Universidad Francisco de Paula Santander
Vigilada Mineducación

DIPLOMADO EN

DERECHO INFORMÁTICO

NUEVAS TECNOLOGÍAS

CONTACTO

Oficina Unidad de Extensión
Vicerrectoría Asistente de Investigación y Extensión UFPS
Email: coordinacionextension@ufps.edu.co
Tel: 5776655- Ext. 170

I. JUSTIFICACIÓN

En la actualidad la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para generar conciencia a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios. Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el porqué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y. debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas. El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

En nuestra región existe un desconocimiento generalizado sobre los procedimientos y protocolos a seguir en caso de un incidente común, así como las técnicas que deben implementarse para prevenir incidentes futuros (reacción - prevención)
De otra parte, una vez se presenta el incidente se requiere conocer sus causas, por lo que se hace necesario tener conocimientos acerca de los métodos y herramientas requeridos para realizar un análisis forense.

Asimismo, el profesional en sistemas pocas veces es consciente de que además de los conocimientos informáticos relacionados con la seguridad, es de vital importancia estar al tanto de la normatividad legal nacional e internacional que rige esta materia, teniendo en cuenta que la aplicación de las diferentes técnicas y procedimientos debe hacerse dentro de los parámetros establecidos por la ley.

Igualmente se debe tener en cuenta el alto impacto nacional y regional que han adquirido los delitos informáticos en sus diferentes modalidades. Según las estadísticas de la Policía Nacional DIJIN - Sección de Delitos Informáticos, para el año 2015, se observa que Cúcuta se encuentra entre las 5 ciudades a nivel nacional donde se comenten más delitos informáticos, lo que evidencia una urgencia manifiesta de desarrollar programas de capacitación en la prevención de incidentes informáticos, telemáticos y de seguridad informática.

Por esta razón la Universidad Francisco de Paula Santander, presenta este Diplomado en Derecho Informático - Nuevas Tecnologías, ofreciendo a la comunidad de la región, un programa académico que brinde soluciones a esta problemática planteada, soportado por las fortalezas, recursos físicos y humanos y la experiencia en programas de pregrado que la Facultad de Ingeniería y derecho de la institución posee.

II. OBJETIVOS

Objetivo General

Proveer a los participantes de las herramientas y técnicas utilizadas en las mejores prácticas aplicadas para el desarrollo y gestión de sistemas de información seguros.

Objetivos Específicos

- Conocer los conceptos sobre Derecho Informático, Seguridad Informática, revisando modelos existentes, aprendiendo sus fortalezas y sus debilidades.
- Comprender la normatividad Nacional e Internacional relacionada con los delitos informáticos conociendo su ámbito y aplicabilidad.
- Preparar profesionales capaces de dar respuesta a las distintas necesidades que se plantean en las sociedades modernas y en sus empresas en el área de seguridad informática

III. COMPETENCIAS

- Aplica conceptos, metodologías y procesos para el aseguramiento de la información.
- Interpreta las normas nacionales e internacionales que regulan lo pertinente al área de Seguridad Informática.
- Reconoce las fallas de seguridad que se presentan en los ambientes de red y los mecanismos que permitan prevenirlos.
- Revisa y analiza estándares nacionales e internacionales sobre administración de evidencia digital y técnicas de informática forense.
- Aplica e identifica los procedimientos a seguir de un primer respondiente a incidentes informáticos y telemáticos CFRI y CSIRT

IV. PLAN DE ESTUDIOS

El Diplomado de “Derecho Informático y Nuevas Tecnologías” está constituido por cuatros (4) módulos hasta completar las 120 horas académicas más un trabajo final que se requiere para obtener el certificado de aprobación correspondiente:

UNIDAD 1. GENERALIDADES INFORMÁTICAS

1.1 Como actúa un primer respondiente clasificación de incidentes, procesos de gestión de incidentes.

1.2 Pasos a seguir ante un incidente común, procesos de planificación y preparación para enfrentar un incidente de seguridad.

1.3 Proceso de atención de incidentes

1.4 Qué hacer frente a los passwords y la encripción de datos

1.5 El PR “Primero Respondiente” ante un siniestro actividades del equipo o responsable por la gestión de incidentes de seguridad

1.6 Adquisición de evidencia volátil, técnicas y herramientas para la formación y entrenamiento en seguridad informática.

1.7 Como prevenir futuros ataques, actividades forenses de un CFRI, CSIRT.

UNIDAD 2. MANEJO DE INCIDENTES Y EVIDENCIA DIGITAL

2.1 Pasos a seguir ante un delito informático cadena de custodia.

2.2 Aspectos Básico de Seguridad ISO 27000, 27001.

2.3 Ethical Hacking aplicado a la computación forense

2.4 Documentación y Reportes del PR

2.5 El talón de aquiles de los antivirus

2.6 Visión Introspectiva de la Informática Forense en Colombia

2.7 Herramientas y Software Forense.

2.8 Trazado de ataque WEB y técnicas de Ingeniería Social

2.9 Seguridad en Redes.

UNIDAD 3. LEGISLACIÓN – DERECHO INFORMÁTICO

3.1 Aspectos Legales de la Computación Forense

3.2 Análisis Ley 1273 de 2009 Ley de Delitos Informáticos

3.2 Aspectos legales relacionados al monitoreo y recolección de evidencia

3.3 Aspectos legales relacionados a la admisibilidad de evidencia

3.4 Casos relacionados en Colombia.

3.5 Qué hacer si usted es perito, prácticas de interrogatorio

UNIDAD 4. LEGISLACIÓN – DERECHO INFORMÁTICO INTERNACIONAL

4.1 Convenio de Budapest

4.2 OICE

4.3 Protocolos Internacionales

V. MATRIZ CURRICULAR

MÓDULOS	HORA	DOCENTE
MÓDULO I: Generalidades Informáticas	30	Marco Antonio Adarme Jaimes
MÓDULO II: Manejo de incidentes y Evidencia Digital	30	César Antonio Villamizar Núñez
MÓDULO III: legislación- Derecho Informático	30	César Antonio Villamizar Núñez
MÓDULO IV: Legislación - Derecho Informático Internacional	30	Álvaro Javier González Sanjuan
TOTAL HORAS	**120**	

VI. PRECIO

$1.200.000 por participante

Universidad Francisco de Paula Santander

Vigilada Mineducación