CIBERSEGURIDAD

Dirigido a la Policía de Investigación de la Fiscalía General del Estado de Veracruz

CAPACITACIÓN ESPECIALIZADA DE ALTO NIVEL

ACADEMIA REGIONAL DE SEGURIDAD PÚBLICA DEL SURESTE

ÍNDICE

INTRODUCCIÓN

La **ciberseguridad** es un tema tan importante que forma parte de la agenda mundial. En la actualidad, la población con acceso a internet, en su mayoría ha sido víctima de un **ciberataque**; empresas, gobierno, hospitales, instituciones financieras, pymes y usuario final están expuestos a las amenazas que hay en la red.

Entender la **importancia de la seguridad informática** nos da una perspectiva más amplia sobre las estrategias, planes y buenas prácticas que se deben implementar en las organizaciones; por lo anterior, es preciso hablar de qué es la ciberseguridad, los tipos de seguridad informática, los ataques cibernéticos más comunes y las soluciones estratégicas a éstos.

De acuerdo a los expertos de Information Systems Audit and Control Association (ISACA), la ciberseguridad se define como "**una capa de protección para los archivos de información**". También, para referirse a la ciberseguridad, se utiliza el término **seguridad informática o seguridad de la información electrónica**.

La evolución de la ciberseguridad brinda un contexto más amplio de cómo fue la transformación al mundo digital y los riesgos que surgieron con este cambio, el primer **hacker** de la historia fue **Nevil Maskelyne**. En 1903, interceptó la primera transmisión de telégrafo inalámbrico, mostrando las vulnerabilidades de este sistema desarrollado por Marconi.

John Draper fue el primer **ciberdelincuente**, mejor conocido como "Captain Crunch". Draper, descubrió que el sonido emitido por un silbato que se obsequiaba en las cajas de cereal de "Cap'n Crunch", podía engañar a la señal de la central telefónica y así poder realizar llamadas gratis.

En los años 70s apareció **el primer malware de la historia**: *Creeper*, un programa que se replicaba así mismo. ¡Este malware mostraba el mensaje "I'm a creeper, catch me if you can!". A partir de ahí, nace el primer antivirus llamado *Reaper*, que su función era la de eliminar las infecciones por Creeper.

Con el paso de los años y los avances tecnológicos, la información en red iba cada vez en aumento, y con ello, su valor e importancia tanto para las organizaciones como para los ciberdelincuentes.

El **malware** en los años 80s incrementó su presencia y a la par se desarrollaron **antivirus** más eficientes. En la actualidad, se utiliza una plataforma de detección

y respuesta de endpoint (EDR) para proteger los equipos de un ataque de malware debido a su gran evolución.

A finales de esta década, **Kevin Mitnick** utilizó **ingeniería social** para tener acceso a información personal y confidencial; este tipo de ciberataque, que comenzó a tener mayor uso en aquella época, sigue siendo una de los métodos más populares para vulnerar los activos de una empresa, sin embargo, se pueden prevenir y reducir con una buena estrategia, formación a colaboradores y protocolos de security awareness.

La regulación del Internet es un reto enorme debido a su carácter internacional y a la variedad en su contenido. A principios de los 90s la necesidad de hacer frente a los **ataques cibernéticos** se convirtió en tema de discusión internacional, la falta de conocimiento sobre el ciberespacio, de medidas de seguridad, jurisdicción y competencia afectaba sobre todo a los países desarrollados, donde el uso de la tecnología y el abuso de usuarios mermaban en la economía y sociedad.

Las primeras acciones para crear mecanismos legales frente a los ciberdelitos fueron locales. En 1986, en Estados Unidos se creó la *Computer Fraud and Abuse Act*; sin embargo, su capacidad se vio sobrepasada por la transformación tecnológica.

Existen 3,000 millones de cibernautas a nivel mundial (40% de la población); en México hay 80.6 millones y la tasa de crecimiento entre 2019 y 2020 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.

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.

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.

El **"Curso de Ciberseguridad",** ha sido diseñado para un proceso teórico-práctico basado en conocimientos sociales, jurídicos y técnicos para capacitar al personal de las instituciones policiales, a fin de que desarrollen y adquieran los conocimientos, habilidades y actitudes necesarias para cumplir con las tareas a desempeñar de acuerdo a las funciones y responsabilidades del área operativa a la que aspira incorporarse.

El objetivo principal del programa es especializar a policías en técnicas y habilidades básicas policiales, con un fuerte énfasis en los derechos humanos y la cultura de la legalidad. El fin es capacitar a los elementos para contribuir efectivamente en la salvaguarda de la sociedad, fortaleciendo el orden público y la paz social. Para cumplir con el objetivo del curso, se diseñaron cuatro asignaturas que suman 40 horas y se impartirán de manera presencial bajo la modalidad de internado.

FUNDAMENTACIÓN

Fundamento Teórico-Práctico

La profesionalización policial se inscribe en el marco del Servicio Profesional de Carrera Policial, previsto como uno de los instrumentos básicos para la formación del personal que integra estas instituciones, a fin de cumplir con los principios constitucionales, así como los de actuación y desempeño policial.

En este sentido, la profesionalización policial, está integrada por los programas de formación inicial y formación continua, que ésta última contempla las etapas de actualización, promoción, especialización y alta dirección.

En razón de lo anterior, el presente programa de capacitación corresponde al de ***Ciberseguridad*** y está basado en el proceso de enseñanza - aprendizaje del constructivismo, cuyo propósito es contribuir con el desarrollo profesional de las policías preventivas y de investigación del país, de manera que se asegure proveerlos de conocimientos y que desarrollen habilidades y destrezas, basadas en competencias y prácticas fundamentales que les permita desempeñar adecuadamente su papel como actores centrales en la protección ejecutiva.

Asimismo, el curso integra contenidos que posibilitan la adquisición de conocimientos y el desarrollo de habilidades cognoscitivas y psicomotrices, así

como la introyección de valores y actitudes congruentes con los requerimientos que plantea el ejercicio de la función policial, orientada al cumplimiento de los principios constitucionales de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos.

De esta forma, se responde a la necesidad de dotar a los miembros de las instituciones policiales de los tres órdenes de gobierno de conocimientos, habilidades, competencias, aptitudes y actitudes para el óptimo desempeño de las funciones operativas.

Por otra parte, queda manifiesta la posibilidad de que cada entidad federativa puede ajustar el plan de acuerdo a requerimientos particulares derivados de las funciones y atribuciones asignadas a la policía, para replantear los conocimientos teóricos y prácticos formulados en el plan curricular.

Marco Legal

El curso de ***Ciberseguridad*** se desarrolla en el marco del **Artículo 21** de la Constitución Política de los Estados Unidos Mexicanos, que señala a la seguridad pública como una función a cargo de la Federación, las Entidades Federativas y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas, en los términos de la ley en la materia. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en la misma Constitución.

La **Ley General del Sistema Nacional de Seguridad Pública**, establece en su **Artículo 47** que "La Federación y las entidades federativas establecerán y operarán Academias e Institutos que serán responsables de aplicar los Programas Rectores de Profesionalización (sic)…", asimismo, en el **Artículo 72** señala al Desarrollo Policial como el conjunto integral de reglas y procesos debidamente estructurados y enlazados entre sí que corresponden la Carrera Policial, los esquemas de profesionalización, la certificación y el régimen disciplinario de los integrantes de las Instituciones Policiales, y tiene por objeto garantizar el desarrollo institucional, fomentar la vocación de servicio y el sentido de pertenencia (sic)…"; en el **Artículo 98**, señala que "La profesionalización es un proceso permanente y progresivo de formación que se integra por las etapas de formación inicial, actualización, promoción, especialización y alta dirección, para desarrollar al máximo las competencias, capacidades y habilidades de los integrantes de las instituciones policiales".

Así mismo **el Plan Nacional de Desarrollo 2019-2024** establece en el punto número uno Política y Gobierno en el apartado de cambio de paradigma social, los siguientes objetivos:

- Cambio de paradigma en seguridad
- Erradicar la corrupción y reactivar la procuración de justicia
- Pleno respeto a los Derechos Humanos
- Emprender la construcción de la paz
- Articular la seguridad nacional, la seguridad pública y la paz

La Ley del Sistema Estatal de Seguridad Pública de Veracruz, en su **Artículo 3°** indica que "La seguridad pública es una función a cargo de la Federación, del Estado y los Municipios, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos; comprende la prevención general y especial de los delitos, la investigación para hacerla efectiva, la sanción de las infracciones administrativas, la investigación y la persecución de los delitos, así como la reinserción social del individuo, en términos de esta Ley, en las respectivas competencias establecidas en la Constitución Política de los Estados Unidos Mexicanos y la Constitución Política del Estado…".

Asimismo, el **Artículo 8°** del ordenamiento citado con anterioridad, señala que "Las Instituciones de Seguridad Pública serán de carácter civil, disciplinado y profesional, su actuación se regirá; además, por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos por la Constitución Política de los Estados Unidos Mexicanos y la Constitución Política del Estado. Asimismo, deberán fomentar la participación ciudadana y rendir cuentas en términos de Ley".

Finalmente, el **Artículo 9°** de dicho ordenamiento señala que: "Las Instituciones de Seguridad Pública del Estado y los municipios, en el ámbito de su competencia y en los términos de esta Ley y demás disposiciones aplicables, deberán coordinarse para:

VI. Regular los procedimientos de selección, ingreso, formación, actualización, capacitación, permanencia, evaluación, reconocimiento, certificación y registro de los servidores públicos de las instituciones de Seguridad Pública del Estado".

El Artículo 2° de la Ley de Seguridad Pública para el Estado de Veracruz, a la letra señala lo siguiente: "La Seguridad Pública es una función prioritaria a cargo del estado y los municipios que lo integran, sin perjuicio de las atribuciones de

otras autoridades, conforme a la Constitución Política de los Estados Unidos Mexicanos".

Asimismo, el **Artículo 3°** del ordenamiento citado con anterioridad, señala que "La seguridad pública tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos, lo cual se alcanzará mediante la prevención, persecución y sanción de las infracciones y delitos, así como la readaptación social del delincuente y del menor infractor".

De igual manera, el **Artículo 7°** del mismo ordenamiento, señala que "La conducta de los miembros de las instituciones policiales del estado y de los municipios se regirá por los principios de legalidad, eficiencia, profesionalismo y honradez".

Beneficios Esperados

Los beneficios que se esperan son:

- Que el policía de investigación actualice y desarrolle las competencias y habilidades dentro del marco constitucional, con el objetivo de tener un mejor desempeño.
- Profesionalizar a los integrantes de las Instituciones policiales de Investigación para el adecuado ejercicio de sus funciones, privilegiando en todo momento una actuación apegada a los principios constitucionales y el pleno respeto a los Derechos Humanos.
- Contar con protocolos que establezcan procedimientos técnicos, para que la actuación de las y los policías se efectúe con eficiencia y profesionalismo ante los casos de violencia de género que se les presenten al realizar sus atribuciones y funciones.
- Que al abordar a un hecho aplique de manera correcta y profesional su labor con estricto apego a derecho, sin violentar sus garantías individuales y respetando sus derechos.
- Que la ciudadanía se sienta segura y protegida al contar con una unidad profesional, responsable y con un alto sentido de empatía con los demás.
- Garantizar que los policías de investigación tengan una vez concluido su curso la capacidad de realizar actividades de prevención, atención e investigación de delitos cibernéticos.
- Elevar la calidad de la atención a las denuncias de delitos cibernéticos.

Beneficios Institucionales

- Esencialmente se busca que la o el policía adquiera los conocimientos prácticos para su formación, proporcionándole las herramientas básicas para su desempeño y que éstos brinden un servicio profesional y de calidad a la ciudadanía con estricto apego a derecho.
- Elevar la calidad de la función que brindan las instituciones en beneficio de la sociedad, a través de la incorporación de un cuerpo de funcionarios públicos profesionales, con los conocimientos teóricos-prácticos y jurídicos necesarios.
- Garantizar que una vez concluido el proceso de evaluación y capacitación del personal que se incorpora en apoyo a la intervención de la función policial, sean congruentes con los requerimientos que plantea el ejercicio de sus funciones, mediante una actuación apegada a los principios constituciones de Legalidad, Eficiencia, Profesionalismo, Honradez, Objetividad y Respeto a los Derechos Humanos.
- En coordinación con los tres niveles de gobierno, ejercer profesionalmente diversos procesos de trabajo vinculados con las diferentes actuaciones derivadas de estas tareas.
- Ser un estratega 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.
- Sentar las bases de un proceso integral de capacitación y desarrollo que en el futuro sirva para un servicio profesional de carrera.

OBJETIVO GENERAL

Al finalizar el curso, la o el participante aplicará sus conocimientos en ***Ciberseguridad*** a su campo laboral; de forma estructurada y apegada a estándares internacionales, con el fin de mantener la seguridad y el orden en redes públicas, hacer respetar las leyes, proteger a la ciudadanía, prevenir el delito, preservar la libertad y actuar ante ciberdelítos.

Dotar a los integrantes encargados de la ciberseguridad de habilidades que les permitan desempeñar mejor sus funciones y fortalezcan las capacidades de prevención de delitos cibernéticos.

OBJETIVOS ESPECÍFICOS

A través del proceso de aprendizaje las y los elementos de instituciones de seguridad pública y procuración de justicia garantizarán su eficiente desempeño aplicando los conocimientos adquiridos para:

- Reducir delitos cometidos en agravio de niñas, niños y adolescentes.
- Incrementar el nivel de seguridad de la red pública de internet.
- Mejorar la calidad de vida dentro de la sociedad, al fomentar las operaciones de comercio electrónico seguro en el país.
- Sensibilizar al personal de la Policía Primer Respondiente, para que, al intervenir en llamados de auxilio, actúe con perspectiva de género a fin que se corroboren los hechos, y en caso de que existan flagrancia, se actúe conforme a la legislación aplicable.

PERFIL DE INGRESO

El aspirante a participar en el curso deberá:

- Ser elemento en activo y contar con CUIP adscrito a alguna institución de Procuración de Justicia como policía de investigación.
- Haber acreditado el programa de Formación Inicial para Policía de Investigación.
- Contar con Certificación aprobada y vigente del Centro Estatal de Evaluación y Control de Confianza o su equivalente en los Centros Federales.
- Tener licenciatura terminada en: informática, o similar, derechos, psicología, o comunicación.
- Contar con las siguientes habilidades:
  - ✓ Vocación de servicio público.
  - ✓ Proactividad para identificar y resolver problemas.
  - ✓ Sensibilidad y convicción en la labor de prevención.
  - ✓ Capacidad eficiente de decisión.
  - ✓ Facilidad de comunicación.
  - ✓ Disponibilidad para trabajar en equipo.

PERFIL DE EGRESO

El policía de investigación tendrá las funciones con apego a los principios constitucionales, mediante las siguientes acciones:

- Desempeñará sus funciones dentro del marco de la legalidad, respetando y aplicando las normas jurídicas que regulan la actuación policial preventiva.
- Contará con las habilidades necesarias para aplicar sus conocimientos en ciberseguridad a su campo laboral y así contrarrestar acciones antisociales.
- Aplicará los principios y reglas que permiten acciones policiales organizadas y sistemáticas.
- Realizará campañas de prevención de delitos cibernéticos
- Capacitará y orientará a la ciudadanía en materia de delitos cibernéticos.
- Identificará y analizará incidentes cibernéticos
- Correlacionará la información sobre el comportamiento de los delitos cibernéticos.
- Analizará y resolverá incidentes de seguridad informática, manejando la información de manera segura acorde con las políticas de seguridad.
- Integrará las carpetas de investigación de delitos cibernéticos.
- Realizará investigaciones en materia de delitos cibernéticos.
- Aplicará conocimientos de la norma ISO/IEC27001:2022: Sistema de Gestión de la Seguridad.

ESTRUCTURA CURRICULAR

El programa tiene una duración de **40 horas** de aprendizaje las cuales se encuentran divididas en 4 módulos de conocimiento.

Ejes Transversales					Clave	Trayecto Formativo	Asignatura	Clave	Total de horas	Horas teóricas	Horas prácticas
PROXIMIDAD	DERECHOS HUMANOS	PERSPECTIVA DE GÉNERO	CULTURA DE LA LEGALIDAD		TF1-TDHFI	Talleres: desarrollo de habilidades para la función de investigador	1. La ciberseguridad	TF1-A-LCS	5	5	N/A
							2. Prevención de delitos cibernéticos	TF1-A-PDC	10	5	5
							3. Identificación y análisis de incidentes cibernéticos	TF1-A-IAIC	10	5	5
							4. Investigación de delitos cibernéticos	TF1-A-IDC	15	5	10
TOTAL									**40**	**20**	**20**

Duración y Horario del Curso:

El programa denominado ***Ciberseguridad,*** tiene un total de **40 horas** de

enseñanza-aprendizaje distribuidas en **4 unidades**, y se desarrollará en una modalidad de internado, trabajando 8 horas diarias de lunes a viernes.

Etapa educativa en que se desarrollará:

El programa de **"*Ciberseguridad*"**, ha sido diseñado en un proceso teórico-práctico basado en conocimientos prácticos, jurídicos y técnicos para capacitar a los elementos de procuración de justicia a fin de que desarrollen y adquieran los conocimientos, habilidades y actitudes necesarias para cumplir con las tareas a desempeñar de acuerdo a las funciones y atribuciones.

Calendario y horario de actividades:

La duración total del curso es de **40 horas,** distribuidas de la siguiente manera:

Unidad	**Total de horas**	**Lunes a viernes 9:00 a 18:00 h**				
		Mes: agosto				
		19	20	21	22	23
		L	M	M	J	V
1. La ciberseguridad	**5**	**5**				
2. Prevención de delitos cibernéticos	**10**	**3**	**7**			
3. Identificación y análisis de incidentes cibernéticos	**10**		**1**	**8**	**1**	
4. Investigación de delitos cibernéticos	**15**				**7**	**8**
TOTAL	**40**	**8**	**8**	**8**	**8**	**8**

Fecha de réplica de curso y/o eventos a realizar:

1. Del 19 al 20 de agosto 2024.

DESARROLLO PROGRAMÁTICO

FICHA TÉCNICA		CLAVE: TF1-A-LCS			
Trayecto formativo		**Talleres: Desarrollo de habilidades para la función de investigador**			
Nombre de la asignatura		1. La ciberseguridad			
Horas mínimas	**5**	**Horas formativas**	**5**	**Horas prácticas**	**N/A**

Ejes transversales	
• Derechos humanos • Proximidad	• Perspectiva de género • Cultura de la legalidad

Caracterización
La asignatura *La ciberseguridad* forma parte del contenido temático del programa de "*Ciberseguridad*" para la formación continua de los elementos para la policía de investigación. Se imparte con la finalidad de desarrollar las competencias necesarias para el ejercicio profesional de las funciones y atribuciones de los funcionarios encargados de hacer cumplir la ley, desde un enfoque de proximidad, perspectiva de género, derechos humanos y cultura de la legalidad.

Relación con otras asignaturas
Prevención de delitos cibernéticos, identificación y análisis de incidentes cibernéticos, investigación de delitos cibernéticos.

Requisitos de ingreso (habilidades)
Ética de trabajo, pensamiento crítico, uso del equipo y materiales de trabajo, trabajo en equipo, comunicación efectiva, pensamiento analítico, habilidades para resolver problemas, habilidades de liderazgo, escucha activa, orientación a resultados, habilidades en Tics.

Objetivo terminal
Conocer la ciberseguridad desde el enfoque policial y de la investigación como una herramienta que se implementa para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos a fin de combatir y reducir los delitos cibernéticos que aquejan en la red pública de internet.

Objetivos específicos
• Entender la importancia de la seguridad informática para tener una mayor perspectiva sobre las estrategias, planes y buenas prácticas que se deben implementar para combatir los ciberdelitos. • Conocer los antecedentes e historia de la ciberseguridad para identificar los tipos de ataques y hackeos que han afectado la red pública del internet. . • Conocer los tipos de seguridad informática para la protección y gestión de la información de los usuarios y reconocer las categorías que existen para determinar las acciones en cada una de ellas • Conocer las técnicas que utilizan los cibercriminales para acceder a redes privadas e instalar malware comprometiendo la información de los usuarios. • Aplicar las estrategias de ciberseguridad como medidas de prevención, mitigación y eliminación de malware. • Conocer la metodología básica de la intervención del Primer Respondiente.

Metodología de enseñanza – aprendizaje
• **Lección magistral:** exponer información actualizada y bien organizada procedente de fuentes diversas y de difícil acceso para el elemento. Facilitar la comprensión y aplicación de los procedimientos específicos de la asignatura. • **Aprendizaje cooperativo:** involucrar a los elementos en el aprendizaje, aplicando cinco elementos que deben estar presentes en el aula cooperativa: interdependencia positiva, interacción cara a cara, responsabilidad individual, habilidades interpersonales y sociales y procesamiento grupal. • **Aprendizaje orientado a proyectos:** enfrentar a los elementos a situaciones que los lleven a construir, comprender y aplicar aquellos conocimientos y habilidades propias de la disciplina conjugando habilidades, actitudes y valores de trabajo. Desarrollar habilidades de trabajo en equipo, lo cual contribuye a preparar a los elementos para un entorno social real. • **Aprendizaje basado en Tics:** estimular el desarrollo de la imaginación como la iniciativa y la personalización del aprendizaje. Las herramientas tecnológicas permiten adaptar el contenido y la metodología de enseñanza a las necesidades individuales de cada estudiante.

Fundamentación
Basado en el objetivo de la Política Nacional de Ciberseguridad para establecer un sistema de responsabilidad compartida entre los actores públicos, privados y sociales que permitan reducir los incidentes y la posible comisión de delitos, a través de la coordinación y atención de los riesgos cibernéticos.

Desarrollo programático	Horas mínimas
1.1 Concepto y Definiciones 1.1.1 Objetivo 1.1.2 Antecedentes de la Ciberseguridad	1
1.2 Regulación del Internet	1

1.2.1. Primeras Acciones Legales	
1.3 Tipos de Seguridad Informática 1.3.1 Áreas Principales 1.3.2 Clasificación 1.3.1.1 Seguridad de hardware 1.3.1.2 Seguridad de software 1.3.1.3 Seguridad de red	1
1.4 Tipos de ciberataques 1.4.1 Ransomware 1.4.1.1 Malware criptográfico 1.4.1.2 Bloqueador 1.4.1.3 Doxware 1.4.1.4 Scareware 1.4.2 Phishing 1.4.3 Adware 1.4.4 Spyware 1.4.5 Troyanos	1
1.5 Estrategias de ciberseguridad 1.5.1 Gestión de Activos 1.5.2 Seguridad de las Operaciones 1.5.3 Gestión de los Incidentes y Recuperación ante Desastres 1.5.4 Control de Acceso a Sistemas y Aplicaciones 1.5.5 Security Awarness	1

Referencias – bibliografía mínima

Gaceta Parlamentaria
https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf
Estrategia Nacional de Ciberseguridad
https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
https://latam.kaspersky.com/resource-center/threats/ransomware
https://blog.avast.com/es/guia-basica-sobre-el-ransomware-y-como-protegerse
https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/
https://www.redeszone.net/tutoriales/seguridad/mensajes-phishing-como-protegernos/
https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/
https://www.derechosdigitales.org/12364/el-convenio-de-budapest-desde-una-perspectiva-de-derechos-humanos/
https://blog.smartekh.com/-pasos-para-una-estrategia-de-ciberseguridad
https://www.pandasecurity.com/spain/mediacenter/consejos
https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/
https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/
https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

FICHA TÉCNICA		CLAVE: TF1-A-PDC			
Trayecto formativo		**Talleres: Desarrollo de Habilidades para la Función de Investigador**			
Nombre de la asignatura		2. Prevención de delitos cibernéticos			
Horas mínimas	**1**	**Horas formativas**	**5**	**Horas prácticas**	**5**

Ejes transversales	
• Derechos humanos • Proximidad	• Perspectiva de género • Cultura de la legalidad

Caracterización

La asignatura *Prevención de Delitos Cibernéticos* forma parte del contenido temático del programa de "*Ciberseguridad*" para la formación continua de los elementos para la policía de investigación.

Se imparte con la finalidad de desarrollar las competencias necesarias para el ejercicio profesional de las funciones y atribuciones de los funcionarios encargados de hacer cumplir la ley, desde un enfoque de proximidad, perspectiva de género, derechos humanos y cultura de la legalidad.

Relación con otras asignaturas

La ciberseguridad, identificación y análisis de incidentes cibernéticos, investigación de delitos cibernéticos.

Requisitos de ingreso (habilidades)

Ética de trabajo, pensamiento crítico, uso del equipo y materiales de trabajo, trabajo en equipo, comunicación efectiva, pensamiento analítico, habilidades para resolver problemas, habilidades de liderazgo, escucha activa, orientación a resultados, habilidades en Tics.

Objetivo terminal

Impulsar la prevención, atención e investigación de los delitos cibernéticos a lo largo del territorio nacional, con el fin de reducir delitos cometidos en agravio de niñas, niños y adolescentes, incrementando los niveles de seguridad en la red pública de internet y buscar el mejoramiento de la calidad de vida dentro de la sociedad, al fomentar las operaciones de comercio electrónico seguro en el país.

Objetivos específicos

- Dotar a los participantes de técnicas y habilidades que les permitan desempeñar mejor sus funciones y fortalezcan las capacidades de prevención de delitos cibernéticos.

- Identificar las principales actividades que deben realizar los elementos encargados de las áreas de ciberseguridad.
- Realizar campañas de prevención de delitos cibernéticos.
- Capacitar y orientar a la ciudadanía en materia de delitos cibernéticos.

Metodología de enseñanza – aprendizaje
• **Aprendizaje basado en Tics:** estimular el desarrollo de la imaginación como la iniciativa y la personalización del aprendizaje. Las herramientas tecnológicas permiten adaptar el contenido y la metodología de enseñanza a las necesidades individuales de cada estudiante. • **Aprendizaje cooperativo:** involucrar a los elementos en el aprendizaje, aplicando cinco elementos que deben estar presentes en el aula cooperativa: interdependencia positiva, interacción cara a cara, responsabilidad individual, habilidades interpersonales y sociales y procesamiento grupal. • **Aprendizaje orientado a proyectos:** enfrentar a los elementos a situaciones que los lleven a construir, comprender y aplicar aquellos conocimientos y habilidades propias de la disciplina conjugando habilidades, actitudes y valores de trabajo. Desarrollar habilidades de trabajo en equipo, lo cual contribuye a preparar a los elementos para un entorno social real.

Fundamentación
Basado en el marco normativo y legal de la función policial enfocado en la actuación del policía de investigación de acuerdo a los Protocolos Nacionales de Actuación y al Código Nacional de Procedimientos Penales.

Desarrollo programático	Horas mínimas
2.1 Estrategias de Prevención de delitos cibernéticos 2.1.1 Definición de delitos cibernéticos 2.1.2 Conceptos básicos 2.1.3 Marco Normativo e Interpretación 2.1.4 Hábitos y uso de internet 2.1.5 Estrategias de Prevención 2.1.6 Plataforma México	2
2.2 Delitos cibernéticos 2.2.1 ¿Qué es internet? 2.2.2 Buscadores y Redes Sociales 2.2.3 Ventajas de Internet 2.2.4 Mal uso de Internet 2.2.5 Perfil del Internauta en México 2.2.6 Contenidos Nocivos 2.2.7 Conductas antisociales 2.2.8 Conductas ilícitas 2.2.9 Conceptos básicos de ataques cibernéticos contra el patrimonio	4

2.2.10 Delitos electrónicos contra la información 2.2.11 Introducción a ataques cibernéticos 2.2.12 Cómo preservar la evidencia digital	
2.3 La Internet de las Cosas 2.3.1 Introducción a internet de las cosas (iot) 2.3.2 Historia 2.3.3 Componentes de iot 2.3.4 Estándares en iot 2.3.5 Tecnologías asociadas al iot 2.3.6 Integración en Dispositivos Inteligentes	2
2.4 Introducción de la Seguridad de la Información 2.4.1 Definición de seguridad de la información 2.4.2 Tipos de seguridad de la información 2.4.3 Objetivos de la seguridad de la información 2.4.4 Amenazas a la seguridad de la información 2.4.5 Evaluación de riesgos 2.4.6 Técnicas de aseguramiento del sistema	2

Referencias – bibliografía mínima

Applicantes Google, http://applicantes.com/google-play-supera-la-app-store-ennumero-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-revenueforecast/. 2013 Reporte Norton PressDeck México, http://es.scribd.com/doc/185270894/2013Reporte-Norton-Press-Deck-México.

FICHA TÉCNICA		CLAVE: TF1-A-PDC			
Trayecto formativo		**Talleres: Desarrollo de Habilidades para la Función de Investigador**			
Nombre de la asignatura		3. Identificación y análisis de incidentes cibernéticos			
Horas mínimas	**10**	**Horas formativas**	**5**	**Horas prácticas**	**5**

Ejes transversales	
• Derechos humanos • Proximidad	• Perspectiva de género • Cultura de la legalidad

Caracterización

La asignatura *Identificación y Análisis de Incidentes Cibernéticos* forma parte del contenido temático del programa de "*Ciberseguridad*" para la formación continua de los elementos para la policía de investigación.

Se imparte con la finalidad de desarrollar las competencias necesarias para el ejercicio profesional de las funciones y atribuciones de los funcionarios encargados de hacer cumplir la ley, desde un enfoque de proximidad, perspectiva de género, derechos humanos y cultura de la legalidad.

Relación con otras asignaturas

Prevención de delitos cibernéticos, prevención de delitos cibernéticos, investigación de delitos cibernéticos.

Requisitos de ingreso (habilidades)

Ética de trabajo, pensamiento crítico, uso del equipo y materiales trabajo, trabajo en equipo, comunicación efectiva, pensamiento analítico, habilidades, para resolver problemas, habilidades de liderazgo, escucha activa, orientación a resultados, habilidades en Tics.

Objetivo terminal

Dotar a los participantes de técnicas y habilidades que les permita desempeñar sus funciones, que fortalezcan las capacidades de atención ciudadana en delitos cibernéticos. Así como correlacionar la información sobre el comportamiento de los delitos cibernéticos y resolver incidentes de seguridad informática, manejando la información de manera segura con las políticas de seguridad.

Objetivos específicos

- Atender, identificar y analizar los reportes ciudadanos en materia de delitos cibernéticos.
- Realizar ciber patrullaje en la red pública de internet y mitigar los riesgos y amenazas en ataques cibernéticos.

- Elaborar y estructurar informes policiales.

Metodología de enseñanza – aprendizaje
• **Aprendizaje basado en Tics:** estimular el desarrollo de la imaginación como la iniciativa y la personalización del aprendizaje. Las herramientas tecnológicas permiten adaptar el contenido y la metodología de enseñanza a las necesidades individuales de cada estudiante. • **Aprendizaje cooperativo:** involucrar a los elementos en el aprendizaje, aplicando cinco elementos que deben estar presentes en el aula cooperativa: interdependencia positiva, interacción cara a cara, responsabilidad individual, habilidades interpersonales y sociales y procesamiento grupal. • **Aprendizaje orientado a proyectos:** enfrentar a los elementos a situaciones que los lleven a construir, comprender y aplicar aquellos conocimientos y habilidades propias de la disciplina conjugando habilidades, actitudes y valores de trabajo. Desarrollar habilidades de trabajo en equipo, lo cual contribuye a preparar a los elementos para un entorno social real. • **Colaboraciones interdisciplinarias:** involucrar a expertos en actuación policial para impartir talleres de experiencias y conferencias grabadas.

Fundamentación
Basado en el marco normativo y legal de la función policial enfocado en la actuación del policía de investigación de acuerdo a los Protocolos Nacionales de Actuación y al Código Nacional de Procedimientos Penales.

Desarrollo programático	Horas mínimas
3.1 Ciber patrullaje en la red pública de internet 3.1.1 Conceptos básicos 3.1.2 Utilización de navegadores 3.1.3 TOR (red de anonimato) 3.1.4 Redes Sociales 3.1.5 Herramientas especializadas 3.1.6 Fraude al sector financiero (carding) 3.1.7 Propiedad Intelectual 3.1.8 Grupos hacktivistas 3.1.9 Ciber patrullaje	2
3.2 Pornografía infantil y trata de personas en internet 3.2.1 Pornografía infantil 3.2.2 Trata de personas 3.2.3 Red pública 3.2.4 Enganchamiento 3.2.5 Información 3.2.6 Correos Electrónicos 3.2.7 Análisis y procesamiento de la información 3.2.8 Redes técnicas	4

3.2.9 Redes de cruces 3.2.10 The National Center for Missing & Exploited Children NCMEC 3.2.11 Deep web	
3.3 Malware, Amenazas y Ataques 3.3.1 Conceptos básicos 3.3.2 Análisis de malware 3.3.3 Resultados del análisis de malware	2
3.4 Seguridad en Redes 3.4.1 Conceptos básicos 3.4.2 Metodologías de evaluación de vulnerabilidades 3.4.3 Anatomía de una intrusión en la red 3.4.4 Seguridad a nivel de la red 3.4.5 Análisis del suceso de seguridad	2
3.5 Seguridad en dispositivos móviles 3.5.1 Redes inalámbricas, dispositivos y características 3.5.2 Regulaciones, estándares 3.5.3 Legislación sobre redes inalámbricas 3.5.4 Conexión, herramientas, terminologías y métodos de seguridad y ataques 3.5.5 Aplicaciones prácticas 3.5.6 Introducción SO móviles 3.5.7 Recomendaciones de seguridad 3.5.8 Bluetooth, definiciones, herramientas, métodos de prevención y ataques	

Referencias – bibliografía mínima

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.
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, 2*000.
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
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.
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 Press LLC, 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.

FICHA TÉCNICA		**CLAVE: TF1-A-IDC**			
Trayecto formativo		**Talleres: Desarrollo de Habilidades para la Función de Investigador**			
Nombre de la asignatura		4. Investigación de Delitos Cibernéticos			
Horas mínimas	**15**	**Horas formativas**	**5**	**Horas prácticas**	**10**

Ejes transversales	
• Derechos humanos • Proximidad	• Perspectiva de género • Cultura de la legalidad

Caracterización
La asignatura *Investigación de Delitos Cibernéticos* forma parte del contenido temático del programa de "*Ciberseguridad*" para la formación continua de los elementos para la policía de investigación. Se imparte con la finalidad de desarrollar las competencias necesarias para el ejercicio profesional de las funciones y atribuciones de los funcionarios encargados de hacer cumplir la ley, desde un enfoque de proximidad, perspectiva de género, derechos humanos y cultura de la legalidad.

Relación con otras asignaturas
Prevención de delitos cibernéticos, identificación y análisis de incidentes cibernéticos, identificación y análisis de incidentes cibernéticos.

Requisitos de ingreso (habilidades)
Ética de trabajo, pensamiento crítico, uso del equipo y materiales de trabajo, trabajo en equipo, comunicación efectiva, pensamiento analítico, habilidades, para resolver problemas, habilidades de liderazgo, escucha activa, orientación a resultados, habilidades en Tics.

Objetivo terminal
Dotar a los participantes de técnicas y habilidades que fortalezcan sus capacidades en investigación de delitos cibernéticos, realizando análisis forenses de dispositivos electrónicos, patrullaje cibernético, así como identificar y evaluar los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información que se maneja dentro de las unidades de prevención del delito cibernético.

Objetivos específicos
• Coadyuvar en la integración de las carpetas de investigación relacionadas con delitos cibernéticos. • Realizar investigaciones en materia de delitos cibernéticos. • Tener conocimiento de la norma ISO/IEC27001:2013, Sistema de Gestión de la Seguridad de la Información. • Atender correctamente las denuncias realizados por la ciudadanía y elaborar los informes policiales.

Metodología de enseñanza – aprendizaje
• **Aprendizaje basado en Tics:** estimular el desarrollo de la imaginación como la iniciativa y la personalización del aprendizaje. Las herramientas tecnológicas permiten adaptar el contenido y la metodología de enseñanza a las necesidades individuales de cada estudiante. • **Aprendizaje cooperativo:** involucrar a los elementos en el aprendizaje, aplicando cinco elementos que deben estar presentes en el aula cooperativa: interdependencia positiva, interacción cara a cara, responsabilidad individual, habilidades interpersonales y sociales y procesamiento grupal. • **Aprendizaje orientado a proyectos:** enfrentar a los elementos a situaciones que los lleven a construir, comprender y aplicar aquellos conocimientos y habilidades propias de la disciplina conjugando habilidades, actitudes y valores de trabajo. Desarrollar habilidades de trabajo en equipo, lo cual contribuye a preparar a los elementos para un entorno social real.

Fundamentación
Basado en el marco normativo y legal de la función policial enfocado en la actuación del policía de investigación de acuerdo a los Protocolos Nacionales de Actuación y al Código Nacional de Procedimientos Penales.

Desarrollo programático	Horas mínimas
4.1 Prevención, respuesta y administración de incidentes 4.1.1 Esquema general de recuperación de incidentes 4.1.2 Ciclo de respuestas a incidentes 4.1.3 Medidas preventivas 4.1.4 Detección de incidentes 4.1.5 Planes de contingencia y procedimientos de recuperación 4.1.6 Acciones a tomar después de recuperar la operación 4.1.7 Manejo de incidentes de seguridad de la información	2
4.2 Sistemas de detección y prevención de intrusos y monitoreo 4.2.1 Conceptos de seguridad informática 4.2.2 Conceptos de detección y prevención 4.2.3 Tipos de IDS/IPS 4.2.4 APT (Amenazas Persistentes Avanzadas) 4.2.5 Metodologías de detección 4.2.6 Progresión de la amenaza 4.2.7 Reconocimiento 4.2.8 Herramientas para detección de tráfico sospechosos 4.2.9 Monitoreo de seguridad de red	2
4.3 Análisis de vulnerabilidades y pruebas de penetración 4.3.1 Metodología para pruebas de penetración 4.3.1 Análisis de vulnerabilidades 4.3.2 Recopilación de información 4.3.3 Reconocimiento 4.3.4 Mapeo 4.3.5 Descubrimiento 4.3.6 Explotación 4.3.7 Pruebas de penetración desde el exterior 4.3.8 Pruebas de penetración desde el interior 4.3.9 Pruebas de penetración al firewall 4.3.10 Pruebas de penetración a los IDS 4.3.11 Metodología de una prueba de penetración a una aplicación web	2
4.4 Hacking Ético 4.4.1 Introducción al ethical hacking 4.4.2 Reconocimiento anticipado 4.4.3 Mapeo de vulnerabilidades 4.4.4 Arquitectura x86 4.4.5 Shellcode 4.4.6 Payloads 4.4.7 Herramientas de auditoría de redes LAN inalámbricas (wifi hacking) 4.4.8 Evaluación de riesgos 4.4.9 Análisis de amenazas y metodología de piratería	2

4.4.10 Medidas de seguridad rudimentarias 4.4.11 Medidas de seguridad avanzadas 4.4.12 Soluciones de hardware y software 4.4.13 Implementación y administración	
4.5 Análisis Forense 4.5.1 Historia de la telefonía celular 4.5.2 Identificación 4.5.3 Extracción de información a los dispositivos de comunicación móvil mediante el empleo de diferentes herramientas tecnológicas 4.5.4 Normas de entrega de los equipos de telefonía 4.5.4.1Lineamientos empleados en la entrega de la cadena de custodia	4
4.6 Fundamentos de la Norma ISO/IEC/ 27001:2021 Sistema de Gestión de la Información 4.6.1 ¿Qué es la seguridad de la información? 4.6.2 ¿Qué son los riesgos de seguridad de la información? 4.6.3 ¿Cómo implementar la seguridad de la información?	3

Referencias – bibliografía mínima

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). G*estión de Incidentes de Seguridad Informática.* Starbook Editorial.
Gómez Vieites, Álvaro. *Enciclopedia de la Seguridad Informática,* Ra-Ma Editorial, 2011.
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.
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

METODOLOGÍA DE ENSEÑANZA – APRENDIZAJE Y REQUERIMIENTOS

A continuación se describen cada una de las metodologías, poniendo énfasis en la forma que contribuyen en el desarrollo de las competencias de los elementos.

La **Metodología de Aprendizaje Integrado y Experiencial** se centra en unir teoría y práctica, utilizando técnicas como simulaciones, estudios de casos y juegos de roles, para fomentar un aprendizaje profundo y significativo.

Por otro lado, la **Metodología de Capacitación Técnica y Táctica** enfatiza en la especialización de habilidades prácticas específicas, como el manejo de armas y tácticas de defensa, esenciales para la eficacia en el campo.

En paralelo, la **Metodología de Desarrollo de Habilidades Interpersonales y Comunicativas** busca fortalecer capacidades en comunicación y mediación, cruciales para una interacción efectiva y empática con la comunidad.

La **Metodología de Formación Ética y Derechos Humanos** prioriza la enseñanza de principios éticos y derechos humanos, asegurando que la actuación policial se alinee con valores de justicia y respeto.

Finalmente, la **Metodología de Evaluación y Retroalimentación Continua** aboga por una evaluación constante y adaptativa del aprendizaje, permitiendo un seguimiento personalizado y enfocado en la mejora continua.

Para lograr que las y los participantes desarrollen los conocimientos, las habilidades y destrezas operativas que exige el presente programa de capacitación, las metodologías de enseñanza-aprendizaje establecidas deben partir necesariamente de situaciones reales a las que se enfrenta de manera cotidiana, a fin de lograr un *aprendizaje significativo*.

En tal sentido, la o el instructor planteará una *metodología activa*, en la que expondrá de manera breve los elementos teóricos reforzados por las experiencias de los participantes. La impartición del programa contemplará en cada curso los siguientes aspectos:

- Introducción al tema: brindar una breve información sobre el objetivo que se pretende alcanzar.
- Actividades *teórico-prácticas* que incluyan a todos los participantes, sea de manera individual o grupal, promoviendo la participación de cada integrante.
- Orientaciones para garantizar la adecuada realización de cada actividad o práctica.
- Cierre del curso.

Lo anterior basado en la teoría constructivista y el aprendizaje experiencial, que postulan que los conocimientos se adquieran mejor a través de la experiencia y la interacción activa con el entorno, así como en principios de formación técnica especializada, enfatizando en la eficacia, seguridad y respuesta efectiva en el campo.

Material de apoyo para el maestro:

- PC con paquetería básica y acceso a Internet
- Cañón proyector
- Plumones para pintarrón
- Pintarrón
- Impresora o posibilidad de impresión y copias
- Hojas blancas
- Computadora portátil con Microsoft Office compatible con equipo de proyección.
- Equipo de audio y video.
- Presentaciones audiovisuales
- Videos
- Imágenes

Material de la institución:

- PC con paquetería básica y acceso a Internet
- Cañón proyector
- Plumones para pintarrón
- Pintarrón
- Bocinas para PC
- Impresora o posibilidad de impresión y copias
- Hojas blancas.
- Computadora por alumno con paquetería office y acceso a wifi

Material del alumno:

Los materiales que deberá presentar el participante son:

- Cuaderno y lapicero para tomar notas sobre la cátedra
- Uniforme operativo
- Manual
- Gafete

EVALUACIÓN Y ACREDITACIÓN

Sistema de evaluación

Para cumplir con los propósitos del presente programa de estudios, la evaluación se concibe como un aspecto fundamental para medir la calidad del aprendizaje y está diseñada con base en el contexto en el que se desarrolla el proceso de enseñanza-aprendizaje, dado que permite valorar los conocimientos adquiridos y las habilidades desarrolladas en el curso.
Para ello se realizarán **tres Evaluaciones:**

1. **Diagnóstica**
2. **Asistencia, comportamiento y participación del alumno**
3. **Evaluación final del curso.**

Criterios

- Se evaluarán los conocimientos, habilidades y actitudes en los contenidos temáticos que serán desarrollados en el programa.
- Se podrán administrar una o varias evaluaciones por módulo.
- La elaboración de la evaluación estará a cargo del docente responsable del módulo. La modalidad que asuma el instrumento de evaluación, será responsabilidad de cada docente.
- Las evaluaciones podrán ser prácticas, ya sea mediante simulaciones, solución de casos, elaboración de escritos propios del rol que desempeña el Mando Policial, etc.

Procedimientos

El procedimiento a seguir, será determinado al asignar a cada uno de estos criterios, el peso porcentual específico que tendrán para determinar la calificación final de cada unidad didáctica; dicha calificación deberá expresarse en términos numéricos, siguiendo la escala que aplica el sistema educativo oficial, empero, invariablemente se deberá de considerar lo siguiente:

- Examen teórico o práctico que puede ser escrito u oral, con valor de 80% de calificación.
- Asistencia aprobatoria 100% de las sesiones, con valor del 10% de calificación total.
- Participación y compromiso, con valor de 10%.

Instrumentos

- El personal docente llevará un registro de asistencia mediante pase de lista al inicio de cada sesión y registrará la participación de los alumnos en clase, de los temas a tratar en la misma.
- Se aplicará una evaluación del Desarrollo de la Actividad Académica Al finalizar el tema de la materia, el personal docente aplicará un examen de conocimientos teórico o práctico pudiendo ser oral o escrito.

Escala de acreditación

El curso se evaluará en una escala numérica de 0 a 10, en la que la mínima para acreditar es **8 (ocho).** La calificación final será resultado del promedio ponderado de los procedimientos orales o escritos y demostrativos con el valor señalado en líneas anteriores en el apartado de procedimientos.

Constancia que se otorga

Al acreditar todos los módulos establecidos en la estructura curricular, y el requerimiento de asistencias, se otorgará **Constancia** misma que tiene validez curricular por haber aprobado satisfactoriamente el programa denominado ***Ciberseguridad*** el cual será expedido por las autoridades correspondientes.

Evaluación del personal docente

Esta evaluación tiene el propósito de que los alumnos emitan una opinión acerca del desempeño del docente o instructor en la enseñanza de la asignatura, así como de la calidad del curso, lugar, ambiente y materiales didácticos, con el fin de mejorar la prestación del servicio que le brinda la institución.

Apoyo que se ofrece a la o el alumno

Se proporcionará a los alumnos el manual del curso, para que sea utilizado como una herramienta de auto aprendizaje, ya que en el proceso el instructor guiara la capacitación especializada, a través de su gestión de habilidades y conocimientos de sus capacitados.

Perfil del Docente:

El docente del curso deberá contar con:

- El perfil profesional que corresponda a la asignatura que habrá de impartir;
- Por lo menos cinco años de experiencia docente en el ámbito de la seguridad pública;
- Competencias en el ámbito de facilitador en solución de conflictos, aplicando en ello diferentes estrategias y recursos didácticos tanto de enseñanza como de evaluación;
- Competencias conductuales, capacidad de dirigir a un grupo creando un clima de compromiso, demostrando en todo momento sólidas bases de comunicación;
- Contar con valores éticos, profesionales, honradez, humildad, responsabilidad etc.

Con la finalidad de obtener los resultados esperados en la aplicación del Protocolo de Actuación Policial ante Hechos Delictivos se establecen los siguientes instructores por asignatura:

ASIGNATURA A IMPARTIR POR EL DOCENTE - FACILITADOR

Ciberseguridad				
Clave	**Trayecto Formativo**		**Clave**	**Asignatura**
TF1-TDHFI	Talleres: desarrollo de habilidades para la función de investigador		TF1-A-LCS	1. La ciberseguridad
			TF1-A-PDC	2. Prevención de delitos cibernéticos
			TF1-A-IAIC	3. Identificación y análisis de incidentes cibernéticos
			TF1-A-IDC	4. Investigación de delitos cibernéticos

Nota: *Se anexa al presente programa, carpeta electrónica con toda la documentación probatoria de cada uno de los docentes – instructores que participarán en la impartición de la capacitación.*

REFERENCIAS

- Gaceta Parlamentaria https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf
- Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf https://latam.kaspersky.com/resource-center/threats/ransomware https://blog.avast.com/es/guia-basica-sobre-el-ransomware-y-como-protegerse https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/ https://www.redeszone.net/tutoriales/seguridad/mensajes-phishing-como-protegernos/ https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ https://www.derechosdigitales.org/12364/el-convenio-de-budapest-desde-una-perspectiva-de-derechos-humanos/ https://blog.smartekh.com/-pasos-para-una-estrategia-de-ciberseguridad https://www.pandasecurity.com/spain/mediacenter/consejos https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/ https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/ https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/
- Applicantes Google, http://applicantes.com/google-play-supera-la-app-store-ennumero-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-revenueforecast/. 2013 Reporte Norton Press Deck México, http://es.scribd.com/doc/185270894/2013Reporte-Norton-Press-Deck-México.

- 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.
- Acuerdo A/024/08*, Procuraduría General de la República, Fiscalía Especial para los Deli*tos 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, 2*000.
- 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
- 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.
- 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 Press LLC, 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.
- 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). G*estión de Incidentes de Seguridad Informática.* Starbook Editorial.
- Gómez Vieites, Álvaro. *Enciclopedia de la Seguridad Informática,* Ra-Ma Editorial, 2011.
- 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.
- 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