INGENIERIA EN TELEINFORMATICA

DIPLOMADO DE PROFUNDIZACIÓN EN SEGURIDAD INFORMATICA Y AUDITORIA

Dirigido a: Personas que se desempeñen en el área de seguridad, auditoria o con Conocimientos en informática, bases de datos y redes de datos.
Duración: 130 Horas presenciales
Inicia: Agosto 24 de 2014
Finaliza: Octubre 25 de 2014
Horario: Viernes y Sábados
Valor: $850.000
Cupos limitados
Informes e Inscripciones: Programa de Ingeniería en Telecomunicaciones e Informática UTCH.
Consultar las condiciones especiales para estudiantes del programa de Ingeniería Teleinformática
Teléfonos: 6726565 ext. 4050, 4051
Correo electrónico:
prog.ing-teleinformatica@utch.edu.co,
d-martha.luna@utch.edu.co,
mluna.docente@gmail.com

Área de Seguridad Informática

- Módulo I: Introducción a la Seguridad Informática.
- Módulo II: Seguridad en Redes y Sistemas Operativos.
- Módulo III: Seguridad en Aplicaciones y Bases de Datos.
- Módulo IV: Sistemas de Detección de Intrusos.
- Módulo V: Sistemas Criptográficos.

Área de Auditoria

- Módulo I: Gestión de la Seguridad Informática.
- Módulo II: Aspectos éticos de la Seguridad Informática.
- Módulo III: Informática Forense.

DIPLOMADO DE PROFUNDIZACIÓN EN SEGURIDAD INFORMATICA Y AUDITORIA

Área: Seguridad Informática y Auditoria

Naturaleza: Teórica-Práctica

No. de Créditos 10

Trabajo Presencial: 120

Trabajo Independiente: 230

Cupo Mínimo: 20 personas

Homologable: SI

Para Particulares:

- Conocimientos en informática, bases de datos, redes.

2. JUSTIFICACIÓN

Hoy en día la información se ha convertido en un activo principal de las organizaciones, razón por la cual, uno de los mayores retos para los departamentos que administran procesos informáticos, es garantizar la seguridad de la información. Asegurar la información en una organización requiere una adecuada combinación de tecnologías, metodologías, estándares, herramientas gerenciales y de la decisión de cuidar la infraestructura informática; para ello, es importante elegir métodos de seguridad idóneos, que protejan las redes de datos y sistemas ante eventuales amenazas.

El tema de seguridad informática se encuentra lleno malas interpretaciones, de tal forma que un alto porcentaje de personas piensan que con el simple hecho de instalar un dispositivo de hardware o un software en sus redes de datos, ya se encuentran protegidos ante ataques; es así como, el diplomado de profundización, busca ofrecer a estudiantes escenarios enfocados a trabajar aspectos relacionados conocimiento y la aplicación adecuada de elementos de sistemas criptográficos, modelos formales de seguridad en sistemas operativos, redes de datos, aplicaciones y base de datos, informática forense, riesgos a los que se está expuesto una organización cuando no se tienen políticas y estrategias que garanticen un nivel de seguridad adecuado para gestionar de manera eficaz sus sistemas de información.
Dado lo anterior, el Diplomado de profundización en las áreas de Seguridad Informática y Auditoria, esta planteado para ser desarrollado por módulos en cada una de las áreas, cinco módulos orientados al área de Seguridad

Informática y tres módulos orientados al área de Auditoria.

3. COMPETENCIAS

Las competencias en la actualidad buscan en los estudiantes tres saberes fundamentales **Saber Conocer, Saber Hacer y Saber Ser,** y sin el ánimo de desconocer dichos saberes, las competencias que los estudiantes que realicen el "DIPLOMADO de Profundización" deberán alcanzar las siguientes competencias:

3.1 Competencias Generales

- Interpretar, analizar y contextualizar los conceptos y herramientas necesarios para proteger la información de una organización ante ataques informáticos.

- Garantizar la integridad de la información con implementación de controles que la aseguren, eligiendo los sistemas y métodos de seguridad idóneos, para proteger las redes y sistemas ante eventuales amenazas.

3.2 Competencias Especificas

- Conocer las técnicas utilizadas para vulnerar la confidencialidad, integridad y disponibilidad de los sistemas de información y las redes de datos.

- Evaluar las soluciones utilizadas para responder a los riesgos organizacionales relacionados con el tratamiento automático de la información.

- Utilizar metodologías permitan la práctica de una cultura de Seguridad Informática.

- Incentivar las buenas prácticas para el diseño de estrategias de seguridad informática en las organizaciones, permitiendo que se convierta en un valor agregado para los procesos de negocio.

4. OBJETIVOS

Los estudiantes que realicen el diplomado de profundización en Seguridad Informática y Auditoria estarán en capacidad de:

- Analizar las vulnerabilidades más frecuentes, utilizadas por los delincuentes informáticos.

- Diseñar soluciones integrales de seguridad informática que respondan a los requerimientos, enmarcadas dentro del contexto tecnológico disponible y acorde con las disposiciones de las exigencias nacionales e internacionales.

- Diseñar procesos de mejoramiento y optimización de sistemas de seguridad

informática mediante la apropiación, adaptación y creación de tecnologías de punta y metodologías para administrar y controlar los riesgos informáticos de las empresas.

- Gestionar proyectos de seguridad de la información teniendo como perspectiva los riesgos inherentes del sistema de información.

- Analizar evidencias digitales en sus diferentes formatos y estrategias de aseguramiento, detallando los riesgos propios de su manejo y presentación.

- Formular modelos enfocados a la seguridad informática que permitan atender contingencias de riesgo informático.

5. CONTENIDO TEMÁTICO Y ANÁLISIS DE CRÉDITOS

Contenido temático ÁREA: SEGURIDAD INFORMÁTICA

• **Módulo I: Seguridad Informática.** En este módulo se exploran los elementos más importantes de un sistema de seguridad, ataques desde un punto de vista genérico, modelos de seguridad informática, tendencias, principios, estándares y buenas prácticas de seguridad informática.

• **Módulo II: Seguridad en Redes y Sistemas Operativos.** En este módulo se busca mostrar un panorama general de las fallas que se presentan en los ambientes de redes de datos tanto cableadas como inalámbricas, los mecanismos para enfrentar deficiencias y sus implicaciones en las arquitecturas de red, así mismo, los estudiantes aprenderán a asegurar las redes tanto cableadas como inalámbricas contra ataques externos e internos, métodos de prevención, realizar sesiones remotas seguras, operar firewalls, filtrado de paquetes y discernir diferentes ataques de seguridad en los sistemas operativos como Windows y Linux.

• **Módulo III: Seguridad en Aplicaciones y Bases de Datos.** El módulo profundiza conceptos básicos de seguridad informática en las aplicaciones y las bases de datos, presenta y desarrolla las tendencias en modelos de seguridad para las aplicaciones y bases de datos, y da criterios y herramientas para enfrentar las inseguridades de la WEB. Así mismo, se estudiara la seguridad a los componentes de aplicaciones web: TLS/SSL, https y uso de certificados en aplicaciones web, la arquitectura de navegadores web, los problemas comunes de seguridad en navegadores y los mecanismos de autenticación de usuarios, manejo de claves, control de acceso.

• **Módulo IV: Sistemas de Detección de Intrusos.** Este módulo presenta conceptos relacionados con Sistema de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS), técnicas y herramientas para crear esquemas seguro y para seleccionar e implementar IDS. Se presentan las metodologías para realizar ataques y definir las estrategias asociadas para obtener un nivel alto de seguridad en los recursos informáticos de las organizaciones.

• **Módulo V: Sistemas Criptográficos.** Este módulo busca que los estudiantes comprendan la aplicación real de criptografía de llave secreta y de llave pública y de estándares y protocolos criptográficos, aplicación de criptografía en firmas digitales, cifrado, procesamiento de certificados digitales, chequeos de integridad utilización de técnicas criptográficas en el aseguramiento de procesos.

ÁREA: AUDITORIA

• **Módulo I: Gestión de la Seguridad Informática.** El módulo busca que los estudiantes diseñen estrategias que permitan proteger los recursos informáticos de las organizaciones, presenta el ciclo de vida de la seguridad informática y los sistemas de gestión de la seguridad informática, profundiza la importancia de las políticas de seguridad informática, haciendo uso de los estándares y normas tanto nacionales como internacionales, comprendiendo sus beneficios y la metodología a usar para implementarlos en una organización.

• **Modulo II: Aspectos éticos de la Seguridad Informática.** En este módulo se realiza un estudio sobre la criminalidad informática y los delitos más frecuentes, profundiza el concepto de Etica Hacking, presenta el modelo conceptual del Hacking y diversas herramientas de Hacking para realizar tareas de análisis de vulnerabilidades y tests de penetración.

• **Módulo III: Informática Forense.** En este módulo se familiariza al estudiante con los elementos involucrados en una investigación forense, se enseña cómo manejar la evidencia digital, explorando técnicas de recolección, preservación, análisis y presentación de la evidencia, se exploran herramientas para enfrentar investigaciones que pueda servir como prueba, identificación de rastros informáticos, buenas prácticas en la administración de la evidencia digital, modelos de investigación forense digital, técnicas antiforenses, retos y riesgos emergentes para la computación forense, así como también las consideraciones legales que un perito informático forense deberá tener en cuenta.

Análisis de Créditos

TEMAS	TRABAJO PRESENCIAL	TRABAJO INDEPENDIENTE	DOCENTE

ÁREA: SEGURIDAD INFORMÁTICA			
Módulo I: Introducción a la Seguridad Informática.	10	20	Alexander Palacios
Módulo II: Seguridad en Redes y Sistemas Operativos.	15	30	Sebastián Castrillón
Módulo III: Seguridad en Aplicaciones y Bases de Datos.	15	30	Alexander Palacios
Módulo IV: Sistemas de Detección de Intrusos.	15	30	Sebastián Castrillón
Módulo V: Sistemas Criptográficos.	15	30	Alexander Palacios 3107683295
ÁREA: AUDITORIA			
Módulo I: Gestión de la Seguridad Informática.	15	30	Alexander Palacios 3107683295 alexander.palacios@correo.policia.gov.co
Módulo II: Aspectos éticos de la Seguridad Informática.	15	30	Jorge Luis Palacios
Módulo III: Informática Forense.	15	30	Jorge Luis Palacios
TOTAL DE HORAS DEL CURSO	115	230	

6. ESTRATEGIAS METODOLÓGICAS

Trabajo presencial:

Se trabajará con la metodología activa de conferencias, talleres, demostraciones, aprendizaje basado en problemas, investigación y análisis de casos. Tendrá un esquema teórico-práctico, en donde el estudiante desarrollará capacidades investigativas y propositivas.

Trabajo independiente:

Lecturas complementarias que contengan un carácter científico, desarrollo de casos o ejercicios complementarios. El estudiante durante el transcurso del diplomado deberá desarrollar un trabajo escrito, el cual será sustentado al finalizar del diplomado, según lo estipulado en el artículo 38 del Acuerdo 03/2013 (Consejo de facultad de Ingeniería).

7. RECURSOS.

- Salón de clase.
- Acceso a servicio Internet.
- Sala de sistemas con la posibilidad de instalación y ejecución de software especializado.
- Sala de proyección y uso de equipos audiovisual

DOCENTES:

Ing. ALEXANDER PALACIOS PALACIOS

Estudios Universitarios
Ingeniero de Sistemas Corporación Universitaria Remington, Especialista en Seguridad Informática Universidad Piloto de Colombia

Cursando Maestría - Instituto Eurotechnology Empresas Titulo: 2° Mòdulo "Dirección Estratégica, Planificación y Control". España - Coruña

Diplomado Universidad de Medellín Gestión Integral de la seguridad
Diplomado Universidad de Medellín Uso de las Tecnologías de la información y la Comunicación en los procesos de Formación

Ing. JORGE LUIS PALACIO VALOYES

PROFESIÓN: INGENIERO DE SISTEMAS, UNIVERSIDAD AUTÓNOMA DE COLOMBIA, 1995

POSTGRADOS:

DOCENCIA UNIVERSITARIA, TERMINACIÓN DE MATERIAS, UCC, 1998

AUDITORIA DE SISTEMAS, TITULADO, UAN, 2002

ESTUDIANTE DE DERECHO, SEGUNDO NIVEL APROBADO, I - 2014

EXPERIENCIA LABORAL

FISCALIA GENERAL DE LA NACIÓN DESDE 1997 A LA FECHA, EN EL CARGO DE PROFESIONAL UNIVERSITARIO II

DOCENTE CATEDRATICO UTCH, UCC, UAN, DESDE 1995 HASTA EL 2013 EN LA UCC Y HASTA LA FECHA EN LA UTCH

ING. SEBASTIÁN CASTRILLÓN RESTREPO

Ingeniero de Control Universidad Nacional de Colombia. Estudiante de Maestría en Telecomunicaciones, tercer semestre U. de Antioquia. Certificado Cisco CCNA Coordinador de Calidad Academia Cisco, Instructor Cisco para CCNA, Coordinador de Calidad Academia Cisco Security – Vmware Grupo de Teleinformática y Teleautomática Facultad de Minas. Gerente de Netmask SAS. Docente de Cátedra Universidad de Antioquía y docente de extensión en el Politécnico Jaime Isaza Cadavid.