1.- Identificación de la Unidad de Aprendizaje					
Nombre de la Unidad de Aprendizaje					
Delitos Cibernéticos					
Clave de la UA	**Modalidad de la UA**	**Tipo de UA**		**Valor de créditos**	**Área de formación**
IF432	Presencial	Curso-Taller		5	CISA
Hora semana		**Horas teoría/semestre**	**Horas práctica/ semestre**	**Total, de horas:**	**Seriación**
3		32	30	62	
Departamento			**Academia**		
Justicia Alternativa, Ciencias Forenses y Disciplinas Afines al Derecho					

Presentación

Según cifras del banco mundial, en 2021 63% de la población mundial utiliza Internet; en México un 76%, y la tasa de crecimiento entre 2020 y 2021 fue de 5 %. Del 2021 al 2022, México fue blanco del 66% de los ataques cibernéticos ocurridos en América Latina, provocando pérdidas de entre 3 mil y 5 mil millones de dólares por año, de acuerdo con la Asociación de Bancos de México.

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.

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Discutir sobre la privacidad y su importancia como	Identificar y evaluar el impacto del delito cibernético sobre la	Evaluar críticamente la relación entre la seguridad y la privacidad

derecho humano Definir, discutir y evaluar los activos, amenazas, vulnerabilidades y riesgos Discutir sobre la prevención situacional de delitos y relacionarla con la prevención y reducción de delitos cibernéticos Describir y discutir las pruebas digitales Describir y diferenciar entre el derecho sustantivo, procesal y preventivo sobre delitos cibernéticos Definir y describir conceptos básicos relacionados con delitos generados con herramientas informáticas.	privacidad Evaluar críticamente las medidas utilizadas para contrarrestar los delitos cibernéticos organizados Discutir las maneras en que las pruebas digitales son autenticadas Identificar, discutir y examinar la necesidad y el rol de las leyes sobre delitos cibernéticos Describir y evaluar la conectividad global y las tendencias del uso de la tecnología. Identificar amenazas que pongan en riesgo la confidencialidad, integridad o disponibilidad de la información.	Explicar y analizar las formas en que se utilizan las tecnologías de la información y la comunicación para cometer delitos cibernéticos organizados Describir y criticar los modelos del proceso del análisis forense digital Evaluar críticamente la protección de los derechos humanos en línea Definir el delito cibernético y discutir la razón por la que se estudia de manera científica

Competencia genérica	**Competencia profesional**
Conocer el objeto de estudio de las ciencias forenses y sus aplicaciones a la investigación de ciberdelitos. Pensamiento crítico. Análisis y seguimiento de pistas.	Establecer el conocimiento sobre la interacción de las ciencias forenses con los entornos cibernéticos. Ética y sentido de la verdad.

Saberes previos del alumno
Identificación y uso de diferentes herramientas TIC

Perfil de egreso al que se abona
Emite dictámenes forenses con base en el análisis, interpretación y síntesis de información documental y digital, mediante uso de tecnologías de la información y comunicación.

Perfil deseable del docente

Conocimientos:
- Conocer los Delitos Cibernéticos en México
- Comprender la Legislación en México
- Identificar los conceptos de tecnologías de la información y comunicación
- Conocer el Perfil del delincuente Cibernético
- Identificar las Conductas y técnicas delictivas

Habilidades:
- Planificar el proceso de enseñanza
- Identificar necesidades de información.
- Organizar información y contenidos relacionados con conductas y técnicas delictivas
- Crear o rehacer contenidos
- Aplicar derechos de autor y licencias a la información y a los recursos creados.
- Aplica estrategias de seguridad

Contenido

Unidad 1. Antecedentes

1.1. Definición y características del delito
1.2. Delito informático
  1.2.1. Julio Téllez V./María de la Luz Lima
  1.2.2. Convenio de ciberdelincuencia
1.3. Delitos Cibernéticos en México
1.4 Delitos Cibernéticos en el Mundo

Unidad 2. Legislación
2.1 Legislación en México
2.2 Ley federal de protección a la propiedad industrial
2.3 Ley federal de derecho de autor
2.4 Ley federal de protección de datos personales en posesión de particulares
2.5 Ley federal de protección de datos personales en posesión de sujetos obligados
2.6 Ley federal de telecomunicaciones y radiodifusión
2.7 Código penal federal
2.8 Código penal del estado de Jalisco
2.9 Ley Olimpia
2.10 Estrategia Nacional de Ciberseguridad
2. 11 Legislación Internacional
2.12 GDPR
2.13 Tratado Budapest (Convenio de Ciberdelincuencia)
2.14 Convenios internacionales de cooperación

Unidad 3. Conceptos de tecnologías de la información y comunicación

3.1 Historia de la computación
3.2 Tipos de lenguajes
3.3 Hardware y Software
3.4 Redes y telecomunicaciones

Unidad 4. Perfil del delincuente Cibernético

4.1 Hacker
4.2 Cracker
4.3 Phreaker

4.4 Insiders
4.5 Ciberdelincuente

Unidad 5. Conductas y técnicas delictivas
5.1. Skimming
5.2. Cracking
5.3. Web defacement
5.4. Pharming
5.5 Espionaje
5.5. Exploits
5.6 Robo de identidad
5.7 Ingeniería social
5.8 Ingeniería inversa
5.9. Malware
- 5.9.1 Virus
- 5.9.2 Ransomware
- 5.9.3 Spyware
- 5.9.4 Keyloggers
- 5.9.5 Worms
- 5.9.6 Backdoors

5.10 Spear phising
5.11 Fuerza bruta
5.12 Phising
5.13 DDoS
5.14 Ataques SCADA
5.15 Botnet
5.16 Pornografía infantil
5.17 Sextorsión
5.18 Ciberbullying
5.19 Sniffing
5.20 Retos suicidas
5.21 Ciberacoso
5.22 Secuestro de cuentas (FB, Twitter, Instagram, etc.)
5.23 Grooming
5.24 Piratería
5.25 Deep Web
5.26 Dark Net
5.27 Ciberterrorismo

Estrategias generales para impartir la unidad de aprendizaje

Diapositivas de PowerPoint, figuras, gráficos, esquemas, imágenes o videos..

Módulo I. Antecedentes

Unidad 1. Antecedentes

1.1. Definición y características del delito
1.2. Delito informático
- 1.2.1. Julio Téllez V./María de la Luz Lima
- 1.2.2. Convenio de ciberdelincuencia

1.3. Delitos Cibernéticos en México
1.4 Delitos Cibernéticos en el Mundo

Competencia Específica

Identificar, examinar y analizar los desafíos técnicos, legales, éticos y operacionales relacionados con la investigación y prevención de los delitos cibernéticos

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Definir y describir conceptos básicos relacionados con la informática	Describir y evaluar la conectividad global y las tendencias del uso de la tecnología	Definir el delito cibernético y discutir la razón por la que se estudia de manera científica

Módulo II. Legislación

Unidad 2. Legislación
2.1 Legislación en México
2.2 Ley federal de protección a la propiedad industrial
2.3 Ley federal de derecho de autor
2.4 Ley federal de protección de datos personales en posesión de particulares
2.5 Ley federal de protección de datos personales en posesión de sujetos obligados
2.6 Ley federal de telecomunicaciones y radiodifusión
2.7 Código penal federal
2.8 Código penal del estado de Jalisco
2.9 Ley Olimpia
2.10 Estrategia Nacional de Ciberseguridad
2. 11 Legislación Internacional
2.12 GDPR
2.13 Tratado Budapest (Convenio de Ciberdelincuencia)
2.14 Convenios internacionales de cooperación

Competencia Específica

Identificar y evaluar críticamente las legislaciones nacionales, regionales e internacionales sobre delitos cibernéticos

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)

Describir y diferenciar entre el derecho sustantivo, procesal y preventivo sobre delitos cibernéticos	Identificar, discutir y examinar la necesidad y el rol de las leyes sobre delitos cibernéticos	Evaluar críticamente la protección de los derechos humanos en línea
Módulo III Conceptos de tecnologías de la información y comunicación		
Unidad 3. Conceptos de tecnologías de la información y comunicación 3.1 Historia de la computación 3.2 Tipos de lenguajes 3.3 Hardware y Software 3.4 Redes y telecomunicaciones		
Competencia Específica		
Evaluar críticamente los estándares y mejores prácticas para las pruebas digitales y el análisis forense digital		
Tipos de saberes		
Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Describir y discutir las pruebas digitales	Discutir las maneras en que las pruebas digitales son autenticadas	Describir y criticar los modelos del proceso del análisis forense digital
Módulo IV Perfil del delincuente Cibernético		
Unidad 4. Perfil del delincuente Cibernético 4.1 Hacker 4.2 Cracker 4.3 Phreaker 4.4 Insiders 4.5 Ciberdelincuente		
Competencia Específica		
Examinar críticamente el hacktivismo, el ciberespionaje, el ciberterrorismo, la guerra cibernética, la guerra de información y la desinformación		
Tipos de saberes		
Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)

Definir, discutir y evaluar los activos, amenazas, vulnerabilidades y riesgos Discutir sobre la prevención situacional de delitos y relacionarla con la prevención y reducción de delitos cibernéticos	Evaluar críticamente las medidas utilizadas para contrarrestar los delitos cibernéticos organizados	Explicar y analizar las formas en que se utilizan las tecnologías de la información y la comunicación para cometer delitos cibernéticos organizados
Módulo V Conductas y técnicas delictivas		
Unidad 5. Conductas y técnicas delictivas 5.1. Skimming 5.2. Cracking 5.3. Web defacement 5.4. Pharming 5.5 Espionaje 5.5. Exploits 5.6 Robo de identidad 5.7 Ingeniería social 5.8 Ingeniería inversa 5.9. Malware 5.9.1 Virus 5.9.2 Ransomware 5.9.3 Spyware 5.9.4 Keyloggers 5.9.5 Worms 5.9.6 Backdoors 5.10 Spear phising 5.11 Fuerza bruta 5.12 Phising 5.13 DDoS 5.14 Ataques SCADA 5.15 Botnet 5.16 Pornografía infantil 5.17 Sextorsión 5.18 Ciberbullying 5.19 Sniffing 5.20 Retos suicidas 5.21 Ciberacoso 5.22 Secuestro de cuentas (FB, Twitter, Instagram, etc.) 5.23 Grooming 5.24 Piratería 5.25 Deep Web 5.26 Dark Net 5.27 Ciberterrorismo		
Competencia Específica		

Definir y diferenciar entre los tipos de delitos cibernéticos

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Discutir sobre la privacidad y su importancia como derecho humano	Identificar y evaluar el impacto del delito cibernético sobre la privacidad	Evaluar críticamente la relación entre la seguridad y la privacidad

Bibliografía básica

MARTÍNEZ, José (2019). Delitos informáticos. A&HP
NAVA, Alberto (2018). Delitos informáticos. Porrúa
NAVA, Alberto (2019). Ciberdelitos. Tirant Lo Blanch.

Bibliografía complementaria

MITNICK, Kevin (2005). The art of intrusion. John Wiley & Sons
MITNICK, Kevin (2001). The art of deception. John Wiley & Sons
TÉLLEZ, Julio (2009). Derecho Informático. McGraw Hill
GOODMAN, Marc (2015). Los delitos del futuro. Ariel.

3.-Evaluación

Criterios de Evaluación (% por criterio)

1. EVALUACIÓN DIAGNÓSTICA
Sin valor acreditable. Aplicada al inicio de cada etapa con la finalidad de identificar los conocimientos previos que posee el estudiante sobre el tema respectivo de etapa.

2. EVALUACIÓN FORMATIVA
Comprende todas las actividades relacionadas con el programa y realizadas por el estudiante, mismas que dan cuenta de su proceso de aprendizaje a lo largo del semestre. Las actividades se evalúan cuantitativamente.

3. EVALUACIÓN SUMATIVA
Para su determinación se toman en cuenta los criterios de desempeño reflejados en las evidencias individuales: Exámenes departamentales, exámenes parciales, actividades de clase, tareas y un proyecto de investigación.

4. EVALUACIÓN CONTINUA
Obtener una calificación suficiente aplicando los criterios que se especifican a continuación:

Criterio	Porcentaje
Tareas	40 %
Reporte de prácticas	50 %
Participación en clase	10 %
TOTAL	**100%**

4.-Acreditación

En concordancia con la normativa universitaria, la asistencia a las actividades presenciales es obligatoria y la participación del alumno en todas las actividades docentes se valorará positivamente en la calificación final. Por ello, será necesario: 1. Haber asistido al menos al 80% de clases magistrales y tutorías 2. Haber realizado su proyecto de investigación y entregado dicho documento.

Lo anterior de acuerdo al REGLAMENTO GENERAL DE EVALUACIÓN Y PROMOCIÓN DE ALUMNOS DE LA UNIVERSIDAD DE GUADALAJARA que señala: Artículo 5. El resultado final de las evaluaciones será expresado conforme a la escala de calificaciones centesimal de 0 a 100, en números enteros, considerando como mínima aprobatoria la calificación de 60. Las materias que no son sujetas a medición cuantitativa, se certificarán como acreditadas (A) o no acreditadas (NA).

Artículo 20. Para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el H. Consejo General Universitario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso.
Artículo 27. Para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso.

5.- Participantes en la elaboración

Código	Nombre
2966256	Luis Pedro García Yáñez
2700735	Laura López López

6.- Fecha de adaptación	
Agosto 2023	