SERIE DE MÓDULOS UNIVERSITARIOS

Ciberdelincuencia

GUÍA DIDÁCTICA

UNODC

La Declaración de Doha:
PROMOVER UNA CULTURA
DE LEGALIDAD

educación para la justicia

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO

EDUCACIÓN PARA LA JUSTICIA
SERIE DE MÓDULOS UNIVERSITARIOS

Ciberdelincuencia

GUÍA DIDÁCTICA PARA DOCENTES

NACIONES UNIDAS
Viena, 2020

Esta guía didáctica es un recurso para los catedráticos.

Esta guía didáctica ha sido desarrollado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) bajo su iniciativa Educación para la Justicia (E4J, por sus siglas en inglés) en línea con su Programa Global para la Implementación de la Declaración de Doha. Forma parte de la serie de Módulos Universitarios sobre ciber-delincuencia de E4J. La totalidad de los materiales de E4J incluye módulos universitarios sobre integridad y ética, lucha contra la corrupción, prevención del delito y justicia penal, delincuencia organizada, trata de personas y tráfico ilícito de migrantes, armas de fuego, delitos contra la vida silvestre, los bosques y la pesca, y lucha contra el terrorismo, además de ciber-delincuencia.

Todos los módulos universitarios de E4J incluyen sugerencias para la realización de ejercicios en clase, evaluación de estudiantes, presentaciones y otras herramientas de enseñanza que los profesores o capacitadores pueden adaptar a sus propios contextos, e integrar dentro de cursos o programas de nivel universitario ya existentes. Este Módulo propone un esquema para una clase de tres horas, pero puede utilizare para presentaciones de menor o mayor duración.

Todos los módulos universitarios de E4J toman en consideración investigaciones y debates académicos existentes y pueden contener información, opiniones y declaraciones de una variedad de fuentes, incluyendo reportes de prensa y de expertos independientes. Las referencias a recursos externos fueron verificadas a la fecha de su publicación. Sin embargo, dado que los sitios web de terceros podrían sufrir modificaciones, le rogamos *nos contacte* si detecta una referencia equivocada o es redirigido a un sitio web con contenido inadecuado. También le solicitamos nos informe en caso de detectar que alguna publicación está vinculada a una versión o sitio web no oficial.

Pese a haber realizado una cuidadosa traducción de este módulo para asegurarnos una traducción al español precisa, la versión oficialmente aprobada es la versión en idioma inglés. Por ende, en caso de duda, le rogamos consultar la correspondiente versión en inglés. Los hipervínculos en el texto llevan a los textos originales en inglés. El género gramatical masculino se utiliza de una manera neutra para referirse a todos los miembros de una especie, sin distinción de sexos.

Condiciones de uso y descargos de responsabilidad para los módulos universitarios.

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites.

El presente documento no ha pasado por los servicios de edición.

Índice

Mensaje de bienvenida

Bienvenidos a la serie de módulos universitarios sobre delitos cibernéticos de Educación para la Justicia (E4J). El equipo de desarrollo de la serie de módulos universitarios sobre delitos cibernéticos ha trabajo intensamente para encontrar los recursos interculturales más relevantes. El delito cibernético es un problema global creciente. Ya sea que eres una pequeña empresa o una empresa que pertenece a la lista de las 500 mejores empresas de los Estados Unidos, estés comprando tu primer teléfono inteligente o estés estudiando para ser un experto en seguridad cibernética, necesitas estar informado sobre este delito.

Internet permite oportunidades de educación y económicas más allá de lo que el mundo jamás haya visto. Sin embargo, esta herramienta da oportunidades sin precedentes para causar daño. Al abusar de la tecnología, los delincuentes cibernéticos pueden arruinar negocios e incluso vidas. Muchas organizaciones del mundo luchan para parar a los delincuentes cibernéticos y ayudar a que los sistemas sean más seguros. No obstante, uno de los mejores métodos para la prevención es la educación.

La serie de módulos universitarios de E4J sobre delitos cibernéticos reúne recursos de todo el mundo relacionados con el delito cibernético, la legislación, la investigación y la prevención. Estos módulos abarcan muchos aspectos de este complejo y fascinante campo, e incluyen tanto conceptos teóricos como conocimientos prácticos. Los módulos presentan temas y recursos requeridos para una educación integral sobre diversos aspectos de los delitos cibernéticos, incluyendo su investigación y prevención.

Los módulos han sido escritos por profesores en ejercicio teniendo en cuenta a los docentes. Nuestro propósito ha sido diseñar una estructura que brinde el mejor apoyo para crear un nuevo curso o nueva serie de cursos, con el menor esfuerzo posible. Sabemos que crear un

curso nuevo usted solo es difícil, especialmente en nuevas áreas de estudio como el delito cibernético. Estos módulos darán a los docentes todas las herramientas que necesiten para desarrollar un excelente programa de estudios.

Visualizamos a un docente utilizando estos módulos para crear un curso que cumpla con las necesidades de sus estudiantes. Nos hemos esforzado para que cada módulo sea lo más independiente posible, a la vez que encaja en un tema general. Alentamos a los docentes a utilizar los módulos de todas las guías didácticas para docentes disponibles para crear un curso especializado que cumpla con los objetivos de educación propios. Por ejemplo, los módulos de la serie de módulos universitarios sobre integridad y ética de E4J se pueden combinar con otros módulos sobre delitos cibernéticos en un curso práctico para los estudiantes que verse sobre la seguridad cibernética y la lucha contra el *bullying* cibernético.

La tecnología y el delito cibernético evolucionan rápidamente. Estos módulos incluyen conceptos centrales para entender el problema del delito cibernético. Sin embargo, los docentes deben ser conscientes de los cambios de panorama con este tipo de delito. Esto es real en especial para las legislaciones sobre delitos cibernéticos locales las cuales se crean y revisan constantemente. Por ejemplo, el *bullying* cibernético es un concepto tan nuevo que muchos países aún no han promulgado una ley relacionada con este delito. Ahora más que nunca las personas tienen acceso a tecnologías como los teléfonos inteligentes y si el hostigamiento en línea aún no es un tema explorado por los legisladores en su país, es probable que lo sea en el futuro. Ahora es el momento para enseñar a la generación futura sobre cómo responder a los tipos de delitos cibernéticos actuales e inminentes de una manera saludable y segura.

Además, los Estados están examinando sus opciones de guerra cibernética y, así como en las guerras tradicionales, habrá consecuencias negativas para los ciudadanos. La educación sobre temas de delitos cibernéticos puede facilitar un diálogo informado y resoluciones pacíficas de los conflictos cibernéticos. Por lo tanto, el mundo necesita desesperadamente un mejor entendimiento del estado actual del delito cibernético, la seguridad cibernética y el ciberespacio en general.

El delito cibernético supone muchos desafíos, pero trabajando juntos podemos hacer de internet un lugar más seguro, protegido y productivo. Nos gustaría agradecerles a ustedes, los docentes, por ayudarnos a enseñar a las próximas generaciones sobre delitos cibernéticos y su prevención.

Resumen ejecutivo

La serie de módulos universitarios de E4J sobre delitos cibernéticos provee a los docentes con guías y recursos para diseñar un curso completo e interdisciplinario sobre delitos cibernéticos. Los módulos dentro de la serie presentan temas y recursos requeridos para una educación integral sobre diversos aspectos de los delitos cibernéticos y su investigación. Los módulos abarcan tendencias, teorías, perspectivas, leyes, medidas y prácticas acerca de los delitos cibernéticos mediante una perspectiva multidisciplinaria.

La guía didáctica para docentes y los 14 módulos son el resultado de un trabajo de líderes expertos y académicos de más de 25 países de seis continentes diferentes. Los módulos abarcan muchos aspectos de este campo sumamente pertinentes, e incluye tanto conceptos teóricos como conocimientos prácticos:

El módulo 1 sirve como una introducción a los delitos cibernéticos e incluye los conceptos clave relacionados con la informática, conectividad mundial, uso de la tecnología y tendencias de delitos cibernéticos, y los desafíos técnicos, legales, éticos y operacionales relacionados con el delito cibernético y su prevención.

El módulo 2 abarca las categorías generales de delitos cibernéticos, particularmente los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, los delitos relacionados con la informática y los contenidos y los tipos de delitos cibernéticos incluidos dentro de estas categorías.

El módulo 3 describe el panorama legal relacionado con el delito cibernético, resalta la necesidad de armonizar la legislación y describe la relación entre las leyes sobre delitos cibernéticos y los derechos humanos. Se presta especial atención a la necesidad de tener leyes sobre delitos cibernéticos para cumplir con el derecho de los derechos humanos y cualquier limitación a ellos debe estar en conformidad con sus normas y principios.

El módulo 4 presenta un resumen del análisis forense digital y las pruebas electrónicas, en particular observando el proceso del análisis forense digital, las prácticas comunes del análisis forense digital, los estándares del análisis forense digital y las pruebas electrónicas y las buenas prácticas del análisis forense digital.

El módulo 5 examina una variedad de partes interesadas (es decir, agencias, organizaciones, empresas e individuos) y sus funciones en las investigaciones de delitos cibernéticos, así como la denuncia de estos delitos, los retos que plantean las investigaciones y el papel de la gestión del conocimiento en las investigaciones de los delitos cibernéticos.

El módulo 6 trata sobre el análisis forense digital y las investigaciones de delitos cibernéticos. Este módulo explora las obligaciones legales y éticas de los investigadores de delitos cibernéticos y profesionales del análisis forense digital, las buenas prácticas en la gestión de pruebas digitales, su análisis, la comunicación de los resultados del análisis forense digital y la evaluación de pruebas digitales.

El módulo 7 presenta una exploración profunda de la cooperación internacional en la medida que se relaciona con el delito cibernético, particularmente de temas de soberanía y jurisdicción, factores que influencian la cooperación internacional, mecanismos formales e informales de cooperación internacional, recopilación de pruebas extraterritoriales y el déficit nacional en la capacidad para conducir investigaciones de delitos cibernéticos.

El módulo 8 explora de manera crítica las estrategias de seguridad cibernética que los países utilizan para proteger las tecnologías de la información y la comunicación (TIC), las características y ciclos de vida de estas estrategias, los marcos utilizados para analizar estas estrategias, así como también los esfuerzos de los países en materia de seguridad cibernética y prevención y la naturaleza y el alcance de las capacidades de estos para proteger las TIC.

El módulo 9 abarca los riesgos de la seguridad cibernética y los conceptos relacionados al riesgo, la investigación sobre la seguridad cibernética y la divulgación de las vulnerabilidades, las estrategias y técnicas de prevención situacional de delitos y las medidas usables de seguridad cibernética que se diseñan para identificar amenazas y vulnerabilidades, y para prevenir, detectar, responder y recuperarse de las amenazas materializadas.

El módulo 10 examina críticamente el impacto de la agregación de datos, así como el impacto de la recopilación, almacenamiento, análisis, uso y divulgación de datos sobre la privacidad y seguridad. Específicamente, este módulo abarca la privacidad como un derecho humano, la relación entre privacidad y seguridad, las maneras en las que el delito cibernético pone en peligro la privacidad y seguridad de datos, y la protección de datos y las leyes de notificación de filtraciones, así como también las maneras en las que los datos son (o pueden ser) protegidos para asegurar a las personas, las propiedades y la información.

El módulo 11 examina la propiedad intelectual y su acceso ilegal, distribución y uso propiciados por medios cibernéticos. Específicamente, este módulo examina qué es la propiedad intelectual, los tipos de propiedad intelectual, las causas, razones y justificaciones de delitos en materia de derechos de autor y de marca propiciados por medios cibernéticos, y medidas protectoras y preventivas contra esos delitos.

El módulo 12 se centra en los delitos cibernéticos interpersonales e incluye material de abuso sexual de niños en línea, acaso cibernético, hostigamiento cibernético, abuso sexual a través

de imágenes, *bullying* cibernético, analizando en particular las dimensiones de género de estos delitos cibernéticos, las maneras en las que se perpetúan, las leyes enfocadas en estos, y la respuesta y esfuerzos mundiales de prevención.

El módulo 13 examina los tipos de delitos que se consideran delitos cibernéticos organizados y los tipos de grupos delictivos organizados que se dedican a los delitos cibernéticos. También se examinan las medidas utilizadas para combatir los delitos cibernéticos organizados.

El módulo 14 examina temas como el hacktivismo, el terrorismo, el espionaje, las campañas de desinformación y la guerra en el ciberespacio, así como también las perspectivas y respuestas nacionales e internacionales a estas actividades cibernéticas. El propósito de este módulo es analizar estos temas e identificar los debates actuales y los puntos de vista conflictivos sobre estos temas dentro y entre los países.

Los módulos, por diseño, contienen elementos que pueden ser personalizados por los docentes de cualquier país para adecuarlos a sus necesidades educacionales. Aunque la serie de módulos universitarios de E4J sobre delitos cibernéticos intenta ser lo más exhaustiva posible, un solo curso puede sentar la base de los conceptos claves relacionados con los delitos cibernéticos. Cada subtema dentro del módulo se puede analizar con más detalle e incluso puede expandirse en su propio curso. Por lo tanto, hemos incluido recursos opcionales para los docentes a fin de desarrollar su conocimiento en áreas relacionadas. La meta de estos módulos es que el conocimiento mundial sobre el delito cibernético progrese, incluyendo su investigación y prevención. Si bien estos módulos proveen una sólida base acerca del conocimiento sobre el delito cibernético, alentamos a los docentes a sumar sus propias experiencias y personalizar el material educativo y los ejemplos para adaptarlos al contexto local de manera que desarrollen el contenido educativo de mejor manera.

El propósito de esta guía es explicar el proceso mental detrás del desarrollo de estos módulos y los principios que orientaron su desarrollo.

Introducción

Educación para la Justicia (E4J) se desarrolló como parte del Programa Global de la UNODC para apoyar objetivos clave de la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco Más Amplio del Programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y Promover el Estado de Derecho a Nivel Nacional e Internacional y la Participación Pública (la Declaración de Doha), adoptada por el 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal del 2015, y

refrendada por la Asamblea General de las Naciones Unidas en su resolución 70/174 (A/RES/70/174). La declaración reconoce la importancia fundamental de la educación universal para niños y jóvenes como clave para la prevención del delito, terrorismo y corrupción, así como también para promover el desarrollo sostenible.

El objetivo de la iniciativa E4J es crear una cultura de legalidad entre niños y jóvenes a través de la provisión de materiales educativos apropiados para la edad en temas relacionados con justicia penal, prevención del delito y Estado de derecho, y la integración de esos materiales en el plan de estudios de todos los niveles de educación. En el nivel universitario, E4J brinda apoyo a los académicos en sus actividades de investigación y enseñanza relacionadas con las áreas de mandato de la UNODC, que incluye la prevención del delito, la lucha contra la corrupción, la delincuencia organizada, la trata de personas y tráfico de migrantes, las armas de fuego, los delitos cibernéticos, los delitos contra la vida silvestre, los bosques y la pesca, la lucha contra el terrorismo, y también la integridad y ética. Esta serie de módulos abarca una de esas áreas de mandato: el delito cibernético.

Pocas actividades personales y profesionales han permanecido intactas debido a las tecnologías de la información y la comunicación (TIC). Por esta razón, es importante la educación de los usuarios sobre las TIC. También su educación es crucial en vista del déficit en la capacidad mundial actual para lidiar con los delitos cibernéticos y los temas relacionados con la seguridad cibernética (UNODC, 2013; Frost & Sullivan Executive Briefing, 2017). Las herramientas y los marcos de evaluación que se han desarrollado para analizar las capacidades en materia de seguridad cibernética de países, organizaciones y empresas claramente lo demuestra (para mayor información consulte Delitos Cibernéticos-Módulo 8).

El delito cibernético requiere una respuesta multidimensional que combine la educación, las leyes, la conciencia social, la capacitación de los organismos encargados de hacer cumplir las leyes, la cooperación de los intermediarios de internet, entre otros. En este sentido, los déficits de capacidad nacional necesitan subsanarse educando a las generaciones de profesionales actuales y futuras y brindando formación en temas de delitos cibernéticos y seguridad cibernética a los profesionales que no pertenecen al ámbito de la justicia penal, las leyes y la informática. De hecho, el déficit actual existe debido a la falta de un enfoque multidisciplinario sobre delitos cibernéticos y seguridad cibernética. Para llenar este vacío, la serie de módulos sobre delitos cibernéticos utiliza un enfoque multidisciplinario a fin de analizar los temas principales sobre delitos cibernéticos, estrategias y medidas de seguridad cibernética, pruebas digitales, análisis forense digital, leyes sobre delitos cibernéticos y prácticas investigativas. Particularmente, los módulos abarcan las buenas prácticas en la prevención de delitos cibernéticos y seguridad cibernética identificadas por los países del mundo en el Proyecto del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013. Estas mejores prácticas incluyen el desarrollo de una base de conocimientos sólida sobre delitos cibernéticos y seguridad cibernética; campañas de educación y sensibilización; en general, capacidad en

materia de justicia penal y, en particular, capacidad para hacer cumplir la ley; marcos legales nacionales, regionales e internacionales sobre delitos cibernéticos y su armonización; y cooperación internacional entre organismos y organizaciones nacionales, regionales e internacionales, así como también el sector privado, en asuntos de delitos cibernéticos.

La interconexión e interdependencia de las sociedades ha brindado oportunidades inconmensurables para el crecimiento económico, empleo y comunicaciones y conexiones interpersonales. Sin embargo, esta interconexión e interdependencia ha creado numerosas vulnerabilidades que pueden ser (y han sido) aprovechadas por diferentes actores que ya no están restringidos por el tiempo y espacio al cometer una actividad ilegal. Estos delincuentes cibernéticos pueden cometer delitos cibernéticos independientemente de su ubicación geográfica a cualquier momento y en cualquier lugar del mundo que cuente con conexión a internet. Por estas razones, la prevención de delitos cibernéticos y la seguridad cibernética son de suma importancia.

Además de analizar la prevención de delitos cibernéticos y la seguridad cibernética, los módulos también abarcan temas centrales relacionados con los delitos cibernéticos, tales como la privacidad y protección de datos. La privacidad y protección de datos no solo salvaguardan a las personas frente a los delitos cibernéticos al protegerlas a ellas y a sus datos de los delincuentes cibernéticos, sino que también permiten y facilitan a las personas ejercer sus derechos humanos en línea. Estos módulos también introducen temas críticos sobre delitos cibernéticos y seguridad cibernética, causas y factores que influyen en los delitos cibernéticos y los motivos, tácticas, objetivos y métodos de operación de estos delincuentes, así como también qué hace que las personas, empresas o gobiernos sean blanco de estos delitos y qué se puede hacer para prevenirlos y proteger a los afectados.

La serie de módulos universitarios de E4J sobre delitos cibernético incluye los siguientes módulos:

- Módulo 1: Introducción al Delito Cibernético
- Módulo 2: Tipos Generales de Delitos Cibernéticos
- Módulo 3: Marcos Jurídicos y Derechos Humanos
- Módulo 4: Introducción al Análisis Forense Digital
- Módulo 5: Investigaciones de Delitos Cibernéticos
- Módulo 6: Aspectos Prácticos de Investigaciones de Delitos Cibernéticos y Análisis Forense Digital
- Módulo 7: Cooperación Internacional contra los Delitos Cibernéticos
- Módulo 8: Seguridad Cibernética y Prevención del Delito Cibernético: Estrategias, Políticas y Programas
- Módulo 9: Seguridad Cibernética y Prevención del Delito Cibernético: Aplicaciones y Medidas Prácticas

- Módulo 10: Privacidad y Protección de Datos
- Módulo 11: Delitos contra la Propiedad Intelectual Propiciados por Medios Cibernéticos
- Módulo 12: Delitos Cibernéticos Interpersonales
- Módulo 13: Delitos Cibernéticos Organizados
- Módulo 14: Hacktivismo, Terrorismo, Espionaje, Campañas de Desinformación y Guerra en el Ciberespacio

Nótese que la secuencia de módulos está diseñada para ofrecer un conocimiento fundamental y se puede cambiar de manera flexible y modular dependiendo del nivel esperado dela clase. Los módulos reúnen teorías, investigaciones y práctica, y se desarrollaron en consulta con un grupo de expertos en educación. Todos los módulos combinan enfoques prácticos y teóricos para los temas específicos sobre delitos cibernéticos y siguen la misma estructura básica:

Introducción. Cada módulo incluye una introducción que se utiliza para establecer el interés, la necesidad y propósito del contenido, y provee un resumen del tema o temas tratados.

Objetivos de aprendizaje. Cada módulo incluye los objetivos de aprendizaje esperados en forma de logros de aprendizaje, que abarcan los logros de aprendizaje esperados (los objetivos de aprendizaje se analizan con mayor detalle en la siguiente sección de esta guía, «5.3. Logros de aprendizaje y herramientas de evaluación».

Temas clave. Cada módulo resalta los temas principales sobre el módulo. Se incluyen recuadros con casos interesantes y temas y preguntas de investigación que resaltan los temas cruciales sobre los delitos cibernéticos (p. ej., recuadros temáticos y de «¿Sabían que...?»), así como también, ejemplos interesantes y notas sobre los temas. Esta sección del módulo también incluye listas de referencias acerca de la literatura e investigación académica y profesional citados dentro del módulo, así como también referencias de casos y leyes dentro de este.

Ejercicios. Los ejercicios en cada módulo están diseñados para estimular la resolución de problemas y la capacidad de pensamiento crítico de los estudiantes. También se utilizan para evaluar el aprendizaje de los estudiantes y les permite aplicar lo que aprendieron en clase (estos ejercicios se exploran con mayor detalle en la siguiente sección de esta guía, «5.3. Logros de aprendizaje y herramientas de evaluación»). Los docentes tienen la posibilidad de adaptar y personalizar estos ejercicios para que encajen con sus necesidades y contexto local.

Lecturas principales y avanzadas. Cada módulo tiene lecturas principales y avanzadas. La sección de lecturas principales contiene literatura básica sobre el tema y el material tratado en el módulo, y se deben usar para el desarrollo de la clase o el curso. La sección de lecturas avanzadas incluye mayor información sobre los temas tratados en el módulo y pueden usarse para explorar los temas con más detalle, complementar lecturas básicas, desarrollar otras

clases o cursos enteros sobre los temas tratados o para adaptar el contenido a los antecedentes académicos de los estudiantes en la clase o la disciplina académica relacionada con el curso. Los docentes pueden incluir lecturas basadas en sus necesidades, habilidades y preferencias, así como también su acceso a estas.

> *¿Sabían que...?*
>
> La iniciativa de Educación para la Justicia (E4J) de la UNODC tiene una biblioteca de recursos que es de acceso abierto al material educativo. Para más información, visite: http://www.unodc.org/e4j-library.

Estas lecturas principales y avanzadas incluyen publicaciones de código abierto y cerrado. Las *publicaciones de código abierto* están disponibles de manera gratuita y sin ninguna licencia especial o compra del trabajo. Estas lecturas principales y avanzadas incluyen enlaces por donde se puede acceder a la publicación. Las *publicaciones de código cerrado* incluyen artículos de revistas académicas y libros que están disponibles solo mediante suscripciones a las bases de datos de revistas académicas (p. ej., Taylor and Francis, Sage, Jstor, Springer y Wiley, por mencionar algunos,) o para su compra. Sin embargo, existen excepciones. Para los artículos de revistas académicas, se pueden contactar a los autores y realizar una petición de su trabajo (los detalles de contacto de los autores se encuentran en los artículos). Estos artículos también pueden publicarse en sitios de investigación compartida como ResearchGate y Academic.edu. Si los artículos completos no están publicados en estos sitios, se puede contactar a los autores para solicitar esta información siempre que esta solicitud respete las leyes nacionales de propiedad intelectual. Para los libros, se puede contactar con los autores y solicitarles una copia de sus libros para su donación a una biblioteca universitaria.

> *Nota*
>
> Muchas de las lecturas principales y avanzadas están en inglés. Se puede contactar a la UNODC para recibir asistencia en la traducción de estas publicaciones a otros idiomas.

Estructura de clase recomendada. Cada módulo incluye una estructura de clase recomendada que incorpora múltiples modalidades de aprendizaje y la secuencia de temas y actividades sugeridas. La parte expositiva de la clase tiene como objetivo reforzar lo que aprendieron los estudiantes en las lecturas y los ejercicios, y se diseñan otras actividades de evaluación para aplicar lo que aprendieron en las lecturas. El desglose en los módulos está diseñado con base en una clase de tres horas. Los docentes pueden adaptar la estructura en función de sus necesidades y los horarios de la clase. Cada módulo se diseñó para incorporar aproximadamente doce horas teóricas de aprendizaje (alrededor de seis horas de tiempo de

preparación, tres horas de asistencia a clase y tres horas de evaluación/tareas). No obstante, los docentes pueden extender el contenido a más de una clase o un curso completo.

Evaluación del estudiante. Además de los ejercicios, cada módulo incluye preguntas de repaso para evaluar el aprendizaje del estudiante y otras formas de evaluación, como tareas asignadas, estudios de caso, trabajos grupales e instrucciones para la «prueba de conocimientos», que piden a los alumnos contestar una pregunta con base en la información provista para evaluar cuánto recuerdan y comprenden la información (la evaluación del estudiante se explora con mayor detalle en la siguiente sección de esta guía, «5.3 Logros de aprendizaje y herramientas de evaluación»).

Herramientas didácticas adicionales. Cada módulo contiene herramientas didácticas adicionales que pueden usarse dentro del curso, así como sitios web importantes que incluyen información general para el material tratado en el módulo, material similar al que se trató en el módulo o mayor información que la que se trató en el módulo, además de videos destinados a resaltar ciertas partes del módulo y usarse a criterio del docente para resaltar temas principales o para ilustrar temas tratados en el módulo (estas herramientas de enseñanza se exploran con mayor detalle en la siguiente sección de esta guía, «5. Métodos de enseñanza y aprendizaje»).

Los módulos no incluyen todos los temas. Los módulos están simplemente diseñados para resaltar los temas clave relacionados con los temas tratados en los módulos y para asistir a los docentes en la enseñanza de estos temas, brindando un marco básico para la clase y recomendando ejercicios, tareas y lecturas principales y avanzadas para los docentes, los estudiantes y otros interesados en aprender acerca del delito cibernético y temas relacionados con este. Los módulos no están diseñados específicamente para estudios especializados en delitos cibernéticos, pero sí para cada docente que esté interesado en integrar materiales relacionados con los delitos cibernéticos en cursos de otras disciplinas académicas o en añadir o crear cursos nuevos relacionados con los delitos cibernéticos a programas académicos. Los docentes de múltiples disciplinas pueden utilizar los módulos en el nivel de pregrado y posgrado.

Métodos de enseñanza y aprendizaje

Los módulos universitarios de E4J sobre delitos cibernéticos proveen materiales y herramientas pedagógicas para ayudar a los docentes a enseñar sobre delitos cibernéticos y temas relacionados con los delitos cibernéticos. Los módulos se diseñaron con diferentes estilos de aprendizaje, múltiples modalidades de aprendizaje, logros de aprendizaje y herramientas para la evaluación del estudiante en mente.

Estilos de aprendizaje

Las personas aprenden y retienen información de manera diferente. Debido a esto, los cursos deberían adaptarse a diferentes maneras de aprender. Los módulos sobre delitos cibernéticos están diseñados para adaptarse a diferentes estilos de aprendizaje, lo que se refiere a la manera en que la información se entiende, recuerda, expresa, aplica, sintetiza y evalúa. Existen diferentes estilos de aprendizaje, entre ellos están el visual, el auditivo, el lector-escritor, el kinestésico (también conocido como las modalidades VARK; Fleming y Mills, 1992):

- Los estudiantes *visuales* aprenden con sus ojos; es decir, ellos aprenden con base en lo que sus ojos ven, puede ser a partir de diapositivas de PowerPoint, figuras, gráficos, esquemas, imágenes o videos (para mencionar algunos).

- Los estudiantes *auditivos* aprenden con sus oídos. Estos estudiantes consumen y procesan la información que escuchan, como las exposiciones (es decir, es una forma de discurso donde la información se presenta, explica y analiza) o discusiones.

- Los estudiantes *lector-escritor*, como su nombre lo dice, aprenden leyendo el material y tomando notas sobre este.

- Los estudiantes *kinestésicos* aprenden al participar en una tarea (es decir, hacen algo). Ellos aprenden aplicando lo que aprendieron en estudios de caso y ejercicios prácticos.

Lo que se cree es que los estudiantes prefieren cierto estilo de aprendizaje y que la educación debería adaptarse a estos estilos. Sin embargo, la literatura no respalda esta teoría (Brown, McDaniel y Roediger, 2014).

¿Quiere aprender más acerca de la investigación sobre la enseñanza y aprendizaje en la educación superior?

Lea:

Ambrose, Susan, Michael W. Bridges, Michele DiPietro, Marsha C. Lovett, and Marie K. Norman. (2010). *How Learning Works: Seven Research-Based Principles for Smart Teaching*. Jossey-Bass.

Bain, Ken. (2004). *What the Best College Teachers Do*. Harvard University Press.

Brown, Peter, Mark McDaniel, and Henry L. Roediger. (2014). *Make It Stick: The Science of Successful Learning*. Harvard University Press.

Lang, James M. (2016). *Small Teaching: Everyday Lessons from the Science of Learning*. Jossey-Bass.

Segal, Mark (2013). *How To Train: A Practical Guide for Training and Working with Others*

Angele Attard, Emma Di Iorio, Koen Geven, Robert Santa (2010). *Student-Centred Learning - Toolkit for students, staff and higher education institutions*

Si bien es cierto que algunos estudiantes prefieren leer o escuchar la clase mientras que otros prefieren participar en discusiones o escribir, ninguna evidencia respalda la idea de que los estudiantes aprenden de manera efectiva cuando trabajan en su estilo de aprendizaje preferido. En efecto, algunos investigadores han descubierto que los estudiantes suelen equivocarse cuando predicen el tipo de actividad que produce el mejor aprendizaje para ellos. De hecho, el aprendizaje es más efectivo cuando requiere algún esfuerzo por parte del estudiante, lo que significa que los estudiantes pueden aprender de manera más eficaz cuando se les pide participar en actividades que ellos encuentran desafiantes.

Todo esto conduce a una conclusión importante acerca de los tipos de actividades de participación que deberían diseñarse para los estudiantes: *deben ser variados*. Si el docente no hace nada más que exponer, los estudiantes que no responden muy bien a las exposiciones —por ejemplo, porque tienen dificultad para prestar atención por largos periodos de tiempo— están en desventaja. Asimismo, si el docente no hace nada más que hacer que los estudiantes participen en debates, a aquellos estudiantes que les gustaría tener la oportunidad de leer o escuchar en silencio a un experto están en desventaja. Cuando los docentes organicen sus planes de clase para cualquiera de los módulos, deben considerar la manera de ofrecer diversos métodos para que los estudiantes se involucren de manera activa con el material de

aprendizaje. Todos los módulos sobre delitos cibernéticos contienen recomendaciones para una participación activa en diferentes maneras.

Metacognición

«La metacognición se refiere a la habilidad de las personas de entender su nivel de conocimiento y sus habilidades de aprendizaje» (Guía del docente sobre integridad y ética de E4J).

¿Desea saber más?

Consulte:

- E4J Integrity and Ethics Teaching Guide.
- How to Get the Most Out of Studying: Part 1 of 5, "Beliefs That Make You Fail... Or Succeed," https://www.youtube.com/watch?v=RH95h36NChI.
- How to Get the Most Out of Studying: Part 2 of 5, "What Students Should Know About How People Learn," https://www.youtube.com/watch?v=9O7y7XEC66M.
- How to Get the Most Out of Studying: Part 3 of 5, "Cognitive Principles for Optimizing Learning," https://www.youtube.com/watch?v=1xeHh5DnCIw.
- How to Get the Most Out of Studying: Part 4 of 5, "Putting Principles for Learning into Practice," https://www.youtube.com/watch?v=E9GrOxhYZdQ.
- How to Get the Most Out of Studying: Part 5 of 5, "I Blew the Exam, Now What?" https://www.youtube.com/watch?v=-QVRiMkdRsU.

Múltiples modalidades de aprendizaje

Los módulos contemplan múltiples estilos de aprendizaje al incluir exposiciones, discusiones, ejercicios, estudios de caso, escenarios hipotéticos, preguntas de repaso, asignación de tareas y herramientas técnicas adicionales, como videos y sitios web. Las partes expositivas, así como los videos, promueven el *aprendizaje pasivo del estudiante*. Para promover el *aprendizaje activo del estudiante*, las clases deben incorporar discusiones, ejercicios, estudios de caso, escenarios hipotéticos, preguntas de repaso, entre otras tareas (consulte, por ejemplo, Berkeley Center for Teaching & Learning y Yale Poorvu Center for Teaching and Learning). Debido a que algunos estudiantes prefieren trabajar solos (estudiantes *solitarios*) y otros en grupo (estudiantes *sociales*), tanto las tareas individuales como las grupales están contempladas en la serie de módulos sobre delitos cibernéticos. Por consiguiente, en los módulos se incorporan las múltiples modalidades de aprendizaje para reflejar la diferencia en estilos de aprendizaje y para promover el aprendizaje pasivo y activo.

Nota

Los docentes pueden adaptar los ejercicios y tareas en la serie de módulos sobre delitos cibernéticos para incorporar otras técnicas de aprendizaje activo.

Para mayor información sobre estas técnicas, consulte:
Berkeley Centre for Teaching & Learning, Active Learning Strategies, https://teaching.berkeley.edu/active-learning-strategies.
Yale Poorvu Center for Teaching and Learning, Active Learning, https://poorvucenter.yale.edu/ActiveLearning.

Los módulos se basan en modelos de aprendizaje participativo (aprender al resolver problemas utilizando su propia experiencia y habilidades) y modelos de aprendizaje experiencial (aprender mediante la experiencia), que promueven el aprendizaje mutuo y activo, el empoderamiento de los estudiantes y las reflexiones críticas sobre las ideas y la práctica. Los módulos se diseñaron de esta manera para estimular las formas de pensamiento más allá de la recordación básica y la memorización del contenido (es decir, habilidades de pensamiento crítico). Benjamin Bloom, un psicólogo educativo, desarrolló una taxonomía sobre el desarrollo cognitivo en 1953 (conocido como la taxonomía de Bloom), que incluye una variedad de habilidades cognitivas que se utilizan mayormente en el mundo académico. La taxonomía de Bloom (1953) identifica seis niveles o dominios cognitivos: *conocimiento* (destreza para recordar la información); *comprensión* (destreza para entender la información); *aplicación* (destreza para utilizar lo aprendido); *análisis* (destreza para analizar la información); *síntesis* (destreza para crear nuevos conocimientos a partir de combinar el conocimiento previo con otra información) y *evaluación* (destreza para juzgar la información) (consulte la figura 2). Estas habilidades cognitivas abarcan habilidades esenciales, como la *resolución de problemas* (la destreza para reconocer un problema, identificar estrategias para resolver un problema al proponer soluciones, evaluar estas soluciones tomando en cuenta la información contextual disponible y analizar los resultados de las soluciones propuestas) y el *pensamiento creativo*, según el cual las personas combinan su conocimiento, destrezas y habilidades actuales en maneras nuevas o únicas para solucionar problemas.

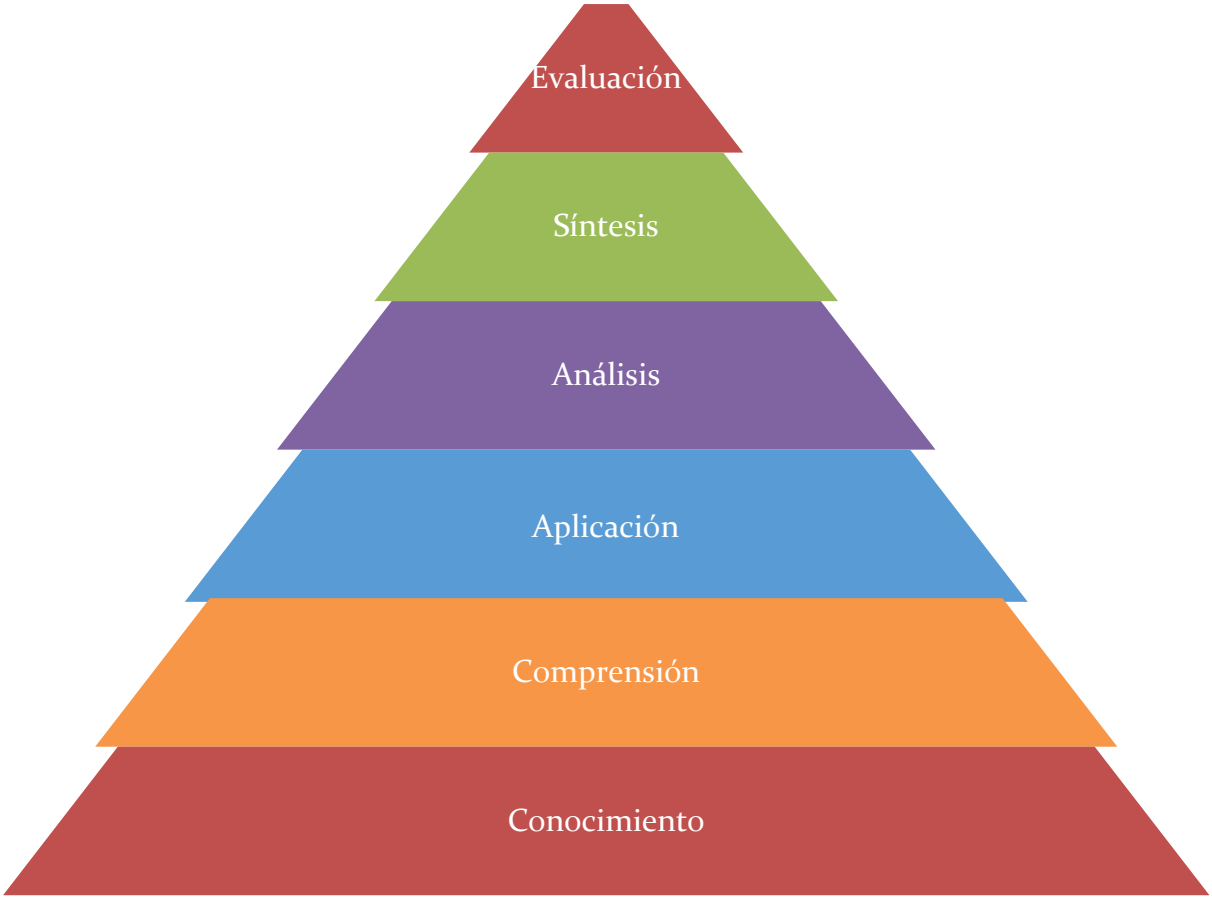

Figura 2 Taxonomía de Bloom (1953)

Anderson y Krathwohl revisaron la taxonomía de Bloom en 2011 (figura 3), cubriendo una serie de habilidades cognitivas desde el nivel más bajo de pensamiento hasta el más alto: *recordar*, *comprender*, *aplicar*, *analizar*, *evaluar* y *crear*. La taxonomía original y revisada de Bloom explica el aprendizaje del estudiante.

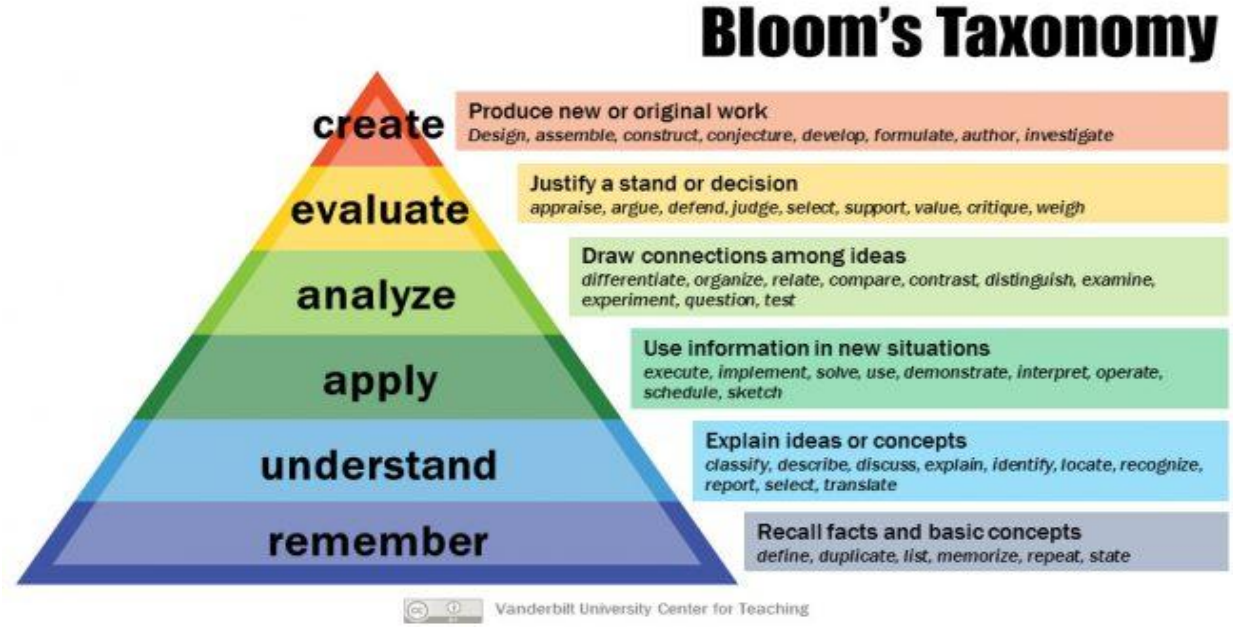

Figura 3 Taxonomía revisada de Bloom (2001)

Bloom's Taxonomy	Taxonomía de Bloom
create	crear
evaluate	evaluar
analyze	analizar
apply	aplicar
understand	comprender
remember	recordar

Produce new or original work *Design, assemble, construct, conjecture, develop, formulate, author, investigate*	**Producir trabajos nuevos u originales** *Diseñar, reunir, construir, conjeturar, desarrollar, formular, escribir, investigar*
Justify a stand or decision *appraise, argue, defend, judge, select, support, value, critique, weigh*	**Justificar una posición o decisión** *evaluar, argumentar, defender, juzgar, elegir, apoyar, valorar, criticar, sopesar*
Draw connections among ideas *differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test*	**Conectar ideas** *diferenciar, organizar, relacionar, comparar, contrastar, distinguir, examinar, experimentar, cuestionar, probar*
Use information in new situations *execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch*	**Utilizar información en situaciones nuevas** *ejecutar, implementar, resolver, utilizar, demostrar, interpretar, gestionar, programar, esbozar*
Explain ideas or concepts *classify, describe, discuss, explain, identify, locate, recognize, report, select, translate*	**Explicar ideas o conceptos** *clasificar, describir, discutir, explicar, identificar, localiza, reportar, seleccionar, traducir*
Recall facts and basic concepts *define, duplicate, list, memorize, repeat, state*	**Recordar hechos o conceptos básicos** *Definir, repetir, hacer listas, memorizar, repetir, describir*

Logros de aprendizaje y herramientas de evaluación

Los logros de aprendizaje identifican el conocimiento, actitudes, habilidades y destrezas de los estudiantes al indicar el tipo de comportamiento que deberían ser capaces de tener al finalizar el curso. Los logros de aprendizaje basados en la taxonomía revisada de Bloom (Anderson and Krathwohl, 2001) identifican las siguientes expectativas para el desempeño académico de los estudiantes: los estudiantes demuestran que saben algo (*recordar*), entienden algo (*comprender*), pueden aplicar lo que aprendieron (*aplicar*), pueden analizar la información (*analizar*), pueden evaluar la información (*evaluar*) y pueden desarrollar algo nuevo (*crear*).

Los logros de aprendizaje incluyen el logro observable que se espera de los estudiantes y que puede demostrarse mediante las herramientas de evaluación utilizadas en el curso. Los *objetivos de aprendizaje* definen lo que los estudiantes *deberían* aprender en el curso (es decir, lo que *deberían* ser *capaces de hacer* al finalizar el curso). Las *herramientas de evaluación* determinan si se cumplieron los logros de aprendizaje y en qué medida. De este modo, es imperativo que los objetivos de aprendizaje y las herramientas de evaluación están alineados. En palabras simples, el contenido de las herramientas de evaluación debería coincidir con los objetivos que se evalúan.

Hay varias herramientas de evaluación que se pueden utilizar para evaluar el aprendizaje del estudiante. Estas herramientas de evaluación pueden diseñarse para analizar de manera objetiva el comportamiento del estudiante o analizar el comportamiento de manera subjetiva (Schwarts, s. f.; Center for Advanced Research on Language Acquisition, s. f.). Las *evaluaciones objetivas* requieren que los estudiantes elijan una respuesta de las opciones provistas (Schwarts, s. f.). Estos tipos de evaluación incluyen *preguntas de opción múltiple,* donde los estudiantes deben elegir una de las respuestas disponibles para la pregunta o afirmación hecha o *preguntas de verdadero o falso*, donde los estudiantes determinan la veracidad de la afirmación (Center for Advanced Research on Language Acquisition, s. f.). Las evaluaciones objetivas tienen como objetivo principal examinar la destreza de los estudiantes para reconocer el contenido correcto y, si están diseñadas correctamente, para comprender el contenido (Schwartz, s. f.). Es importante mencionar que las evaluaciones objetivas también pueden acceder a otras habilidades cognitivas si se diseñan correctamente (Schwartz, s. f.).

Por lo contrario, las *evaluaciones subjetivas* pueden evaluar múltiples logros de aprendizaje más allá de los que las evaluaciones objetivas comúnmente evalúan, especialmente aquellos que se basan en las habilidades cognitivas como el análisis, la evaluación y la creación. Estos tipos de evaluación incluyen estudios de caso, ejercicios, tareas y preguntas de repaso (Schwartz, s. f.). En los módulos, las preguntas de repaso, por ejemplo, están diseñadas para evaluar las destrezas de los estudiantes para recordar, comprender, aplicar, analizar, evaluar o crear información. Las preguntas de repaso son una forma de evaluación subjetiva. Algunas preguntas de repaso tienen respuestas cortas diseñadas para evaluar las destrezas para recordar la información y respuestas largas diseñadas para evaluar la destreza para recordar, analizar, evaluar, organizar y sintetizar el material como respuesta a las preguntas. Los estudiantes también cuentan con ejercicios, estudios de caso, escenarios hipotéticos para «aplicar» las teorías y conceptos que aprendieron sobre casos o escenarios de delitos cibernéticos y evaluar soluciones actuales y desarrollar respuestas a los delitos cibernéticos.

¿Necesita ayuda para crear logros de aprendizaje y herramientas de evaluación del estudiante?

Muchas instituciones académicas brindan orientación sobre el desarrollo de logros de aprendizaje y herramientas de evaluación del estudiante basados en la taxonomía de Bloom (original y revisada). También se proporciona orientación sobre el lenguaje que se debe utilizar para redactar los logros de aprendizaje y lo que se debe evitar. Algunos ejemplos de sitios web son:

- Iowa State University, Center for Excellent in Teaching and Learning, Revised Bloom's Taxonomy. http://www.celt.iastate.edu/teaching/effective-teaching-practices/revised-blooms-taxonomy/.
- University of Toronto, Center for Teaching Support & Innovation, Writing Learning Outcomes Using Bloom's Revised Taxonomy. https://teaching.utoronto.ca/wp-content/uploads/2015/08/Learning-Outcomes-Using-Blooms-Taxonomy.pdf.
- Utica College, Bloom's Taxonomy of Measurable Verbs. https://www.utica.edu/academic/Assessment/new/Blooms%20Taxonomy%20-%20Best.pdf.

Por último, la enseñanza debería adaptarse a múltiples estilos de aprendizaje e incluir múltiples modalidades de aprendizaje para inspirar a los estudiantes a participar activamente en los cursos respondiendo a las preguntas para debatir (las que tienen como objetivo verificar la comprensión de los estudiantes sobre material del curso), participar en asignaciones grupales y aplicar y explicar su conocimiento mediante ejercicios, preguntas de repaso y asignaciones de tareas.

Directrices para la adaptación y diseño de los módulos

Los módulos universitarios de E4J sobre delitos cibernéticos han sido deliberadamente diseñados para ser adaptados. Cada módulo presenta una estructura para una clase de tres horas, pero puede ser utilizado para sesiones más cortas o más largas. Los siguientes párrafos brindan ejemplos de los tipos de adaptación que pueden ocurrir. No es una lista exhaustiva y se puede ampliar cuando se necesite.

Para poder apoyar aún más a los docentes, la UNODC apreciaría recibir cualquier versión adaptada de los módulos de E4J (los mensajes se pueden enviar a e4j.cyberprevent@un.org). Luego, E4J compartirá estas versiones adaptadas con su comunidad de docentes como ejemplos de cómo se pueden adaptar los módulos para diferentes regiones, contextos y disciplinas.

Localización del contenido

El docente puede seguir estos pasos para localizar el contenido:

- Determinar si existe algún contenido que pueda ser considerado ofensivo en un contexto cultural local y eliminar o adaptar tal parte del contenido
- Brindar una introducción personalizada que refiera a los marcos legales y estudios de caso relevantes, quizá ejemplos recientes que aparecieron en los medios locales
- En caso de que sea necesario, reemplazar o complementar las lecturas, estudios de caso y ejercicios existentes con ejemplos que reflejen el contexto local
- En caso de que sea necesario, traducir el contenido al idioma local
- Adaptar el contenido para que se relacione de mejor manera a cierta disciplina, sector o industria

Integración dentro de un curso existente

Todos los módulos de E4J están diseñados para ser utilizados de manera independiente o integrados dentro de un curso existente. Como se mencionó anteriormente, la estructura modular permite a los docentes elegir solo aquellos que son relevantes dentro de un contexto específico. Los docentes tienen diversas opciones para utilizar un módulo de E4J. Un módulo independiente puede ofrecerse como una adición voluntaria u obligatoria a un curso; por ejemplo, como un taller ofrecido fuera de las sesiones normales programadas. También se puede ofrecer como parte de sesiones de verano, invierno o temporales, o como sesiones públicas con la participación de estudiantes que no están registrados.

La integración de un módulo dentro de un curso existente requiere de planificación debido a que una sesión específica debe ser programada en el esquema de un curso. Dicha planificación, dependiendo de la institución académica, debe pasar por procesos de aprobación interna. Sin embargo, los docentes suelen contar con suficiente flexibilidad para introducir contenidos nuevos, pero relacionados, en el esquema de un curso. Por ejemplo, en un curso de delito transnacional, delito o criminología existe la posibilidad de que haya un enfoque existente sobre delitos cibernéticos. En tal caso, el docente bien puede reemplazar el contenido

existente con los módulos de E4J, o adaptarlo o unirlo con el contenido de E4J. En caso de que no exista contenido sobre delitos cibernéticos, el docente tendrá que reorganizar el contenido actual para crear espacio en el esquema del curso para el material de E4J. Entonces, familiarizarse con los requisitos académicos de las instituciones específicas sigue siendo responsabilidad del docente. El proceso descrito anteriormente puede que no siempre sea posible.

Cambio en la duración

Se recomienda un espacio de tres horas. Dependiendo del estilo y del tamaño de la clase, se podría impartir un módulo típico de E4J, con todos los ejercicios, evaluación del estudiante o herramientas didácticas adicionales en un espacio de tres horas. Estos requisitos de tiempo para las clases varían entre las instituciones y los programas. Las sesiones presenciales de pregrado son a menudo más cortas y se realizan más de un día a la semana. Por esta razón, el contenido de un módulo de E4J puede que se extienda en dos o más sesiones. En cambio, las sesiones presenciales de posgrado pueden durar dos o tres horas, las cuales pueden ser suficientes para abarcar el contenido de un módulo completo. Sin embargo, algunos docentes podrían querer expandir el módulo en dos sesiones, ya que el intervalo entre las dos sesiones permitiría a los estudiantes procesar e interiorizar los materiales de mejor manera. En algunos casos, los docentes podrían querer añadir contenido adicional para ofrecer un taller de medio día o incluso uno de un día completo. No existen directrices rígidas sobre este asunto y los docentes deberían hacer ajustes para adaptarlos a sus circunstancias.

Desarrollo de un curso independiente

Cada módulo de la serie sobre delitos cibernéticos tiene una sección llamada «Estructura de clase recomendada», la cual se describe a continuación: «La siguiente es una estructura recomendada para la clase. Los estudiantes deben realizar las lecturas principales antes de ir a clase. La exposición tiene como objetivo reforzar lo que aprendieron con las lecturas y los ejercicios están diseñados para aplicar lo que aprendieron en dichas lecturas. El siguiente desglose está diseñado con base en una clase de tres horas. Los docentes pueden adaptar la estructura en función de sus necesidades y los horarios de la clase». Las secciones de la «Estructura de clase recomendada» dentro de la serie de módulos sobre delitos cibernéticos son muy flexibles y brindan sugerencias de alto nivel sobre el contenido y la estructura de un curso independiente. También puede utilizarse para brindar ideas para añadir contenido a talleres o sesiones más largas.

Puede que los docentes quieran combinar los módulos disponibles o combinen el contenido de diferentes módulos sobre delitos cibernéticos para crear un curso. Las combinaciones se determinarán de acuerdo a los requisitos institucionales o del cuerpo docente y se comunicarán según las prioridades temáticas. Los docentes también podrían considerar las combinaciones que involucren los módulos de E4J en otras áreas. Se recuerda en este contexto que E4J también ofrece series de módulos universitarios sobre los mandatos principales de la UNODC que abordan la integridad y ética; la lucha contra la corrupción; la prevención del delito y justicia penal; la delincuencia organizada; la trata de personas/el tráfico de migrantes; las armas de fuego; los delitos contra la vida silvestre, los bosques y la pesca y la lucha contra el terrorismo. Dada la disponibilidad de las series de módulos universitarios de E4J sobre una variedad de áreas y temas y en el contexto de la infinidad de posibilidades provistas mediante las diferentes extensiones, toda la serie de módulos universitarios de E4J es adaptable a muchos entornos distintos.

Resumen de los módulos sobre delitos cibernéticos

Los 14 módulos sobre delitos cibernéticos están disponibles en el sitio web de E4J. La UNODC los ofrece como recursos educativos abiertos (REA) para asistir a los docentes en su preparación y dictado de clases universitarias sobre delitos cibernéticos. Los usuarios pueden visitar el sitio web de E4J, descargar y copiar la información, documentos y material para uso no comercial. Con fines de seguimiento, la UNODC desearía ser informada acerca de la manera en la cual se utilizó el material y cuántos estudiantes participaron (los mensajes deberían enviarse a e4j.cyberprevent@un.org). Los usuarios también pueden contactar con E4J o registrarse en el sitio web de E4J para recibir actualizaciones de las noticias.

Los resúmenes de los módulos, incluidos los logros de aprendizaje y el mapeo de las herramientas de evaluación para los logros de aprendizaje, se encuentran a continuación (hacer clic en el hipervínculo del título para acceder al módulo completo).

Módulo 1: Introducción al Delito Cibernético

Las tecnologías de la información y la comunicación (TIC) han transformado la manera en la que las personas dirigen negocios, compran bienes y servicios, envían y reciben dinero, se comunican, comparten información, interactúan con personas y forman y cultivan relaciones

con otros. Esta transformación, así como el uso y dependencia crecientes de las TIC en el mundo, crea vulnerabilidades para los delincuentes y otros agentes malintencionados que tienen como objetivo las TIC o las utilizan para cometer delitos. Este módulo introduce conceptos clave relacionados con el delito cibernético, qué es el delito cibernético, internet, tecnología y tendencias de delito cibernético y los desafíos técnicos, legales, éticos y operacionales relacionados con el delito cibernético y su prevención.

Logros de aprendizaje

L1 Definir y describir conceptos básicos relacionados con la informática
L2 Describir y evaluar la conectividad global y las tendencias del uso de la tecnología
L3 Definir el delito cibernético y discutir la razón por la que se estudia de manera científica
L4 Discutir y analizar las tendencias del delito cibernético
L5 Identificar, examinar y analizar los desafíos técnicos, legales, éticos y operacionales relacionados con la investigación y prevención de los delitos cibernéticos

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento	Ejercicio n.° 1: Asignación; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento Evaluación	Ejercicio n.° 2; Ejercicio n.° 3; Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento	Preguntas de repaso; Discusión en clase
L4	Conocimiento/remembranza Compresión/entendimiento Análisis	Preguntas de repaso; Discusión en clase
L5	Compresión/entendimiento Aplicación Análisis	Ejercicio n.° 4; Preguntas de repaso; Discusión en clase; Estudio de caso

Módulo 2: Tipos Generales de Delitos Cibernéticos

Los delitos cibernéticos incluyen «nuevos» delitos, los cuales son posibles debido a la existencia de las tecnologías de la información y la comunicación (TIC), así como los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos y los delitos

tradicionales facilitados de alguna manera por las TIC, que incluyen delitos relacionados con la informática y los contenidos. Este módulo abarca diferentes tipos de delitos cibernéticos, particularmente delitos cibernéticos que se consideran delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, delitos relacionados con la informática y los contenidos.

Logros de aprendizaje

L1 Definir los tipos generales de delitos cibernéticos
L2 Identificar y discutir las categorías de delitos cibernéticos y los delitos incluidos dentro de estas categorías
L3 Diferenciar entre las diferentes formas de delitos cibernéticos
L4 Describir y explicar las maneras en las cuales se cometen ciertos delitos cibernéticos

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza	Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento Aplicación Evaluación	Ejercicio n.° 1; Ejercicio n.° 2; Tarea n.°1; Tarea n.° 2; Preguntas de repaso; Discusión en clase
L3	Análisis	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Análisis	Preguntas de repaso; Discusión en clase

Módulo 3: Marcos Jurídicos y Derechos Humanos

Las legislaciones nacionales, regionales e internacionales pueden regir el comportamiento en el ciberespacio y regular los asuntos de justicia penal relacionados con los delitos cibernéticos. Estas leyes no solo establecen normas y expectativas de comportamiento, sino también los procedimientos que deben seguirse si estas no se cumplan. Sin embargo, los delitos cibernéticos principales en las legislaciones nacionales no están armonizados entre países y complican la cooperación internacional en los asuntos de justicia penal (discutido en detalle en Delitos Cibernéticos-Módulo 7: Cooperación Internacional contra el Delito Cibernético y en la serie de módulos universitarios de E4J sobre la delincuencia organizada, particularmente en

el Módulo 11: Cooperación Internacional en la Lucha contra la Delincuencia Organizada Transnacional).

El objetivo de este módulo es describir el panorama legal relacionado con el delito cibernético, resaltar la necesidad de armonizar la legislación y describir la relación entre las leyes sobre delitos cibernéticos y los derechos humanos. Como se muestra en este módulo, las leyes sobre delitos cibernéticos deben cumplir con el derecho de los derechos humanos y cualquier limitación debe estar en conformidad con sus normas y principios.

Logros de aprendizaje

L1 Identificar, discutir y examinar la necesidad y el rol de las leyes sobre delitos cibernéticos
L2 Describir y diferenciar entre el derecho sustantivo, procesal y preventivo sobre delitos cibernéticos
L3 Identificar y evaluar críticamente las legislaciones nacionales, regionales e internacionales sobre delitos cibernéticos
L4 Evaluar críticamente la protección de los derechos humanos en línea

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento Análisis	Ejercicio n.° 2; Ejercicio en línea; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Análisis	Ejercicio en grupo; Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento Evaluación	Preguntas de repaso; Discusión en clase
L4	Evaluación	Ejercicio n.° 1; Ejercicio n.° 3; Prueba de conocimiento; Preguntas de repaso; Discusión en clase

Módulo 4: Introducción al Análisis Forense Digital

El *análisis forense digital* se refiere al proceso de recuperación, conservación, análisis y presentación de *pruebas electrónicas* para su uso en investigaciones y enjuiciamientos de varias formas de delito, incluyendo el delito cibernético. Este módulo provee un resumen de las pruebas de análisis forense digital y electrónicas, en particular observando el proceso del análisis forense digital, prácticas de análisis forense digital comunes, estándares de pruebas de análisis digitales forenses y electrónicas, y las mejores prácticas en el análisis forense digital.

Logros de aprendizaje

L1 Discutir datos e identificar fuentes de datos
L2 Describir y discutir las pruebas digitales
L3 Comparar y contrastar las diferencias entre las pruebas digitales y las pruebas tradicionales
L4 Discutir las maneras en que las pruebas digitales son autenticadas
L5 Describir y criticar los modelos del proceso del análisis forense digital
L6 Evaluar críticamente los estándares y mejores prácticas para las pruebas digitales y el análisis forense digital

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento	Preguntas de repaso; Discusión en clase
L3	Análisis	Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Evaluación	Ejercicio en grupo; Preguntas de repaso; Discusión en clase
L5	Conocimiento/remembranza Compresión/entendimiento Evaluación	Preguntas de repaso; Discusión en clase
L6	Evaluación	Ejercicio n.° 2: Asignación; Preguntas de repaso; Discusión en clase

Módulo 5: Investigaciones de Delitos Cibernéticos

Existen muchas partes interesadas (organismos, organizaciones, empresas y personas) involucradas en la investigación de delitos cibernéticos. La naturaleza y grado de su participación depende del tipo de delitos cibernéticos cometido. La participación de las partes interesadas también se determina por la ubicación geográfica de estas y de las leyes contra delitos cibernéticos en su país. Sobre la base del Módulo 4: Introducción al Análisis Forense Digital, el módulo 5 examina de manera crítica los procesos que intervienen en la denuncia de delitos cibernéticos y de las partes interesadas responsables de investigarlos. Se le presta mayor atención a las trabas encontradas durante las investigaciones de delitos cibernéticos (para información sobre cooperación internacional en investigaciones de delitos cibernéticos, consulte el Módulo 7: Cooperación Internacional contra Delitos Cibernéticos y la serie de módulos universitarios de E4J sobre delincuencia organizada; en particular, consulte el Módulo 11: Cooperación Internacional para Combatir la Delincuencia Organizada Internacional) y al papel de la gestión del conocimiento en las investigaciones de delitos cibernéticos. El Módulo 6: Aspectos Prácticos de las Investigaciones de Delitos Cibernéticos y Análisis Forense Digital abarca la manera en la que se deben llevar a cabo las investigaciones de delitos cibernéticos y el análisis forense digital.

Logros de aprendizaje

L1 Discutir y evaluar las prácticas de denuncia de delitos cibernéticos
L2 Identificar y discutir las partes interesadas involucradas en las investigaciones de delitos cibernéticos
L3 Explicar y evaluar de críticamente los recursos aprovechados durante una investigación de delitos cibernéticos y las trabas encontradas por los investigadores
L4 Describir y valorar el papel de la gestión del conocimiento en las investigaciones de delitos cibernéticos

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Compresión/entendimiento Evaluación	Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento	Tarea n.° 1; Ejercicio n.° 1; Ejercicio n.° 3; Preguntas de repaso; Discusión en clase

L3	Aplicación Análisis Evaluación	Ejercicio n.° 2; Tarea n.° 2; Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Análisis Evaluación	Ejercicio n.° 3; Preguntas de repaso; Discusión en clase

Módulo 6: Introducción a los Aspectos Prácticos de Investigaciones de Delitos Cibernéticos y Análisis Forense Digital

Cuando se investiga un delito, es muy probable que los organismos encargados de hacer cumplir la ley enfrenten las tecnologías de la información y la comunicación (TIC) durante dicha investigación. Las TIC pueden ser el objetivo de un delito cibernético, utilizadas para cometer un delito cibernético o contener pruebas de un delito. Las TIC y los datos que estas contienen se analizan para identificar las pruebas de la actividad delictiva. La investigación busca establecer de manera científica los hechos de un caso mediante el uso de pruebas digitales. La función del investigador es identificar dichas pruebas y reconstruir la secuencia de hechos del delito (o delito cibernético) o la que conduce al delito (o delito cibernético). Este módulo analiza la manera en la que se identifican las pruebas digitales, en particular el análisis forense digital (discutido en Delitos Cibernéticos-Módulo 4), que es el proceso mediante el cual las pruebas digitales de delitos y delitos cibernéticos se recopilan, obtienen, conservan, analizan, interpretan, comunican y presentan durante los procedimientos judiciales.

Logros de aprendizaje

L1 Identificar, analizar y evaluar críticamente las obligaciones legales y éticas de los investigadores de delitos cibernéticos y los profesionales del análisis forense digital
L2 Identificar las fases esenciales en el proceso del análisis forense digital
L3 Articular y evaluar críticamente las formas de identificar, recopilar, obtener y conservar pruebas digitales
L4 Discutir y valorar los procesos implicados en el análisis de pruebas digitales y la comunicación de los hallazgos basados en dicho análisis
L5 Explicar y aplicar un marco para evaluar la admisibilidad de las pruebas digitales en los tribunales

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Tarea n.° 3; Tarea n.° 4; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento	Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento Aplicación Análisis Evaluación	Ejercicio n.° 1; Ejercicio n.° 2; Preguntas de repaso; Discusión en clase
L4	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Ejercicio n.° 3; Tarea n.° 1; Preguntas de repaso; Discusión en clase
L5	Compresión/entendimiento Aplicación Análisis	Tarea n.° 2; Preguntas de repaso; Discusión en clase

Módulo 7: Cooperación Internacional contra los Delitos Cibernéticos

Un delito cibernético lo puede cometer un delincuente en cualquier parte del mundo con conexión a internet. Los efectos adversos de los delitos cibernéticos se pueden experimentar fuera del país donde reside el perpetrador. La naturaleza transnacional de este delito desafía las nociones de jurisdicción y requiere de la cooperación de los agentes de justicia penal en todo el mundo (consulte también la serie de módulos universitarios de E4J sobre delincuencia organizada, en particular el Módulo 11: Cooperación Internacional para Combatir la Delincuencia Organizada Internacional). Se ha observado esta cooperación, por ejemplo, en las investigaciones internacionales de mercados ilícitos en línea (o mercador negros), como Darkode(es decir, un mercado negro conocido por vender bienes y servicios ilícitos que incluyen acceso a datos robados y programas maliciosos). Los esfuerzos coordinados entre las autoridades encargadas de hacer cumplir la ley de 20 países condujeron a la identificación, arresto y búsqueda de miembros y asociados de este sitio (Departamento de Justicia de los

Estados Unidos, 2015). A pesar de esto y de otros esfuerzos cooperativos exitosos entre países, todavía existen barreras para la cooperación internacional contra los delitos cibernéticos. Este módulo explora las nociones de soberanía y jurisdicción relacionadas con el delito cibernético, los mecanismos de cooperación internacional y los desafíos para la cooperación internacional.

Logros de aprendizaje

L1 Describir y diferenciar entre soberanía y jurisdicción, y aplicarlas a los delitos cibernéticos
L2 Comparar, contrastar y valorar los distintos mecanismos formales de cooperación internacional
L3 Evaluar los mecanismos informales de cooperación internacional
L4 Discutir y comparar las prácticas de retención, conservación y acceso de datos entre países
L5 Identificar y evaluar los desafíos relacionados con pruebas extraterritoriales
L6 Discutir el déficit de capacidad nacional para realizar investigaciones de delitos cibernéticos y su impacto en la cooperación internacional

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Compresión/entendimiento Análisis	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Ejercicio n.° 2; Tarea n.° 1; Tarea n.°2; Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento Evaluación	Tarea n.° 1; Tarea n.° 2; Preguntas de repaso; Discusión en clase
L4	Conocimiento/remembranza Compresión/entendimiento Evaluación	Ejercicio n.° 3; Preguntas de repaso; Discusión en clase
L5	Conocimiento/remembranza Compresión/entendimiento Evaluación	Tarea n.° 2; Preguntas de repaso; Discusión en clase
L6	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Tarea n.° 2; Preguntas de repaso; Discusión en clase

Módulo 8: Seguridad Cibernética y Prevención del Delito Cibernético: Estrategias, Políticas y Programas

La tecnología de la información y la comunicación (TIC) es fundamental para el desarrollo nacional y mundial al facilitar la innovación y el crecimiento económico. La creciente interdependencia de los dispositivos digitales dentro de los países, así como también las crecientes conexiones de red con los sistemas digitales de otros países, han hecho que las TIC sean vulnerables a los delitos cibernéticos. Debido a que los delitos cibernéticos podrían tener un impacto negativo en la seguridad nacional, en la internacional y en la economía mundial, la protección de las TIC se considera de fundamental importancia a nivel nacional e internacional. Por consiguiente, países de todo el mundo han publicado estrategias en las que se describe cómo se protegerán las TIC de los delitos cibernéticos y de los delincuentes cibernéticos. El módulo 8 examina críticamente estas estrategias y las herramientas utilizadas para evaluarlas, así como la seguridad cibernética de los países y los esfuerzos de prevención del delito.

Logros de aprendizaje

L1 Discutir sobre la gobernanza de internet e identificar y evaluar sus principios, los conflictos que surgen en la realización de estos principios y las barreras para la gobernanza de la internet universal
L2 Describir las características básicas de las estrategias en materia de seguridad cibernética y diferenciar entre la seguridad cibernética y las estrategias de prevención de delitos cibernéticos
L3 Explicar y evaluar los objetivos y el ciclo de vida de las estrategias nacionales de seguridad cibernética
L4 Identificar, examinar y evaluar los marcos de cooperación internacional en temas de seguridad cibernética
L5 Evaluar los esfuerzos nacionales e internacionales para mejorar la postura de los países en cuestión de la seguridad cibernética

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento Evaluación	Ejercicio n.° 1; Tarea n.° 1; Preguntas de repaso; Discusión en clase

L2	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Ejercicio n.° 2; Preguntas de repaso; Discusión en clase
L3	Aplicación Análisis Evaluación	Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Aplicación Análisis Evaluación	Ejercicio n.° 3; Preguntas de repaso; Discusión en clase
L5	Evaluación	Tarea n.° 2; Preguntas de repaso; Discusión en clase

Módulo 9: Seguridad Cibernética y Prevención del Delito Cibernético: Aplicaciones y Medidas Prácticas

La *seguridad cibernética* se refiere a las estrategias, políticas, directrices, procedimientos, prácticas y medidas que se diseñan para identificar amenazas y vulnerabilidades, para prevenir amenazas que provienen del aprovechamiento de las vulnerabilidades, para mitigar el daño causado por amenazas materializadas y para salvaguardar a las personas, las propiedades y la información. Sobre la base del Módulo 8: Seguridad Cibernética y Prevención de Delitos Cibernéticos: Estrategias, Políticas y Programas, el módulo 9 desarrolla los aspectos prácticos de la seguridad cibernética y la prevención de delitos cibernéticos, incluyendo las evaluaciones de riesgo y las medidas que se utilizan para prevenir, detectar, enfrentar y recuperarse de incidentes vinculados a la seguridad cibernética.

Logros de aprendizaje

L1 Definir, discutir y evaluar los activos, amenazas, vulnerabilidades y riesgos
L2 Identificar y evaluar las maneras en las que se divulgan las vulnerabilidades
L3 Describir y criticar la relación entre seguridad cibernética y usabilidad
L4 Discutir sobre la prevención situacional de delitos y relacionarla con la prevención y reducción de delitos cibernéticos
L5 Discutir y analizar la detección de incidentes, respuestas y recuperación

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento Evaluación	Preguntas de repaso; Discusión en clase
L2	Compresión/entendimiento Evaluación	Ejercicio n.° 1; Tarea n.° 1; Tarea n.°2; Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento Análisis Evaluación	Tarea n.° 3; Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Aplicación Síntesis/creación	Ejercicio n.° 2; Preguntas de repaso; Discusión en clase
L5	Compresión/entendimiento Análisis	Ejercicio n.° 3; Estudio de caso; Preguntas de repaso; Discusión en clase

Módulo 10: Privacidad y Protección de Datos

Tanto los delincuentes como los delincuentes cibernéticos buscan datos personales y los utilizan para cometer delitos y delitos cibernéticos. Estos datos personales se pueden obtener de varias fuentes (estas fuentes se discuten en Delitos Cibernéticos-Módulo 4: Introducción al Análisis Forense Digital). Estos datos pueden revelar información acerca de la edad, raza, etnicidad, nacionalidad, género, creencias religiosas y políticas, orientación sexual, pensamientos, preferencias, pasatiempos, historial médico y problemas de salud, trastornos psíquicos, profesión, situación de empleo, servicio militar, afiliaciones, relaciones, geolocalización, hábitos, rutinas y otras actividades de las personas, entre otras informaciones (consulte Delitos Cibernéticos-Módulo 4: Introducción al Análisis Forense Digital). Estos datos personales, cuando se agregan, pueden brindar una imagen casi completa de la vida personal y profesional de las personas.

El módulo 10 examina críticamente el impacto de la agregación de datos, así como el impacto de la recopilación, almacenamiento, análisis, uso y divulgación de datos sobre la privacidad y seguridad. Específicamente, este módulo abarca la privacidad como un derecho humano, la relación entre privacidad y seguridad, las maneras en las que el delito cibernético pone en peligro la privacidad y seguridad de datos, y la protección de datos y las leyes de notificación

de filtraciones, así como también las maneras en las que los datos son (o pueden ser) protegidos para asegurar a las personas, las propiedades y la información.

Logros de aprendizaje

L1 Discutir sobre la privacidad y su importancia como derecho humano
L2 Identificar y evaluar el impacto del delito cibernético sobre la privacidad
L3 Evaluar críticamente la relación entre la seguridad y la privacidad
L4 Criticar las leyes sobre la protección de datos y notificación de filtraciones y las prácticas en las naciones
L5 Evaluar críticamente las prácticas para hacer cumplir la protección de datos y recomendar maneras efectivas para protegerlos

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Compresión/entendimiento	Ejercicio n.° 3; Preguntas de repaso; Discusión en clase
L2	Compresión/entendimiento Análisis	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L3	Evaluación	Ejercicio n.° 1; Tarea n.° 1; Preguntas de repaso; Discusión en clase
L4	Evaluación	Ejercicio n.° 1; Ejercicio n.° 2; Tarea n.°2; Preguntas de repaso; Discusión en clase
L5	Síntesis/creación	Ejercicio n.° 2; Preguntas de repaso; Discusión en clase

Módulo 11: Delitos contra la Propiedad Intelectual Propiciados por Medios Cibernéticos

Internet y los dispositivos digitales que funcionan con internet son multiplicadores de fuerza para los delitos de propiedad intelectual debido a que permiten que esta se suba a la nube, copie, descargue y comparta de manera instantánea en todo el mundo. La cooperación internacional y regional sobre el delito de propiedad intelectual y los temas sobre la protección son fundamentales. Esta cooperación puede involucrar la implementación de leyes de propiedad nacionales, regionales e internacionales y el desarrollo de la capacidad nacional para proteger la propiedad intelectual y prevenir delitos en materia de propiedad intelectual en línea y fuera de línea. Finalmente, el delito de propiedad intelectual priva a los creadores e innovadores y a aquellos que ponen a disposición la propiedad intelectual de las ganancias económicas por sus creaciones, innovaciones, identificadores únicos o información no divulgada.

El módulo 11 analiza la propiedad intelectual y su acceso, distribución y uso sin autorización propiciados por medios cibernéticos. Específicamente, este módulo examina qué es la propiedad intelectual, los tipos de propiedad intelectual, las causas, razones y justificaciones de delitos en materia de derechos de autor y de marca propiciados por medios cibernéticos, y medidas protectoras y preventivas contra esos delitos.

Logros de aprendizaje

L1 Discutir sobre la propiedad intelectual y la importancia de su protección
L2 Diferenciar entre las diversas formas de propiedad intelectual
L3 Evaluar críticamente las legislaciones nacionales, regionales e internacionales y los tratados relativos a la protección de la propiedad intelectual
L4 Identificar y discutir diversas teorías criminológicas, sociológicas, psicológicas y económicas y evaluar críticamente su aplicabilidad a los delitos en materia de derechos de autor y de marca propiciados por medios cibernéticos
L5 Evaluar críticamente la protección de la propiedad intelectual nacional, regional e internacional y los esfuerzos de prevención

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Compresión/entendimiento	Ejercicio n.° 3; Ejercicio n.° 4; Tarea n.°3; Preguntas

		de repaso; Discusión en clase
L2	Análisis	Tarea n.° 2; Ejercicio n.° 3; Preguntas de repaso; Discusión en clase
L3	Evaluación	Tarea n.° 2; Tarea n.° 3; Preguntas de repaso; Discusión en clase
L4	Conocimiento/remembranza Compresión/entendimiento Evaluación	Ejercicio n.° 1; Tarea n.° 1; Preguntas de repaso; Discusión en clase
L5	Evaluación	Ejercicio n.° 1; Ejercicio n.° 2; Ejercicio n.°4

Módulo 12: Delitos Cibernéticos Interpersonales

Las tecnologías de la información y la comunicación (TIC) brindan innumerables oportunidades para participar en asuntos cívicos y políticos, así como en actividades sociales, además de tener el potencial de dar acceso a posibilidades educativas y económicas a las personas, sin importar su ubicación geográfica. Las TIC también brindan incalculables oportunidades a los usuarios para comunicarse y compartir información. Sin embargo, estas oportunidades pueden ser mal utilizadas por otros para explotar y abusar sexualmente de niños y adultos, para cometer actos agresivos y perjudiciales para la sociedad y para incitar la violencia y otras formas de agresión contra los individuos, grupos o determinadas poblaciones con la intención de causarles daño. El módulo 12 explora algunos de estos delitos cibernéticos, especialmente el abuso y la explotación sexual de niños; la intimidación cibernética, el acoso cibernético y el *bullying* cibernético; diversos tipos de delitos cibernéticos relacionados con el género (p. ej., el abuso sexual con uso de imágenes y la sextorsión) y las medidas que se toman para contrarrestar, combatir y prevenir estos delitos cibernéticos.

Logros de aprendizaje

L1 Definir el delito cibernético interpersonal
L2 Definir y diferenciar entre los tipos de delitos cibernéticos interpersonales
L3 Describir y analizar las maneras en las que las tecnologías de la información y la comunicación se utilizan para facilitar estos tipos de delitos cibernéticos interpersonales
L4 Identificar y analizar de manera crítica cuál es el papel que juega la ley para tratar estos delitos cibernéticos
L5 Reconocer y evaluar los obstáculos para prevenir y responder a distintos tipos de delitos cibernéticos interpersonales

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza	Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento Análisis	Ejercicio n.° 2; Tarea n.° 4; Preguntas de repaso; Discusión en clase
L3	Compresión/entendimiento Análisis	Ejercicio n.° 1; Tarea n.° 1; Tarea n.° 3; Tarea n.° 4; Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Evaluación	Tarea n.° 2; Preguntas de repaso; Discusión en clase
L5	Compresión/entendimiento Evaluación	Ejercicio n.° 1; Ejercicio n.° 3; Ejercicio n.° 4; Tarea n.° 4; Preguntas de repaso; Discusión en clase

Módulo 13: Delitos Cibernéticos Organizados

Internet proporciona a los delincuentes acceso a las víctimas y a los clientes en cualquier parte del mundo con conexión a internet. Estos delincuentes se aprovechan de la facilidad con la que la información, las comunicaciones y el dinero navegan por el ciberespacio. Asimismo, utilizan internet para compartir conocimientos y comunicarse sin ser detectados; vender datos, bienes y servicios robados; lavar dinero adquirido de forma ilícita, así como intercambiar tácticas y herramientas de delincuencia cibernética utilizadas para cometer delitos cibernéticos. Estos delincuentes pueden operar solos o en diferentes tipos de grupos delictivos organizados. El módulo 13 examina los tipos de delitos que se consideran delitos cibernéticos organizados y los tipos de grupos delictivos organizados que se dedican a los delitos cibernéticos. También se examinan las medidas utilizadas para combatir los delitos cibernéticos organizados.

Logros de aprendizaje

L1 Describir los delitos cibernéticos organizados y los grupos delictivos que participan en ellos
L2 Identificar y discutir las estructuras y características de los grupos delictivos organizados que participan en los delitos cibernéticos organizados
L3 Examinar los diferentes tipos de delitos cibernéticos organizados

L4 Explicar y analizar las formas en que se utilizan las tecnologías de la información y la comunicación para cometer delitos cibernéticos organizados
L5 Evaluar críticamente las medidas utilizadas para contrarrestar los delitos cibernéticos organizados

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Conocimiento/remembranza Compresión/entendimiento	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento	Ejercicio n.° 1; Preguntas de repaso; Discusión en clase
L3	Conocimiento/remembranza Compresión/entendimiento Análisis	Preguntas de repaso; Discusión en clase
L4	Compresión/entendimiento Aplicación Análisis	Ejercicio n.° 3; Tarea n.° 1; Preguntas de repaso; Discusión en clase
L5	Evaluación	Ejercicio n.° 2; Tarea n.° 2; Tarea n.° 3; Tarea n.° 4; Preguntas de repaso; Discusión en clase

Módulo 14: Hacktivismo, Terrorismo, Espionaje, Campañas de Desinformación y Guerra en el Ciberespacio

El módulo 14 de la serie de módulos universitarios de E4J sobre delitos cibernéticos examina temas como el hacktivismo, el terrorismo, el espionaje, las campañas de desinformación y la guerra en el ciberespacio, así como también las perspectivas y respuestas nacionales e internacionales a estas actividades cibernéticas. El propósito de este módulo es analizar estos temas e identificar los debates actuales y los puntos de vista conflictivos sobre estos temas dentro y entre los países.

Logros de aprendizaje

L1 Examinar críticamente el hacktivismo, el ciberespionaje, el ciberterrorismo, la guerra cibernética, la guerra de información, la desinformación y el fraude electoral
L2 Discutir y analizar críticamente los marcos jurídicos que rigen estas actividades
L3 Evaluar críticamente la legalidad de las respuestas a estas actividades
L4 Proponer respuestas legales a algunas de estas actividades

Evaluación del aprendizaje del estudiante

Logros de aprendizaje	Taxonomía de Bloom (Original/revisado)	Herramientas de evaluación
L1	Análisis	Ejercicio n.° 1; Ejercicio n.° 2; Ejercicio n.° 4; Tarea n.°1; Tarea n.° 2; Preguntas de repaso; Discusión en clase
L2	Conocimiento/remembranza Compresión/entendimiento Análisis	Ejercicio n.° 1; Ejercicio n.° 2; Tarea n.°1; Tarea n.° 2; Tarea n.° 3; Preguntas de repaso; Discusión en clase
L3	Evaluación	Ejercicio n.° 3; Tarea n.° 2; Tarea n.°3; Preguntas de repaso; Discusión en clase
L4	Síntesis/creación	Ejercicio n.° 3; Ejercicio n.° 4; Tarea n.° 4; Discusión en clase

Conclusión

La iniciativa de E4J ofrece un enfoque innovador para la educación sobre los delitos cibernéticos en todos los tres niveles de educación, un área que es de suma importancia para abordar el déficit actual mundial en la prevención del delito cibernético y la capacidad en materia de seguridad cibernética. La Oficina de las Naciones Unidas contra la Droga y el Delito tiene la esperanza de que las universidades en el mundo usen la serie de módulos universitarios de E4J sobre delitos cibernéticos y de que esta añada valor a los cursos nuevos o existentes que se ofrecen, tanto para los estudiantes como para los docentes.

Referencias

Anderson, Lorin W. and David R. Krathwohl. (2001). *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*, Complete Edition. Longman.

Berkeley Centre for Teaching & Learning, Active Learning Strategies, https://teaching.berkeley.edu/active-learning-strategies.

Bloom, Benjamin S. (1956). *Taxonomy of educational objectives* Book 1: Cognitive domain. Addison-Wesley Longman.

Brown, Peter, Mark McDaniel, and Henry L. Roediger. (2014). *Make It Stick: The Science of Successful Learning*. Harvard University Press.

Center for Advanced Research on Language Acquisition (CARLA) (n.d.). Continuous Improvement: Objectivity and Subjectivity in Evaluation. University of Minnesota. http://carla.umn.edu/assessment/vac/improvement/p_6.html.

Schwartz, Michelle. (s. f.). Matching Assessments to Learning Outcomes Ryerson University, Learning & Teaching Office. https://www.ryerson.ca/content/dam/lt/resources/handouts/examslearningoutcomes.pdf

Segal, Mark (2013). *How To Train: A Practical Guide for Training and Working with Others* https://marksegaldotnet.files.wordpress.com/2011/07/howtotrain-marksegal3.pdf.

Yale Poorvu Center for Teaching and Learning, Active Learning, https://poorvucenter.yale.edu/ActiveLearning.

Reconocimientos

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) desarrolló esta Guía didáctica para docentes y la serie de módulos universitarios sobre delitos cibernéticos mediante la iniciativa de Educación para la Justicia (E4J) y en consonancia con el Programa Mundial para la Aplicación de la Declaración de Doha.

La UNODC desea agradecer a la Sra. Marie-Helen Maras de la Universidad de la Ciudad de Nueva York, Escuela de Justicia Penal John Jay, por su papel destacado en elaborar esta guía y los módulos relacionados. Además, a la UNODC le gustaría agradecer al Sr. Joshua James de la Universidad de Hallym, República de Corea, por su contribución a esta guía y los módulos relacionados.

Asimismo, la UNODC reconoce con profunda gratitud a aquellos que apoyaron el desarrollo de los módulos y la Guía didáctica para docentes revisando borradores y participando en la reunión del Grupo de Expertos E4J en agosto y noviembre de 2018, que incluyó a diversos expertos académicos que no pudieron participar en los Talleres de expertos en persona (en orden alfabético):

Sr. Nikolay Akatyev (Horangi Cyber Security)
Sr. Albert Antwi-Boasiako (Kwame Nkrumah University of Science and Technology, Ghana)
Sr. Vladimir Aras (Federal Prosecutor, Federal University of Bahia, Brasil)
Sr. Angel Jr Averia (Philippine Computer Emergency Response Team)
Sr. Roderic Broadhurst (Australian National University)
Sr. Robin Bryant (Canterbury Christ Church University, Reino Unido)
Sr. Lennon Chang (Monash University, Australia)
Sr. Yannick Chatelain (Grenoble School of Management, Francia)
Sr. Pavan Duggal (Supreme Court of India)
Sra. Myriam Dunn Cavelty (Swiss Federal Institute of Technology)
Sra. Asher Flynn (Monash University, Australia)
Sr. Zhixiong Huang (Wuhan University, China)
Sra. Laura Huey (University of Western Ontario, Canadá)
Sr. Abhaya Induruwa (Canterbury Christ Church University, Reino Unido)
Sra. Bahija Jamal (Hassan II University, Marruecos)
Sr. Oleksandr Komarov (Yaroslav Mudryi National Law University, Ukraine)
Sr. Edwin Kruisbergen (Ministry of Justice and Security, Países Bajos)
Sr. Alexander Kukhianidze (Tbilisi State University, Georgia)
Sr. Chat Le Nguyen (Fiji National University)
Sr. Asaf Lubin (Yale College, Estados Unidos)
Sr. Stephen Mason (Reino Unido)
Sr. Milos Mijomanovic (INTERPOL)
Sr. Brian Nussbaum (University at Albany, Estados Unidos)
Sr. Adedeji Oyenuga (Lagos State University, Nigeria)
Sr. Sergey Petrenko (Innopolis University, Federación Rusa)
Sr. Nigel Phair (University of Canberra, Australia)
Sr. James Popham (Wilfrid Laurier University, Canadá)
Sra. Pauline Reich (Nanyang Technological University, Singapur)
Sr. Nodirbek Salaev (Tashkent State University of Law, Uzbekistán)
Sr. Yun Shen (Symantec Research Labs)
Sr. Ahmed Shosha (Nile University, Egipto)
Sr. Vaclav Stupka (Masaryk University, República Checa)
Sr. Nedko Tagarev (University of National and World Economy, Bulgaria)
Sr. Hamed Tofangsaz (University of Waikato, Nueva Zelanda)
Sra. Bermet Tursunkulova (American University of Central Asia, Kirguistán)

Sr. Ian Walden (Queen Mary, University of London, Reino Unido)
Sr. David Wall (University of Leeds, Reino Unido)
Sra. Elena Yi (Yaroslav Mudryi National Law University, Ucrania)

La UNODC también agradece a sus colegas de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, en especial al Sr. Tim Engelhardt.

La UNODC también reconoce las contribuciones de los miembros del personal de la UNODC, quienes fueron los responsables de desarrollar esta guía y los módulos relacionados. Sra. Kamola Ibragimova, Sr. Patrick Boismenu, Sr. Neil J. Walsh, Sr. Marco Teixeira, Sra. Julia Pilgrim, Sra. Bianca Kopp. Los siguientes miembros del personal también realizaron contribuciones valiosas: Sr. Oleksiy Feshchenko, Sra. Malin Oestevik, Sra. Nayelly Loya Marin, Sra. Wendy O'Brien, Sra. Alexandra Martins, Sra. Riikka Puttonen, Sr. Dimosthenis Chrysikos, Sra. Flavia Romiti, Sra. Jenna Dawson-Faber, Sr. Arturo Laurent, Sr. Joaquin Zuckerberg.

Apéndice A: Glosario de términos

Este glosario incluye los términos discutidos en los 14 módulos sobre delitos cibernéticos.

Controles de acceso. Medidas que establecen privilegios, determinan acceso autorizado y previenen el acceso no autorizado.

Huella digital activa. Creada por los datos provistos por el usuario.

Estafa nigeriana. Fraude informático que involucra el pedido de un pago por adelantado para completar la transferencia, depósito u otra transacción a cambio de una mayor suma de dinero.

Amenazas persistentes avanzadas. Individuos o grupos que persistentemente marcan como objetivo a una entidad. También conocidos como *APT* (por sus siglas en inglés).

Denominaciones de origen. Símbolos de calidad del producto y la reputación del lugar de su creación, el cual no puede utilizarse a menos que el producto haya sido desarrollado en aquella región de acuerdo a los estándares de práctica. También conocidas como *indicaciones geográficas*.

Anonimato. Protección de la identidad de los individuos para permitirles participar en actividades sin revelar su identidad o sus acciones hacia otros.

Anonimizadores. Estos servidores proxy permiten que los usuarios oculten datos de identidad al enmascarar su dirección IP y sustituirla por una dirección IP diferente. También conocidos como *servidores proxy anónimos*.

Servidores proxy anónimos. Estos servidores proxy permiten que los usuarios oculten datos de identidad al enmascarar su dirección IP y sustituirla por una dirección IP diferente. También conocidos como *anonimizadores*.

Antianálisis forense digital. Herramientas y técnicas utilizadas para obstruir las investigaciones de delitos cibernéticos y los esfuerzos del análisis forense digital. También conocidos como *antianálisis forense*.

Antianálisis forense. Herramientas y técnicas utilizadas para obstruir las investigaciones de delitos cibernéticos y los esfuerzos del análisis forense digital. También conocido como *antianálisis forense digital*.

Análisis de aplicaciones y archivos. Tipo de análisis que se realiza para examinar las aplicaciones y los archivos en un sistema informático para determinar el conocimiento, la intención y las capacidades del transgresor para cometer delitos cibernéticos.

Activo. Algo que se considera importante o de mucho valor.

Atribución. Determinación de quién o qué es responsable del delito cibernético.

Disponibilidad. Datos, servicios y sistemas que son accesibles bajo petición.

Puerta trasera. Portal secreto que se utiliza para acceder a los sistemas sin autorización.

Mejores pruebas. Pieza original de las pruebas o un duplicado exacto del original.

Macrodatos. Grandes volúmenes de datos estructurados y no estructurados que pueden consolidarse y analizarse para revelar información acerca de asociaciones, patrones y tendencias.

Ataque de fuerza bruta. Uso de un *script* o un *bot* para adivinar las credenciales de los usuarios.

Rastreo. Proceso de rastrear actos ilícitos hasta dar con el origen del delito cibernético. También conocidos como búsqueda del origen.

Código *bot*. Tipo de programa malicioso que permite el control remoto de estos dispositivos y los utiliza para cometer delitos cibernéticos, robar información o participar en ataques cibernéticos.

Propietario de *bots*. Controlador de los dispositivos digitales infectados con *bots*.

Red *bot*. Red de computadoras infectadas con códigos *bot*.

Alojamiento a prueba de balas. Servicio que permite a los delincuentes utilizar servidores para cometer delitos cibernéticos, almacenar contenidos ilícitos y proteger contenidos ilícitos para que las autoridades encargadas de hacer cumplir la ley no puedan acceder a ellos o retirarlos de la red.

Plan de continuidad de las operaciones. Esquema de instrucciones que se deben seguir y acciones que se deben realizar en caso de un incidente de seguridad cibernética. También conocido como *plan de gestión de emergencias*.

Catphishing. Falsas o engañosas promesas de amor y compañía diseñadas para estafar a los individuos para quitarles su tiempo, dinero u otros artículos.

Censura. Prohibición de información, representaciones visuales, comunicaciones orales o escritas prohibidas por ley o su represión por parte de un Gobierno, comunidad o grupo debido a que son ilegales o vistos como perjudiciales, poco populares, indeseables o políticamente incorrectos.

Cadena de custodia. Registro detallado de las pruebas, su condición, recopilación, almacenamiento, acceso, transferencia y razones para su acceso y transferencia; es importante para asegurar la admisión de las pruebas digitales en muchos tribunales.

Captación de niños con fines sexuales (*child grooming).* Instigación o captación de niños con fines sexuales.

Trata sexual de menores. Actuar de alguna manera para reclutar, dirigir, causar, mantener o de alguna otra manera facilitar la explotación sexual comercial infantil.

Imágenes de abusos sexuales de niños. Representación del abuso sexual de niños u otros actos sexuales en donde se los utiliza.

Abuso sexual de niños a pedido. Los espectadores pueden participar activamente en el abuso comunicándose con el niño o la niña, con el abusador sexual o facilitador del abuso sexual y solicitando actos físicos o sexuales específicos que el niño o niña debe realizar o deben realizarle.

Evidencia circunstancial. Evidencia que infiere la verdad sobre un asunto.

Web limpia. Sitios web indexados que son accesibles, están disponibles para el público y se pueden buscar utilizando los motores de búsqueda tradicionales. También conocida como la *web de superficie* o *web visible*.

Código de ética. Directrices que abarcan la conducta correcta e incorrecta para fundamentar la toma de decisiones.

Explotación sexual comercial infantil. Término utilizado para describir una variedad de actividades que involucran el abuso sexual de niños para obtener algún tipo de remuneración de valor monetario o no monetario.

Datos informáticos. Cualquier forma de representación de la información que se procesa por el sistema de un dispositivo digital. También conocidos como *informática* o *datos*.

Equipo informático de respuesta de emergencia. Equipo que presta soporte para incidentes de seguridad cibernética. También conocido como *equipo de respuesta a incidentes de seguridad cibernética*.

Informática. Cualquier forma de representación de la información que se procesa por el sistema de un dispositivo digital. También conocido como *datos informáticos* o *datos*.

Red de computadoras. Dos o más computadoras que envían y reciben datos entre ellas.

Equipo de respuesta a incidentes de seguridad cibernética. Equipo que presta soporte para incidentes de seguridad cibernética. También conocido como *equipo informático de respuesta de emergencia*.

Sistema informático. Dispositivo independiente o en red que realiza el procesamiento de datos, entre otras funciones.

Confidencialidad. Sistemas, redes y datos protegidos y a los que solo los usuarios autorizados pueden acceder.

Sesgo de confirmación. Proceso a través del cual los individuos buscan y apoyan resultados que respaldan sus hipótesis de trabajo y descartan los resultados que entran en conflicto con ellas.

Datos con contenido. Palabras en comunicaciones escritas o palabras habladas.

Divulgación coordinada de vulnerabilidades. Práctica de intercambiar información armonizada y divulgar vulnerabilidades a las partes interesadas relevantes junto con las tácticas utilizadas para su mitigación.

Derechos de autor. Productos creativos, como obras artísticas y literarias, protegidos por ley.

Desplazamiento de delitos. Cuando un delito que fue pensado para un objetivo inicial se comete contra un objetivo distinto como consecuencia de las medidas de seguridad adoptadas.

Reconstrucción del delito. Este proceso busca determinar *quién* fue el responsable del delito, *qué* ocurrió, *dónde* ocurrió, *cuándo* tuvo lugar y *cómo* se desarrolló, a través de la identificación, cotejo y vinculación de datos. También conocido como *reconstrucción del evento*.

Infraestructura crítica. Sectores esenciales designados que se consideran fundamentales para el adecuado funcionamiento de la sociedad.

Criptomonedas. Una forma de moneda digital segura que utiliza codificación avanzada.

Cryptojacking. Una táctica a través de la cual la potencia de procesamiento de computadoras infectadas se utiliza para obtener criptomonedas para el beneficio financiero de la persona (o personas) que contralan los dispositivos digitales infectados con *bots*.

Delitos dependientes de la cibernética. Un delito cibernético que no podría ser posible sin internet y las tecnologías digitales.

Delitos propiciados por medios cibernéticos. Un delito cibernético facilitado por internet y las tecnologías digitales.

Delitos cibernéticos organizados. Un término utilizado para describir una actividad delictiva continua que opera racionalmente para sacar provecho de actividades ilícitas que tienen demanda en línea.

Delincuentes cibernéticos organizados. Un grupo estructurado de tres o más personas que existe durante cierto tiempo y que actúa en contubernio con el fin de cometer uno o más delitos graves o tipificados con arreglo a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional del 2000, el cual opera en línea total o parcialmente, para obtener, directa o indirectamente, un beneficio financiero u otro material.

Proxies cibernéticos. Uso de intermediarios para contribuir directa o indirectamente a un delito dependiente de la cibernética intencionalmente apuntando a un Estado.

Criptomercados. Un sitio web que utiliza la criptografía para proteger a sus usuarios.

Bullying cibernético. Uso de las tecnologías de la información y la comunicación por parte de los niños para molestar, humillar, insultar, ofender, hostigar, alarmar, acosar, abusar o de alguna otra manera atacar a otro niño o niños.

Ciberespionaje. Uso de las tecnologías de la información y la comunicación por parte de actores gubernamentales, grupos patrocinados o dirigidos por el Estado u otros que actúan en nombre de un Gobierno, para obtener acceso no autorizado a sistemas y datos en un esfuerzo por recopilar información de inteligencia sobre sus objetivos con el fin de mejorar la seguridad nacional, la competitividad económica o la fuerza militar de su propio país.

Hostigamiento cibernético. Uso de las tecnologías de la información y la comunicación (TIC) para humillar, fastidiar, atacar, amenazar, alarmar, ofender o abusar verbalmente de un individuo (o individuos).

Programas de secuestro mediante cifrado. Programa malicioso que infecta el dispositivo digital de un usuario, cifra los documentos del usuario y amenaza con borrar archivos y datos si la víctima no paga el rescate.

Desprestigio cibernético. Publicación u otras formas de distribución de información falsa o rumores acerca de un adulto o niño con el fin de dañar su posición social, sus relaciones interpersonales o su reputación.

Ciberespacio. Entorno al que se accede mediante tecnologías digitales que funcionan con internet en el que se realizan actividades en línea.

Acoso cibernético. Uso de las tecnologías de la información y la comunicación para cometer una serie de actos durante un periodo de tiempo para hostigar, fastidiar, atacar, amenazar, asustar o abusar verbalmente a un individuo (o individuos).

Seguridad cibernética. Recopilación de estrategias, marcos y medidas diseñados para identificar amenazas y vulnerabilidades de los sistemas, redes, servicios y datos para estas amenazas; prevenir el aprovechamiento de las vulnerabilidades, mitigar los daños causados por amenazas materializadas y salvaguardar a las personas, las propiedades y las tecnologías de la información y las comunicaciones.

Postura sobre seguridad cibernética. Término utilizado para describir las capacidades de seguridad cibernética de un país, organización o negocio.

Ciberterrorismo. Delitos dependientes de la cibernética perpetrados contra la infraestructura crítica para causar alguna forma de daño y provocar miedo en la población objetiva.

Guerra cibernética. Actos cibernéticos que comprometen y perturban los sistemas de infraestructura crítica, lo que equivale a un ataque armado.

Web oscura. Parte de la red informática mundial que es conocida por sus sitios web ocultos que albergan actividades, bienes y servicios ilícitos y solo se puede acceder a ellos mediante un software especializado. También conocida como red oscura.

Red oscura. Parte de la red informática mundial que es conocida por sus sitios web ocultos que albergan actividades, bienes y servicios ilícitos y solo se puede acceder a ellos mediante un software especializado. También conocida como web oscura.

Datos. Cualquier forma de representación de la información que se procesa por el sistema de un dispositivo digital. También conocido como *datos informáticos* o *informática*.

Análisis de ocultación de datos. Tipo de análisis que busca datos ocultos en un sistema.

Conservación de datos. Se realizan solicitudes a los proveedores de servicios en un esfuerzo por conservar los datos antes de que se eliminen o se alteren de alguna manera.

Minería de datos. Recuperación de información de grupos de datos.

Protección de datos. Salvaguarda de la información personal y regulación de su recopilación, almacenamiento, análisis, uso e intercambio.

Protección de datos por diseño. Medidas de privacidad integradas en el diseño de sistemas y tecnologías. También conocido como *privacidad por diseño*.

Ataque DDoS. Uso de muchas computadoras y otras tecnologías digitales para conducir ataques coordinados con la intención de sobrecargar a los servidores para evitar el acceso del usuario legítimo. También conocido como un *ataque de denegación de servicio distribuido*.

Web profunda. Parte de la red informática mundial que no está indexada por motores de búsqueda y a la que no se puede acceder de manera fácil o no está disponible para el público.

Ataque de denegación de servicio distribuido. Delito cibernético que interfiere con los sistemas sobrecargando a los servidores con solicitudes para impedir que el tráfico legítimo acceda a un sitio o utilice un sistema. También conocido como ataque DoS.

Diseño de patentes. Una forma de propiedad intelectual que incluye diseños que se crean con el propósito específico de ser estéticamente agradables para los consumidores e impactar en su decisión entre productos. También conocido como *diseño industrial*.

Disuasión. Disuadir una actividad ilícita mediante castigos.

Pruebas digitales. Datos obtenidos de las tecnologías de la información y la comunicación. También conocidas como *pruebas electrónicas*.

Huella digital. Los datos que dejan los usuarios de las TIC que pueden revelar información sobre ellos, incluyendo edad, género, raza, etnicidad, nacionalidad, orientación sexual, ideas, preferencias, hábitos, pasatiempos, historia clínica y problemas de salud, trastornos psíquicos, situación de empleo, afiliaciones, relaciones, geolocalización, rutinas, entre otras.

Proceso del análisis forense digital. Búsqueda, recuperación, conservación y mantenimiento de las pruebas digitales; la descripción, explicación y el establecimiento del origen de las

pruebas digitales y su importancia; el análisis de la las pruebas y su validación, confiablidad y relevancia para el caso, así como la presentación de pruebas pertinentes al caso.

Análisis forense digital. Rama de la ciencia forense que aplica cuestiones de derecho a la tecnología de la información y la comunicación y las pruebas digitales.

Piratería digital. Descarga ilegal de una película de un sitio web de terceros que no tiene el derecho de distribuir esta obra protegida por derechos de autor.

Evidencia directa. Evidencia que establece un hecho.

Desinformación. Difusión deliberada de información falsa.

Desinhibición. Proceso en el que un individuo demuestra una falta de moderación social en su comportamiento en línea.

Anonimato desasociado. Distanciamiento entre el comportamiento en línea y el comportamiento fuera de línea del individuo como resultado del anonimato que se le brinda como usuario de internet y de las tecnologías digitales.

Imaginación disociativa. El usuario percibe el espacio cibernético como un foro en el que las reglas de las interacciones diarias, códigos de conducta, normas sociales o leyes no aplican, lo que causa que el individuo se desinhiba y comience a actuar de una manera contraria a las reglas de las interacciones diarias, códigos de conducta, normas sociales o leyes.

Ataque de denegación de servicio distribuido. Uso de muchas computadoras y otras tecnologías digitales para conducir ataques coordinados con la intención de sobrecargar a los servidores para evitar el acceso del usuario legítimo. También conocido como un ataque DDoS.

Dogpiling. Una táctica mediante la que los usuarios de un espacio virtual bombardean a las víctimas con mensajes ofensivos, insultos y amenazas para callar a la víctima, forzarla a retractarse o pedir perdón por algo que presuntamente dijo u obligarla a retirarse de la plataforma.

Nombre de dominio. Representación de una dirección IP en un navegador de internet (o web).

Sistema de nombres de dominio. Permite el acceso a internet traduciendo nombres de dominio a una dirección IP.

Ataque DoS. Delito cibernético que interfiere con los sistemas sobrecargando a los servidores con solicitudes para impedir que el tráfico legítimo acceda a un sitio o utilice un sistema. También conocido como *ataque de denegación de servicio*.

Doxing. Información personal de los individuos publicada en línea para causarle algún tipo de daño.

Doxware. Una forma de programa de secuestro mediante cifrado que los autores utilizan contra las víctimas y que libera los datos del usuario si este no paga el rescate para descifrar los archivos y datos.

Doble incriminación. Cláusula en los tratados que exige que los actos se consideren ilegales en los países cooperantes.

eDiscovery (descubrimiento electrónico). Proceso de investigar, identificar y conservar los datos digitales para usarlos como evidencia en un proceso judicial.

Fraude electoral. Uso de tácticas ilegales para influenciar las elecciones.

Pruebas electrónicas. Datos obtenidos de las tecnologías de la información y la comunicación. También conocidas como *pruebas digitales*.

Plan de gestión de emergencias. Esquema de instrucciones que se deben seguir y acciones que se deben realizar en caso de un incidente de seguridad cibernética. También conocido *como plan de continuidad de las operaciones*.

Codificación. Medida que bloquea el acceso a la información y comunicaciones de los usuarios a terceros.

Reconstrucción del evento. Este proceso busca determinar *quién* fue responsable del evento, *qué* ocurrió, *dónde* ocurrió, *cuándo* tuvo lugar y *cómo* se desarrolló el evento, a través de la identificación, cotejo y vinculación de datos. También conocida como *reconstrucción del delito*.

Teoría de la utilidad esperada. Teoría que sostiene que las personas se involucran en determinadas acciones cuando la utilidad esperada de estas acciones es mayor que la utilidad esperada por involucrarse en otras acciones.

Noticias falsas. Propaganda y desinformación disfrazada de noticias reales.

Quinto dominio. Término utilizado para describir el ciberespacio como otro dominio de guerra.

Cortafuego. Una medida de seguridad que restringe la libre circulación de la información al bloquear los datos de tráfico no autorizados.

Relevancia forense. La relevancia forense de los datos se determina según si las pruebas digitales vinculan o descartan una conexión entre el autor del delito y el objetivo; si apoyan o refutan el testimonio del autor del delito, la víctima o los testigos; si identifican al autor o autores del delito cibernético; si proporcionan pistas para la investigación; si brindan información sobre la manera de operar del autor del delito y si demuestran que se produjo un delito.

Rescate de archivos. Búsqueda basada en identificadores de contenido.

Equipo de respuesta inicial. Personas que son las primeras en responder en una escena y son responsables de asegurar las pruebas en la escena.

Divulgación masiva de vulnerabilidades. Publicar de manera pública las vulnerabilidades de un software o hardware en línea mediante foros en línea y sitios web antes de tener una solución disponible.

Análisis funcional. Evaluación del desempeño y las capacidades de los sistemas y dispositivos involucrados en los eventos.

Disuasión general. Castigo diseñado para enviar un mensaje a otras personas de que por un comportamiento ilícito similar se recibirá un castigo severo similar.

Indicaciones geográficas. Símbolos de calidad del producto y la reputación del lugar de su creación, el cual no puede utilizarse a menos que el producto haya sido desarrollado en aquella región de acuerdo a los estándares de práctica. También conocidas como *denominaciones de origen*.

Hackeo. Acceso sin autorización a sistemas, redes y datos.

Disco duro. Memoria interna y persistente en una computadora.
De oídas. Declaraciones fuera de la corte.

Hash. Valor generado.

Human flesh search engine (motor de búsqueda de carne humana). Término utilizado para describir a los usuarios en línea que trabajan juntos para identificar un objetivo y cometer un abuso coordinado en línea en contra de este.

Gestión de la identidad. Proceso de autenticación de las identidades de los usuarios, identificando los privilegios asociados y otorgando acceso al usuario basado en estos privilegios.

Delito relacionado con la identidad. Un transgresor asume o se apropia de manera ilegal de la identidad de la víctima o utiliza la identidad o la información asociada con dicha identidad con propósitos ilegales.

Abuso sexual a través de imágenes. Una forma de violencia sexual donde las imágenes o los videos sexualmente explícitos de las víctimas se crean, distribuyen o se amenaza con su distribución intencionalmente sin el consentimiento de las víctimas. Esto puede causar algún tipo daño a la víctima o beneficiar al transgresor de alguna manera (p. ej., ganancia monetaria, gratificación sexual, construcción del estatus social y más).

Tratamiento de imágenes. Creación de una copia duplicada del contenido del dispositivo digital.

Detección de incidentes. Proceso de identificar amenazas por medio de un intenso monitoreo de activos y una búsqueda de actividad anómala.

Sistemas de control industrial. Sistemas que comandan y controlan los procesos de la infraestructura crítica.

Diseños industriales. Una forma de propiedad intelectual que incluye diseños que se crean con el propósito específico de ser estéticamente agradables para los consumidores e impactar en su decisión entre productos. También conocidos como *diseños de patentes*.

Guerra de la información. Recopilación, distribución, modificación, interrupción, interferencia, corrupción y degradación de la información con el fin de obtener alguna ventaja sobre un adversario.

Teoría de la inoculación. Esta teoría sostiene que la manera de inocular a los individuos de los intentos de persuasión de otros es exponerlos a estos y darles herramientas necesarias para resistir dichos intentos.

Integridad. Cuando los datos son precisos y confiables y no han sido modificados.

Propiedad intelectual. Productos de la creatividad, como obras, innovaciones, creaciones, expresiones de ideas originales, prácticas y procesos de negocios secretos, a los que los individuos tienen derechos tal como lo establece la ley.

Gobernanza de internet. Creación y aplicación de los principios, reglas y procedimientos de internet por parte de diversas partes interesadas para guiar su uso y formar su desarrollo.

Internet de las cosas. Red interconectada e interoperable de dispositivos con conexión a internet que facilitan el monitoreo de objetos, personas, animales y plantas, así como la recopilación, almacenamiento, examinación y difusión de información sobre ellos.

Tasa de penetración de internet. Porción de la población en un área que utiliza internet.

Dirección de protocolo de internet. Identificador único asignado por un proveedor de servicios de internet a un dispositivo digital conectado a internet para conectarse a internet. También conocida como *dirección IP*.

Proveedor de internet. Provee servicios de internet a un sistema informático o un sistema de otro dispositivo digital.

Troles cibernéticos. Individuos que publican comentarios groseros, agresivos y ofensivos a propósito para crear conflicto y descontento en línea.

Dirección IP. Identificador único asignado por un proveedor de servicios de internet a un dispositivo digital conectado a internet para conectarse a internet. También conocida como *dirección de protocolo de internet*.

Delito cibernético interpersonal. Delitos cibernéticos que cometen algunos individuos contra otros individuos con los que se comunican, interactúan o con los que tienen algún tipo de relación real o imaginaria.

Sistema de detección de intrusos. Medida de seguridad cibernética que permite la detección de ataques cibernéticos, así como el acceso y uso no autorizados de sistemas, redes, datos, servicios y recursos afines.

Jurisdicción. Poder y autoridad del Estado para hacer cumplir la ley y sancionar el incumplimiento con leyes.

Indicadores clave del desempeño. Medidas que se utilizan para determinar el progreso hacia la realización de objetivos estratégicos de la estrategia nacional de seguridad cibernética.

Comisiones rogatorias. Solicitudes escritas de tribunales nacionales para pedir pruebas de un país extranjero.

Transmisión en vivo de abuso sexual de niños. La transmisión del abuso sexual de niños en tiempo real para espectadores (con frecuencia) en ubicaciones remotas.

Extracción lógica. Búsqueda y obtención de pruebas de una ubicación en un sistema de archivos.

Búsqueda de palabras clave. Búsqueda basada en términos provistos por un investigador.

Gestión del conocimiento. Proceso de identificación y evaluación de las necesidades de conocimiento y del uso de activos de conocimiento.

Programa malicioso. Software malicioso.

Metadatos. Datos sobre el contenido. También conocidos como *datos sin contenido*.

Microlavado. Una forma de lavado de dinero donde el transgresor lava un monto significativo de dinero mediante múltiples y pequeñas transacciones.

Malinformación. Información falsa o inexacta.

Lavado de dinero. Ocultamiento de ganancias ilícitas mediante una combinación de transacciones legítimas e ilegítimas.

Mulas de dinero. Individuos que cometen delitos o delitos cibernéticos con o sin su conocimiento, obteniendo y transfiriendo bienes ilícitos, involucrándose en servicios ilícitos, o recibiendo o transfiriendo ilegalmente dinero a otros a cambio de una remuneración.

Morphing. Cuando el rostro o cabeza de la víctima se superpone sobre los cuerpos de otras personas con fines difamatorios, pornográficos o de abuso sexual.

Tratado de asistencia judicial recíproca. Acuerdo entre países para cooperar en las investigaciones y procesamientos judiciales de ciertos o todos los delitos proscritos por ambas partes según la legislación nacional.

Neutralidad de la red. Requiere que todos los datos, independientemente de la fuente, se traten con igualdad.

Técnicas de neutralización. Técnicas utilizadas para superar o minimizar las emociones negativas relacionadas con la participación en actividades ilegales.

Datos sin contenido. Datos sobre el contenido. También conocidos como *metadatos*.

Abuso sexual de niños en línea. Uso de las tecnologías de la información y la comunicación como *medio* para abusar sexualmente de niños.

Explotación sexual de niños en línea. Uso de las tecnologías de la información y la comunicación como medio para explotar sexualmente de los niños, donde el abuso sexual de niños u otros actos sexualizados que usan niños involucran algún tipo de intercambio.

Suplantación de identidad en línea. Suplantación de identidad de las víctimas al crear cuentas con nombres similares y usar imágenes existentes de ellas.

Delincuencia organizada. Una empresa delictiva continua que trabaja racionalmente para sacar provecho de actividades ilícitas que tienen gran demanda en línea.

Análisis de propiedad y posesión. Tipo de análisis que se utiliza para determinar la persona que creó, accedió o modificó los archivos en un sistema informático.

Roasting. Cuando los individuos conscientemente publican imágenes o videos de sí mismos en las redes sociales e invitan a otros a publicar insultos sobre ellos.

Teoría de las actividades rutinarias. Una teoría que sostiene que los delitos ocurren cuando dos elementos están presentes: un *delincuente motivado* y una *víctima propicia* y cuando un elemento está ausente: un *guardián eficaz*.

Pedófilo. Una persona interesada sexualmente en niños.

Huella digital pasiva. Datos que se obtienen y que accidentalmente dejan los usuarios de internet y de la tecnología digital.

Patente. «Una patente es un derecho exclusivo que se concede sobre una invención (innovación o creación), que es un producto o un proceso que ofrece, en general, una manera novedosa de hacer algo o brinda una nueva solución técnica a un problema» (OMPI, s. f.).

Troles de patentes. Estos individuos no crean ni inventan nada, simplemente compran patentes para licenciárselas a otros y demandan a cualquier persona, grupo u organización que infringen sus patentes adquiridas.

Autonomía personal. La habilidad de tomar decisiones y actuar de la forma que uno escoja, libre de coerción.

Pharming. Creación de un sitio web falso y duplicado que está diseñado para engañar a los usuarios para que estos ingresen sus credenciales de inicio de sesión.

Phishing. El envío de un correo electrónico con el enlace de un sitio web para que los usuarios hagan clic. Este podría descargar un programa malicioso en el dispositivo digital del usuario o enviarlos a un sitio web malicioso diseñado para robar sus credenciales.

Extracción física. Búsqueda y obtención de pruebas del lugar dentro de un dispositivo digital que contiene las pruebas.

Privacidad. Derecho a la intimidad y a no ser observado; la capacidad de mantener secretos los pensamientos, creencias, identidad y comportamientos propios y el derecho de escoger y controlar cuándo, qué, por qué, dónde, cómo y a quién se le revela información sobre uno y en qué medida esa información es relevada.

Privacidad por diseño. Medidas de privacidad integradas en el diseño de sistemas y tecnologías. También conocida como *protección de datos por diseño*.

Derecho preventivo. Normas jurídicas que se enfocan en la regulación del riesgo y buscan prevenir delitos o, al menos, reducir el posible daño en caso de un delito.

Derecho procesal. Normas jurídicas que abarcan los procesos y procedimientos que se deben seguir para aplicar el derecho sustantivo, las normas que permiten su aplicación y las normas y estándares en procedimientos de justicia penal.

Servidor proxy. Servidor intermediario que se utiliza para conectar un cliente con un servidor al que el cliente solicita recursos.

Seudonimización. Proceso mediante el cual los datos de identificación en un registro son reemplazados por identificadores artificiales.

Programa de secuestro. Programa malicioso diseñado para secuestrar el sistema, los archivos o datos de un usuario y devolverle el control después de que este pague el rescate.

Recuperación. Identificación, creación e implementación de medidas de resiliencia y la restauración de los sistemas, redes, servicios y datos que estaban inaccesibles o fueron modificados, dañados o afectados durante el incidente.

Análisis relacional. La determinación de los individuos involucrados y lo que hicieron y la conexión y relaciones entre estos individuos.

Resiliencia. La capacidad de resistir interrupciones, adaptarse a condiciones cambiantes y recuperarse de incidentes de TIC, y proteger la confidencialidad, integridad y disponibilidad de sistemas, redes, servicios y datos.

Divulgación responsable de vulnerabilidades. La práctica de no revelar la vulnerabilidad hasta que la organización responsable provea una solución.

Riesgo. El impacto de una amenaza y la probabilidad de que ocurra.

Evaluación de riesgos. La evaluación de la probabilidad de una amenaza, su impacto y la exposición de un activo a esta amenaza.

Tratamiento de riesgos. Respuestas a los riesgos.

Script. Programa informático.

Proveedor de servicios. Provee servicios a un sistema informático o un sistema de otro dispositivo digital.

Sexteo. Material autogenerado sexualmente explícito.

Sextorción. Forma de hostigamiento cibernético donde se amenaza a la víctima con publicar contenido sexualmente explícito si no se cumplen las demandas del agresor.

Prevención situacional de delitos. Medidas utilizadas para prevenir y reducir delitos.

Smishing. *Phishing* a través de mensajes de texto. También conocido como *phishing por SMS*.

Phishing por SMS. *Phishing* a través de mensajes de texto. También conocido como *smishing*.

Fraude basado en la ingeniería social. Engañar a la víctima para que revele o brinde información personal o dinero al delincuente.

Soberanía. El derecho de un país para ejercer autoridad sobre su propio territorio.

Dilema social. Cuando los individuos toman decisiones pensando en el interés personal más que en el interés colectivo o de grupo, incluso cuando el interés colectivo es más beneficioso que el propio.

Introyección solipcística. Cuando el usuario crea imágenes ficticias de otros y de sus características, incluyendo las relaciones interpersonales que sostiene con ellos, en ausencia de datos contextuales a partir de información imaginaria más que real.

Ingeniería social. Táctica mediante la cual el autor de un delito engaña al objetivo para que revele información o realice otra acción.

Spam. Envío de correos electrónicos no solicitados.

Spearphishing. Envío de correos electrónicos con archivos adjuntos o enlaces infectados diseñados para engañar al receptor para que haga clic en los archivos adjuntos o enlaces.

Disuasión específica. Castigar a los individuos que cometen delitos con el fin de que paren las actividades ilícitas si es que el castigo supera las ventajas de cometer un delito.

Programas espía. Programas maliciosos diseñados para monitorear sistemas infectados de manera encubierta y recopilar y transmitir esta información al creador o usuario del programa espía.

Programas de acosadores. Tipo de programas espía que puede instalarse en la computadora de las víctimas, en sus teléfonos inteligentes o en otros dispositivos digitales que funcionan con internet para recabar y retransmitir las acciones del usuario en esos dispositivos, desde correos electrónicos enviados y recibidos hasta fotografías tomadas y teclas pulsadas.

Procedimientos operativos estándar. Documentos que incluyen las políticas y actos secuenciales que deben seguirse para investigar los delitos cibernéticos y para manejar las pruebas digitales que se encuentra en la tecnología de la información y la comunicación.

Esteganografía. Ocultación sigilosa de datos tanto ocultando el contenido como volviéndolo invisible.

Derecho sustantivo. Normas jurídicas que rigen el comportamiento y las responsabilidades de las personas sobre las que el Estado tiene jurisdicción.

Web de superficie. Sitios web indexados que son accesibles, están disponibles para el público y se pueden buscar utilizando los motores de búsqueda tradicionales. También conocida como la *web limpia* o *web visible*.

Swappers. Intercambios semiautomáticos de criptomonedas.

Análisis temporal. La determinación de los eventos de tiempo que ocurrieron y la secuencia de dichos eventos.

Soberanía territorial. Ejercicio completo y exclusivo de autoridad y poder del Estado sobre su territorio geográfico.

Amenaza. Una circunstancia que puede causar daño.

Análisis de tiempo. Tipo de análisis que busca crear una línea de tiempo o una secuencia de acciones en el tiempo mediante el uso de marcas de tiempo que condujeron a un evento o para determinar la hora y la fecha en que un usuario realizó alguna acción.

Búsqueda del origen. Proceso de rastrear actos ilícitos hasta dar con el origen del delito cibernético. También conocido como *rastreo*.

Secretos comerciales. Información valiosa sobre procesos y prácticas comerciales que son secretos y protegen la ventaja competitiva de una empresa.

Robo de secretos comerciales. Robo de un secreto comercial fuera de línea o en línea para obtener una ventaja competitiva desleal.

Falsificación de marcas. Uso intencional sin autorización de una marca para etiquetar un bien o servicio que no proviene de la marca del propietario.

Marcas registradas. Identificadores que distinguen la fuente de un bien o servicio.

Datos de tráfico. Datos transmitidos mediante una red de computadoras (o red).

Troyano. Programa malicioso diseñado para parecerse a un programa legítimo con el fin de engañar al usuario para que descargue el programa, el cual infecta el sistema informático del usuario para espiarlo, robarle o causarle daños.

Espacio no asignado. Espacio disponible para su uso debido a que se borró el contenido o nunca se utilizó.

Usabilidad. Facilidad con la que se pueden utilizar los dispositivos digitales.

Web visible. Sitios web indexados que son accesibles, están disponibles para el público y se pueden buscar utilizando los motores de búsqueda tradicionales. También conocida como *web limpia* o *web de superficie*.

Vulnerabilidad. Exposición a daños.

Virus. Programa malicioso que requiere de la actividad del usuario para expandirse.

Vishing. *Phishing* a través de las telecomunicaciones.

Ataque de abrevadero. Colocar un programa malicioso en los sitios web más frecuentados de los objetivos para finalmente infectar sus sistemas y obtener acceso no autorizado a ellos.

Rastreadores web. Aplicaciones diseñadas para navegar la red informática mundial para lograr objetivos específicos.

Whaling. Pretender ser un ejecutivo de alto cargo en una empresa, abogado, contador u otra posición de autoridad y confianza, a fin de engañar a los empleados para que le envíen dinero.

Programa parásito. Programa malicioso independiente que se expande sin necesidad de que el usuario realice alguna actividad.

Bloqueador de escritura. Diseñado para prevenir la alteración de datos durante el proceso de copia.

Ataque de día cero. Vulnerabilidades previamente desconocidas que se explotan una vez identificadas.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org