10. CURSO DE ESPECIALIZACIÓN PARA INTEGRANTES DE LAS UNIDADES DE POLICÍA CIBERNÉTICA

CURSO DE ESPECIALIZACIÓN PARA INTEGRANTES DE LAS UNIDADES DE POLICÍA CIBERNÉTICA

I. ÍNDICE

II. INTRODUCCIÓN 195
III. OBJETIVO GENERAL 197

Nivel 0
IV. OBJETIVOS ESPECÍFICOS 198
V. PERFIL DE INGRESO 198
VI. PERFIL DE EGRESO 198
VII. ESTRUCTURA CURRICULAR 199
VIII. CONTENIDO TEMÁTICO 199
IX. METODOLOGÍA DE ENSEÑANZA APRENDIZAJE 205
X. PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN 205
XI. INFORMACIÓN DEL INSTRUCTOR 206

Nivel 1
IV. OBJETIVOS ESPECÍFICOS 206
V. PERFIL DE INGRESO 206
VI. PERFIL DE EGRESO 206
VII. ESTRUCTURA CURRICULAR 207
VIII. CONTENIDO TEMÁTICO 207
IX. METODOLOGÍA DE ENSEÑANZA APRENDIZAJE 215
X. PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN 215
XI. INFORMACIÓN DEL INSTRUCTOR 216

Nivel 2
IV. OBJETIVOS ESPECÍFICOS 217
V. PERFIL DE INGRESO 217
VI. PERFIL DE EGRESO 217
VII. ESTRUCTURA CURRICULAR 218
VIII. CONTENIDO TEMÁTICO 218
IX. METODOLOGÍA DE ENSEÑANZA APRENDIZAJE 227
X. PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN 227
XI. INFORMACIÓN DEL INSTRUCTOR 228

II. INTRODUCCIÓN

Existen 3 000 millones de cibernautas a nivel mundial (40% de la población); en México hay 53.9 millones y la tasa de crecimiento entre 2013 y 2014 fue de 5.3%. En 2012 se estima que 55.6 millones de personas fueron afectadas por ataques a nivel mundial; en México fueron 14.8 millones.[1]

A nivel mundial México ocupa el primer lugar en virus informáticos por encima de China y Brasil; en América Latina México ocupa el segundo lugar en fraudes electrónicos (debajo de Brasil); y el tercer lugar en ataques a páginas web (debajo de Brasil y Perú). Las ganancias del cibercrimen mundial se encuentran en un rango de 300 a 500 mil MDD anuales y en México se estima que en 2013 hubo pérdidas de 3 mil MDD debido al cibercrimen.[2]

El Modelo de Policía Cibernética establece los cimientos para aumentar las capacidades del Estado Mexicano para prevenir e investigar los delitos cibernéticos. De acuerdo con la ONU, sólo 1% de los delitos informáticos son denunciados a la policía.

La implementación estratégica y estructurada de este modelo impulsará la atención oportuna a las denuncias ciudadanas, fortaleciendo los canales de coordinación y las capacidades de investigación, así como la integración de estadísticas nacionales sobre ciberdelincuencia en nuestro país que permitan generar políticas públicas en materia de prevención.

Contexto Nacional

Las entidades federativas no cuentan con capacidades de Policía Cibernética robustas. El 40% de las entidades cuentan con Unidades de Policía Cibernética, de ellas, sólo 10% cuenta con la infraestructura y capacidades mínimas para su operación.

La falta de cultura de seguridad informática de la población y el incremento de los delitos cibernéticos han generado la necesidad de impulsar una reforma legislativa en materia de delitos cibernéticos.

No se dispone de indicadores estadísticos de ciberdelincuencia a nivel nacional. Se requiere fortalecer la celebración de tratados internacionales que formalicen la colaboración con policías cibernéticas de otros países.

MARCO LEGAL

La Constitución Política de los Estados Unidos Mexicanos, en su Artículo 21, párrafos noveno y décimo, dispone que la seguridad pública es una función a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, que comprende la prevención de delitos, la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas en los términos de la ley.

---

[1] International Telecommunications Union (ITU), ICT Indicators 2005 a 2014.

[2] 2013 Reporte Norton PressDeck México, http://es.scribd.com/doc/185270894/2013-Reporte-Norton-Press-Deck-México.

El Programa Nacional de Seguridad Pública 2013-2018 establece, dentro de sus estrategias, la detección y atención oportuna de los delitos cibernéticos, y prevé como una de sus líneas de acción el desarrollo de un Modelo de Policía Cibernética para las entidades federativas. Esto, en virtud del fortalecimiento de las capacidades humanas, tecnológicas y la infraestructura para atender incidentes de seguridad cibernética.

El Plan Nacional de Desarrollo 2013-2018 establece, entre otras metas nacionales, un México en Paz y prevé como una de sus líneas de acción, impulsar mecanismos de concertación de acciones nacionales que permitan la construcción y desarrollo de las condiciones que mantengan vigente el proyecto nacional, a fin de generar una posición estratégica del país en el ámbito global.

La Ley General del Sistema Nacional de Seguridad Pública, reglamentaria de la disposición Constitucional aludida, establece en su Artículo 2° que la Seguridad Pública tiene como fines salvaguardar la integridad y derechos de las personas, preservar las libertades, el orden y la paz públicos, y comprende la prevención especial y general de los delitos, la investigación para hacerla efectiva, la sanción de las infracciones administrativas, así como la investigación y persecución de los delitos y la reinserción social del individuo, en términos de dicha Ley.

La Ley de Planeación establece, en su Artículo 37, que el Ejecutivo Federal, por sí o a través de sus dependencias, y las entidades paraestatales podrán concertar la realización de las acciones previstas en el Plan y los programas, con las representaciones de los grupos sociales o con los particulares interesados.

PNSP: 2.7.6. *Desarrollar un modelo de policía cibernética para las Entidades Federativas*

PNSP: 2.7. *Detectar y atender oportunamente los delitos cibernéticos*

Resultados generales esperados

1. Garantizar que los integrantes tengan, una vez concluida la formación de las Unidades de la Policía Cibernética, la capacidad de realizar actividades de prevención, atención e investigación de delitos cibernéticos.

2. Elevar la calidad de la atención a las denuncias de delitos cibernéticos.

3. Brindar una formación integral con un contenido que posibilite la adquisición de competencias para el óptimo desempeño de sus funciones.

Beneficios institucionales del curso

1. Ser una estrategia clave en la implementación del Modelo de la Policía Cibernética, brindando con ello una adecuada atención a las denuncias ciudadanas y mandamientos judiciales y ministeriales.

2. Sentar las bases de un proceso integral de capacitación y desarrollo que en el futuro sirva para un servicio profesional de carrera.

CARACTERÍSTICAS CURRICULARES

Con base en el Acuerdo 12/XL/16 del Consejo Nacional de Seguridad Pública, donde se establece la elaboración de un Modelo Homologado de Unidades de Policía Cibernética y el proceso gradual para su implementación, publicado en el Diario Oficial de la Federación el 9 de septiembre del 2016, se propone crear un Programa de Formación Especializada para los integrantes de las Unidades de Policías Cibernéticas, dividido de acuerdo con la madurez actual de las Unidades de Policía Cibernética estatales, en tres niveles. El primero se denomina de "Prevención de Delitos Cibernéticos" o "Nivel 0"; el segundo "Atención Ciudadana a Delitos Cibernéticos e Identificación y Análisis de Incidentes Cibernéticos" o "Nivel 1"; y, el tercero, "Investigación de Delitos Cibernéticos y Seguridad de la Información" o "Nivel 2". En donde el nivel 0, se refiere a las Entidades Federativas que aún no cuentan con una Unidad de Policía Cibernética establecida, mientras que, en el segundo supuesto, dichas entidades federativas cuentan con una unidad básica que requiere de una primera especialización; y el nivel 2, se refiere a las entidades federativas que requieren de una capacitación especializada a mayor profundidad.

Cabe mencionar que la madurez de las diversas Unidades de Policía Cibernética no es limitativa para que sus integrantes cursen un determinado nivel de formación, en virtud de que la capacitación se vincula a los procesos y actividades que se desempeñan en dichas Unidades.

III. OBJETIVO GENERAL

Con el Curso de Especialización para Integrantes de las Unidades de Policía Cibernética, la Comisión Nacional de Seguridad, a través de la Policía Federal (PF) y junto con el Secretariado

Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) formarán y actualizarán al personal para contribuir:

- En la implementación de un Modelo de Unidad de Policía Cibernética que impulse la prevención, atención e investigación de los delitos cibernéticos a lo largo del territorio nacional.
- En la reducción de delitos cometidos en agravio de niñas, niños y adolescentes.
- En el incremento del nivel de seguridad de la red pública de internet.
- En el mejoramiento de la calidad de vida dentro de la sociedad, al fomentar las operaciones de comercio electrónico seguro en el país.

En relación con lo anterior y de conformidad con la madurez de las Unidades de Policía Cibernética de las entidades federativas, se proponen tres etapas de capacitación, mismas que se describen a partir de sus propios objetivos específicos.

NIVEL 0

"PREVENCIÓN DE DELITOS CIBERNÉTICOS" O "NIVEL 0"

IV. OBJETIVOS ESPECÍFICOS

- Homologar la capacitación de los integrantes de las Unidades de Policía Cibernética Estatales del país.
- Dotar a los integrantes de las Unidades de Policía Cibernética de técnicas y habilidades que les permitan desempeñar mejor sus funciones y fortalezcan las capacidades de prevención de delitos cibernéticos.
- Identificar las actividades principales que deben realizar los integrantes de las Unidades de Policía Cibernética para prevenir los delitos cibernéticos.
- Realizar campañas de prevención de delitos cibernéticos.

V. PERFIL DE INGRESO

Considerando que el programa establece un modelo de formación, el perfil de ingreso determina únicamente los requisitos que deberá reunir el aspirante para garantizar un buen aprovechamiento académico y un apropiado desempeño de sus actividades.

- Tener licenciatura terminada en cualquiera de las siguientes carreras: Informática o similar, Derecho, Psicología, Comunicación, Diseño Gráfico; titulado y con cédula profesional.
- Estar en pleno ejercicio de sus derechos.
- Haber acreditado los exámenes de control y confianza.
- Haber cursado el Programa de Formación Inicial para Policía Preventivo.

VI. PERFIL DE EGRESO

El egresado, al término del plan académico, adquirirá los siguientes conocimientos, habilidades y actitudes:

Conocimientos:

1. Podrá realizar campañas de prevención de delitos cibernéticos.
2. Podrá capacitar y orientar a la ciudadanía en materia de delitos cibernéticos.

Habilidades:

1. Promoverá la cultura de prevención en delitos cibernéticos.
2. Concertará convenios para impulsar campañas de prevención.

Actitudes:

1. Demostrará un pensamiento socialmente comprometido para asumir una actitud positiva y de cambio para realizar actividades de prevención de conductas que afecten a la ciudadanía relacionadas con delitos cibernéticos.
2. Mostrará interés en los diversos procesos que conlleva las campañas de prevención.

VII. ESTRUCTURA CURRICULAR

La duración total del curso es de **90 horas**, distribuidas en jornadas completas de lunes a viernes, con 6 horas diarias de clase y descanso los fines de semana.[3]

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

DURACIÓN

UNIDADES	DURACIÓN
1. Estrategias de prevención de delitos cibernéticos.	35
2. Amenazas dentro del internet (delitos cibernéticos).	25
3. Nuevas tecnologías y el uso del internet de las cosas.	10
4. Introducción a la seguridad de la información.	20
TOTAL	**90 HORAS**

VIII. CONTENIDO TEMÁTICO

FORMACIÓN ESPECIALIZADA EN "PREVENCIÓN DE DELITOS CIBERNÉTICOS" O "BÁSICO, MADUREZ 0"

Duración: 90 horas

1. ESTRATÉGIAS DE PREVENCIÓN DE DELITOS CIBERNÉTICOS.

Duración: 35 horas.

[3] Queda a consideración de la Institución que solicita la capacitación, si el personal reclutado necesariamente deberá permanecer internado durante el desarrollo del curso; el calendario es una propuesta que deberá ajustarse según necesidades.

Objetivo de aprendizaje
Desarrollar programas y campañas de prevención en materia de delitos cibernéticos dirigidas a diversos sectores de la sociedad.

CONTENIDO

Unidad I. ¿Qué son los delitos cibernéticos?
1.1. Definición de los delitos cibernéticos.

Unidad II. Conceptos básicos
2.1. Seguridad de la información.
2.2. Mecanismos de seguridad.
2.3. La guerra de la información y la evolución de internet.
2.4. Prevención del delito cibernético orientado a la ciudadanía.
2.5. Mejores prácticas en la investigación de delitos cibernéticos.
2.6. Monitoreo en la red pública de internet.

Unidad III. Marco normativo e interpretación.
3.1. Marco legal.
3.2. Tipificación de los delitos.
3.3. Armonización legislativa en materia de delitos cibernéticos.
3.4. Convenio de Budapest.

Unidad IV. Hábitos y uso de internet.
4.1. Características de los cibernautas.
4.2. ¿Qué dispositivos utilizan los cibernautas para conectarse a internet?
4.3. Principales actividades que realizan las personas en internet.
4.4. Análisis de hábitos y uso de internet en el país.

Unidad V. Estrategias de prevención.
5.1. Incidencia delictiva.
5.2. Regionalización del país.
5.3. Planeación campañas de prevención.
5.4. Diseños de publicidad de programas y campañas de prevención.
5.5. Diseño e implementación de campañas de prevención de delitos cibernéticos dirigidas a la ciudadanía.

Unidad VI. Plataforma México.
6.1. Presentación, temario y finalidad de Plataforma México (PM).
6.2. Antecedentes de PM.
6.3. Marco legal.
6.4. Concepto y elementos de PM.
6.5. Ciclo básico de inteligencia.
6.6. Ámbitos de colaboración.
6.7. Beneficios.
6.8. Evaluación y clausura.

FUENTES DE CONSULTA

- Applicantes Google, http://applicantes.com/google-play-supera-la-app-store-en-numero-de-aplicaciones/.
- Candau Romero, Javier. "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", Capítulo VI, Estrategias Nacionales de Ciberseguridad, Ciberterrorismo, Instituto Español de Estudios Estratégicos, 2011.
- *Convenio sobre la Ciberdelincuencia,* Serie de Tratados Europeos No. 185, Council of Europe, 2001.
- *Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno,* ONUDC, 2013.
- *Estudio sobre los hábitos del Internet en México*, AMIPCI 2016.
- ICT Reports, Unión Internacional de Telecomunicaciones, 2014.
- Internet Trends 2014, KPCB, www.kpcb.com/InternetTrends.
- International Telecommunications Union (ITU), ICT Indicators 2005 a 2014 y Reporte Norton "Online Family" 2012.
- Panorama del Ciberdelito en Latinoamérica, LACNIC, 2011.
- *Tendencias en seguridad cibernética en América Latina y el Caribe,* Organización de Estados Americanos y Symantec, 2014.
- Worldwide mobile app revenues in 2015, 2015 and 2020 (in billion U.S. dollars), STATISTA,http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/.
- 2013 Reporte Norton PressDeck México, http://es.scribd.com/doc/185270894/2013-Reporte-Norton-Press-Deck-México.

2. AMENAZAS DENTRO DE INTERNET (DELITOS CIBERNÉTICOS).

Duración: 25 horas.

Objetivo de aprendizaje

Identificar las ventajas y mal uso de internet, así como las conductas constitutivas del delito, ataques cibernéticos contra el patrimonio y contra la información.

CONTENIDO

Unidad I. ¿**Qué es Internet?**

1.1. Buscadores y redes sociales.

Unidad II. Ventajas de Internet.

2.1. Correo electrónico.
2.2. Búsquedas.
2.3. Compras y ventas.
2.4. Pago de servicios
2.5. Descargas.
2.6. Localización.
2.7. Juegos.
2.8. Redes sociales.

2.9. Traductores.
2.10. Educación en línea.
2.11. Cámaras de vigilancia
2.12. Soporte remoto.
2.13. Clima.
2.14. Noticias.
2.15. Visitas virtuales.
2.16. Edición de imágenes y videos.
2.17. Simulaciones.
2.18. Manuales y videotutoriales.

Unidad III. Mal uso de Internet
3.1. Correos maliciosos.
3.2. Mal uso de la información.
3.3. Fraude electrónico.
3.4. *Phising* y *smishing*.
3.5. Virus informáticos.
3.6. Información pública.
3.7. Excesos.
3.8. Conductas antisociales.

Unidad IV. Perfil del internauta en México.
4.1. Redes sociales.
4.2. Qué son los delitos cibernéticos.
4.3. Delitos electrónicos contra niñas, niños y adolescentes.

Unidad V. Contenidos nocivos.
5.1. Pornografía, suicidio, armamento, trastornos alimenticios, prácticas satánicas, violencia en videojuegos.

Unidad VI. Conductas antisociales.
6.1. *Ciberbullying, grooming, sexting, sextorsión*, amenazas y suplantación de identidad.

Unidad VII. Conductas Ilícitas.
7.1. Pederastia, lenocinio, turismo sexual, trata de personas, corrupción de menores y pornografía infantil.

Unidad VIII. Conceptos básicos de ataques cibernéticos contra el patrimonio.
8.1. Arte sacro, piezas arqueológicas, especies en peligro de extinción, *phishing, spearphishing, pharming, smishing* y *vishing*.

Unidad IX. Delitos electrónicos contra la información.
9.1. Infraestructura crítica, instituciones académicas, instituciones privadas.

Unidad X. Introducción a ataques cibernéticos.
10.1. *Defacement* (alteración de contenido Web), DoS/DDoS (negación de servicio, infección por código malicioso, baja o nula configuración de seguridad en los sistemas, divulgación

no autorizada de información, envío de correo spam (correos no deseados) e ingeniería social.

Unidad XI. Cómo preservar la evidencia digital.
11.1. Metodología para la captura de la evidencia.

FUENTES DE CONSULTA

- Carpentier, Jean Francois. La seguridad Informática en la PYME. Situación actual y mejores prácticas. Ediciones ENI.
- Rascagneres, Paul. Seguridad Informática y Malwares. Análisis de amenazas e implementación de contramedidas. Ediciones ENI. 2016
- Reyes G., Félix A. y Carlos Andrés Lugo González. Amenazas informáticas en la WEB 3.0: Guía P. (Edición Kindle).

3. NUEVAS TECNOLOGÍAS Y EL USO DE INTERNET DE LAS COSAS.
Duración: 10 horas.

Objetivo de aprendizaje
Entender los principales conceptos subyacentes al internet de las cosas. Desarrollar entornos del internet de las cosas.

CONTENIDO

Unidad I. Introducción a internet de las cosas (IoT)
1.1. Introducción a IoT.
1.2. Historia.
1.3. Componentes de IoT.
1.4. Arquitectura del IoT.
1.5. Estándares en IoT.

Unidad II. Tecnologías asociadas al IoT
2.1. Plataformas de hardware y software para IoT.
2.2. Sensores, tipos de sensores y fuentes de alimentación.
2.3. Redes de sensores y transmisión de datos.
2.4. Sistemas de comunicación inalámbrica.
2.5. Introducción a la seguridad y la privacidad.

Unidad III. Integración en Dispositivos Inteligentes
3.1. Dispositivos inteligentes y sensores.
3.2. Desarrollo de aplicaciones.

FUENTES DE CONSULTA

- González Pérez, Pablo, Germán Sánchez Garcés y José Miguel Soriano de la Cámara. Pentesting con Kali, 0xWord, 2015.

- Introducción a la Internet de las Cosas, PacoMaroto's IoT Blog, The Blog that all IoT experts must read.
- Morcillo, Francisco. Las claves de la ciudad inteligente, Open Data, Lot y M2M, El triángulo de las Smart Cities, Thinking about Smart Cities post., 2014.
- Nam, Taewoo y Theresa A. Pardo. Conceptualizing Smart City with dimensions of technology, people and institutions, Center for Technology in Government, NY., 2011.

4. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN.

Duración: 20 horas.

Objetivo de aprendizaje

Conocer los conceptos en materia de seguridad de la información.

CONTENIDO

Unidad I. Definición de seguridad de la información.

1.1. ¿Qué es la seguridad de la información?

Unidad II. Tipos de seguridad de la información.

2.1. Seguridad lógica.
2.2. Seguridad física.
2.3. Seguridad administrativa.

Unidad III. Objetivos de la seguridad de la información.

3.1. Definir objetivos de seguridad de la información.

Unidad IV. Fundamentos de la seguridad de la información.

4.1. Confidencialidad.
4.2. Integridad.
4.3. Disponibilidad.

Unidad V. Amenazas a la seguridad de la información.

5.1. Tipos de amenazas.

Unidad VI. Evaluación de riesgos.

6.1. Evaluación de riesgos.

Unidad VII. Técnicas de aseguramiento del sistema

7.1. Técnicas de aseguramiento.

FUENTES DE CONSULTA

- González Pérez, Pablo; Germán Sánchez Garcés y José Miguel Soriano de la Cámara. Pentesting con Kali, 0xWord, 2015.
- Ramió Aguirre, Jorge. Seguridad Informática y Criptografía, Dpto. de Publicaciones E.U.I., 2006.

– Russell, Debby y G.T. Gangemi. Computer Security Basics, O'Reilly Media. 1991
– Siyan, Karajit y Chrys Hare. Internet y seguridad en redes, Edit. Prentice Hall, 1995.

IX. METODOLOGÍA DE ENSEÑANZA-APRENDIZAJE

– Exposición a cargo del ponente.
– Preguntas y respuestas (participación dirigida).
– Lecturas obligatorias.
– Material de apoyo para el maestro y de consulta para el alumno.

X. PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN

La evaluación se concibe como un proceso para estimar los resultados del proceso de enseñanza-aprendizaje, dado que permite valorar los conocimientos adquiridos y las habilidades desarrolladas en el curso. Para cada una de las materias, se prevé una evaluación especial atendiendo a los conocimientos y habilidades que se impartieron; sin embargo, se deberá realizar el siguiente proceso:

- Un examen inicial del curso para valorar el nivel del grupo a capacitar.
- La evaluación referente a cada materia.
- Un examen final.

La escala de calificación será de 0 a 10, en la que la mínima para acreditar es 8 (ocho); al término del programa, se entregará una constancia por las autoridades estatales correspondientes, quienes deberán informar por oficio al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y a la Policía Federal la totalidad del personal capacitado para los fines pertinentes de la política pública y consolidación de las Unidades de Policía Cibernética.

Evaluación del proceso educativo. Aunado a la evaluación interna del conocimiento del alumno, se evaluará el desempeño del docente y de la institución que brindó la capacitación mediante la aplicación de una encuesta de satisfacción.

Para tener derecho a la evaluación, se deberá cumplir con 95% de asistencia.
- Examen final que evaluará la capacidad del alumno: 70%
- Participación y asistencia: 30%

El curso se desarrollará en un aula que cumpla con los siguientes requerimientos:
- Espacio adecuado para el número de participantes (15 a 30).
- Ventilación e iluminación propicia.
- Toma y extensiones de corriente eléctrica.

Para la impartición del curso es necesario contar con el siguiente material:
- Computadora portátil con Microsoft Office compatible con equipo de proyección.
- Una computadora por alumno.

- Proyector.
- Equipo de audio y video.
- Rotafolio o pintarrón con marcadores.

XI. INFORMACIÓN DEL INSTRUCTOR

El aspirante a docente de los cursos de "PREVENCIÓN DE DELITOS CIBERNÉTICOS" o "NIVEL 0" para integrantes de las Unidades de Policía Cibernética deberá contar con:

a) Título de licenciatura, maestría o doctorado con cédula profesional expedida por la Secretaría de Educación Pública, relacionado con la asignatura que habrá de impartir.
b) Por lo menos tres años de experiencia docente comprobable en el ámbito de la materia a impartir.

NIVEL 1

"ATENCIÓN CIUDADANA A DELITOS CIBERNÉTICOS E IDENTIFICACIÓN Y ANÁLISIS DE INCIDENTES CIBERNÉTICOS" O "NIVEL 1"

IV. OBJETIVOS ESPECÍFICOS

- Homologar la capacitación de los integrantes de las Unidades de Policía Cibernética estatales del país.
- Dotar a los integrantes de las Unidades de Policía Cibernética de técnicas y habilidades que les permitan desempeñar mejor sus funciones, que fortalezcan las capacidades de atención y orientación ciudadana en delitos cibernéticos.
- Correlacionar la información sobre el comportamiento de los delitos cibernéticos.
- Analizar y resolver incidentes de seguridad Informática, manejando la información de manera segura acorde con las políticas de seguridad.

V. PERFIL DE INGRESO

Considerando que el programa establece un modelo de formación, el perfil de ingreso determina únicamente los requisitos que deberá reunir el aspirante para garantizar un buen aprovechamiento académico y un apropiado desempeño de sus actividades.

- Tener licenciatura terminada en cualquiera de las siguientes carreras: Informática o similar, Derecho o Psicología, titulado y con cédula profesional.
- Tener experiencia profesional comprobable de 2 años.
- Estar en pleno ejercicio de sus derechos.
- Tener vigentes los exámenes de control y confianza.

VI. PERFIL DE EGRESO

Al término del plan académico, el egresado habrá adquirido los siguientes conocimientos, habilidades y actitudes:

Conocimientos:

1. Atenderá reportes ciudadanos en materia de delitos cibernéticos.
2. Identificará y analizará incidentes cibernéticos.
3. Realizará monitoreo de la red pública de internet.
4. Correlacionará la información sobre el comportamiento de los delitos cibernéticos.
5. Analizará y resolverá incidentes de seguridad Informática, manejando la información de manera segura acorde con las políticas de seguridad.

Habilidades:

1. Atenderá correctamente las denuncias realizadas por la ciudadanía.
2. Identificará y analizará incidentes cibernéticos.
3. Realizará ciberpatrullaje en la red pública de internet.
4. Mitigará los riesgos y amenazas en ataques cibernéticos.
5. Elaborará y estructurará informes policiales.

Actitudes:

1. Demostrará un pensamiento socialmente comprometido para asumir una actitud positiva y de cambio frente a los problemas de las personas en situación de víctima.
2. Mostrará interés en los diversos procesos que conlleva la atención ciudadana e identificación de incidentes cibernéticos.

VII. ESTRUCTURA CURRICULAR

La duración total del curso es de **70 horas**, en jornadas completas de lunes a viernes, con 6 horas diarias de clase y descanso los fines de semana.[4]

Cuando el policía se encuentra en activo en la Unidad de Policía Cibernética por más de dos años, podrá cursar el siguiente programa curricular de especialización intermedia para mejorar en sus funciones.

DURACIÓN

UNIDADES	DURACIÓN
1. Ciberpatrullaje en la red pública de internet.	10
2. Pornografía infantil y trata de personas en internet.	15

[4] Queda a consideración de la Institución que solicita la capacitación, si el personal reclutado necesariamente deberá permanecer internado durante el desarrollo del curso; el calendario es una propuesta que deberá ajustarse según las necesidades.

3. *Malware*, amenazas y ataques.	15
4. Seguridad en redes.	10
5. Seguridad en dispositivos móviles.	10
6. *Password*: enfrentar el control de accesos.	10
TOTAL	**70 HORAS**

VIII. CONTENIDO TEMÁTICO

1. CIBERPATRULLAJE EN LA RED PÚBLICA DE INTERNET.
Duración: 10 horas.

Objetivo de aprendizaje
Realizar ciberpatrullaje en la red pública de internet con la finalidad de prevenir y perseguir actividades delictivas.

CONTENIDO

Unidad I. Conceptos básicos.
1.1. Internet.
1.2. Navegadores o buscadores.
1.3. Aplicaciones *(Software)*.
1.4. Correo Electrónico.
1.5. Dispositivos electrónicos.
1.6. Redes de comunicación.
1.7. Redes Sociales.
1.8. Dirección IP.
1.9. *Darknet*.
1.10. *Deepweb*.

Unidad II. Utilización de navegadores.
2.1. Ventajas en la utilización de diversos navegadores (Chrome Google, Internet Explorer, Safari, Fox, Opera, etcétera).
2.2. Introducción al Lenguaje HTML (Hyper Text Markup Language).
2.3. ¿Cómo navegar de manera anónima?

Unidad III. TOR (red de anonimato).
3.1. Navegador/buscador TOR "The Onion Router".

Unidad IV. Redes sociales.
4.1. Facebook.
4.2. Twitter.
4.3. Linkedin.
4.4. Google+.
4.5. YouTube.
4.6. WhatsApp.

Unidad V. Introducción a herramientas especializadas.
5.1. Whois.
5.2. Maltego.
5.3. Kali Linux.
5.4. Tweet Deck.
5.5. Awesome Screenshot.
5.6. Evil foca.
5.7. BeCyPDFMetaEdit.
5.8. Aplicaciones para el monitoreo de incidentes: Zona-h, Dark-h, Hootsuite y Pastebin.

Unidad VI. Fraude al sector financiero.
6.1. *Carding*, Tarjetas de crédito.

Unidad VII. Propiedad intelectual.
7.1. Delitos en materia de derechos de autor.
7.2. Piratería.

Unidad VIII. Grupos *hacktivistas.*
8.1. Seguimiento de grupos hacktivistas en internet.
8.2. Seguimiento de grupos hacktivistas en redes sociales.
8.3. Seguimiento de grupos hacktivistas en foros.
8.4. Elaboración de informes de grupos hacktivistas.
8.5. Prevención de ataques a las infraestructuras informáticas por grupos hacktivistas.

Unidad IX. Ciberpatrullaje.
9.1 Aplicación de navegadores/buscadores y herramientas especiales para realizar el Ciberpatrullaje.
9.2 Elaborar informes del Ciberpatrullaje.

FUENTES DE CONSULTA

- González Pérez, Pablo; Germán Sánchez Garcés y José Miguel Soriano de la Cámara. *Pentesting con Kali*, 0xWord, 2015.
- Muñiz Troyano, Javier y Juan Diego Polo. Community Manager, Estrategia de gestión en redes sociales, Alfaomega, Altaria Editorial, 2014.
- Stallings, William. Network and Internet Network Security: Principles and Practice. Prentice Hall, 1995.
- Siri, Santiago. Hacktivismo: La red y su alcance para revolucionar el poder, Penguin Random House Grupo Editorial Argentina. 2015.

2. PORNOGRAFÍA INFANTIL Y TRATA DE PERSONAS EN INTERNET.
Duración: 15 horas.

Objetivo de aprendizaje
Desarrollar acciones de prevención e investigación de los delitos o conductas antisociales que

se cometen a través de medios electrónicos, cibernéticos o tecnológicos, en agravio de niñas, niños y adolescentes, así como la trata de personas. Ello mediante la atención a mandamientos ministeriales y judiciales y en colaboración con organismos nacionales e internacionales, con preponderancia en el interés superior de la infancia, principalmente de bienestar y seguridad de su libre desarrollo psico-sexual y de su personalidad.

CONTENIDO

Unidad I. Pornografía infantil.
1.1. ¿Qué es la pornografía infantil?

Unidad II. Trata de personas
2.1. ¿Qué es la trata de personas?

Unidad III. Red pública
3.1. La relación de la red pública de internet y el delito de pornografía infantil y trata de personas.

Unidad IV. Enganchamiento
4.1. Métodos de enganchamiento en la red pública de internet.

Unidad V. Información
5.1. Recopilación de información en la red pública de internet.

Unidad VI. Correos electrónicos
6.1. Investigación de correos electrónicos.

Unidad VII. Redes sociales
7.1. Investigación en las redes sociales.

Unidad VIII. Análisis y procesamiento de la información
8.1. Análisis y procesamiento de la información relacionada con la pornografía infantil y trata de personas.

Unidad IX. Redes técnicas
9.1. Redes técnicas.

Unidad X. Redes de cruces
10.1. Redes de cruces.

Unidad XI. The National Center for Missing & Exploited Children NCMEC
11.1. ¿Qué es el NCMEC?
11.2. Investigaciones en colaboración con el NCMEC.

Unidad XII. *Deep web*
12.1. *Deep Web*: la pornografía infantil y trata de personas.

FUENTES DE CONSULTA

- Acuerdo A/024/08, *Procuraduría General de la República, Fiscalía Especial para los Del*itos de Violación contra las Mujeres y Trata de Personas, www.pgr.gob.mx/Fiscalías/fevimtra.
- Azaola, Elena. Infancia Robada, *Niñas y Niños Víctimas de Explotación Sexual en México, DIF/UNICEF/CIESAS,* 2000.
- Estrategia Digital Nacional, Presidencia de la República, México, 2014.
- Ibarra Sánchez, Ernesto. Protección de Niños en la Red: Sexting, Ciberbullying y Pornografía Infantil, Instituto de Investigaciones Jurídicas, UNAM, 2014.
- Programa Nacional de Seguridad Pública 2014 – 2018, Presidencia de la República, México, 2014.
- Programa para la Seguridad Nacional 2014-2018, Presidencia de la República, México, 2014.
- Ramírez Marín, Juan. "Prostitución Infantil, Fenómeno de una Sociedad Indiferente", en Quorum Legislativo 91, octubre-diciembre 2007, Cámara de Diputados.
- Reglamento de la Ley de la Policía Federal, Diario Oficial de la Federación, 2010 (última modificación 22-agosto-2014).
- The National Center for Missing & Exploited Children, www.missingkid.com

3. *MALWARE*, AMENAZAS Y ATAQUES.

Duración: 15 horas.

Objetivo de aprendizaje

Contar con los conocimientos básicos para llevar a cabo un análisis de código malicioso que determine el comportamiento para prevenir futuras afectaciones.

CONTENIDO

Unidad I. Conceptos básicos.

1.1. Definición de la seguridad informática.
1.2. Reseña histórica del ***malware***.
1.3. Técnicas de propagación del ***malware***.
1.4. Montaje en un entorno de análisis seguro.

Unidad II. Análisis de *malware*.

2.1 Objetivos del análisis de ***malware***.
2.2 Escaneo y perfilado del código malicioso.
2.3 Tipos de análisis de ***malware***: estático y dinámico.
2.4. Herramientas para el análisis de ***malware.***

Unidad III. Resultados del análisis de *malware*.

3.1 Identificación, propósito, funcionalidades y capacidades del ***malware***.
3.2 Métodos y herramientas de prevención y protección

FUENTES DE CONSULTA

Básica:

- Dowd, Mark; John McDonald y Justin Schuh. El Arte de la Valoración de Seguridad de Softwares: Identificando y Previniendo Vulnerabilidades de Software. 2006.
- Eilam, Eldad. Reversing: Secrets of reverse engineering, John Wiley & Sons, 2005.
- Jakobsson, Markus. The Death of the Internet, John Wiley & Sons, Inc. 2012.
- Rascagneres, Paul. Seguridad Informática y Malwares. Análisis de amenazas e implementación de contramedidas. Ediciones ENI. 2016
- Sikorski, Michael y Andrew Honig. Análisis Práctico del Malware: La guía práctica para la disección del Software Malicioso, No Starch Press. 2012.
- Szor, Peter. El arte de la investigación y defensa en los virus de computadora, Addison-Wesley, 2005.

Herramientas:

- Análisis de código dañino, IOC Finder, Mandiant.
- Análisis de código dañino, IOC Editor, Mandiant.
- Análisis de código dañino, Redline, Mandiant.
- Análisis de código dañino, IDA, Hex-Rays.
- Análisis de código dañino, OllyDbg, OlehYuschuk.
- Análisis de código dañino**,** HijackThis, Trend Micro.
- Análisis de código dañino, IceSword, pjf.

4. SEGURIDAD EN REDES.

Duración: 10 horas.

Objetivo de aprendizaje

Reconocer los riesgos y amenazas a la seguridad de la red, así como implementar medidas de seguridad a través de herramientas especializadas.

CONTENIDO

Unidad I. Conceptos básicos.

1.1. Vulnerabilidad.
1.2. Amenazas.

Unidad II. Metodologías de evaluación de vulnerabilidades.

2.1. Demostración del escáner de evaluación de vulnerabilidades: Zenmap.
2.2. Demostración del escáner de evaluación de vulnerabilidades: Accunetix.

Unidad III. Anatomía de una intrusión en la red.

3.1. Intrusión en la red.

Unidad IV. Seguridad a nivel de la red.

4.1. Configuración de un *router*.
4.2. Configuración de una Interfaz *firewall*.
4.3. Instalación y configuración del Snort IDScenter.

Unidad V. Análisis del suceso de seguridad.
5.1. Analizador Wireshark.
5.2. Analizador ErPra.
5.3. Analizador NetworkMiner

FUENTES DE CONSULTA

- Areitio Bertolín, Javier. *Seguridad de la Información. Redes, informática y sistemas de información,* Paraninfo, 2008.
- Carracedo Gallardo, Justo. *Seguridad en Redes Telemáticas,* McGraw Hill, 2004.
- Dordoigne, José. *Redes Informáticas. Nociones fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6…)*, Ediciones ENI, 2011.
- Fish, E. y G. B. White. *Secure Computers and Networks.* CRC PressLLC, 2000.
- Katz, Matías. *Redes y Seguridad.* Editorial Alfaomega, 2013.
- McNab, Chris. *Seguridad de Redes,* Segunda Edición, Anaya Multimedia, 2004.
- Stallings, William. *Comunicaciones y Redes de Computadores,* Prentice Hall 1997.

5. SEGURIDAD EN DISPOSITIVOS MÓVILES.

Duración: 10 horas.

Objetivo de aprendizaje

Aprender a desarrollar un plan de seguridad para que la organización se encuentre protegida en el espacio y contexto de la movilidad y comunicaciones inalámbricas, así como adquirir los conocimientos sobre las redes inalámbricas y el buen uso de configuraciones en dispositivos móviles, evitando la fuga de información, que hoy en día es uno de los casos más repetidos.

CONTENIDO

Unidad I. Definición, tipos de redes inalámbricas, dispositivos y características.
1.1. Definiciones y conceptos.
1.2. Reconocimiento de redes.
1.3. Arquitectura y diseño.
1.4. Dispositivos inalámbricos.

Unidad II. Regulaciones, estándares.
2.1. Legislación sobre redes inalámbricas.

Unidad III. Procesos de conexión, herramientas, terminologías y métodos de seguridad y ataques.
3.1. Armado y conexión.
3.2. Implementación.
3.3. Reconocimiento de herramientas de auditorías inalámbricas.
3.4. Conocimiento de técnicas de ataques sobre la plataforma inalámbrica.
3.5. Medidas de seguridad.

Unidad IV. Aplicaciones prácticas.
4.1. Laboratorio: Armado de red inalámbrica y auditoria.

Unidad V. Introducción SO móviles.
5.1. Introducción sobre Android.
5.2. Reconocimiento de S.O.
5.3. Introducción sobre IOS.
5.4. Reconocimiento de S.O.
5.5. Otros sistemas operativos (Windows Phone, Symbian, Black Berry OS).

Unidad VI. Recomendaciones de seguridad.
6.1. Metodologías de aplicación de seguridad en móviles.
6.2. Uso correcto y buena implementación en las corporaciones.
6.3. Políticas específicas de implementación.

Unidad VII. Bluetooth: definiciones, herramientas, métodos de prevención y ataques.
7.1. Arquitectura y diseño.
7.2. Conexiones.
7.3. Implementación.
7.4. Reconocimiento de herramientas de auditorías inalámbricas.

FUENTES DE CONSULTA

Básica

- Ramachandran, Vivek. Backtrack 5 Wireless Penetration Testing. 2011. Referencias ISBN 978-1-849515-58-0 - http://www.amazon.es/Backtrack-Wireless-Penetration-Testing-Beginners/dp/1849515581
- Wright, Joshua y Johnny Cache. Hacking Exposed-Wireless: Wireless Security Secrets & Solutions. 2010. Ed. Alfa Omega. Referencias ISBN-13: 978-0071666619 -http://www.amazon.com/Hacking-Exposed-Wireless-Security-Colutions/dp/0071666613

Complementaria

1. Cisco. Redes Inalámbricas por Cisco. 2014. Disponible desde: http://www.cisco.com/web/ES/solutions/es/wireless_network/index.html
2. IEEE Standards. Principales estándares inalámbricos. 2014. Disponible desde http://ieeestandards.galeon.com/aficiones1573579.html
3. Google. Políticas de buen uso en Android. 2014. Disponible desde https://support.google.com/a/users/answer/190930?hl=es

6. *PASSWORD*: ENFRENTAR EL CONTROL DE ACCESOS.

Duración: 10 horas.

Objetivo de aprendizaje

Conocer la relación entre el control de accesos y la seguridad, a fin de identificar las distintas etapas en el proceso de acceso a un sistema y las formas de identificarse.

CONTENIDO

Unidad I. Conceptos básicos.
1.1. Contraseñas.
1.2. Identificación.
1.3. Autenticación.
1.4. Autorización.

Unidad II. Clasificación de los controles.
2.1. Momento del acceso.
2.2. Recursos utilizados.
2.3. Single Sign-On.

Unidad III. Ataques a las contraseñas.
3.1. Fuerza bruta.
3.2. Diccionarios.
3.3. Métodos híbridos.
3.4. Hash precalculados.
3.5. Adivinación.
3.6. Sniffing.
3.7. Ingeniería social.

FUENTES DE CONSULTA

- Agé, Marion et al. (2015) Seguridad Informática: Hacking Ético. Conocer el ataque para una mejor defensa, Ediciones ENI.
- Benchimol, Daniel (Coord.) Hacking desde cero: Conozca sus vulnerabilidades y proteja su información, USERS, Fox Andina, Buenos Aires, 2011.
- Erickson, John (2008). Hacking: Técnicas Fundamentales (Hackers y Seguridad), Anaya Multimedia.
- Gómez Vieites, Álvaro (2011). Enciclopedia de la Seguridad Informática, Ra-Ma Editorial.

IX. METODOLOGÍA DE ENSEÑANZA-APRENDIZAJE

- Exposición a cargo del ponente.
- Preguntas y respuestas (participación dirigida).
- Lecturas obligatorias.
- Material de apoyo para el maestro y de consulta para el alumno.

X. PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN

La evaluación se concibe como un proceso para estimar los resultados del proceso de enseñanza-aprendizaje, dado que permite valorar los conocimientos adquiridos y las habilidades desarrolladas en el curso. Para cada una de las materias, se prevé una evaluación

especial atendiendo a los conocimientos y habilidades que se impartieron; sin embargo, se deberá realizar el siguiente proceso:

- Un examen inicial del curso para valorar el nivel del grupo a capacitar.
- La evaluación referente a cada materia.
- Un examen final.

La escala de calificación será de 0 a 10, en la que la mínima para acreditar es 8 (ocho); al término del programa, las autoridades estatales correspondientes entregarán una constancia y deberán informar por oficio al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y a la Policía Federal sobre la totalidad del personal capacitado, para los fines pertinentes de la política pública y consolidación de las Unidades de Policía Cibernética.

Evaluación del proceso educativo. Aunado a la evaluación interna del conocimiento del alumno, se evaluará el desempeño del docente y de la institución que brindó la capacitación mediante la aplicación de una encuesta de satisfacción.

Para tener derecho a la evaluación, se deberá cumplir con 95% de asistencia.
- Examen final que evaluará la capacidad del alumno: 70%
- Participación y asistencia: 30%

El curso se desarrollará en un aula que cumpla con los siguientes requerimientos:
- Espacio adecuado para el número de participantes (15 a 30).
- Ventilación e iluminación propicia.
- Toma y extensiones de corriente eléctrica.

Para la impartición del curso es necesario contar con el siguiente material:
- Computadora portátil con Microsoft Office compatible con equipo de proyección.
- Una computadora por alumno.
- Proyector.
- Equipo de audio y video.
- Rotafolio o pintarrón con marcadores.

XI. INFORMACIÓN DEL INSTRUCTOR

El aspirante a docente del curso de formación especializada intermedia para integrantes de las Unidades de Policía Cibernética deberá contar con:

a) Título de maestría o doctorado con cédula profesional expedida por la Secretaría de Educación Pública, relacionado con la asignatura que habrá de impartir.
b) Por lo menos cuatro años de experiencia docente comprobable en el ámbito de la seguridad informática.

NIVEL 2

**"INVESTIGACIÓN DE DELITOS CIBERNÉTICOS
Y SEGURIDAD DE LA INFORMACIÓN" O "NIVEL 2"**

IV. OBJETIVOS ESPECÍFICOS

- Homologar la capacitación de los integrantes de las Unidades de Policía Cibernética estatales del país.
- Dotar a los integrantes de la Unidades de Policía Cibernética de técnicas y habilidades que les permitan desempeñar mejor sus funciones y que fortalezcan las capacidades de Investigación de delitos cibernéticos.
- Realizar análisis forense de dispositivos electrónicos.
- Realizar patrullaje cibernético.
- Identificar y evaluar los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información que se maneja dentro de la Policía Cibernética.

V. PERFIL DE INGRESO

Considerando que el programa establece un modelo de formación, el perfil de ingreso determina únicamente los requisitos que deberá reunir el aspirante para garantizar un buen aprovechamiento académico y un apropiado desempeño de sus actividades.

- Tener licenciatura terminada en cualquiera de las siguientes carreras: Informática o similar, Derecho; titulado y con cédula profesional.
- Tener experiencia profesional comprobable de 3 años.
- Estar en pleno ejercicio de sus derechos.
- Tener vigentes los exámenes de control y confianza.

VI. PERFIL DE EGRESO

Al término del plan académico, el egresado adquirirá los siguientes conocimientos, habilidades y actitudes:

Conocimientos:

1. Coadyuvará en la integración de las carpetas de investigación relacionadas con delitos cibernéticos.
2. Realizará investigaciones en materia de delitos cibernéticos.
3. Tendrá conocimiento de la norma ISO/IEC27001:2013, Sistema de Gestión de la Seguridad de la Información.

Habilidades:

1. Atenderá correctamente las denuncias realizadas por la ciudadanía.
2. Elaborará informes policiales.

Actitudes:

1. Demostrará un pensamiento socialmente comprometido para asumir una actitud positiva y de cambio frente a los problemas de las personas en situación de víctima.
2. Mostrará interés en los diversos procesos que conlleva una investigación hasta su finalización.

VII. ESTRUCTURA CURRICULAR

La duración total del curso es de **100 horas**, distribuidas en jornadas completas de lunes a viernes, con 6 horas diarias de clase y descanso los fines de semana.[5]
La estructura curricular comprende las unidades o módulos del plan de estudios con la duración en horas y el total de cada una de ellas.

DURACIÓN

UNIDADES	DURACIÓN
1. Prevención, respuesta y administración de incidentes.	20
2. Sistemas de detección y prevención de intrusos y monitoreo.	10
3. Análisis de vulnerabilidades y pruebas de penetración.	20
4. *Hacking* ético.	20
5. Análisis forense.	20
6. Fundamentos de la norma ISO/IEC 27001:2013, Sistema de Gestión de la Seguridad de la Información.	10
TOTAL	**100 HORAS**

VIII. CONTENIDO TEMÁTICO

1. PREVENCIÓN, RESPUESTA Y ADMINISTRACIÓN DE INCIDENTES.

Duración: 20 horas.

Objetivo de aprendizaje
Identificar las problemáticas generadas por el uso de las tecnologías de información y comunicaciones con la finalidad de prevenir, dar respuesta y administrar incidentes cibernéticos.

CONTENIDO

Unidad I. Esquema general de recuperación de incidentes.

[5] Queda a consideración de la Institución que solicita la capacitación, si el personal reclutado necesariamente deberá permanecer internado durante el desarrollo del curso; el calendario es una propuesta que deberá ajustarse según las necesidades.

Unidad II. Ciclo de respuesta a incidentes.

Unidad III. Medidas preventivas.
3.1. Análisis de riesgos.
3.2. Procedimientos y políticas de seguridad.
3.3. Controles automatizados.
3.4. Equipo de respuesta a incidentes.
3.5. Simulacros.

Unidad IV. Detección de incidentes.
4.1. Reporte de incidentes.
4.2. Administración de incidentes.

Unidad V. Planes de contingencia y procedimientos de recuperación.
5.1. Estructura del documento del plan de contingencia.
5.2. Procedimientos y políticas de respaldo de información.
5.3. Procedimiento de acción ante un estado de contingencia.

Unidad VI. Acciones a tomar después de recuperar la operación.
6.1. Introducción al análisis forense de equipos de cómputo.

Unidad VII. Manejo de incidentes de seguridad de la información.
7.1. Procedimientos para el manejo de incidentes.
7.2. Prevención y caso práctico.

FUENTES DE CONSULTA

- Aquino Luna, Rubén *et al.*, Manual: Gestión de Incidentes de Seguridad Informática, América Latina y Caribe, Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), Proyecto AMPARO, México, www.proyectoamparo.net. 2010.
- Dowd, Mark; John McDonald y Justin Schuh. El Arte de la Valoración de Seguridad de Softwares: Identificando y Previniendo Vulnerabilidades de Software, 2006.
- González Pérez, Pablo; Germán Sánchez Garcés y José Miguel Soriano de la Cámara. Pentesting con Kali, 0xWord, 2015.
- Gómez Vieites, Álvaro (2011). Gestión de Incidentes de Seguridad Informática. Starbook Editorial.
- Gómez Vieites, Álvaro. Enciclopedia de la Seguridad Informática, Ra-Ma Editorial, 2011.

2. NÚCLEO DE FORMACIÓN: SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS Y MONITOREO.

Duración: 10 horas.

Objetivo de aprendizaje
Detectar y realizar el monitoreo de intrusos para prevenir acciones maliciosas.

CONTENIDO

Unidad I. Conceptos de seguridad informática.

Unidad II. Conceptos de detección y prevención.

Unidad III. Tipos de IDS/IPS.

Unidad IV. APT (Amenazas Persistentes Avanzadas).

Unidad V. Metodologías de detección.

Unidad VI. Progresión de la amenaza.

Unidad VII. Reconocimiento.
7.1 Tradicional: Escaneo de puertos y hosts.
7.2 Actual. Buscadores, Redes Sociales, Metadatos.
7.3 Compromiso.
7.4. Explotación.
7.5. Escalamiento de Privilegios.

Unidad VIII. Herramientas para detección de tráfico sospechoso.

Unidad IX. Monitoreo de seguridad de red.

FUENTES DE CONSULTA

Básico:

- Gestión de la Seguridad Informática, Herramientas y técnicas para prevenir y combatir ataques a los sistemas informáticos de una empresa, RU.
- Gómez Vieites, Álvaro (2011). Enciclopedia de la Seguridad Informática, Ra-Ma Editorial.
- González Pérez, Pablo; Germán Sánchez Garcés y José Miguel Soriano de la Cámara. *Pentesting con Kali*, 0xWord, 2015.
- Manual CEH (Certified Ethical Hacker v7).
- Seguridad Informática, Fabián Portantier by RedUS.

Herramientas:
- Detección y prevención de intrusiones (HIDS), OSSEC, Trend Micro, Inc.
- Detección y prevención de intrusiones (HIDS), Tripwire, Tripwire, Inc.
- Cifrado de TrueCryp, TrueCryptFoundation.

3. ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.
Duración: 20 horas.

Objetivo de aprendizaje
Realizar análisis de vulnerabilidades y pruebas de penetración de sistemas informáticos.

CONTENIDO

Unidad I. Metodología para pruebas de penetración.

Unidad II. Análisis de vulnerabilidades.
2.1.Técnicas para detección de vulnerabilidades.

Unidad III. Recopilación de información.

Unidad IV. Reconocimiento.

Unidad V. Mapeo.

Unidad VI. Descubrimiento.

Unidad VII. Explotación.

Unidad VIII. Pruebas de penetración desde el exterior.

Unidad IX. Pruebas de penetración desde el interior.

Unidad X. Pruebas de penetración al *firewall*.

Unidad XI. Pruebas de penetración a los IDS.

Unidad XII. Metodología de una prueba de penetración a una aplicación web.

FUENTES DE CONSULTA

- Caballero Quezada, Alonso Eduardo. Hacking con Kali Linux, Curso Virtual, http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf
- Dowd, Mark; John McDonald y Justin Schuh. El Arte de la Valoración de Seguridad de Softwares: Identificando y Previniendo Vulnerabilidades de Software, 2006.
- González Pérez, Pablo; Sánchez Garcés, Germán; Soriano De La Cámara, José Miguel Pentesting con Kali, 0xWord, 2015.
- Manual CEH (Certified Ethical Hacker v7).
- Polstra, Philip. Hacking and penetration testing with low power devices, editorial Syngress.
- Wilhelm, Thomas y Jason Andress, Ninja Hacking: Unconventional penetration testing tactics and techniques, Editorial Syngress, 2010.

***4. HACKING* ÉTICO.**
Duración: 20 horas.

Objetivo de aprendizaje
Desarrollar la mentalidad de un *hacker*, así como entender las metodologías utilizadas durante un *ethical hack*. Desarrollar habilidades utilizadas por los *ethical hackers,* así como las herramientas y conceptos que utilizan.

CONTENIDO

Unidad I. Introducción al *ethical hacking*.
1.1. Metodologías del *ethical hacking.*
1.2. Herramientas comerciales.

Unidad II. Reconocimiento anticipado.
2.1. Estrategias sigilosas.
2.2. Evadiendo IDS/IPS.
2.3. Reconocimiento de red pasivo.
2.4. Escaneo inactivo.
2.5. Recopilación automatizada de metadatos.

Unidad III. Mapeo de vulnerabilidades.
3.1. Mapeo de vulnerabilidades del lado del cliente.

Unidad IV. Arquitectura x86.
4.1. Fundamentos computacionales.
4.2. Registros del CPU.
4.3. Segmentos de la memoria.

Unidad V. *Shellcode*.
5.1. ¿Qué es una *shellcode*?

Unidad VI. *Payloads*.
6.1. Eligiendo el *Payload* correcto para un *Pentest*.
6.2. Tipos más comunes de *shellcodes*.

Unidad VII. Herramientas de auditoría de redes LAN inalámbricas, (Wifi hacking).
7.1. Herramientas de descubrimiento.
7.2. Descifradores de contraseñas.
7.3. Administración y control de redes.
7.4. Analistas de protocolos inalámbricos.
7.5. Configuración de fábrica.
7.6. Filtros de contraseñas.
7.7. Detectores de sistemas operativos y escaneadores de puertos.
7.8. *Application niffers.*
7.9. Secuestro *(hijacking)* de cuentas de usuario.
7.10. Herramientas de bloqueo.
7.11. Descifradores WEP.
7.12. Opciones predeterminadas del sistema operativo.

Unidad VIII. Evaluación de riesgos.
8.1. Activos a proteger.
8.2. Amenazas contra las cuales protegerse.
8.3. Medidas de seguridad básicas.

Unidad IX. Análisis de amenazas y metodología de piratería (*hacking*).
9.1. Perfil del objetivo.
9.2. Seguridad física.
9.3. Ingeniería social.
9.4. Puertos inalámbricos.
9.5. Denegación del servicio (DoS).
9.6. Control no autorizado.

Unidad X. Medidas de seguridad rudimentarias.
10.1. SSID.
10.2. Filtros MAC.
10.3. WEP Estática.
10.2. Configuraciones Predeterminadas.
10.5. Actualizaciones de *Firmware*.
10.6. Seguridad Física.

Unidad XI. Medidas de seguridad avanzada.
11.1. Política de Seguridad Inalámbrica.
11.2. Autenticación y Encriptación.
11.3. DMZ y VLANs Inalámbricas.
11.4. Auditorías.
11.5. DHCP Autenticado.
11.6. Patrones de Tráfico.

Unidad XII. Soluciones de *hardware* y *software*.
12.1. Esquemas de encriptación.
12.2. Enrutadores-switches.
12.3. Firewalls.
12.4. Soluciones VPN para IP móviles.
12.5. Switches, VLANs y HUBS.

Unidad XIII. Implementación y administración.
13.1. Diseño e implementación.
13.2. Configuración y ubicación del equipamiento.
13.3. Interoperabilidad y capas.
13.4. Administración de la seguridad.

FUENTES DE CONSULTA

Básica

- Agé, Marion *et al., Seguridad Informática: Hacking Ético. Conocer el ataque para una mejor defensa,* Ediciones ENI, 2015.
- Cache, Johnny; Joshua Wright y Vincent Liu, Hacking Wireless, Anaya Multimedia, 2011.
- Erickson, John. Hacking: Técnicas Fundamentales (Hackers y Seguridad), Anaya Multimedia, 2008.
- Manual CEH (Certified Ethical Hacker v7).

– Wilhelm, Thomas y Jason Andress, Ninja Hacking: Unconventional penetration testing tactics and techniques, Editorial Syngress, 2010.

Herramientas
- Detección y prevención de intrusiones (HIDS), OSSEC, Trend Micro, Inc.
- Detección y prevención de intrusiones (HIDS), Tripwire, Tripwire, Inc.
- Limpieza de metadatos por MetaShield Protector, Informática64.
- Limpieza de metadatos por Metadact-, Litéra.
- Cifrado de True Cryp, True Crypt Foundation.

5. ANÁLISIS FORENSE.
Duración: 20 horas.

Objetivo de aprendizaje
Aplicar el procedimiento de identificación, recolección y manejo de evidencia digital, a fin de garantizar la integridad de la información

CONTENIDO

Unidad I. Historia de la telefonía celular.
1.1. Antecedentes de la telefonía celular.
- 1.1.1. Primera generación de la telefonía celular.
- 1.1.2. Segunda generación de la telefonía celular.
- 1.1.3. Tercera generación de la telefonía celular.
- 1.1.4. Cuarta generación de la telefonía celular.
- 1.1.5. Evolución de la telefonía celular.

1.2. Compañías proveedoras de servicios de comunicación móvil.
- 1.2.1. Compañías proveedoras.
- 1.2.2. Servicios que ofrecen los proveedores de servicios de comunicación móvil.
- 1.2.3. Tecnologías.
  - 1.2.3.1. Tipos de tecnologías de comunicación móvil.
    - 1.2.3.1.1. GSM.
    - 1.2.3.1.2. CDMA.
    - 1.2.3.1.3. IDEN.

1.3. Componentes principales de los equipos de comunicación móvil.
- 1.3.1. *Handset* o cuerpo del dispositivo de comunicación móvil.
- 1.3.2. Batería.
- 1.3.3. Tarjeta SIM y Micro SIM.
- 1.3.4. Contraseñas: PIN, PUK, etcétera.
- 1.3.5. Memoria externa y sus variedades.

Unidad II. Identificación.
2.1. Identificación de equipos móviles.
- 2.1.1. Marca, modelo y serie.
- 2.1.2. IMEI.
- 2.1.3. FCC ID.

2.1.4. Identificación a través de etiquetas.
2.1.5. Estado del equipo de comunicación móvil (especificar condiciones, ejemplo: buen estado, regular, malo, etcétera).
2.1.6. Compañía.
2.2. Fijación.
2.2.1. Fijación fotográfica particular del equipo de comunicación móvil.
2.2.2. Desarme del equipo de comunicación móvil.
2.2.3. Fijación de características del equipo de comunicación móvil.
2.2.4. IMEI.
2.2.5. Número de serie del equipo de comunicación móvil.
2.2.6. FCC ID.
2.2.7. Tarjeta SIM.
2.2.8. Número de serie de la batería.
2.2.9. Memoria Micro SD, M2.

Unidad III. Extracción de información a los dispositivos de comunicación móvil mediante el empleo de diferentes herramientas tecnológicas.
3.1. *Cellebrite*.
3.1.1. Selección de marca y modelo.
3.1.2. Realizar la configuración en el equipo de comunicación móvil.
3.1.3. Extracción de información de la tarjeta SIM.
3.1.4. Extracción de información del equipo de comunicación móvil.
3.1.5. Análisis del reporte de extracción.
3.2. *CellDeck*.
3.2.1. Selección de marca y modelo.
3.2.2. Realizar la configuración en el equipo de comunicación móvil.
3.2.3. Extracción de información de la tarjeta SIM.
3.2.4. Extracción de información del equipo de comunicación móvil.
3.2.5. Análisis del reporte de extracción.
3.3. XRY
3.3.1. Selección de marca y modelo.
3.3.2. Realizar la configuración en el equipo de comunicación móvil.
3.3.3. Extracción de información de la tarjeta SIM.
3.3.4. Extracción de información del equipo de comunicación móvil.
3.3.5. Análisis del reporte de extracción.

Unidad IV. Normas de entrega de los equipos de telefonía móvil.
4.1. Lineamientos empleados en la entrega de la cadena de custodia.
4.1.1. Verificación física.
4.1.2. Verificación de documentación.
4.1.3. Técnicas empleadas en la entrega y embalaje.
4.1.4. Llenado de formatos.
4.1.5. Fijación fotográfica durante el embalaje.
4.2. Entrega de documentación.
4.2.1. Contestación de oficio.
4.2.2. Informes.
4.2.3. Tarjetas.

FUENTES DE CONSULTA

- Alleyne, Robert. Computer Forensic Bible: The Ultimate Guide to Computer Forensic and Cyber Crime. 2015.
- Garrido Caballero, Juan. Análisis forense digital en entornos Windows. 0xWord.
- Hayes, Darren R. A practical guide to computer Forensics Investigations. Pearson IT Cretification, 2014.
- Lázaro Domínguez, Francisco. Introducción a la Informática Forense. Ra-Ma Editorial, 2013.
- Mahalik, Heather; Rohit Tamma y Satish Bommisetty. Practical Mobile Forensics – Second Edition. Packt Publishing, 2016.
- Stirparo, Pasquale y Mattia Epifani. Learning iOS Forensics. Packt Publishing, 2015.
- www.dragonjar.org

6. FUNDAMENTOS DE LA NORMA ISO/IEC 27001:2013, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Duración: 10 horas.

Objetivo de aprendizaje

Conocer los fundamentos teóricos respecto a la seguridad de la información y cómo implementarla en las organizaciones.

CONTENIDO

Unidad I. ¿Qué es seguridad de la información?

1.1. Confidencialidad.
1.2. Disponibilidad.
1.3. Integridad.

Unidad II. ¿Qué son riesgos de seguridad de la información?

2.1. ¿Qué es un riesgo?
2.2. ¿Qué es el análisis de riesgos?
2.3. ¿Qué son los controles de seguridad de la información?
2.4. ¿Cómo tratar los riesgos de seguridad de la información?

Unidad III. ¿Cómo **implementar la seguridad de la información?**

3.1. ¿Cómo implementar la seguridad de la información?
3.2. ¿Qué es ISO/IEC 27001:2013?
3.3. ¿Qué es ISO 31000?
3.4. Beneficios de seguridad de la información.

FUENTES DE CONSULTA

- ISO/IEC 27001:2013 “Sistemas de Gestión de Seguridad de la Información”.
- ISO 31000 “Guía Gestión de Riesgos”.
- NIST 800-30 “Risk Management”.
- Certified Ethical Hacker.

IX. METODOLOGÍA DE ENSEÑANZA-APRENDIZAJE

- Exposición a cargo del ponente.
- Preguntas y respuestas (participación dirigida).
- Ejercicios de identificación de riesgos vs. controles.
- Material de apoyo para el maestro y de consulta para el alumno.

X. PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

La evaluación se concibe como un proceso para estimar los resultados del proceso de enseñanza-aprendizaje, dado que permite valorar los conocimientos adquiridos y las habilidades desarrolladas en el curso. Para cada una de las materias, se prevé una evaluación especial atendiendo a los conocimientos y habilidades que se impartieron; sin embargo, se deberá realizar el siguiente proceso:

- Un examen al iniciar el curso para valorar el nivel del grupo a capacitar.
- La evaluación referente a cada materia.
- Un examen final.

La escala de calificación será de 0 a 10, en la que la mínima para acreditar será 8 (ocho); al término del programa, las autoridades estatales correspondientes entregarán la constancia y deberán informar por oficio al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y a la Policía Federal, sobre la totalidad del personal capacitado, para los fines pertinentes de política pública y consolidación de las Unidades de Policía Cibernética.

Evaluación del proceso educativo. Aunado a la evaluación interna del conocimiento del alumno, se evaluará el desempeño del docente y de la institución que brindó la capacitación mediante la aplicación de una encuesta de satisfacción.

Para tener derecho a la evaluación, se deberá cumplir con 95% de asistencia.
Examen final que evaluará la capacidad del alumno: 70%.
Participación y asistencia: 30%.

El curso se desarrollará en un aula que cumpla con los siguientes requerimientos:

- Espacio adecuado para el número de participantes (15 a 30).
- Ventilación e iluminación propicia.
- Toma y extensiones de corriente eléctrica.

Para la impartición del curso es necesario contar con el siguiente material:

- Computadora portátil con Microsoft Office compatible con equipo de proyección.
- Una computadora por alumno.
- Proyector.
- Equipo de audio y video.
- Rotafolio o pintarrón con marcadores.

XI. INFORMACIÓN DEL INSTRUCTOR

El aspirante a docente del curso de **"INVESTIGACION DE DELITOS CIBERNÉTICOS Y SEGURIDAD DE LA INFORMACIÓN" o "NIVEL 2"** para integrantes de la Unidad de Policía Cibernética deberá contar con:

a) Título de maestría o doctorado con cédula profesional expedida por la Secretaría de Educación Pública, relacionado con la asignatura que habrá de impartir.
b) Por lo menos cinco años de experiencia docente comprobable en el ámbito de la materia a impartir.