DIPLOMADO EN SEGURIDAD Y AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

DURACIÓN

5 MESES

COLEGIO POSTGRADO UTEPSA

www.utepsa.edu

GENERALIDADES

OBJETIVO GENERAL

Dotar al estudiante de conocimientos, habilidades y destrezas destinadas al análisis, planificación, preparación y ejecución de procesos de Seguridad y Auditoría en Tecnologías de la Información.

OBJETIVOS ESPECÍFICOS

- Conocer sobre la seguridad en TI
- Identificar las normas que apoyan la seguridad y la auditoria en TI
- Identificar los riesgos de la seguridad en TI
- Establecer los controles de seguridad en TI
- Planificar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Analizar amenazas de seguridad
- Identificar vulnerabilidades
- Aplicar Hacking Ético y Test de Penetración.
- Conocer el marco de trabajo de COBIT
- Comprender el enfoque de Gobierno y Dirección en TI
- Comprender las características del proceso de auditoría de TI
- Elegir y aplicar TAACs
- Determinar las acciones previas de una auditoría de TI
- Ejecutar de forma metódica el proceso de auditoría

PERFIL PROFESIONAL

El educando que concluya y apruebe cada uno de los módulos de formación estará capacitado de tal manera que puede:

- Diferenciar entre Seguridad Informática y Seguridad de la Información, dentro de un escenario estratégico de Procesos de Negocio.
- Identificar los riesgos y establecer los controles de Seguridad, para planificar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) en el marco de la norma ISO 27001.
- Analizar amenazas e identificar vulnerabilidades, para aplicar de forma eficiente el Hacking Ético.
- Conocer el marco de trabajo de COBIT, el gobierno y la dirección en Tecnologías de la Información, para implantar o implementar buenas prácticas.
- Comprender cada una de las características del proceso de auditoría de Tecnologías de la Información, para elegir y aplicar las Técnicas de Auditoría Asistidas por Computadora (TAAC) más adecuadas.
- Determinar las acciones previas a la aplicación de una auditoría de TI y ejecutar de forma metódica el proceso de auditoría.

CONTENIDO

MÓDULO I
SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN Y NORMATIVIDAD

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Diferenciar entre Seguridad Informática y Seguridad de la Información, para comprender el escenario estratégico del Proceso de Negocio, considerando las causas de fallos, pérdidas, problemas, daños y normas de seguridad dentro de un modelo orientado a procesos.

UNIDADES TEMÁTICAS

1. Introducción a la Seguridad en Tecnologías de la Información
   - ¿Qué es Seguridad de la Información?
   - Causas comunes de fallos
   - Resultado para la empresa
   - Terminología
2. Visión Tecnológica
   - Tipos de tecnologías
   - Inconvenientes

3. Visión Estratégica
   - Modelo de Gestión de Seguridad de la Información no dirigido por la Tecnología sino orientado a Procesos de Negocio
   - Herramienta de Toma de Decisiones sobre Seguridad de la Información
4. Normatividad Vigente
   - ISO 27001
   - ISO 27002
   - Estándar BS 25999
   - Normas bolivianas vigentes

MÓDULO II
RIESGO, CONTROLES E IMPLEMENTACIÓN DE UN SGSI

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Identificar los riesgos y establecer los controles de Seguridad, para planificar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), considerando las actuales prácticas realizadas en el marco de la norma ISO 27001.

UNIDADES TEMÁTICAS

1. Gestión de Riesgo bajo la norma ISO 27001
   - El Riesgo
   - Proceso de análisis
   - Valoración de riesgos
2. El Control y la Seguridad
   - El Control
   - Tipos de Controles
   - Selección, tratamiento e implementación de Controles
3. SGSI y su proceso de planificación
   - Definición
   - Preparación
   - Determinación de las necesidades de protección
   - Establecimiento de los requisitos de Seguridad
   - Selección de los controles de Seguridad
   - Organización de la Seguridad
   - Elaboración del Plan de Seguridad
4. Proceso de Implementación del SGSI
   - Programa de Desarrollo de la Seguridad de la Información

- Factores Críticos de éxito

5. Proceso de Verificación del SGSI
   - Métodos de medición
   - Indicadores de medición

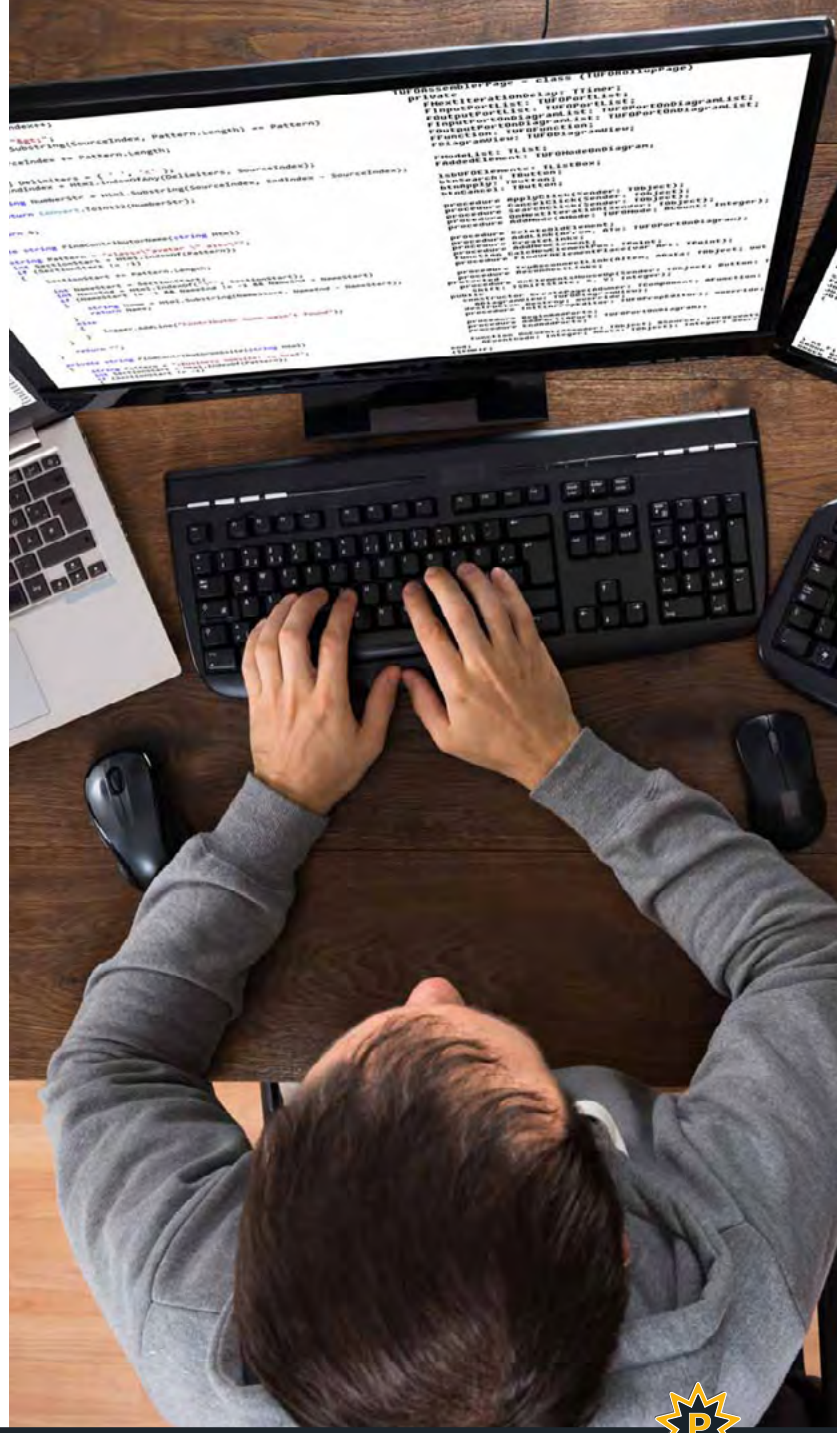
MÓDULO III
ETHICAL HACKING Y TEST DE PENETRACIÓN

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Analizar amenazas e identificar vulnerabilidades, para aplicar de forma eficiente el Hacking Ético, considerando técnicas intrusivas modernas y metodologías apropiadas para cada tipo de ataque informático.

UNIDADES TEMÁTICAS

1. Análisis y tratamiento de Amenazas y Vulnerabilidades
   - Tipos de Amenazas
   - Tratamiento de Vulnerabilidades
2. Hacking Ético
   - Hacking Ético Externo



- Hacking Ético Interno
- Hacking de Aplicaciones Web
- Herramientas de Hacking Ético

3. Pruebas de ingeniería Social
   - Comportamiento humano
   - Tipos de Pruebas
4. Informática Intrusiva y Test de Penetración
   - Principios de Testeo
   - Metodologías de Testeo OSSTMM, ISSAF, OWASP
   - Test de Penetración

MÓDULO IV
COBIT, GOBIERNO Y DIRECCIÓN DE TI

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Conocer el marco de trabajo de COBIT, el gobierno y la dirección en Tecnologías de la Información, para implantar o implementar buenas prácticas, considerando modelos actuales de aplicación en el marco de normas internacionales de ISACA.

UNIDADES TEMÁTICAS

1. El marco de TI y COBIT
   - Estándares y Marcos de Trabajo: ITIL, Serie ISO/IEC 27000, Serie ISO/IEC 31000- COBIT e ISACA
2. Gobierno y Dirección de TI
   - Evaluar, Orientar y Supervisar
   - Alinear, Planificar y Organizar
   - Construir, Adquirir e Implementar
   - Entregar, dar Servicio y Soporte
   - Supervisar, Evaluar y Verificar
3. Marco de Trabajo
   - Principios de COBIT 5
   - Metas, Ciclo de Vida y Buenas prácticas
4. Implantación e implementación
   - Fases de Implementación del Ciclo de Vida
5. Modelo de Capacidad de los Procesos
   - Niveles de Madurez
   - Niveles de Capacidad de Procesos ISO/IEC 15504
   - Atributos de Madurez vs. Atributos de Proceso
   - Catalizadores

MÓDULO V
AUDITORIA DE TI Y TÉCNICAS DE AUDITORÍA ASISTIDA POR COMPUTADOR

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Comprender cada una de las características del proceso de auditoría de Tecnologías de la Información, para elegir y aplicar las Técnicas de Auditoría Asistidas por Computadora (TAAC) más adecuadas, considerando las prácticas más modernas en cuanto a planificación, ejecución y generación de informes y reportes que permitan la mejora continua del negocio.

UNIDADES TEMÁTICAS

1. Auditoría de Tecnologías de la Información
   - Legislación Nacional e Internacional
   - Principios
   - Objetivo de la Auditoría de TI
   - Características del Proceso de Auditoría
2. Marco conceptual de las Técnicas de Auditoría Asistidas por Computadora TAAC
   - TAAC Definición
   - Técnicas Manuales vs Técnicas Asistidas

- Estándares que apoyan las TAAC
- Diseño de pruebas para utilización de TAAC
- Auditoria alrededor, a través y dentro del computador

3. Marco aplicativo de las TAAC:
   - Aplicación de TAAC
   - Técnicas administrativas
   - Técnicas para evaluar los controles de Aplicaciones en Producción
   - Técnicas para Análisis de Transacciones
   - Técnicas para el Análisis de Datos
   - Técnicas para el Análisis de Aplicaciones
4. Informes y documentación de las técnicas asistidas por computador
   - Planificación de TAAC
   - Ejecución de TAAC y Tipos de Software
   - Documentación de TAAC
   - Informes y reportes

MÓDULO VI
PROCESO DE AUDITORÍA, INFORMES Y DOCUMENTOS DE TRABAJO

COMPETENCIAS POR GENERARSE EN EL MÓDULO

Determinar las acciones previas a la aplicación de una auditoría de TI, para ejecutar de forma metódica el proceso de auditoría, considerando técnicas y metodologías previamente estudiadas, dentro de un marco de trabajo óptimo para la elaboración del informe final de resultados.

UNIDADES TEMÁTICAS

1. Acciones previas de una Auditoría de TI
   - Conocimiento Preliminar
   - Planeación
   - Riesgo y materialidad de la auditoría
   - Acciones de solicitud de información
   - Estudio y evaluación del control interno
   - Programación
   - Integración

2. Ejecución de la Auditoría
   - Inicio de la auditoría
   - Desarrollo de procedimientos
   - Auditoría a la Seguridad y a la Infraestructura tecnológica
   - Aplicación de Técnicas manuales y TAACs
   - Formulación de posibles observaciones y/o recomendaciones
   - Comunicación de posibles observaciones y/o recomendaciones
   - Archivo de papeles de trabajo
   - Cierre de auditoría
3. Elaboración del Informe de Resultados
   - Evaluación de observaciones y/o recomendaciones
   - Documentación e información
   - Procedimientos análisis y evaluación de aclaraciones y comentarios
   - Resultados de informes técnicos
   - Elaboración del informe
   - Aprobación

METODOLOGÍA

MODALIDADES Y REQUISITOS DE GRADUACIÓN

Necesariamente implica la finalización del Programa correspondiente, aprobando todos los módulos.
Para graduarse satisfactoriamente debe reunir los siguientes requisitos mínimos:

- Asistencia del 80% de las clases de cada módulo.
- Aprobación de los exámenes o proyectos en cada eje temático según disposición de sus docentes.

En todos los programas la aprobación mínima es con 51 puntos.

REQUISITOS DE INSCRIPCIÓN

- 1 Fotocopia legalizada de Título en Provisión Nacional o Diploma Académico.
- 1 Certificado de Nacimiento Original
- 1 Fotocopia simple de Cédula de Identidad
- 3 fotos tamaño 3x4 cm. con fondo rojo, traje formal.

Solicite Información a:
postgrado@utepsa.edu

363-9390

- 692 00357
- 692 00356
- 692 00358