27. CURSO DE ACTUALIZACIÓN TALLER DE ANÁLISIS DE INFORMACIÓN A TRAVÉS DE REDES

CURSO DE ACTUALIZACIÓN TALLER DE ANÁLISIS DE INFORMACIÓN A TRAVÉS DE REDES

I. ÍNDICE

II. INTRODUCCIÓN

Antecedentes

El Programa Rector de Profesionalización (PRP) es el instrumento que establece los lineamientos, programas, actividades y contenidos mínimos para la profesionalización del personal de las Instituciones de Seguridad Pública. En él se contempla el servicio de carrera, cuyo objetivo es desarrollar un sistema de carácter obligatorio y permanente que se base en los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos. En este sentido, la profesionalización de las Instituciones mencionadas se integra con los programas de formación inicial y continua, que contempla las etapas de actualización, especialización y alta dirección.

Según se establece en el PRP, la formación continua es un proceso para desarrollar al máximo las competencias, capacidades y habilidades de los integrantes de las Instituciones de Seguridad Pública, procuración de justicia y sistema penitenciario de todo el país; busca desarrollar, complementar, perfeccionar, actualizar y especializar los conocimientos y habilidades necesarios para el eficaz y eficiente desempeño de sus integrantes y prepararlos para funciones de mayor responsabilidad, así como certificarlos en sus niveles de capacitación.

El presente curso se alinea con los programas de Prioridad Nacional, para consolidar las áreas de análisis y estadísticas del programa denominado Sistema Nacional de Información, en el rubro de dotación y capacitación de recursos humanos, según los acuerdos 08/XXXVI/14 y 07/XXXVII/14, aprobados por el Consejo Nacional de Seguridad Pública en sus Trigésima Sexta y Séptima Sesiones Ordinarias y publicados en el Diario Oficial de la Federación.

El recurso humano principal se centra en el Analista de Información, que consiste en una persona formada y especializada en el estudio lógico y sistemático de la información, así como en la comunicación de los resultados, que faciliten la toma de decisiones. Es un especialista a cargo de recibir información, estudiarla, producirla y reordenarla, a fin de considera su confiabilidad, validez y relevancia. Integra los datos en un todo coherente, coloca la información evaluada en contexto y produce un producto de inteligencia que incluye la evaluación de sucesos y juicios sobre las implicaciones de la información.

Los analistas de información conforman equipos de trabajo que identifican patrones de conductas, perfiles criminales y asociaciones de datos relacionados entre sí, a fin de emitir propuestas de innovación y renovación que dan respuesta a las necesidades y expectativas de posibles rutas de acción; asimismo, evalúan cada riesgo de acuerdo con la probabilidad de una consecuencia específica y su posible impacto. Además, identifican áreas a intervenir, diagnostican y establecen prioridades.

III. OBJETIVO GENERAL

Utilizar de manera eficiente internet como fuente de información para identificar datos útiles en la búsqueda de información, en el marco de una investigación penal, en coordinación con la Policía y en auxilio del Ministerio Público.

IV. OBJETIVOS ESPECÍFICOS

- Conocer cómo funciona internet y las formas de análisis en línea.
- Experimentar las herramientas para capturar evidencia en línea.
- Localizar e investigar correos electrónicos y sitios web.
- Identificar el uso de internet por grupos criminales.
- Distinguir el uso de buscadores, redes sociales y espacios públicos cibernéticos.
- Analizar el manejo de casos de investigación.
- Mantener la seguridad de la institución mientras conducen investigaciones en línea.

V. PERFIL DE INGRESO

Para integrarse, deberán contar con los requisitos siguientes:

- Ser analistas de información de las Instituciones de Seguridad Pública, procuración de justicia, sistema penitenciario, así como de todas aquellas áreas de gobierno que directa o indirectamente cuenten con empleados que realicen esta actividad.
- Tener título profesional de licenciatura o grado académico afín, o bien, contar con dos años de experiencia dentro de la Procuraduría, o seguridad pública estatal o municipal.
- Género indistinto.
- Habilidades para trabajar en equipo.
- Manejo de investigación.
- Resolución de problemas.
- Toma de decisiones.
- Sentido de responsabilidad.
- Actitud de compromiso laboral.
- Actitud de apego y respeto a las normas y valores institucionales.
- Actitud de discreción y confiabilidad.
- Actitud de compromiso hacia el manejo de información confidencial.
- Responsable.
- Vocación de servicio.
- Ética personal y profesional.
- Valores: solidaridad, bien común y respeto.
- Los demás requisitos que establezcan los ordenamientos jurídicos conducentes.
- Tener un conocimiento básico de lo siguiente:
  - Navegar y utilizar el sistema Windows.
  - Ubicar archivos y aplicaciones utilizando métodos diversos.
  - Menú de inicio.
  - Explorador de Windows.
  - Windows Explorer.
  - Bandeja de sistema.
  - Manejar múltiples aplicaciones abiertas.
  - Crear y comprimir archivos.
  - Navegar aplicaciones basadas en la web.

VI. PERFIL DE EGRESO

Al egresar del curso, el participante contará con:

- Conocimientos teóricos fundamentales para desarrollar los objetivos generales y específicos de este curso, en su entorno laboral.
- Las herramientas esenciales para cumplir con sus funciones a través de los protocolos establecidos.
- Datos que conformen un todo coherente, y colocará la información evaluada en contexto con el fin de producir un producto de inteligencia que incluye la evaluación de sucesos y juicios sobre las implicaciones de la información.

VII. ESTRUCTURA CURRICULAR

Comprende las unidades o módulos del plan de estudios con la duración en horas y el total de cada una de ellas.

MATERIA	HORAS
1. El uso de internet por delincuentes.	20
2. Introducción a las investigaciones en línea.	26
3. Herramientas para obtener evidencias en línea.	24
4. Medios sociales.	8
5. Evidencia en internet.	12
TOTAL	**90**

VIII. CONTENIDO TEMÁTICO

1. EL USO DE INTERNET POR DELINCUENTES.

Duración: 20 horas.

Objetivo de aprendizaje

Identificar las maneras en que los delincuentes utilizan internet para sus propósitos.

CONTENIDO

1.1. Funcionamiento de Internet.
  1.1.1. Definir Internet.
  1.1.2. Identificar los dispositivos que conforman Internet.
  1.1.3. Explicar cómo se envía y recibe la información por Internet.
  1.1.4. Identificar el órgano regulador que controla la infraestructura básica de Internet y las convenciones de denominación.
1.2. Definir el delito cibernético.
  1.2.1. Identificar los propósitos de las actividades por Internet.

1.2.2. Describir tipos de herramientas de Internet empleadas por los delincuentes para sus Propósitos.
1.2.3. Definir las respuestas reactivas y proactivas al delito cibernético.

2. INTRODUCCIÓN A LAS INVESTIGACIONES EN LÍNEA.
Duración: 26 horas.

Objetivo de aprendizaje
Experimentar la explotación de información como producto del análisis con el fin de investigar delitos en el marco legal en México.

CONTENIDO

2.1. Identificar las tecnologías en línea/Internet utilizadas y explotadas por los criminales.
2.1.1. Describir cómo los investigadores utilizan tecnologías de Internet para obtener evidencias.
2.1.2. Analizar tendencias actuales en el uso criminal de tecnologías de Internet.
2.1.3. Analizar las tendencias actuales sobre el uso policial de las tecnologías de Internet.
2.2. Seguridad del oficial en línea.
2.2.1. Explicar cómo se protege una computadora de ataques cibernéticos.
2.2.2. Hacer una lista de tipos de información que su dirección IP puede revelar.
2.2.3. Acceder a Internet mediante un servidor proxy y explicar el uso apropiado de los servidores proxy.
2.2.4. Definir máquinas virtuales y describir su uso apropiado.
2.3. Manejo de caso de análisis para investigación de delitos.
2.3.1. Explicar la importancia de almacenar evidencia digital de manera segura.
2.3.2. Analizar la necesidad de mantener una estructura de gestión de archivos normalizada.
2.3.3. Crear una estructura de gestión de archivos normalizada.
2.4. Plataforma México.
2.4.1. Presentación, temario y finalidad de Plataforma México (PM).
2.4.2. Antecedentes de PM.
2.4.3. Marco legal.
2.4.4. Concepto y elementos de PM.
2.4.5. Ciclo básico de inteligencia.
2.4.6. Ámbitos de colaboración.
2.4.7. Beneficios.
2.4.8. Evaluación y clausura.

3. HERRAMIENTAS PARA OBTENER EVIDENCIAS EN LÍNEA.
Duración: 24 horas.

Objetivo de aprendizaje
Identificar los tipos de herramientas para obtener evidencia mediante internet, con el fin de auxiliar al ministerio publico en la búsqueda de datos útiles para la investigación de delitos.

CONTENIDO

3.1. Identificar los tipos de herramientas disponibles para captar evidencias.
- 3.1.1. Instalar y configurar las herramientas para obtener evidencias.
- 3.1.2. Utilizar las herramientas para obtener evidencias en línea.

3.2. Correo electrónico.
- 3.2.1. Explicar cómo se transmite el correo electrónico.
- 3.2.2. Aplicar cada uno de los pasos del proceso de rastreo de los correos electrónicos.
- 3.2.3. Reconocer el correo electrónico falsificado o manipulado para ocultar la identidad del remitente.
- 3.2.4. Identificar el proceso legal pertinente para obtener información del abonado del proveedor de servicio de internet.
- 3.2.5. Describir cómo los convenios internacionales ayudan a las investigaciones del delito informático entre fronteras.

3.3. Sitios Web
- 3.3.1. Explicar la manera en que se obtienen, administran y hospedan los dominios.
- 3.3.2. Identificar los métodos que se utilizan para ocultar la propiedad de dominio.
- 3.3.3. Realizar búsquedas en Whois para identificar la propiedad de dominio.
- 3.3.4. Determinar la ubicación del hospedero del sitio web.
- 3.3.5. Identificar los métodos utilizados para ocultar la ubicación del hospedero.

3.4. Motores de Búsqueda.
- 3.4.1. Distinguir entre un motor de búsqueda y un directorio web.
- 3.4.2. Identificar ejemplos de motores de búsqueda y directorios web.
- 3.4.3. Explicar cómo buscar de manera eficiente utilizando operadores.
- 3.4.4. Demostrar prácticas de búsqueda eficientes.

4. MEDIOS SOCIALES.
Duración: 8 horas.

Objetivo de aprendizaje
Definir los medios sociales y cómo utilizarlos para la identificación de delincuentes o personas relacionadas con un asunto de investigación penal.

4.1. Definir la Web 2.0 y los medios sociales.
- 4.1.1. Describir la manera en que los medios pueden ser utilizados por delincuentes para la actividad ilícita.
- 4.1.2. Practicar el trabajo en línea en los ambientes de los medios sociales.
- 4.1.3. El uso de las herramientas de investigación de los medios sociales.

4.2. Cibercafés.
- 4.2.1. Describir la configuración de red común y el flujo de información.
- 4.2.2. Identificar las estrategias para investigar la actividad de internet originada en los cibercafés.
- 4.2.3. Identificar las estrategias para investigar la actividad de internet originada en las redes Wi-Fi abiertas.
- 4.2.4. Analizar los temas legales asociados con la obtención de pruebas en los cibercafés y sitios Wi-Fi abiertos.

5. EVIDENCIA EN INTERNET.
Duración: 12 horas.

Objetivo de aprendizaje
Identificar los tipos de evidencia forense digital, su manejo y usos en la judicialización de un asunto penal con el fin de dar soporte a la investigación.

CONTENIDO

5.1. Identificar las razones para proporcionar los antecedentes y objetivos de la investigación a los peritos forenses.
  5.1.1. Identificar los tipos de pruebas que pueden obtenerse de una computadora.
  5.1.2. Analizar e interpretar los datos del informe forense.
  5.1.3. Determinar los pasos siguientes en la investigación.
5.2. Ejercicios finales.
  5.2.1. Rastrear correos electrónicos múltiples en busca de trazas.
  5.2.2. Investigar un sitio web.
  5.2.3. Explotar los medios sociales.
  5.2.4. Realizar búsquedas en internet.
  5.2.5. Documentar y administrar la evidencia.
  5.2.6. Analizar de manera critica la información obtenida a partir de la evidencia recolectada.

IX. METODOLOGÍA DE ENSEÑANZA-APRENDIZAJE

Este curso combina adecuadamente la teoría con la práctica, a fin de garantizar un mejor aprovechamiento de la información adquirida por los participantes. En ese sentido, se utilizarán las técnicas didácticas siguientes: expositiva, método demostrativo, diálogo-discusión y técnica grupal.

En el desarrollo de la capacitación se realizará el intercambio de experiencias mediante la actividad de los participantes, donde el docente fungirá como coordinador y no como simple transmisor de conocimientos; para tal efecto, buscar en la interacción dinámica promover en el grupo el trabajo en equipo que los lleve a debates y discusiones entre alumno y docente donde externen y sea posible conocer las argumentaciones conceptuales y técnicas de cada uno de ellos.

Materiales de apoyo para el docente-instructor
Instalaciones y recursos materiales

- Hojas de rotafolio.
- Pintarrón.
- Plumones de colores.
- Equipo de cómputo.
- Proyector.

X. PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

A. Criterios

- Aplicación de una evaluación diagnóstica con preguntas exploratorias sobre el tema.
- Para tener derecho a evaluación, los participantes deben cumplir un mínimo de 90% de asistencias.
- Evaluación final teórica formativa con base en reactivos: 60%.
- Observación directa del instructor respecto a las prácticas realizadas: 40%.
- El curso se evaluará mediante escala numérica de 0 a 10, teniendo como calificación mínima aprobatoria 8.

B. Procedimiento

Para tener derecho a evaluación los participantes deben cubrir, cuando menos, 80% de la asistencia registrada:

- Asistencia normal.
- Asistencia con retardo.

Respecto a los procedimientos de evaluación estrictamente académica se consideran los siguientes criterios:

- Cumplimiento.
- Redacción: expresión escrita.
- Contenido: nivel de análisis de la temática.
- Presentación.
- Participación en los ejercicios prácticos.
- Expresión oral en la discusión y análisis de casos.

C. Instrumentos

- Registro diario de asistencia.
- Aplicación de examen escrito.

D. Documento que se otorgará

- Constancia de acreditación del curso.

XI. FUENTES DE CONSULTA

– Cámara de Diputados del H. Congreso de la Unión (15 de agosto de 2016), *Constitución Política de los Estados Unidos Mexicano*s, en: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm.
– Lineamientos establecidos por el Centro Nacional de Información.
– Reglamento Interior de la Secretaría de Gobernación.
– http://www.pcmag.com/article2/0,2817,2388024,00.asp.
– http://www.ibtimes.com/articles/115849/20110224/craigslist-anonymousclassifieds-facebook-crimesociety
– http://www.domaintools.com
– http://www.dnsstuff.com/

- http://www.checkdomain.com
- http://www.whois.net
- http://www.networksolutions.com/whois/index.jsp
- http://www.tracemyip.org.
- http://thepiratebay.sx.
- www.ebay.com
- www.ubid.com
- www.overstock.com
- www.tinychat.com
- http://www.forensicfocus.com/forums
- http://technet.microsoft.com/en-us/library/cc512596.aspx.
- http://www.scmagazine.com/news-briefs-hacktivist-group-anonymous-duqu-malware-reports-andmore/article/217170/.
- http://en.wikipedia.org/wiki/Silk_Road_(marketplace).
- Christin, Nicolas (2013), *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. Carnegie Mellon INI/CyLab. pág. 8.
- http://edition.cnn.com/2013/09/26/opinion/bergen-twitter-terrorism/index.html#!
- http://www.thejakartapost.com/news/2012/07/09/terrorist-financing-cybercrime-and-underground-economy.html.