



FICHA DE DATOS DE PROGRAMAS DE EDUCACIÓN CONTINUADA

NOMBRE DEL EVENTO DIPLOMADO EN INFORMATICA FORENSE

OBJETIVO

- Con el desarrollo del Diplomado se pretende que los estudiantes conozcan:
- Delitos y actividades ilícitas
- El derecho y la informática
- El entorno de investigación
- La informática forense
- Preservación de la evidencia
- El análisis de la evidencia
- El análisis forense a sistemas Windows
- El análisis forense sistemas Linux
- La investigación digital
- La presentación de evidencias

CONTENIDO

MODULO #	TEMA	DURACION (HORAS)	DOCENTE	FECHAS
MODULO I. CONCEPTOS BASICOS Y NORMATIVIDAD Sesión 1	CONCEPTOS BASICOS Y NORMATIVIDAD Capitulo 1. DELITOS Y ACTIVIDADES ILICITAS	3	John Jairo Ruiz Concha	18 junio
	<ul style="list-style-type: none"> • Introducción a la Seguridad Informática • Delitos Informáticos • Cybercrimen como amenaza actual • Delincuente Informático (cibercriminal) • Laboratorio de Tools. prácticos 	7		y 19 junio
	Capitulo 2. EL DERECHO Y LA INFORMATICA <ul style="list-style-type: none"> • La evidencia digital. • Cadena de custodia. • La escena del crimen. 			

	<ul style="list-style-type: none"> • La Ley sobre Delitos Informáticos - Lo que un investigador debe conocer de derecho • Incautación de equipos. • Laboratorio - instalación de Herramientas I... 			
<p>MODULO II. TECNICAS BASICAS Y APLICABILIDAD A LA EVIDENCIA.</p> <p>Sesión 2</p>	<p>Capitulo 3. CONOCIENDO EL ENTORNO DE INVESTIGACIÓN.</p> <ul style="list-style-type: none"> • El disco duro • Estructura Interna del Disco • Tablas de particiones. • Mitos del Formateo De Discos • • Técnicas Básicas de Recuperación de Datos • El protocolo TCP/IP • Los datos en las Redes. • Laboratorio - Tools Herramientas II 	<p>3</p> <p>7</p>	<p>John Jairo Ruiz Concha</p>	<p>25 junio</p> <p>Y</p> <p>26 junio</p>
<p>Sesión 3.</p>	<p>Capítulo 4. LA INFORMATICA FORENSE La informática forense Metodología de análisis La línea de tiempo (timeline)</p> <p>Identificación de la evidencia Actividades PRE al proceso de Extracción de Datos. Lo que debe conocer un Investigador antes de Tomar el Caso. Laboratorios Prácticos</p>	<p>3</p> <p>7</p>	<p>Víctor Hugo Rico Macías</p>	<p>02 julio</p> <p>03 julio</p>
<p>Sesión 4.</p>	<p>Capítulo 5. PRESERVACIÓN DE LA EVIDENCIA Hash MD5, SHA1 Algoritmos de Encriptación Extrayendo imágenes de discos duros. Extrayendo imágenes de la memoria RAM. Extrayendo datos de la RED Laboratorio s - Prácticos</p>	<p>3</p> <p>7</p>	<p>Víctor Hugo Rico Macías</p>	<p>09 julio</p> <p>10 julio</p>

MODULO III. ANALISIS Y APLICABILIDAD DE TECNICAS FORENSES	Capítulo 6. ANALIZANDO LA EVIDENCIA Analizando las imágenes de discos duros	3	Víctor Hugo Rico Macías	16 julio
	Sesión 5 Analizando las imágenes de la memoria RAM. Analizando Imágenes de la RED. Laboratorio s - Prácticos	7		17 julio
Sesión 6.	Capítulo 7 ANALISIS FORENSE SISTEMAS WINDOWS Extrayendo evidencia volátil Analizando el registro	3	Víctor Hugo Rico Macías	23 julio
	Analizando los logs del sistema Análisis usando máquinas virtuales Desbloqueo de claves La esteganografía. Laboratorios - prácticos	7		24 julio
Sesión 7.	Capítulo 8. ANALISIS FORENSE SISTEMAS LINUX Extrayendo evidencia volátil	3	Víctor Hugo Rico Macías	30 julio
	Analizando los logs del sistema Análisis usando máquinas virtuales Desbloqueo de claves La esteganografía. Laboratorios - Prácticos	7		31 julio
Sesión 8.	Capítulo 9. INVESTIGACIONES DIGITAL Metodología de la investigación digital Aplicando el modelo SKRAM	3	Víctor Hugo Rico Macías	13 agosto
	Investigación de una cuenta de correo Investigación de un sitio web Laboratorio geo localización y extorsión por correos .	7		14 agosto

Sesión 9.	<p>Capítulo 10. PRESENTACION DE EVIDENCIAS.</p> <p>Armado de un informe final del Perito Forense Introducción al peritaje ante la Ley. Laboratorio - Practico</p> <p>Laboratorio Complementario 1. caso práctico. Aplicación de Conceptos y uso de herramientas en la recolección de evidencia. Laboratorio Complementario 3. Caso práctico: Labs de Practico de Imágenes de Disco duro y análisis de Datos de evidencia Digital.</p> <p>Manejo inicial del caso documentación y preparación.</p> <p>Inicio del proceso y definición del final con informe</p>	3	Víctor Hugo Rico Macías	20 agosto
	7	21 agosto		
Sesión 10.	<p>Laboratorio Complementario 2. Caso práctico.</p> <p>Caso de Correo extorsivo.</p> <p>Practica de Geo localización y de Análisis del procedimiento con relación al informe.</p> <p>Conclusiones y Aclaración de dudas y Sesión de introducción al análisis forense en redes.</p> <p>Aspecto teórico</p> <p>Demos de trabajo de análisis forense en redes</p>	3	Víctor Hugo Rico Macías	27 agosto
	7	28 agosto		
Total Horas		100		

DOCENTES

Víctor Hugo Rico Macías

JOHN JAIRO RUIZ CONCHA

FECHA DE INICIO 18 de junio
HORARIO viernes de 5pm a 9pm y sábados de 9am a 12pm – 1pm a 5pm
DURACIÓN 140 horas
LUGAR Unidad Central del Valle sala informática ambiental
COSTOS \$850.000
ORGANIZADOR ing. Edgar Sandoval a.
INFORMES E INSCRIPCIONES 3152761270
DIRIGIDO A estudiantes de sistemas, derecho, responsables de TIC, entidades externas en el manejo de procesos de seguridad y judiciales.