UNIVERSIDAD MARIANO GALVEZ DE GUATEMALA
FACULTAD DE INGENIERIA EN SISTEMAS DE INFORMACION
LICENCIATURA EN ADMINISTRACION DE SISTEMAS DE INFORMACION
JORNADA DIARIA VESPERTINA 26/09/2023

Curso: **Seguridad de Sistemas** Código: **538**

Pre-requisitos: **533**

PROGRAMA DEL CURSO

JUSTIFICACION:

Las operaciones de negocios y su administración dependen en gran parte de la tecnología, específicamente de las tecnologías de información (TI) (IT – Information Technologies). Por lo tanto, las estrategias de TI deben estar perfectamente alineadas con las estrategias de negocio.

La tendencia actual esta orientada al incremento gradual del soporte que las TIs brindan a las estrategias de negocio. Esto genera un alto grado de dependencia.

Conforme las empresas alcanzan mayores grados de madurez, necesitan implementar dentro de su cultura de negocios, el aseguramiento de los sistemas de información y el Gobierno de TI (IT Governance). Esto significa, la adopción de políticas y normativas generalmente aceptadas, mejores prácticas, para incrementar el aseguramiento de uno de sus mayores capitales, la información relativa a sus negocios.

La administración del riesgo operativo y del riesgo financiero regularán las estrategias de negocio. La administración del riesgo tecnológico regulará el aseguramiento de los sistemas de información.

DESCRIPCIÓN:

En la actualidad las tecnologías de información (TI) conforman el apoyo más importante en cualquier tipo de empresa. El aseguramiento de los sistemas de información es un proceso continuo, conforme varían y se incrementan las estrategias de negocio, aunado a las amenazas y vulnerabilidades que se presentan en el mercado, se elevarán los niveles de riesgo inherente a la utilización de tecnología. De acuerdo con lo anterior, es necesario brindar al estudiante los conocimientos sobre las principales metodologías para el aseguramiento de los sistemas de información y la implementación del Gobierno de TI.

OBJETIVO GENERAL:

Proporcionar al estudiante los conocimientos esenciales que le sirven para administrar de forma eficiente el riesgo tecnológico, en aquellas empresas que utilizan el procesamiento electrónico de datos para procesar la información económica, contable y de toma de decisiones.

Esto implica, la capacidad de realizar diagnósticos, desarrollar proyectos de implementación de políticas, normativas y mejores prácticas que estén correctamente alineadas a las estrategias de negocio y a la situación real de las empresas.

OBJETIVOS ESPECIFICOS:

- Se refuercen los conocimientos sobre los sistemas de información, automatizados en cuanto a planeación, análisis, diseño e implantación y producción.
- Proporcionar recomendaciones prácticas y posibles, a los riesgos identificados dentro de las áreas de la empresa.
- Aplicar los procedimientos básicos y primordiales para el aseguramiento de los sistemas de información.
- Elegir técnicas, herramientas, métodos de análisis, a utilizar para el aseguramiento de los sistemas de información.
- Evaluar las aplicaciones desde el punto de vista operativo, de entrada, proceso y salida de los datos de acuerdo a las necesidades de la empresa.
- Evaluar la parte de seguridad de los datos y sistemas aplicativos.
- Establecer los lineamientos para fortalecer la seguridad física y la seguridad lógica de TI.
- Establecer los lineamientos para fortalecer las relaciones entre Seguridad de los Sistemas y Auditoria de Sistemas.
- Establecer los lineamientos para fortalecer las relaciones con los clientes internos, externos y proveedores de nuestras tecnologías de información.

CONTENIDOS MINIMOS:

- Unidad I:
  - Conceptos básicos de Seguridad Informática
  - Finalidades de la Seguridad Informática
  - Fundamentos de la Seguridad Informática
  - Objetivos generales y específicos de la Seguridad Informática
  - Metodologías para el desarrollo e implementación de la Seguridad Informática
  - Etapas de madurez de la Seguridad Informática
  - Laboratorios

- Unidad II:
  - Procesos de Seguridad Informática
  - Campos de acción de la Seguridad Informática
  - Relación de la Seguridad Informática con otras ciencias de la Administración. Riesgo Operativo y Riesgo Financiero. Riesgo Tecnológico
  - Laboratorios

- Unidad III:
  - Principales estrategias del Cyber-crimen. Análisis retrospectivo, actualizado y a futuro.
  - Leyes y reglamentos de la República de Guatemala, relacionados con Seguridad Informática
  - Gobierno de TI. Estrategias de implementación
  - Laboratorios

- Unidad IV:
  - Definición de Cyber-crimen
  - Metodologías, políticas y normativas generalmente aceptadas. ISO, ITIL, COBIT, PCI.
  - Organizaciones internacionales que combaten el Cyber-crimen. IOCE. CERT.
  - Mejores practicas para Seguridad Informática
  - Hacking ético
  - Herramientas administrativas para proyectos de Seguridad Informática
  - Laboratorios

- Unidad V:
  - Ámbitos de control físico y lógico. Controles de Seguridad Informática
  - Controles de seguridad física
  - Controles de seguridad lógica
  - Aseguramiento del Data Center (Centro de Datos)
  - Aseguramiento de la calidad los servicios que brinda TI. Productos de hardware y software. Control de Cambios. Control de Accesos
  - Virtualización de servidores. Globalización de servicios. Ambientes homogéneos. Procesos de Hardening y Patching. Continuidad
  - Estrategias tecnológicas. e-commerce, e-banking. Firma digital. IT Mobile. Otros
  - Laboratorios

- Unidad VI
  - Toma de decisiones criticas en proyectos de Seguridad Informática
  - Manejo de presupuestos en proyectos de Seguridad Informática
  - Dificultades de la Seguridad Informática. Análisis retrospectivo, actualizado y a futuro.
  - Reseña sobre Business Continuity Planning, Disaster Recovery Planning y su relación con la Seguridad Informática
  - Retos y proyecciones de TI, del Cyber-crimen y de la Seguridad Informática. Acompañamiento del marco normativo legal
  - Especializaciones en Seguridad Informática: CISM, CISA, CISSP, CCNA, ITIL
  - Laboratorios

BIBLIOGRAFÍA: