una Auditoría de Sistemas de Información, e informar adecuadamente de los resultados de ésta. Adicionalmente, los estudiantes serán capaces de planificar, ejecutar y controlar este tipo de auditoría, enfrentándose con seguridad a los riesgos encontrados en los sistemas computacionales de la empresa, generando los procedimientos de auditoría necesarios usando modernas tecnologías de información.*
COMPETENCIAS QUE COMPROMETE EL MÓDULO	*Los estudiantes deberán ser capaces de enfrentar una Auditoría de Sistemas de Información, e informar adecuadamente de los resultados de ésta. Adicionalmente, los estudiantes serán capaces de planificar, ejecutar y controlar este tipo de auditoría, enfrentándose con seguridad a los riesgos encontrados en los sistemas computacionales de la empresa, generando los procedimientos de auditoría necesarios usando modernas tecnologías de información.*

SUBCOMPETENCIAS DEL MÓDULO	1. Comprender los Fundamentos y Principios de Seguridad de la Información 2. Comprender y Analizar Fundamentos y Principios de Arquitectura de Seguridad de Computación en la Organización 3. Conocer y Aplicar las Mejores Prácticas de Seguridad de la información para Computación en la Organización, basado en estándares familia ISO 27000, NIST, SANS. 4. Comprender y Analizar Fundamentos y Principios de Seguridad en Redes y Telecomunicaciones 5. *Entender y Desarrollar un plan estratégico de Seguridad Informática* 6. *Entender y Desarrollar un plan de continuidad de negocios* 7. *Entender y Desarrollar una Auditoría Informática de Negocios para un ámbito empresarial*

UNIDADES DE APRENDIZAJE	• **Módulo I: Fundamentos de Seguridad de la Información** • Motivación • Introducción • Islas de Gestión • El ciclo de Gestión de Seguridad de la Información. • SGSI - Un Sistema de Seguridad de la Información en la Institución/Organización. • Comité de Seguridad de la Información: su Conformación y Responsabilidad • Políticas de Seguridad de la Información y aspectos transversales

	• **Módulo II: La importancia del Balance entre Objetivos de Gestión y Objetivos Técnicos**
	  • Introducción
	  • ISO 27000
	  • Riesgos
	  • Continuidad de Negocios
	  • PCI
	  • SSI
	  • Otros

	• **Módulo III: Arquitectura y Modelos de Seguridad**
	  • Conceptos de control y seguridad
	  • Modelos de seguridad
	  • Criterios de evaluación de seguridad
	  • Seguridad en entornos cliente/servidor, 3 tier, Cloud
	  • Seguridad y la arquitectura de redes
	  • Arquitectura de la seguridad IP

	• **Modulo IV: Seguridad en Internet, Redes y Telecomunicaciones** • Gestión de la seguridad en las comunicaciones • Protocolos de red • Métodos de identificación y autenticación • Comunicación de datos • Mecanismos de seguridad de Internet y Web • Diferentes métodos de ataque • Seguridad en multimedios
	Módulo V: Continuidad del Negocio y Recuperación de Desastres • *Plan de continuidad de negocios (BCP)* • *Análisis de impacto (BIA), matriz de riesgo* • *Plan de recuperación de desastres (DRP)*

	Módulo VI: Auditoría de Sistemas • Conceptos • Tipos de auditorias Desarrollo de auditoria de aplicación

METODOLOGÍA(S) A USAR	Los contenidos formales y las visiones sobre el tema se entregarán a través de clases expositivas. Las habilidades específicas se mostrarán en las clases y se ejercitarán a través de talleres grupales e individuales basados en trabajos entregados durante las clases. El curso contempla la ejecución de las actividades pedagógicas que se señalan a continuación y tienen como objetivo afianzar la actividad de aprendizaje de los contenidos del curso: a. Exposición • Exposición presencial de los relatores de los contenidos del Curso, según temario de este. b. Trabajo y Taller Grupal • Desarrollar trabajo grupal y un taller grupal y general para cada uno Informe Resumen de un paper seleccionado, el Informe no debe tener más de 10 páginas, y debe ser desarrollado fuera de las horas de clases. a. Trabajo y Taller Individual • Desarrollar trabajo y un taller Individual y generar por cada uno un Informe Resumen de un trabajo seleccionado, el Informe no debe tener más de 10 páginas y un resumen ejecutivo en formato de presentación, no debe tener más de 5 slides y debe ser desarrollado fuera de las horas de clases. c. Evaluación Individual • Dos Evaluación realizada a cada participante al final del curso basado en las preguntas/respuestas desarrolladas durante toda la dictación de este. Tendrá un formato de selección múltiple.

EVALUACIÓN DEL APRENDIZAJE	***Parte teórica (60%)*** *Prueba 1 de conceptos asociados a las Unidades 1 y2 (25%)* *Prueba 2 de conceptos asociados a la Unidad 3 y 4 (25%)* *Prueba 3 de conceptos asociados a la Unidad 5 y 6 (25%)* *Controles (3) de lectura (25%)* ***Parte práctica (40%)*** *Desarrollo y presentación de* *1) Trabajo Grupal: Analisis y desarrollo de un caso de ataque importante al sistema de una organización importqnte (30%)* *2) Trabajo Grupal: Vulnerabilidades en redes (30%)* *3) Trabajo individual: Vulnerabilidades en teléfonos celulares (40%)* *Existirá una instancia de recuperación de una Prueba Teórica que incluirá toda la materia del curso, por lo que no será necesario justificar la inasistencia a Prueba. En consecuencia, solo se puede faltar a rendir una prueba durante el módulo; para las otras inasistencias se evaluará con la nota mínima. A esta instancia también podrán acceder voluntariamente quienes habiendo rendido todas la pruebas teóricas, deseen reemplazar su peor nota teórica.* *Adicionalmente, existirá la instancia de Prueba de Recuperación, para quienes estén en condición de reprobación, establecida en el reglamento académico de la Escuela, que se ponderará con un 30% y la nota de presentación con un 70%Se Complementara en el transcurso del desarrollo del módulo.*

BIBLIOGRAFÍA	• Getting an Information Security Job For Dummies, Peter H Gregory • Information Security The Complete Reference, 2nd Edition, Editor Mark Rhodes-Ousley, 2013 • Managing Risk and Information Security, Malcolm Harkins, 2013 • Information Security Risk Analysis, 2 Ed., Thomas R. Peltier, 2005 • Carbanak APT, The Great Bank Robbery, Caspersky Labs, 2015 • Hacking Wireless Networks, Module 15, • Hacking Mobile Platforms, Module 16 Tambien • Familia de Estándares ISO 27000 • CISSP • www.nist.org • www.sans.org *Los papers y libros estarán en el Educandus incluidos los de lectura obligatoria para Controles*