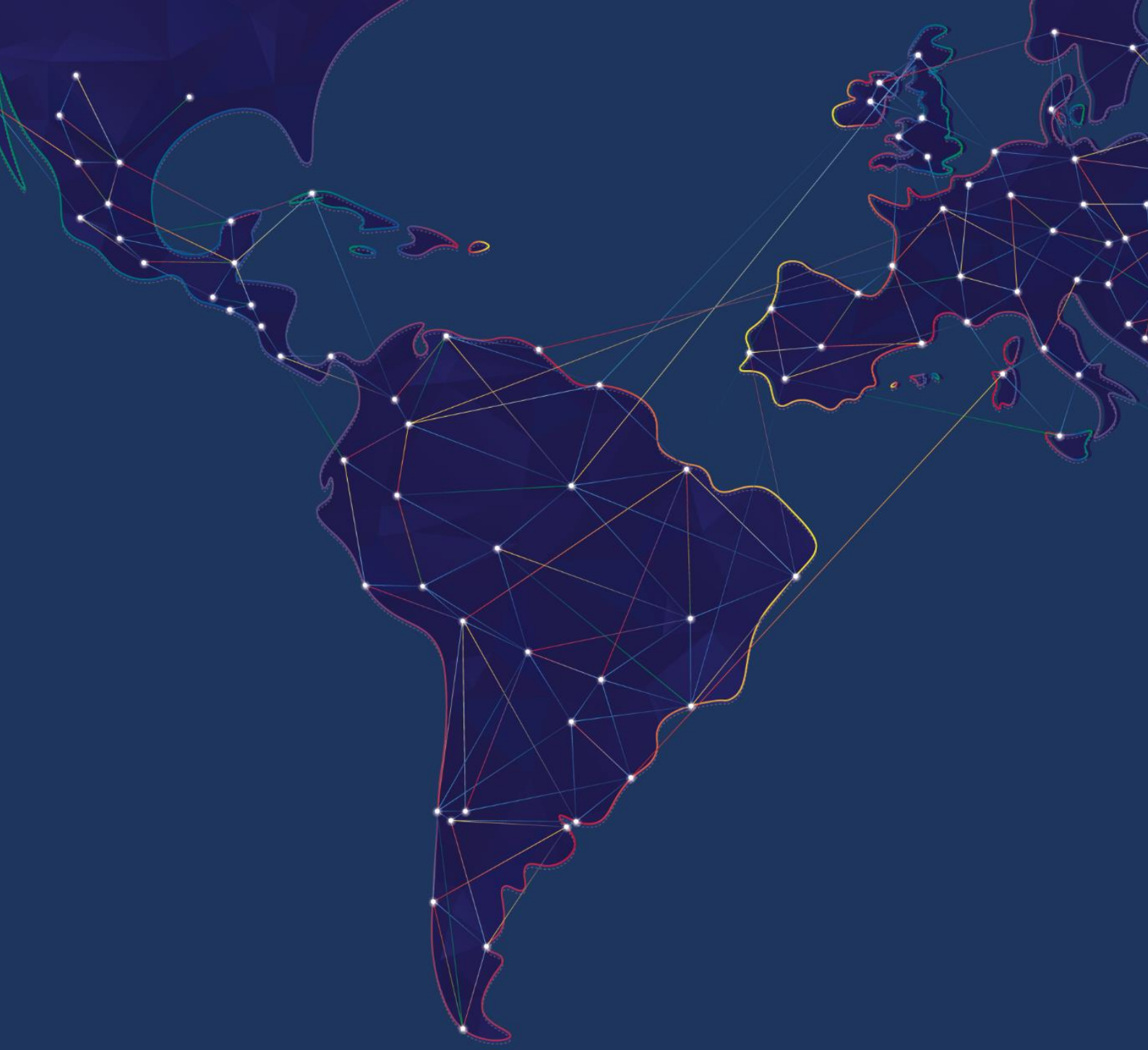

Diciembre de 2021

Armonización de la especialización en lucha contra el cibercrimen en América Latina

Coordinadora: Janett García

Autores: Adrián Acosta, Janett García, Pedro Gómez, Alberto Redondo

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Contenido

1. INTRODUCCIÓN

1.1. Antecedentes

El programa EL PAcCTO está dando continuidad a la lucha contra el cibercrimen mediante actividades de carácter regional y multipaís. De manera destacada, se han realizado cuatro talleres regionales (Quito, octubre de 2017; San Salvador, noviembre de 2018; Santiago de Chile, octubre de 2019; virtual, julio de 2021), además de otras actividades de carácter operativo y legislativo. De todas estas actividades se han determinado los desafíos comunes entre AL y la UE:

- La necesidad de una gestión compleja de los datos. Esto se refiere a la protección de datos personales frente a robos masivos, las técnicas de encriptación compleja, el uso de criptomonedas y la propia gobernanza de internet.
- La deslocalización, con servicios escondidos en la internet oculta y servicios en nube inalcanzables dentro de las jurisdicciones nacionales.
- La necesidad de armonización legal entre los países, tomando como referencia internacional el Convenio del Consejo de Europa sobre la Ciberdelincuencia, más conocido como Convenio de Budapest.
- La necesidad de una cooperación internacional efectiva, tanto en investigaciones de cibercrimen como frente a ciberataques a gran escala.
- La conveniencia de la colaboración pública - privada, por un lado, para las relaciones con los grandes operadores tecnológicos y, por otro, para el desarrollo de herramientas de investigación.
- Finalmente, la necesidad de concienciar a la sociedad del buen uso del ciberespacio, con todo su potencial, y la prevención frente al cibercrimen.

Estas prioridades se han centrado en tres aspectos, definidos por las instituciones latinoamericanas:

a) El refuerzo de las redes regionales: la CiberRed - Red de Fiscales Iberoamericanos sobre Cibercrimen Red de la AIAMP, creada en febrero de 2018, y la Red CibEL@ - Policías de Europa y Latinoamérica contra el Cibercrimen, impulsada por EL PAcCTO.

b) La armonización de la formación de especialistas en cibercrimen para todas las instituciones de la cadena penal: cuerpos policiales, ministerios públicos y poderes judiciales.

c) La sensibilización de la sociedad y de las propias instituciones acerca de una de las temáticas más presentes y difíciles de entender: las criptodivisas.

1.2. Diseño

El presente informe se refiere a **la armonización de la formación de especialistas en cibercrimen**. Esto debe facilitar la cooperación internacional efectiva, al partir todas ellas de bases de conocimiento comunes en materias técnicas y procesales. Los aspectos a tener en cuenta son:

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LÍNGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

- La formación inicial en los centros de ingreso en los cuerpos de policía y a las fiscalías. Se orienta a personas no especialistas que pueden encontrarse con casos que tengan elementos tecnológicos, como un sencillo teléfono móvil. Por lo general, consiste en pautas de actuación sencillas para preservar pruebas y no alterar el "escenario digital", así como contactar a unidades especializadas.
- La estructuración de contenidos sistemáticos, carácter técnico, procedimental y jurídico.
- La definición de niveles de especialización, en función del tipo de unidad en la que se trabaje. Se trata de una distinción más teórica que real, pues es posible fusionar varios niveles cuando se lleve a cabo un curso. Sin embargo, puede permitir aprovechar recursos formativos más técnicos que se pueden impartir con mayor rapidez.
- La formación conjunta entre instituciones, lo que permite distinguir contenidos comunes a fiscalías y policías, más contenidos exclusivos de cada una de ellas. Por su conformación, la formación judicial requiere un tratamiento diferente, pues priman aspectos jurídicos y procesales.
- La formación híbrida o en línea, como modelo ideal de interoperabilidad y de aprovechamiento de recursos birregionales. Esto implica la realización de un mapeo de capacidades formativas en América Latina.

Lo normal es que los órganos centrales lideran la transmisión de conocimientos y buenas prácticas. En definitiva, se trata de implantar sistemas estables, preferentemente interinstitucionales, con **modelos interoperables**, con carácter interinstitucional, práctico y con un fuerte componente en línea. En un futuro, esto puede dar lugar a un sistema reconocido de certificaciones.

En este aspecto, será importante la coordinación con el *Latin American and Caribbean CyberCapacities Center* (LAC4) que el programa CyberNet está desarrollando en la República Dominicana durante 2021.

1.3. Modelo de trabajo

Se toma como referencia una experiencia similar desarrollada por la UE entre 2010 y 2011: el Proyecto EU-DEFI (*"European Union – Delivering Excellence in Financial Investigation"*), cuya finalidad fue potenciar y homogeneizar la investigación financiera en la UE, con tres objetivos:

- La confección de un Manual de Investigación Financiera.
- La definición de niveles de formación como investigador, así como los contenidos a estudiar en cada uno.
- El establecimiento de los requisitos que deben cumplir los centros de certificación de investigadores financieros.

Tuvo su origen en la "Comunicación sobre Prevención de y Lucha contra el Crimen Organizado en el Sector Financiero", de la Comisión Europea, en 2004. Se trataba de una de las iniciativas prioritarias de la Dirección General de Justicia e Interior. El Proyecto fue presentado por tres países: Reino Unido (*"National Policing Improvement Agency"*), Italia (*"Scuola di Perfezionamento per le Forze di Polizia"* y *"Scuola di Policía Tributaria – Guardia di Finanza"*) y España (Guardia Civil).

El proceso dio inicio con una consulta a los Estados Miembros y las instituciones de la UE para definir los contenidos y niveles, con el siguiente resultado:

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

- Ocho capítulos:

  - Tipologías.
  - Normativa (nacional e internacional).
  - La prueba y la actuación judicial.
  - Trazabilidad de bienes (patrimonio real y nominal, confiscaciones, bloqueos o congelamientos, trusts, etc.).
  - Cooperación internacional.
  - Inteligencia (fuentes de información, tratamiento de la información, etc.).
  - Análisis e Interpretación (terminología financiera, análisis de cuentas, herramientas financieras, "desenmascaramiento" de actividades aparentemente lícitas, etc.).
  - Estrategia, política y gestión de casos (cuándo y cómo usar la investigación financiera, autónoma o en conjunción con otras investigaciones, qué difundir, etc.).

- Tres niveles:

  - Nivel 1: *"EU Financial Investigador"*. Engloba, como mínimo, los 8 temas anteriores. Se ha de impartir dentro de la institución del investigador.
  - Nivel 2: *"Expert EU Financial Investigador"*. Los 8 temas anteriores, pero con mayor profundidad. Se supone participación de instituciones externas a la del investigador (universidad, etc.).
  - Nivel 3: Estratégico, orientado a jefes de policía, de unidades de investigación, etc., con la finalidad de hacerles entender la problemática financiera y la necesidad de investigarla. Corresponde a CEPOL.

2. DESCRIPCIÓN GENERAL

2.1. Proceso de trabajo

El modelo EUDEFI ha sido objeto de debate en el "Taller Redes UELLA y CibEL@: Criptodivisas y CTO", celebrado en Quito, del 05 a 07 de octubre de 2021. En él han participado instituciones de Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Francia, Guatemala, Honduras, México, Panamá, Paraguay, Perú, Portugal, República Dominicana y Uruguay, así como la AIAMP, la CJI y GAFILAT. También han asesorado Eurojust y Europol.

Durante este taller, se definieron los contenidos que se desarrollan a continuación.

2.2. Módulos

Se definen siete módulos:

1. Conceptos básicos.
2. Marco Legal.
3. Tipologías: introducción general y delitos.
4. Evidencia Digital
5. Investigación e inteligencia.
6. OSINT.
7. Cooperación Internacional.

Los módulos son comunes para cuerpos policiales, ministerios públicos y judicatura. Simplemente se tendrán que adaptar en cada caso, con mayor énfasis en los aspectos de interés específico.

2.3. Niveles

Se definen los siguientes modelos de cursos:

a) **Curso de acceso**. Se orienta a:

- Personal de nuevo ingreso en la institución, en especial atendiendo a la recogida de denuncias y la actuación como primer respondiente. Se imparte en la escuela de acceso a la institución.
- Personal de unidades no especializadas.

b) **Curso de investigador/a o fiscal especializada/o**. Para personal de unidades especializadas contra el cibercrimen.

c) **Curso de fiscal o investigador/a experta/o**. Se trata de un grado mayor de conocimientos que el curso anterior. Se puede plantear que se acceda por experiencia a este nivel, para promover y reconocer la pertenencia a unidades especializadas.

   Este curso puede omitirse, o fusionarse con el anterior. Es una referencia académica, más que una necesidad.

d) **Curso estratégico**. Se dirige a personal decisor en políticas públicas y en las instituciones, con contenidos adaptados en cada caso: problemáticas, amenazas, necesidades, condicionantes, etc. Es recomendable que incluya visitas a instalaciones de unidades de lucha contra el cibercrimen.

e) **Cursos complementarios**. Se trata de formaciones ad hoc en materias concretas: por ejemplo, actualización, conocimiento de nuevas problemáticas y herramientas, temáticas urgentes, profundización en aspectos específicos, etc. Puede realizarse mediante autocapacitación, en algunos casos.

Los cursos se plantean de manera progresiva, cada uno de los tres primeros (o dos) partiendo del anterior. Deben complementar carga teórica y práctica, presencial y virtual, con clases técnicas y conferencias magistrales. Se considera conveniente que existan exámenes, trabajos académicos y pruebas prácticas para obtener la titulación correspondiente.

La armonización de los cursos también puede dar lugar a la creación de una red de formadoras/es reconocidas/os, que permita compartir las mejores experiencias. En paralelo, las titulaciones favorecen la estabilidad del personal en las unidades especializadas.

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

3. MÓDULOS

3.1. Módulo 1: Conceptos básicos

3.1.1. Descripción general

El propósito de este módulo es introducir al estudiante en el lenguaje técnico que se utiliza de acuerdo a los componentes de un sistema informático, adoptando una terminología común y presentando unos conceptos básicos en la materia sobre los que se basará la capacitación. Así mismo, introducir las nociones a la terminología judicial relacionada con los ilícitos penales cometidos en entornos digitales.

3.1.2. Desglose de contenidos

- Historia del computador, identificación de sus partes y su funcionamiento
- Qué son las TICS - Tecnología de la Información y las comunicaciones
- Redes sociales: Qué es y cómo funciona, función principal, tipos de redes sociales, redes de mensajería, diferencia entre social media y red social.
- Plataformas digitales que brindan servicio de correo electrónico, partes de un correo electrónico, identificación de encabezados
- Interconexión: topologías, redes, sistemas, seguridad
- Ecosistema de internet: Compuesta por tres capas. Primera Capa: Infraestructura: Servidores, ISP, torres, satélites, entre otros.
  Segunda Capa: Lógica: Protocolo IP, ICANN, nombres de dominios, RIR.
  Tercera Capa: Social y Económica
- Conceptos básicos sobre blockchain y criptoactivos.
- Glosario de términos (INCIBE).
- Conocer la función que cumplen a nivel ciber las Instituciones: policiales, Fiscalías, CERTs, centros tecnológicos. A nivel de la propia institución realizar especial énfasis en su estructura.

3.2. Módulo 2: Marco Legal

3.2.1. Descripción general

Este módulo está diseñado para abordar la legislación internacional que tiene relación de forma directa o indirecta con la lucha contra la delincuencia en la red. Aunque existe una normativa transnacional que puede servir como referencia, cada país tiene adaptado a su derecho interno este fenómeno.

Por todo ello, este punto ofrece conocer el marco jurídico de referencia, tanto en materia de lucha contra la ciberdelincuencia, como también aquella normativa existente que atañe a los derechos humanos y su posible vulneración a través de las nuevas tecnologías, con el fin de proteger la integridad de los datos personales de cada internauta.

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LÍNGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

3.2.2. Desglose de contenidos

- Legislación penal y procesal – tipificación.
- Jurisprudencia penal y procesal.
- Normativa administrativa de interés
- Normatividad Agente Encubierto Virtual
- Legislación internacional.
- Estadísticas delincuenciales y judiciales (sentencias).
- Derechos Humanos en la red (poblaciones vulnerables Casuística – Genocidio Vs Facebook en pleno Siglo XXI)
- Ley de Protección de Datos y privacidad (legislación).
- Normatividad de Criptoactivos desarrollada por cada país (derecho comparado).
- Estrategias nacionales aplicado a cada país.

3.3. Módulo 3: Tipologías

3.3.1. Descripción general

La delincuencia en la red está en constante evolución y la complejidad de las conductas desarrolladas en este entorno complican su identificación. Para enfrentarse con solvencia a esta nueva realidad, el investigador debe conocer tanto las principales tipologías como los modus operandi relacionados con ellas.

Aquí, el estudiante, identificará no sólo las actividades delictivas en cuestión, sino también las formas de hacerle frente a ciertos delitos en los entornos digitales. Comprender la diversidad de las modalidades es necesario para evaluar los métodos de investigación judicial que mejor se ajusten de acuerdo al tipo de delito.

3.3.2. Desglose de contenidos

- Acceso abusivo a un sistema informático
- ¿Qué es la ingeniería social y cuáles son sus técnicas?
- ¿Qué es el *criptojaking* y minería de datos?
- Violación de datos personales
- ¿Qué es el *SIM Swapping*?
- Suplantación de páginas web
- Uso de software malicioso
- ¿Qué es el *ransomware*?
- Hurto por medios informáticos
- ¿Qué es el *phishing*, *smishing* y *vishing* y cómo funciona?
- Cómo funciona las estafas tipo BEC
- Troyanos bancarios
- Compromiso de credenciales de pago (*carding*)

3.4. Módulo 4: Evidencia Digital

3.4.1. Descripción general

Una de las dificultades para afrontar los delitos en entornos digitales es la volatilidad de la información que se maneja en el momento; por ello, es necesario que el estudiante logre aplicar no sólo los conceptos teóricos de las tipologías del delito, sino la forma de preservar la evidencia digital para que ésta no sea eliminada o alterada.

En este módulo, el estudiante debe aplicar técnicamente cómo se lleva a cabo el proceso de identificación, preservación y recolección de la evidencia digital salvaguardando el principio de conservación de la cadena de custodia.

3.4.2. Desglose de contenidos

- ¿Qué es la informática forense?
- Norma ISO/IEC 27037 establece las directrices para la identificación, recopilación, adquisición y preservación de evidencia digital
- Talleres prácticos

3.5. Módulo 5: Investigación e inteligencia

3.5.1. Descripción general

Este módulo será el más práctico para el estudiante; se le enseñará el tratamiento a la víctima, prestando especial atención al proceso de recogida de la denuncia y la metodología que se debe emplear para una correcta preservación de la evidencia digital y cómo aplicar los mecanismos judiciales para abordar la investigación del delito.

Así mismo, debe aprender a procesar la escena del delito de acuerdo a los principios de preservación de los elementos materiales de prueba y evidencia física, sabiendo identificar aquellas evidencias relacionadas con los delitos tecnológicos.

Por otra parte, es importante que el estudiante aprenda a plasmar en un informe de policía judicial, no sólo el conocimiento técnico-científico aplicado en los métodos y procesos, sino también las formas en que se desarrolló la investigación siguiendo la trazabilidad tanto de las actividades como de la evidencia digital.

3.5.2. Desglose de contenidos

- Recepción de la denuncia relacionado con medios informáticos
- Actos urgentes – casuística.
- Tendencias y principales modus operandi
- Manejo del lugar de los hechos escena digital
- Cadena de custodia
- Registros. Recogida y conservación de evidencias. Descripción.

- Guías para solicitudes de preservación a plataformas digitales
- Cooperación policial
- Trazabilidad de criptoactivos, tipologías de ciberlavado y organizaciones criminales. Requerimientos policiales a exchangers
- Programa Metodológico (órdenes a policía judicial y elaboración de informes)
- Talleres prácticos

3.6. Módulo 6: OSINT

3.6.1. Descripción general

Este módulo permite, por un lado, conocer las diferentes fuentes de información abiertas existentes en internet para emplearlas en beneficio de la investigación, y por otro aprender una metodología que permita explotar estos contenidos en beneficio de la investigación.

El propósito es que el estudiante pueda aplicar de forma metodológica unas técnicas que le permitan extraer información de interés para poder elaborar inteligencia criminal. Así de esta manera estará en disposición, no solo de dar respuesta a las demandas de inteligencia de las propias investigaciones, sino también abrir nuevas vías de investigación o complementar actuaciones en curso.

3.6.2. Desglose de contenidos

- Metodología OSINT
- Navegadores Chrome, Firefox
- Navegador Tor, máquinas virtuales
- Motores de búsqueda
- Búsqueda de redes sociales y comunidades en línea
- Investigando billeteras de criptomonedas (Herramientas OSINT para la trazabilidad de transacciones e identificación de cuentas de depósito de exchanges)
- Fundamentos básicos de Foca, Maltego, Shodan

3.7. Módulo 7: Cooperación Internacional

3.7.1. Descripción general

Es necesario conocer la legislación que ha nacido en el derecho internacional respecto a la cibercriminalidad, por ende, el estudiante aprenderá cómo se llevan a cabo los mecanismos de cooperación según los tratados internacionales; para aplicar los conceptos teóricos, técnicos y judiciales en la identificación de actividades delictivas trasnacionales.

3.7.2. Desglose de contenidos

- Convenio de Budapest
- II Protocolo adicional Convenio de Budapest

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

- Requerimiento s judiciales a plataformas digitales
- Introducción de la prueba electrónica transfronteriza en el proceso penal
- Procedimientos de solicitud de apoyo a INTERPOL y EUROPOL
- Delito Transnacional una mirada desde REMJA- EUROPOL- EUROJUST-Red de Fiscales de Iberoamérica y Red CibEL@.

4. CONSIDERACIONES FINALES

Dado que en 2021 ha sido imposible realizar un mapeo de centros especializados en AL, es conveniente empezarlo a lo largo de 2022 y mantenerlo abierto en el futuro. El LAC4 puede beneficiarse de estos contactos, llegar a acuerdos con los de mayor interés y mantener la iniciativa en el futuro. Las redes CiberRed y CibEL@ pueden canalizar el inicio de este proceso.

Finalmente, cabe recomendar a los países que dispongan de un modelo de examen de certificación en función de los niveles y módulos, que en el futuro puedan ser interoperables. Mientras, las certificaciones del Consejo de Europa y del *European Cybercrime Training and Education Gropup* (ECTEG) pueden ser una buena referencia.

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA EXPERTISE FRANCE
Socios coordinadores iila CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

ANEXO I: FICHAS RESUMEN

Módulo 1: Conceptos básicos	
Descripción	El propósito de este módulo es introducir al estudiante en el lenguaje técnico que se utiliza de acuerdo a los componentes de un sistema informático, adoptando una terminología común y presentando unos conceptos básicos en la materia sobre los que se basará la capacitación. Así mismo, introducir las nociones a la terminología judicial relacionada con los ilícitos penales cometidos en entornos digitales.

- Historia del computador, identificación de sus partes y su funcionamiento
- Qué son las TICS - Tecnología de la Información y las comunicaciones
- Redes sociales: Qué es y cómo funciona, función principal, tipos de redes sociales, redes de mensajería, diferencia entre social media y red social.
- Plataformas digitales que brindan servicio de correo electrónico, partes de un correo electrónico, identificación de encabezados
- Interconexión: topologías, redes, sistemas, seguridad
- Ecosistema de internet: Compuesta por tres capas. Primera Capa: Infraestructura: Servidores, ISP, torres, satélites, entre otros.
- Segunda Capa: Lógica: Protocolo IP, ICANN, nombres de dominios, RIR.
- Tercera Capa: Social y Económica
- Conceptos básicos sobre blockchain y criptoactivos.
- Glosario de términos (INCIBE).
- Conocer la función que cumplen a nivel ciber las Instituciones: policiales, Fiscalías, CERTs, centros tecnológicos. A nivel de la propia institución realizar especial énfasis en su estructura.

Módulo 2: Marco Legal	
Descripción	Este módulo está diseñado para abordar la legislación internacional que tiene relación de forma directa o indirecta con la lucha contra la delincuencia en la red. Aunque existe una normativa transnacional que puede servir como referencia, cada país tiene adaptado a su derecho interno este fenómeno.

	Por todo ello, este punto ofrece conocer el marco jurídico de referencia, tanto en materia de lucha contra la ciber-delincuencia, como también aquella normativa existente que atañe a los derechos humanos y su posible vulneración a través de las nuevas tecnologías, con el fin de proteger la integridad de los datos personales de cada internauta.

- Legislación penal y procesal – tipificación.
- Jurisprudencia penal y procesal.
- Normativa administrativa de interés
- Normatividad Agente Encubierto Virtual
- Legislación internacional.
- Estadísticas delincuenciales y judiciales (sentencias).
- Derechos Humanos en la red (poblaciones vulnerables Casuística – Genocidio Vs Facebook en pleno Siglo XXI)
- Ley de Protección de Datos y privacidad (legislación).
- Normatividad de Criptoactivos desarrollada por cada país (derecho comparado).
- Estrategias nacionales aplicado a cada país.

Módulo 3: Tipologías	
Descripción	La delincuencia en la red está en constante evolución y la complejidad de las conductas desarrolladas en este entorno complican su identificación. Para enfrentarse con solvencia a esta nueva realidad, el investigador debe conocer tanto las principales tipologías como los modus operandi relacionados con ellas. Aquí, el estudiante, identificará no sólo las actividades delictivas en cuestión, sino también las formas de hacerle frente a ciertos delitos en los entornos digitales. Comprender la diversidad de las modalidades es necesario para evaluar los métodos de investigación judicial que mejor se ajusten de acuerdo al tipo de delito.

- Acceso abusivo a un sistema informático
- ¿Qué es la ingeniería social y cuáles son sus técnicas?
- ¿Qué es el criptojaking y minería de datos?
- Violación de datos personales
- ¿Qué es el SIM Swapping?
- Suplantación de páginas web

- Uso de software malicioso
- ¿Qué es el ransomware?
- Hurto por medios informáticos
- ¿Qué es el phishing, smishing y vishing y cómo funciona?
- Cómo funciona las estafas tipo BEC
- Troyanos bancarios
- Compromiso de credenciales de pago (carding)

Módulo 4: Evidencia Digital	
Descripción	Una de las dificultades para afrontar los delitos en entornos digitales es la volatilidad de la información que se maneja en el momento; por ello, es necesario que el estudiante logre aplicar no sólo los conceptos teóricos de las tipologías del delito, sino la forma de preservar la evidencia digital para que ésta no sea eliminada o alterada. En este módulo, el estudiante debe aplicar técnicamente cómo se lleva a cabo el proceso de identificación, preservación y recolección de la evidencia digital salvaguardando el principio de conservación de la cadena de custodia.

- ¿Qué es la informática forense?
- Norma ISO/IEC 27037 establece las directrices para la identificación, recopilación, adquisición y preservación de evidencia digital
- Talleres prácticos

Módulo 5: Investigación e inteligencia	
Descripción	Este módulo será el más práctico para el estudiante; se le enseñará el tratamiento a la víctima, prestando especial atención al proceso de recogida de la denuncia y la metodología que se debe emplear para una correcta preservación de la evidencia digital y cómo aplicar los mecanismos judiciales para abordar la investigación del delito.

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA · EXPERTISE FRANCE
Socios coordinadores iila · CAMÕES INSTITUTO DA COOPERAÇÃO E DA LÍNGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

	Así mismo, debe aprender a procesar la escena del delito de acuerdo a los principios de preservación de los elementos materiales de prueba y evidencia física, sabiendo identificar aquellas evidencias relacionadas con los delitos tecnológicos. Por otra parte, es importante que el estudiante aprenda a plasmar en un informe de policía judicial, no sólo el conocimiento técnico-científico aplicado en los métodos y procesos, sino también las formas en que se desarrolló la investigación siguiendo la trazabilidad tanto de las actividades como de la evidencia digital.
- Recogida de denuncia. - Recepción de la denuncia relacionado con medios informáticos - Actos urgentes – casuística. - Tendencias y principales modus operandi - Manejo del lugar de los hechos escena digital - Cadena de custodia - Registros. Recogida y conservación de evidencias. Descripción. - Guías para solicitudes de preservación a plataformas digitales - Cooperación policial - Trazabilidad de criptoactivos, tipologías de ciberlavado y organizaciones criminales. Requerimientos policiales a exchangers - Programa Metodológico (órdenes a policía judicial y elaboración de informes) - Talleres prácticos	

Módulo 6: OSINT	
Descripción	Este módulo permite, por un lado, conocer las diferentes fuentes de información abiertas existentes en internet para emplearlas en beneficio de la investigación, y por otro aprender una metodología que permita explotar estos contenidos en beneficio de la investigación. El propósito es que el estudiante pueda aplicar de forma metodológica unas técnicas que le permitan extraer información de interés para poder elaborar inteligencia criminal. Así de esta manera estará en disposición, no solo de dar respuesta a las demandas de inteligencia de las propias investigaciones, sino también abrir nuevas vías de investigación o complementar actuaciones en curso.

- Metodología OSINT
- Navegadores Chrome, Firefox
- Navegador Tor, máquinas virtuales
- Motores de búsqueda
- Búsqueda de redes sociales y comunidades en línea
- Investigando billeteras de criptomonedas (Herramientas OSINT para la trazabili-dad de transacciones e identificación de cuentas de depósito de exchanges)
- Fundamentos básicos de Foca, Maltego, Shodan

Módulo 7: Cooperación Internacional	
Descripción	Es necesario conocer la legislación que ha nacido en el derecho internacional respecto a la cibercriminalidad, por ende, el estudiante aprenderá cómo se llevan a cabo los mecanismos de cooperación según los tratados internacionales; para aplicar los conceptos teóricos, técnicos y judiciales en la identificación de actividades delictivas trasnacionales.

- Convenio de Budapest
- II Protocolo adicional Convenio de Budapest
- Requerimientos judiciales a plataformas digitales
- Introducción de la prueba electrónica transfronteriza en el proceso penal
- Procedimientos de solicitud de apoyo a INTERPOL y EUROPOL
- Delito Transnacional una mirada desde REMJA- EUROPOL- EUROJUST-Red de Fiscales de Iberoamérica y red Cibel@.

Programa liderado por FIIAPP COOPERACIÓN ESPAÑOLA EXPERTISE FRANCE
Socios coordinadores iila CAMÕES INSTITUTO DA COOPERAÇÃO E DA LÍNGUA PORTUGAL
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Programa liderado por
FIIAPP COOPERACIÓN ESPAÑOLA
EXPERTISE FRANCE
Socios coordinadores
iila
CAMÕES INSTITUTO DA COOPERAÇÃO E DA LÍNGUA PORTUGAL
MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS
PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA