GESTIÓN Y ADMINISTRACIÓN DE SEGURIDAD DE IT CONTRA LOS RIESGOS INFORMÁTICOS EMPRESARIALES

EVENTO CON MODALIDAD EN LINEA UTILIZANDO HERRAMIENTAS TECNOLOGICAS

ÁREA TÉCNICA

Total de Horas: 20 horas
Inversión total del curso: $270.00 USD
Inversión Empresa o Participante: (apoyo 100% INSAFORP)
Horario: lunes miércoles y jueves de 6:00 a 08:30 pm (2.5 horas por día)
Fechas de Clases: Mayo (5, 12, 13, 17, 19, 20, 24, 26) de 2021

Dirigido a: Profesionales en el área de TI, Auditores de Sistemas, Servidores, Infraestructura y Redes. Estudiantes en carreras de informática.

Requisitos indispensables para el participante: Poseer computadora de escritorio, o Laptop mínimo recomendado de capacidad es de 2 GB de Memoria RAM, procesador Intel Pentium 4, 2,5 3 GHz o equivalente. a 800 Mhz, 750 Mb Libres de espacio en disco duro con conexión a Internet

Descripción: Vivimos en un mundo donde la tecnología es parte fundamental del quehacer de las sociedades en todos los aspectos de la vida, el uso de la tecnología generó un fuerte cambio en la forma de socializar y de aprender, pero sobre todo en la forma de hacer negocios, ya que el uso de la tecnología implica nuevos retos para la actividad económica de una organización y dependerá de la eficiencia y eficacia, en la implementación de la misma en los procesos del negocio, que permitirá obtener de ella el beneficio esperado, por lo cual es necesario aplicar las medidas de seguridad basándose en las mejoras prácticas internacionales y para ello es necesario conocerlas

Objetivos de la capacitación:

1. Adquirir los conocimientos necesarios para detectar los riesgos y amenazas informáticas.
2. Adquirir los conocimientos necesarios para administrar y gestionar los riesgos y las amenazas tecnológicas.
3. Conocer los marcos regulatorios y los estándares internacionales relacionados con la seguridad de la Información.
4. Comprender como la técnica de ingeniería social es una de las mayores amenazas para la seguridad de la información.
5. Conocer las técnicas utilizadas por los atacantes o hackers para vulnerar un sistema informático.
6. Conocer las técnicas utilizadas para llevar a cabo test de penetración y análisis de vulnerabilidades.
7. Adquirir los conocimientos prácticos reales para realizar ataques a los sistemas informáticos bajo los principios de un Ethical Hacking.
8. Conocer y aplicar las técnicas de análisis forense aplicado a la tecnología de información.
9. Aprender a utilizar las herramientas más especializadas para realizar análisis de vulnerabilidad y Ethical hacking.

Temas a desarrollar:

1. Gestión de Seguridad de TI
2. Gobierno de Seguridad de TI
3. Estrategia de Seguridad de TI
4. Normativas estándares y controles internacionales.

Resumen del especialista:

Mario Orellana Castillo, Con 17 años de experiencia en el sector Energía, Retail y Tecnología; se ha desempeñado como funcionario público a cargo del Departamento de TI del Ministerio de Obras Públicas, Transporte y Vivienda de El Salvador; además de consultor y asesor experto en seguridad y tecnología para los sectores Finanzas, Salud, Telecom y BPOs. Cuenta con más de 20 Certificaciones Internacionales en Seguridad e Infraestructura Tecnológica, respaldadas por la Computer Technology Industry Association, EC-Council, Microsoft y Mile2 Security; así mismo, es instructor certificado por Microsoft y Mile2. Ha sido parte de los lanzamientos de distintas líneas de productos de Microsoft Windows Server, y charlas para ICANN, Microsoft y OWASP en distintos países de la región. En la actualidad, forma parte del equipo de expertos que imparte especializaciones en Seguridad Informática en el campus de Postgrados de la Universidad Don Bosco.