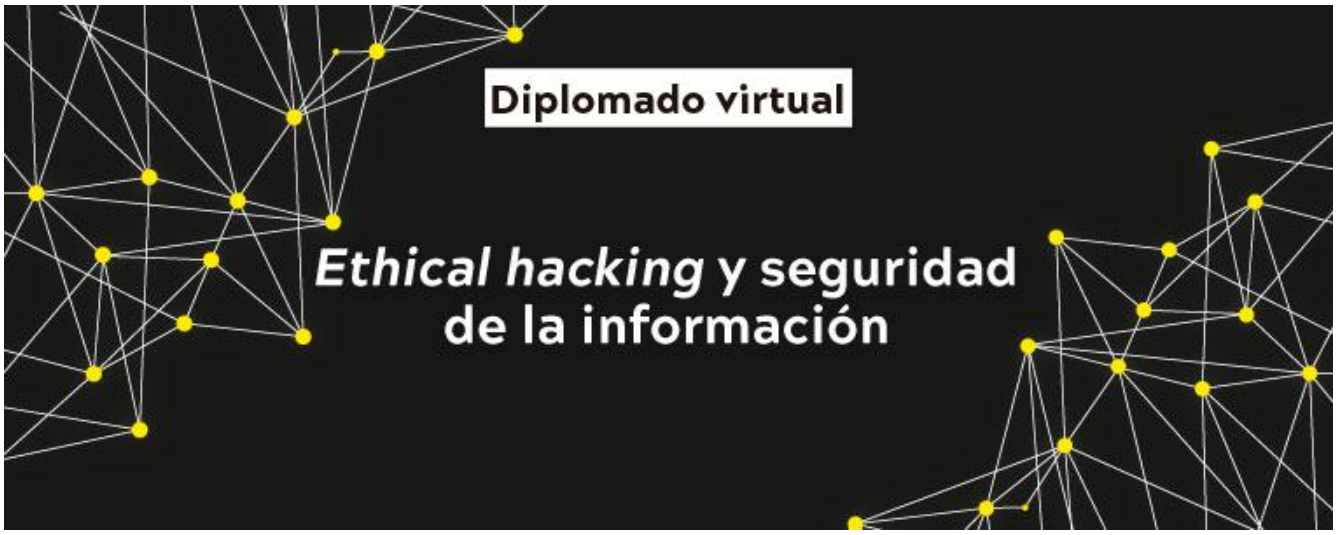
División de Educación Continuada
Facultad de Ingeniería
Programa de Ingeniería de Sistemas



INTENSIDAD	**120 Horas**
FECHA INICIO	Marzo 22 del 2022
FECHA FINAL	Mayo 20 del 2022
HORARIO	Virtual – Plataforma Online
INVERSIÓN POR PARTICIPANTE	**$ 1.764.000**
DESCUENTOS	* 10% por matrícula de dos o más personas * 10% por Afiliado a Colsubsidio y Compensar * 15% por Comunidad El Bosque Aplica para personas naturales. *- Los Descuentos No son Acumulables*

Justificación

Hoy por hoy la información está definida como el activo más valioso de una organización, los costos derivados de situaciones de inseguridad en los sistemas de información, no son únicamente costos económicos directos, sino que también afectan legal y reputacionalmente a la empresa. Lo anterior, sumado a un entorno tecnológico, donde las tecnologías de información evolucionan rápidamente cada día, hace complejo el hecho de manejar grandes volúmenes de datos, y por tanto cada vez más, la seguridad de la información constituye un factor estratégico y es necesaria para tomar las medidas y/o controles, lineamientos de protección necesarios e impulse el cumplimiento de los objetivos de las organizaciones, haciendo de su estudio un aspecto diferenciados para cualquier profesional relacionado con las tecnologías de la información.

La falta de sensibilización de las compañías y sus directivos ante el adecuado manejo de la información, que en muchos casos no le dan la importancia necesaria por su intangibilidad, hacen que las medidas y/o controles de seguridad no ofrezcan las garantías apropiadas para mejorar la productividad de los sistemas de información y redes de datos, sino que por el contrario influyen en el bajo rendimiento de equipos y aplicaciones, afectando sus operaciones y por ende los objetivos estratégicos de la organización.

En este contexto, es de vital importancia existencia de personal capaces de identificar, alertar, establecer y mantener controles que permitan no solo a las organizaciones sino también a particulares, lidiar con un sin número de amenazas que atentan contra nuestros activos de información, así como también contra nuestra privacidad.

En este orden de ideas la "Universidad el Bosque" ofrece a la comunidad el "Diplomado en Ethical Hacking y Seguridad de la Información" cuyo objetivo es abordar la problemática de la seguridad de la información y la protección de datos, abarcando todos los aspectos estratégicos, técnicos y legales, bajo marcos de referencia, normatividad y mejores prácticas de la industria.

Objetivo General

Ofrecer al profesional la capacitación adecuada en los aspectos más relevantes de la Seguridad de la Información y Ethical Hacking, para su fortalecimiento profesional y su posterior aplicabilidad en el entorno empresarial (y/o personal).

Objetivos Específicos

- Adquirir las habilidades y destrezas necesarias en la aplicación de las diferentes tecnologías de Seguridad Informática y de Ethical Hacking.
- Adquirir las habilidades y destrezas en la identificación y explotación de vulnerabilidades más utilizadas hoy día.
- Identificar el tipo de análisis de seguridad más adecuado a las necesidades de la organización.
- Implementar las medidas adecuadas para prevenir los diferentes tipos de ataques informáticos.
- Gestionar efectivamente los resultados identificados en el análisis de seguridad.
- Comunicar de forma adecuada las necesidades y resultados a la alta dirección.
- Adquirir el conocimiento sobre los diferentes perfiles de potenciales atacantes informáticos.
- Adquirir los conocimientos para realizar un efectivo proceso de gestión de riesgos.
- Conocer la metodología para diseñar un plan de continuidad de negocio.
- Adquirir las habilidades y destrezas en el diseño de un plan de auditoría de sistemas de gestión
- Obtener bases sólidas para emprender el diseño e implementación de un Sistema de Gestión de Seguridad de la Información

Metodología:

El diplomado será desarrollado de manera virtual con el apoyo de casos de estudio, talleres, videos, discusión online y material referente al tema de estudio.

CONTENIDO DEL DIPLOMADO

Módulo	Objetivo y Duración	Temática
Módulo 1 **Fundamentos de SI y Criptografía**	Familiarizar al estudiante en los conceptos fundamentales y la importancia de la Criptografía en la SI [2 semanas]	1.- Principios de la SI 2.- Seguridad física y lógica 3.- fundamentos de criptografía
Módulo II **Ethical Hacking I** **(Introducción – Metodologías)**	Iniciar el estudio de Ethical Hacking, cuáles son los tipos de análisis, metodologías utilizadas. [3 semanas]	1.- Introducción 2.- Tipos de análisis de seguridad 3.- Metodologías utilizadas 4.- Presentación de informes
Módulo III **Ethical Hacking II** **(Actividades prácticas)**	Adquirir las destrezas y habilidades en las diferentes técnicas utilizadas. [4 semanas]	1.- Escaneo de redes 2.- Virus y gusanos 3.- Secuestro de sesión 4.- Hackeo de servidores web 5.- Hackeo de aplicaciones web 6.- Inyección de SQL 7.- Hackeo de redes inalámbricas 8.- Evasión de IDS, Firewalls, HoneyPots 9.- Desbordamiento de memoria 10.- Pruebas de penetración
Módulo IV **Gestión del Riesgo, Auditoría de Sistemas de gestión y continuidad Negocio**	Orientar al estudiante sobre los conceptos fundamentales para llevar a cabo una gestión de riesgos efectiva, evaluar a través del proceso de auditoría y diseñar y establecer un plan de continuidad de negocio.	1.- Conceptos generales de la gestión de riesgos. 2.- Metodología para la identificación, análisis y evaluación de riesgos. 3.- Metodología para diseñar, implementar y mantener un PCN. 4.- Planeación y ejecución de un programa de auditoría de sistemas de gestión. 5.- Estándares de auditoria a sistemas de información.

EQUIPO DOCENTE

Wilson Mauro Rojas Reales.

Ingeniero de Sistemas, especialista en Seguridad de la Información (Universidad de los Andes), especialista en Docencia Universitaria (Universidad Piloto de Colombia), actualmente cursa una Maestría en Seguridad de las Tecnologías de la Información (Universidad Oberta de Catalunya), ha cursado estudios de ITIL V3, Cobit, SARO, SARLAFT, controles y seguridad informática, entre otros. Posee más de 15 años de experiencia laboral, ha trabajado en el sector financiero, público, privado. Ha ocupado cargos como Director de Sistemas, Asesor, Consultor, actualmente se desempeña como docente en el programa de pregrado de Ingeniería de Sistemas de la Universidad el Bosque, Director de proyectos de postgrados (en la especialización de Seguridad en Redes telemáticas) y como Asesor en un proyecto con la Defensoría del Pueblo de Ecuador (DPE) mediante la empresa AECInter S.A.

Fredy Alonso Cardona

Ingeniero Electrónico de la Universidad Nacional de Colombia, especialista en Gestión de sistemas y tecnologías de la información en la empresa (Universidad EAN en convenio con U. Politécnica de Madrid), auditor interno de sistemas de gestión de seguridad de la información basados en la norma ISO27001, certificado en Cobit, ha cursado estudios de continuidad del negocio, ITIL V3, riesgos, sus controles y de seguridad informática, entre otros. Cuenta con 7 años de experiencia laboral, ha trabajado en el sector financiero y de telecomunicaciones. Ha ocupado cargos como coordinador de centro de operaciones de red (NOC), ingeniero de soporte en redes y seguridad informática, actualmente se desempeña como Analista de Seguridad de la Información en una empresa del sector financiero.

Alfonso Carvajal Soto

Ingeniero de Sistemas de la Universidad Piloto de Colombia, especialista en Administración de Riesgos Informáticos de la Universidad Externado de Colombia certificado Cobit Foundations y Check Point CCSA, ha cursado estudios de informática forense CHFI (Computer Hacking Forensic Investigator), Ethical Hacking (CEH - Certified Ethical Hacker), ECSA/LPT (Certified Security Analyst), ITIL V3, SARO, SARLAFT y tecnologías de seguridad informática, entre otros. Posee más de 10 años de experiencia laboral en el sector financiero y las telecomunicaciones. Ha desempeñado cargos como Coordinador de Seguridad Informática, Coordinador de centro de operaciones de seguridad SOC y Asesor en Seguridad de la Información, actualmente se desempeña como Analista de Seguridad de la Información en una entidad del sector financiero.