Ciberdelito II

Guía práctica para un abordaje integral del fenómeno

Análisis forense digital. Cooperación internacional. Ciberseguridad. Privacidad y protección de datos.

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Federal Ministry
Republic of Austria
European and International Affairs

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

UPC
Universidad Peruana de Ciencias Aplicadas

Dra. Zoraida Ávalos Rivera
Fiscal de la Nación

Mtr. Aurora Castillo Fuerman
Fiscal Superior y Jefa de la Unidad Especializada en Ciberdelincuencia

Revisión y adaptación
Oficina de Análisis Estratégico contra la Criminalidad - OFAEC

Traducción
Centro de Servicios de Traducción de la Universidad Peruana de Ciencias Aplicadas (UPC)

Diseño y diagramación
IQ Comunicación Integral S.A.C.
hola@iq.pe

Impresión
Zona Comunicaciones S.A.C.
zonacomunicaciones.sac@gmail.com

Primera edición
Marzo 2022

Estos módulos fueron elaborados por UNODC en el marco del Programa Global para la Implementación de la Declaración de Doha. En estos módulos se ha usado indistintamente los términos ciberdelitos y delitos cibernéticos.

El contenido de esta publicación no implica expresión de opinión o consentimiento de parte del Secretariado de las Naciones Unidas en relación con el estatus legal de ningún país, territorio, ciudad o área o de sus autoridades, o respecto a las delimitaciones de sus fronteras o territorio. La mención de nombres de empresas y/o productos comerciales no implica aprobación por parte de las Naciones Unidas.

Ciberdelito II

Guía práctica para un abordaje integral del fenómeno

Análisis forense digital. Cooperación internacional.
Ciberseguridad. Privacidad y protección de datos.

UNODC
Oficina de las Naciones Unidas
contra la Droga y el Delito

Agradecimientos

Esta publicación ha sido posible gracias al Programa Global de Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC), con el apoyo del Ministerio Federal de Asuntos Europeos e Internacionales de la República de Austria, la Sección de Asuntos Antinarcóticos y Aplicación de la Ley de los Estados Unidos de América (INL), la Unidad Fiscal Especializada en Ciberdelito, la Red de Fiscales de Ciberdelito y el Centro de Servicios de Traducción de la Universidad Peruana de Ciencias Aplicadas (UPC).

Índice

Presentación

Toda sociedad sigue un proceso de desarrollo continuo de cambios. Hoy, a inicios de la tercera década del siglo XXI, nuestra sociedad se considera «genéticamente digital». Ello se define por el uso constante de las tecnologías de la información y comunicación, sostenida en el desarrollo de las tecnologías y ciertos rasgos de la vida moderna: la ubicuidad, la presencia de la velocidad, el anonimato en internet; en síntesis, una mirada de potenciales espacios para el logro de la libertad y las capacidades humanas, pero también espacios donde emergen los riesgos y las vulnerabilidades.

En estos espacios potencialmente negativos surge la denominada ciberdelincuencia, que se presenta como manifestación global y genérica de la delincuencia originada por el riesgo inherente al uso y utilización de las tecnologías de la información y comunicación en la actual sociedad. Su expresión, empero, es más compleja: debe entenderse como concepto comprehensivo de un conjunto de figuras sustantivas y normativas de tipos delictivos con entidad y sustantividad propia, el que tiene como característica ser un delito transnacional.

En este contexto, en el Perú, a fines del año 2020, por una decisión de mi despacho, se ha comenzado la especialización del Ministerio Público en la materia mediante la conformación de la Unidad Fiscal Especializada en Ciberdelincuencia, la misma que se implementó en el presente año, además de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro y la Red de Fiscales a nivel nacional; las cuales se sumaron a la ya implementada Unidad de Análisis Digital Forense de la Oficina de Peritajes del Ministerio Público. No obstante, los estudios o compendios académicos relacionados con la ciberdelincuencia aún son escasos en nuestro país.

Por tales motivos, saludo y agradezco la contribución de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) que a través de su Programa Global de Ciberdelito, pone a disposición una serie de módulos sobre ciberdelincuencia elaborados de la mano de expertos académicos de todo el mundo y que presenta temas y reúne recursos relacionados con el delito cibernético, su legislación, prevención e investigación; necesarios para una educación integral sobre esta compleja problemática. Además, incluye conceptos teóricos y prácticos respecto de la materia.

Estoy convencida de que el esfuerzo en la difusión de este material de estudio servirá para el aprendizaje y capacitación de los fiscales, personal forense, y de apoyo que laboran en el Ministerio Público, contribuyendo al conocimiento en esta materia y a la elaboración de estrategias adecuadas para enfrentar ese tipo de criminalidad.

Lima, octubre de 2021.
Zoraida Ávalos Rivera
Fiscal de la Nación

Prólogo

La pandemia del COVID-19 ha cambiado el mundo. El impacto en la salud pública, las crisis humanitarias y las crisis económicas han exacerbado los desafíos relacionados a la desigualdad, el crimen y el terrorismo. Estos constituyen retos globales y demandan una respuesta colectiva del sistema internacional.

En este contexto, es importante destacar que han pasado un poco más de 20 años desde la suscripción de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, también conocida como la Convención de Palermo (2000). Este instrumento internacional da los lineamientos para una reacción mundial a un desafío transnacional.

En el mismo sentido, la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC) ha presentado recientemente la Estrategia 2021 – 2026 que nos da lineamientos de acción y coordinación para el presente quinquenio. La Estrategia enfatiza que la misión de UNODC es contribuir a la paz y a la seguridad global, a los derechos humanos y al desarrollo para forjar un mundo más seguro frente a las drogas, el crimen, la corrupción y el terrorismo. Asimismo, se remarca que nuestras intervenciones prestarán especial atención a la protección de los niños, la igualdad de género, el empoderamiento de las mujeres y los jóvenes.

El ciberdelito es una forma de delincuencia transnacional en evolución. La naturaleza compleja de estos ilícitos que se llevan a cabo en un ámbito sin fronteras como es el ciberespacio, se ve agravada por la creciente participación de grupos de crimen organizado. Los autores de estas conductas y sus víctimas pueden estar ubicados en diferentes regiones y los efectos del delito pueden afectar a sociedades de todo el mundo, lo que pone de relieve la necesidad de montar una respuesta urgente, dinámica y de carácter internacional.

UNODC promueve la creación de capacidades de respuesta sostenibles a largo plazo en la lucha contra el ciberdelito, mediante el apoyo a las estructuras y la acción por parte de los Estados. Específicamente, UNODC aprovecha su experiencia especializada en los sistemas de justicia penal, para brindar asistencia técnica en el desarrollo de capacidades; la prevención y la concientización; la cooperación internacional; la recopilación de datos, la investigación y el análisis del ciberdelito.

En el contexto del COVID-19, nuestras dinámicas sociales han cambiado: la nueva normalidad nos ha obligado a adaptarnos al trabajo virtual, a la educación virtual y a actividades sociales online. Así como las dinámicas sociales han evolucionado, las modalidades delictivas también lo han hecho.

UNODC ha identificado que en el contexto de la pandemia del COVID-19, el ciberdelito ha evolucionado y ha crecido. El teletrabajo ha aumentado el universo de potenciales víctimas. Los usuarios toman mayores riesgos en línea mientras están en casa, lo cual, inintencionalmente, expone los sistemas informáticos de sus empresas frente a ciberdelincuentes. Ante este escenario, el fortalecimiento del Estado de Derecho, a través de la capacitación rigurosa y constante de los operadores de justicia, se hace fundamental.

La única manera de afrontar este fenómeno de una manera integral es trabajar sobre la prevención, detección temprana y persecución desde una óptica multidisciplinaria. Esto requiere de un esfuerzo y estrategia conjunta por parte de los Estados.

Es en esa lógica, que la formación y conocimiento –tanto del fenómeno general, como de su faz técnica, legal y su intersección con diferentes tópicos-, resulta uno de los primeros pasos de esta acción global para afrontar el ciberdelito.

En línea con lo expuesto, el Programa Global de Ciberdelito de la UNODC, en coordinación con el Ministerio Público del Perú, viene desarrollando una serie de actividades para contribuir al desarrollo de las competencias de los fiscales especializados en esta temática. En esa línea, hemos adaptado los módulos de ciberdelito en un conjunto de cuatro publicaciones, con el objetivo de aportar con la producción de contenido especializado en la temática, lo que ayuda a una comprensión, abordaje, investigación y administración de justicia especializada en este tema.

Estos módulos de ciberdelito representan un aporte invaluable a esos fines, creados en el marco del Programa Global de Doha, a través de la participación de destacados docentes especializados en la temática, quienes han implementado una novedosa metodología que abarca aspectos legales, técnicos y prácticos, proveyendo las herramientas necesarias para un sólido y multicomprensivo estudio del fenómeno de la ciberdelincuencia.

Esta publicación le brindará al lector un marco conceptual, información especializada y buenas prácticas para hacer frente de una manera integral a una problemática mundial cada vez más creciente. Es nuestro deseo que sirva para promover el cumplimiento de la ley en temas de ciberdelito, ayudar a prevenir los riesgos y las amenazas de internet, y favorecer la protección de niños, niñas y adolescentes en el ciberespacio. Y de esta forma, contribuir a los avances del país en su camino hacia la Agenda 2030 para el Desarrollo Sostenible.

Antonino De Leo
Representante de la Oficina de las Naciones Unidas contra las Drogas y el Delito para Perú y Ecuador, responsable de la coordinación de las operaciones en Argentina, Chile, Paraguay y Uruguay

Resumen ejecutivo

Esta serie de módulos provee a los especialistas con guías y recursos sobre delitos cibernéticos. Los módulos presentan temas respecto a diversos aspectos de los delitos cibernéticos y su investigación, así como abarcan tendencias, teorías, perspectivas, leyes, medidas y prácticas acerca de los delitos cibernéticos mediante una perspectiva multidisciplinaria.

Los 15 módulos son el resultado de un trabajo de líderes **expertos de más de 25 países de seis continentes.** Los módulos abarcan muchos aspectos de este campo sumamente pertinentes, e incluyen conceptos tanto teóricos como prácticos.

Módulo 6: Aspectos prácticos de investigaciones de delitos cibernéticos y análisis forense digital

Trata sobre el análisis forense digital y las investigaciones de delitos cibernéticos. De igual manera, 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.

Módulo 7: Cooperación internacional contra los delitos cibernéticos

Presenta una investigación profunda de la cooperación internacional y su relación con el delito cibernético, particularmente en 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.

Módulo 8: Seguridad cibernética y prevención del delito cibernético: estrategias, políticas y programas

Examina 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 analizarlas, así como también los esfuerzos de las naciones en materia de seguridad cibernética y prevención, y la naturaleza y el alcance de las capacidades de estas para proteger las TIC.

Módulo 9: Seguridad cibernética y prevención del delito cibernético: aplicaciones y medidas prácticas

Abarca los riesgos de la seguridad cibernética y los conceptos relacionados con estos, la investigación sobre la seguridad cibernética y la divulgación de las vulnerabilidades, las estrategias y técnicas de prevención situacional de delitos y las medidas de seguridad cibernética que se diseñan para identificar amenazas y vulnerabilidades, y para prevenir, detectar, responder y recuperarse de las amenazas materializadas.

Módulo 10: Privacidad y protección de datos

Examina de manera crítica el impacto tanto de la agregación de datos como 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 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, además de las formas en que los datos son (o pueden ser) protegidos para asegurar a las personas, las propiedades y la información.

La serie de módulos sobre delitos cibernéticos intenta ser lo más completa posible, y puede sentar la base de los conceptos clave relacionados con los delitos cibernéticos. De esta manera, es posible analizar con más detalle cada subtema dentro del módulo. Por lo tanto, hemos incluido recursos opcionales para los especialistas, 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.

La meta de estos módulos es que ***el conocimiento mundial sobre el ciberdelito progrese****, incluyendo su investigación y prevención.*

Si bien todos los módulos proveen una sólida base acerca del conocimiento sobre el delito cibernético, alentamos a los especialistas a sumar sus propias experiencias y personalizar el material y los ejemplos para adaptarlos al contexto local y sus necesidades, de manera que desarrollen mejor el contenido aquí expuesto.

Aspectos prácticos de investigaciones de delitos cibernéticos y análisis forense digital

Módulo 6

Módulo 6: Aspectos prácticos de investigaciones de delitos cibernéticos y análisis forense digital

Introducción

Cuando se investiga un delito, es más que probable que los organismos encargados de hacer cumplir la ley se encuentren con las tecnologías de la información y la comunicación (TIC) durante dicha investigación. Las TIC pueden ser el objetivo de un delito, utilizarse para cometer un delito o contener pruebas de dicho delito. Las TIC y los datos que estas contienen se analizan para identificar pruebas de actividad delictiva. Esta 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). Este módulo analiza la manera en que se identifican las pruebas digitales, en particular el análisis forense digital (discutido en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital), que es el proceso mediante el cual las pruebas digitales de delitos y delitos cibernéticos se recolectan, obtienen, conservan, analizan, interpretan, comunican y presentan durante los procedimientos judiciales.

Objetivos

- Identificar, analizar y evaluar de manera crítica las obligaciones legales y éticas de los investigadores de delitos cibernéticos y los profesionales del análisis forense digital.
- Identificar fases esenciales en el proceso del análisis forense digital.
- Articular y evaluar de manera crítica las formas de identificar, recolectar, obtener y conservar pruebas digitales.
- Debatir y valorar los procesos implicados en el análisis de pruebas digitales y la comunicación de los resultados basados en dicho análisis.
- Explicar y aplicar un marco para evaluar la admisibilidad de pruebas digitales en los tribunales.

Cuestiones clave

Las investigaciones de delitos cibernéticos pueden ser proactivas, en respuesta a la inteligencia, o reactivas, en respuesta a la identificación o denuncia a las autoridades competentes. La entidad observadora o la parte interesada ante la que se denuncian los delitos cibernéticos determinará quién participará en la investigación.

Nota

Aunque este módulo está enfocado en investigaciones sobre delitos cibernéticos y el análisis forense digital en investigaciones para la aplicación de la ley y el proceso judicial para delitos cibernéticos, muchas de las investigaciones sobre delitos cibernéticos y actividades de análisis forense digital son realizadas por personas ajenas al sistema de justicia penal, como organizaciones privadas (consulte Delitos Cibernéticos-Módulo 5: Investigaciones de delitos cibernéticos).

Obligaciones legales y éticas

Los investigadores de delitos cibernéticos (discutidos en Delitos Cibernéticos-Módulo 5: Investigaciones de delitos cibernéticos) y los profesionales del análisis forense digital deben investigar de manera legal y ética los delitos cibernéticos, además de manejar, analizar e interpretar las pruebas digitales y comunicar sus conclusiones (Kizza, 2013; Seigfried-Spellar et al., 2017). Si bien las obligaciones legales están establecidas por el derecho nacional, regional e internacional (consulte el derecho procesal de los delitos cibernéticos y las obligaciones en asuntos de derechos humanos en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos; los requisitos de acceso, retención y conservación de datos en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos, y los requisitos de protección de datos en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos), los organismos gubernamentales o las organizaciones profesionales privadas autoimponen o establecen las obligaciones éticas (siempre que estén presentes) (Roux y Falgoust, 2012; Kizza, 2013; Sharevski, 2015; Seigfried-Spellar et al., 2017). Cuando existe un código de ética (es decir, directrices que abordan la conducta correcta e incorrecta para fundamentar la toma de decisiones), suele incluir lo que los investigadores de delitos cibernéticos o los profesionales del análisis forense digital deben hacer en todo momento y lo que estas personas nunca deben hacer en ninguna circunstancia. Por ejemplo, la Sociedad Internacional de Examinadores Forenses Computacionales (ISFCE) incluye un código de ética que sus miembros deben respetar para garantizar que se cumplan las normas, y que los resultados del proceso del análisis forense digital sean precisos y fiables (ISFCE, s.f.). Este código de ética incluye los comportamientos que los miembros deben adoptar (p. ej., cumplir con órdenes legales y realizar un examen exhaustivo de pruebas de acuerdo con las leyes, estándares, procedimientos y directrices existentes) y los comportamientos prohibidos (p. ej., retener pruebas, realizar análisis o informes sesgados de pruebas y tergiversar las calificaciones) (ISFCE, s.f.). Para lecturas adicionales, consulte también la serie de módulos sobre integridad y ética, particularmente el Módulo 12: Integridad, ética y derecho, así como el Módulo 14: Ética profesional.

Manejo de pruebas digitales

¿Sabían que...?

En el sector privado, la respuesta a los incidentes de seguridad cibernética (p. ej., un ataque de denegación de servicio distribuido, un acceso no autorizado a los sistemas o una violación de datos) incluye procedimientos específicos que deben seguirse para contener el incidente de seguridad cibernética, investigarlo o resolverlo (Coalición de Seguridad Cibernética, 2015). Existen dos formas principales de manejar un incidente de seguridad cibernética: una recuperación rápida o la recopilación de pruebas (Coalición de Seguridad Cibernética, 2015). El primer método, la recuperación rápida, no se refiere a la conservación o recolección de datos, sino a la contención del incidente para minimizar el daño. Debido a su enfoque primario en una respuesta y recuperación rápidas, podrían perderse pruebas vitales. El segundo método consiste en supervisar el incidente de seguridad cibernética, centrándose en la aplicación del análisis forense digital a fin de recopilar pruebas e información sobre el incidente. Debido a que se centra principalmente en la recolección de pruebas, se retrasa la recuperación del incidente de seguridad cibernética. Estos métodos no son exclusivos del sector privado. El método adoptado por el sector privado varía según la organización y las prioridades de dicha organización.

¿Desean saber más?

Cyber Security Coalition. (2015). Cyber Security Incident Management Guide. Agoria.
https://www.agoria.be/upload/agoriav3/Cyber-Security-Incident-Management-Guide-2015.pdf

Las pruebas digitales son volátiles y frágiles, y el manejo inadecuado de estas pruebas puede alterarlas. Debido a su volatilidad y fragilidad, es necesario seguir protocolos para garantizar que los datos no se modifiquen durante su manejo (es decir, durante su acceso, recolección, empaquetado, transferencia y almacenamiento). Estos protocolos definen los pasos que se deben seguir cuando se manejan pruebas digitales. El manejo inicial de pruebas digitales consta de cuatro fases: identificación, recolección, obtención y conservación (ISO/IEC 27037; consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital).

¿Sabían que...?

Existen protocolos para la recolección de pruebas volátiles. Las pruebas volátiles deben recolectarse de acuerdo con el orden de volatilidad; es decir, las pruebas más volátiles deben recolectarse primero, y las menos volátiles, al final. El documento Solicitud de comentarios (RFC) 3227 presenta la siguiente muestra del orden de datos volátiles (de más a menos volátil) para sistemas estandarizados (Brezinski y Killalea, 2002):

- Registros, caché
- Tabla de enrutamiento, ... caché [protocolo de resolución de dirección o ARP], tabla de procesos
- Estadísticas de *kernel*, memoria
- Sistemas de archivos temporales
- Disco duro
- Datos de acceso y monitoreo remoto que son relevantes para el sistema en cuestión
- Configuración física, topología de red
- Medios de almacenamiento

Para más información, consulte:

Brezinski, D. & Killalea, T. (2002). Guidelines for Evidence Collection and Archiving. Request for Comments: 3227. RFC Editor. ***https://www.rfc-editor.org/pdfrfc/rfc3227.txt.pdf***

Identificación

En la fase de identificación, se obtiene información preliminar sobre el caso de delito cibernético antes de recolectar pruebas digitales. Esta información preliminar es similar a la que se busca durante una investigación criminal tradicional. El investigador busca responder a las siguientes preguntas:

- ¿Quién estuvo involucrado?
- ¿Qué ocurrió?
- ¿Cuándo ocurrió el delito cibernético?
- ¿Dónde ocurrió el delito cibernético?
- ¿Cómo ocurrió el delito cibernético?

Las respuestas a estas preguntas proporcionarán a los investigadores una guía sobre cómo proceder con el caso. Por ejemplo, la respuesta a la pregunta «¿Dónde ocurrió este delito?» —es decir, dentro o fuera de las fronteras de un país (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos para obtener información sobre las jurisdicciones)— informará al investigador sobre cómo proceder con el caso (p. ej., qué organismos deben involucrarse o contactarse).

En la fase de identificación, los investigadores de delitos cibernéticos utilizan muchas técnicas de investigación tradicionales (consulte UNODC Actividades policiales: investigación de delitos para un análisis detallado de dichas técnicas), especialmente en lo que respecta a la recopilación de información y pruebas. Por ejemplo, se entrevista a las víctimas, testigos y sospechosos de un delito cibernético para reunir información y pruebas del delito cibernético que está siendo investigado (para obtener una guía sobre cómo entrevistar a los sospechosos y a los testigos y víctimas adultos y niños, consulte: UNODC Módulo 9: Manual sobre la lucha contra la trata de Personas para profesionales de la justicia penal; Manual para la lucha contra la trata de personas de la UNODC; Directrices sobre la justicia en asuntos concernientes a los niños víctimas y testigos de delitos, Resolución 2005/20 del Consejo Económico y Social de la ONU (ECOSOC); Justicia en asuntos concernientes a los niños víctimas y testigos de delitos de la UNODC y Breve introducción a las entrevistas de investigación: guía para profesionales de Boyle y Vullierme, Consejo de Europa).

También se han llevado a cabo investigaciones encubiertas para identificar, investigar y procesar a los delincuentes cibernéticos (se pueden encontrar ejemplos de estas investigaciones en Delitos Cibernéticos-Módulo 12: Delitos cibernéticos interpersonales y en delitos cibernéticos; Módulo 13: Delitos cibernéticos organizados). Además, los investigadores de delitos cibernéticos han realizado vigilancias encubiertas. Esta táctica es un «método particularmente intrusivo para la recolección de pruebas». El uso de medidas de vigilancia encubierta implica un cuidadoso equilibrio entre el derecho a la privacidad del sospechoso y la necesidad de investigar los delitos graves. Las disposiciones sobre la vigilancia encubierta deben respetar plenamente «los derechos del sospechoso». Los órganos y tribunales internacionales de derechos humanos han adoptado diversas decisiones sobre la permisibilidad de la vigilancia encubierta y los parámetros de dichas medidas (UNODC, 2013, p. 13). Incluso los organismos encargados de hacer cumplir la ley han utilizado programas malignos para llevar a cabo la vigilancia, a fin de recopilar información y pruebas sobre delitos cibernéticos. Por ejemplo, los organismos encargados de hacer cumplir la ley en los Estados Unidos utilizan técnicas de investigación de redes (NIT), «códigos y programas maliciosos especialmente diseñados», en sus investigaciones sobre explotación y abuso sexual de menores en línea (Finklea, 2017, p. 2; consulte Delitos Cibernéticos-Módulo 13: Delitos cibernéticos organizados para obtener más información sobre estas técnicas).

Antes de comenzar la recolección de pruebas digitales, el investigador debe definir los tipos de pruebas que busca. Las pruebas digitales pueden encontrarse en dispositivos digitales, como computadoras, discos duros externos, memorias USB, routers, teléfonos inteligentes, tabletas, cámaras, televisores inteligentes, electrodomésticos con conexión a internet (p. ej., refrigeradoras y lavadoras) y consolas de juegos (por citar algunos), así como en recursos públicos (p. ej., plataformas de redes sociales, sitios web y foros de debate) y privados (p. ej., registros de actividad de los usuarios de los proveedores de servicios de internet, registros comerciales de los proveedores de servicios de comunicación, y registros de actividad y contenido de usuario de los proveedores de almacenamiento en la nube). Muchas aplicaciones, sitios web y dispositivos digitales utilizan servicios de almacenamiento en la nube. Por lo tanto, los datos de los usuarios pueden ser almacenados en su totalidad o en fragmentos por muchos proveedores diferentes en servidores situados en múltiples lugares (UNODC, 2013; Quick et al., 2014). Es por este motivo que la obtención de datos de dichos proveedores es un desafío (para más información, consulte Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos). Las pruebas que se busquen dependerán del delito cibernético que está siendo investigado. Si el delito cibernético que se está investigando es un fraude de identidad, se buscarán pruebas de dicho delito en los dispositivos digitales incautados (p. ej., pruebas de una o varias transacciones fraudulentas).

Recolección

En lo que respecta al delito cibernético, el lugar del delito no se limita a la ubicación física de los dispositivos digitales utilizados para cometer el delito cibernético o que fueron objeto de dicho delito cibernético. La escena del delito cibernético también incluye los dispositivos digitales que pueden contener pruebas digitales y abarca múltiples dispositivos, sistemas y servidores digitales. La escena del delito se obtiene cuando el delito cibernético es observado, reportado o sospechado. El primero en responder (discutido en Delitos Cibernéticos-Módulo 5: Investigaciones de delitos cibernéticos) identifica y protege la escena del delito de la contaminación, y conserva las pruebas volátiles aislando a los usuarios de todos los dispositivos digitales encontrados en el lugar del delito (p. ej., manteniéndolos en una habitación o lugar separado) (Casey, 2011; Sammons, 2012; Maras, 2014; Nelson et al., 2015; consulte el recuadro de la Nota a continuación). No se debe dar a los usuarios la oportunidad de seguir utilizando los dispositivos digitales. ***Ni el primero en responder ni el investigador*** deben buscar la asistencia de ningún usuario durante el proceso de búsqueda y documentación. El investigador, si no es el primero en responder, busca en la escena del delito e identifica las pruebas. Antes de recolectar las pruebas, se documenta la escena del delito. La documentación es necesaria a lo largo de todo el proceso de investigación (antes, durante y después de que se hayan obtenido las pruebas). Esta documentación debe incluir información detallada sobre los dispositivos digitales recogidos, incluido el estado operativo del dispositivo —encendido, apagado, modo en espera— y sus características físicas, como la marca, el modelo, el número de serie, las conexiones y cualquier marca u otro daño (Casey, 2011; Sammons, 2012; Maras, 2014; Nelson et al., 2015). Además de las notas escritas, también se necesitan bocetos, fotografías o grabaciones de video de la escena del delito y de las pruebas para documentar la escena y las pruebas (Maras, 2014, pp. 230-233).

Nota

La recopilación de datos volátiles puede alterar el contenido de la memoria de los dispositivos digitales y los datos que estos contienen.

El investigador, o el técnico de la escena del delito, recolecta las pruebas. Los procedimientos de recolección varían en función del tipo de dispositivo digital, y de los recursos públicos y privados que albergan las pruebas digitales (p. ej., computadoras, teléfonos, redes sociales y nubes; para las diferentes prácticas del análisis forense digital relativas al contenido multimedia, videos y teléfonos celulares, consulte el Grupo de Trabajo Científico sobre Pruebas Digitales (SWGDE)). Los organismos encargados de hacer cumplir la ley disponen de procedimientos operativos estándar, que detallan los pasos que deben seguirse para manejar pruebas digitales en dispositivos móviles, objetos con conexión a internet (p. ej., relojes, monitores de actividad física y electrodomésticos), la nube y las plataformas de redes sociales (Borrador de las mejores prácticas para la recolección y conservación, manejo y obtención de pruebas de dispositivos móviles del SWGDE, 2018; Mejores prácticas para la obtención de datos de dispositivos digitales nuevos del SWGDE; Alianza para la Seguridad en la Nube, 2013; Servicio de Policía de Escocia, 2018). ***Se diseña un procedimiento operativo normalizado*** (PON) para ayudar a los investigadores mediante la inclusión de las políticas y actos secuenciales que deben seguirse para investigar delitos cibernéticos de forma que se garantice la admisibilidad de las pruebas recogidas en un tribunal de justicia, así como las herramientas y otros recursos necesarios para llevar a cabo la investigación (p. ej., consulte los siguientes PON: Consejo de Seguridad de Datos de India, 2011; Servicio de Policía de Escocia, 2018). En general, los PON incluyen los procesos que deben seguirse durante una investigación.

Se deben identificar las limitaciones particulares que se pueden encontrar durante la investigación. Por ejemplo, los investigadores de delitos cibernéticos podrían encontrarse con múltiples dispositivos digitales, sistemas operativos y complejas configuraciones de red, lo que requerirá conocimientos especializados, variaciones en los procedimientos de recolección y asistencia para identificar conexiones entre los sistemas y dispositivos (p. ej., una topología de redes). Durante una investigación, también pueden emplearse técnicas antiforenses (discutidas en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital), como la esteganografía (es decir, la ocultación sigilosa de datos, tanto ocultando el contenido como volviéndolo invisible) y el cifrado (es decir, «el bloqueo físico del acceso de terceros a un archivo, ya sea mediante el uso de una contraseña o inutilizando el archivo o aspectos de dicho archivo»; Maras, 2014, p. 204; para más información sobre el cifrado, consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos) (Conlan et al., 2016). Por consiguiente, el investigador debe estar preparado para dichas situaciones y disponer de los recursos humanos y técnicos necesarios para hacer frente a estas limitaciones. Las medidas adoptadas por el investigador en estos casos (p. ej., la capacidad del investigador para obtener las contraseñas de dichos dispositivos o descifrar los archivos), si las hubiere, dependen de las leyes nacionales (consulte el mapa interactivo de Global Partners Digital para más información sobre las leyes y políticas de cifrado de cada país). Las herramientas de análisis forense digital (discutidas en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital) pueden contribuir con dicha labor, por ejemplo, identificando la esteganografía y descifrando los archivos, así como realizando otras actividades fundamentales de análisis forense digital. Se pueden encontrar ejemplos de dichas herramientas en las herramientas para el análisis forense (FTK) de Access Data, Volatile Framework y X-Ways Forensics. Junto con dichos recursos, se necesitan herramientas forenses que contengan los objetos necesarios para documentar la escena del delito, herramientas para desarmar dispositivos y retirar otros tipos de pruebas de la escena del delito, y material necesario para etiquetar y empaquetar las pruebas (p. ej., en el caso de los teléfonos inteligentes, se necesita una bolsa de Faraday, que bloquea las señales inalámbricas hacia y desde el dispositivo digital, y un cargador portátil que se utiliza para transportarlas), entre otros elementos (Casey, 2011; Sammons, 2012; Maras, 2014; Nelson et al., 2015).

La recolección real de las pruebas implica conservar las pruebas volátiles y apagar los dispositivos digitales. El estado de operatividad de los dispositivos digitales encontrados determinará los procedimientos de recolección. Por ejemplo, si se encuentra una computadora y el dispositivo está encendido, se conservan las pruebas volátiles (p. ej., archivos temporales, registro, caché y estado y conexiones de red, entre otras) antes de apagar el dispositivo y recolectarlo (Casey, 2011; Sammons, 2012; Maras, 2014; Nelson et al., 2015). Si el dispositivo está apagado, entonces permanece apagado y se recolecta (Instituto Nacional de Justicia de los Estados Unidos; 2004b; Instituto Nacional de Justicia de los Estados Unidos, 2008). Existen circunstancias en las que los dispositivos digitales no se recolectan y no pueden recolectarse (p. ej., debido al tamaño, a la complejidad de los sistemas o sus configuraciones de hardware y software, porque estos sistemas brindan servicios críticos) (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). En estas situaciones, los datos volátiles y no volátiles se recolectan mediante procedimientos especiales que requieren una obtención en vivo (Sistemas en vivo de captura del SWGDE, 2014). El tipo de dispositivo digital que se encuentre durante una investigación también determinará la manera en que se recolecten las pruebas digitales (consulte, por ejemplo, Mejores prácticas para la conservación y obtención de pruebas de dispositivos móviles del SWGDE, 2018; Mejores prácticas para la obtención de datos de dispositivos digitales nuevos del SWGDE; Instituto Nacional de Justicia de los Estados Unidos, 2007a).

¿Sabían que...?

Se pueden usar comandos para obtener datos volátiles de los sistemas en vivo. Por ejemplo, para los sistemas operativos de Windows se utiliza el comando *ipconfig* para obtener información de red, mientras que para los sistemas operativos de Unix se utiliza el comando *ifconfig*. Tanto para Windows como para Unix, se utiliza el comando *netstat* para obtener información sobre las conexiones de red activas.

¿Desean saber más?

Software Engineering Institute. (2016). Volatile Data Collection. Carnegie Mellon University.
https://www.rand.org/pubs/research_reports/RR2081.html

Amari, K. (2009). Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. SANS Institute InfoSec Reading Room.
https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049

Bolt, S. & Door, E. (2007). Methods for Capturing Volatile Data.
http://hcco4.com/CC/wp-content/uploads/2014/06/VolatileData.pdf

Además de los dispositivos digitales, también se deben recopilar otros elementos relevantes (p. ej., notas o cuadernos que puedan incluir contraseñas u otra información sobre credenciales en línea, teléfonos, máquinas de fax, impresoras, *routers*, etc.). Las medidas que el investigador adopte durante la recolección de pruebas deben documentarse. Cada dispositivo debe ser etiquetado (junto con sus cables de conexión y de alimentación), empaquetado y transportado de vuelta a un laboratorio de análisis forense digital (Instituto Nacional de Justicia de los Estados Unidos; 2004b; Instituto Nacional de Justicia de los Estados Unidos, 2008). Una vez que los artículos son transportados al laboratorio, son «inventariados, registrados y asegurados en una habitación cerrada (...) lejos de temperaturas extremas, humedad, polvo y otros posibles contaminantes» (Maras, 2014, p. 237).

Obtención

Existen diferentes métodos para la obtención. El método adoptado depende del tipo de dispositivo digital. Por ejemplo, el procedimiento para obtener pruebas del disco duro de una computadora es diferente del procedimiento requerido para obtener pruebas digitales de dispositivos móviles, como los teléfonos inteligentes.

A menos que se realice una obtención en vivo, las pruebas se extraen de los dispositivos digitales incautados en el laboratorio forense (es decir, obtención estática). En el laboratorio forense, las pruebas digitales deben extraerse de manera que se conserve la integridad de las pruebas (garantizando que los datos no se alteren); es decir, de manera forense (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). Por lograrlo, las herramientas y técnicas utilizadas para obtener pruebas digitales deben prevenir la alteración de los datos o, cuando no sea posible, al menos reducirla al mínimo (Mejores prácticas para la obtención forense computarizada del SWGDE, 2018). Las herramientas y técnicas utilizadas deben ser válidas y fiables (NIST, s.f.; Directrices recomendadas para las pruebas de validación del SWGDE, 2014; Instituto Nacional de Justicia de los Estados Unidos, 2007b). Se deben identificar y considerar las limitaciones de estas herramientas y técnicas antes de su uso (Mejores prácticas para la obtención forense computarizada del SWGDE, 2018). El Instituto Nacional de Estándares y Tecnología de los Estados Unidos tiene una base de datos de herramientas para el análisis forense digital con capacidad de búsqueda y herramientas multifuncionales (p. ej., herramientas de análisis forense en la nube, entre otras) (para más información sobre las herramientas forenses digitales, consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital).

¿Sabían que...?

El triaje, la ***«revisión de los atributos y contenidos de las fuentes potenciales de datos»***, puede realizarse «antes de la obtención para reducir la cantidad de datos obtenidos, evitar la obtención de información irrelevante o cumplir con las restricciones de la autoridad de búsqueda» (Recolección enfocada y evaluación de pruebas digitales del SWGDE).

¿Desean saber más?

Para obtener más información sobre el triaje, consulte ***Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital.***

Los dispositivos digitales incautados se consideran la fuente primaria de pruebas. El analista forense digital no obtiene datos de la fuente primaria. Por el contrario, se hace un duplicado del contenido de dicho dispositivo y el analista trabaja en la copia. Esta copia duplicada del contenido del dispositivo digital (imágenes) se crea antes de que se realice una obtención estática para mantener la integridad de las pruebas digitales (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). Para verificar si el duplicado es una copia exacta del original, se calcula un valor de hash criptográfico para el original y el duplicado mediante cálculos matemáticos; si coinciden, el contenido de la copia es una imagen espejo (un duplicado) del contenido original (Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). Se debe utilizar un bloqueador de escritura, diseñado para evitar la alteración de los datos durante el proceso de copia (Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital), antes de la extracción, siempre que sea posible, con la finalidad de evitar la modificación de los datos durante el proceso de copia (Mejores prácticas para la obtención forense computarizada del SWGDE, 2018). Es importante señalar que el proceso de obtención descrito anteriormente se aplica principalmente a las computadoras. Cuando se extraen datos de teléfonos celulares y dispositivos similares, en los que el almacenamiento de la memoria no puede separarse físicamente del dispositivo para producir una imagen, se sigue un procedimiento diferente (consulte, por ejemplo, Mejores prácticas para la conservación y obtención de pruebas de dispositivos móviles del SWGDE, 2018; Mejores prácticas para el análisis forense de teléfonos celulares del SWGDE, 2013).

Se realizan dos tipos de extracción: física y lógica. La extracción física implica buscar y obtener pruebas del punto dentro de un dispositivo digital que contiene las pruebas, como el disco duro de una computadora (Maras, 2014). La extracción física puede realizarse mediante búsquedas de palabras clave (basadas en los términos proporcionados por el investigador), el file carving (es decir, «la búsqueda basada en el encabezado, el pie de página y otros identificadores») y el análisis del espacio no asignado (es decir, el «espacio disponible en un sistema porque nunca fue utilizado o porque la información en él fue eliminada»; Maras, 2014, p. 36) y las particiones, que separan los segmentos del disco duro entre sí (Casey, 2011; Maras, 2014; Nelson et al., 2015). La extracción lógica implica buscar y obtener pruebas de la ubicación en que:

> **Se encuentran en relación con el sistema de archivos** de un sistema operativo de computadora, que se utiliza para hacer seguimiento de los nombres y las ubicaciones de los archivos que se almacenan en un medio de almacenamiento como un disco duro. (Maras, 2014, p. 36)

El tipo de extracción lógica que se realiza depende del dispositivo digital, el sistema de archivos, las aplicaciones en el dispositivo y el sistema operativo. Una extracción lógica implica obtener datos de archivos activos y eliminados, sistemas de archivos, espacio no asignado y no utilizado, y datos comprimidos, cifrados y protegidos con contraseña (Nelson et al., 2015; Mejores prácticas para la recolección de pruebas digitales del SWGDE, 2018).

Nota

Una extracción lógica de archivos puede dar lugar a una pérdida de metadatos (es decir, datos sobre los datos) (Mejores prácticas para la obtención forense computarizada del SWGDE, 2018).

Todo el proceso de obtención debe ser documentado. Esta documentación debe incluir información detallada sobre los dispositivos digitales de los que se extrajeron las pruebas, el hardware y el software utilizados para obtener dichas pruebas, la manera en que se extrajeron (es decir, cómo se obtuvieron), cuándo se obtuvieron, dónde se obtuvieron, por qué se obtuvieron, qué pruebas se obtuvieron y por qué razón se obtuvieron (Maras, 2014).

Conservación

La conservación de pruebas busca proteger las pruebas digitales contra las modificaciones. La integridad de las pruebas digitales debe mantenerse en cada fase del manejo de dichas pruebas (ISO/IEC 27037). Los primeros en responder, investigadores, técnicos de la escena del delito o expertos en análisis forense digital deben demostrar, siempre que sea posible, que no se modificaron las pruebas digitales durante la fase de identificación, recolección y obtención; la capacidad de demostrarlo, por supuesto, depende del dispositivo digital (p. ej., computadora y teléfonos móviles) y de las circunstancias que deben enfrentar (p. ej., la necesidad de conservar rápidamente los datos). Para demostrar que no se modificaron las pruebas digitales durante la fase de identificación, se debe mantener una cadena de custodia. La cadena de custodia es:

> "El proceso por el cual los investigadores conservan la escena del delito (o incidente) y las pruebas a lo largo del ciclo de vida de un caso. Esta incluye información sobre quiénes recogieron las pruebas, dónde y cómo se recogieron las pruebas, qué individuos tomaron posesión de las pruebas y cuándo lo hicieron. (Maras, 2014, p. 377; Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital)"

En la cadena de custodia, se deben documentar los nombres, los títulos y la información de contacto de las personas que identificaron, recolectaron y obtuvieron las pruebas, así como de las demás personas que recibieron las pruebas, los detalles sobre las pruebas que fueron trasladadas, la hora y fecha del traslado y el propósito de dicho traslado.

Análisis y presentación de informes

Además del manejo de las pruebas digitales, el proceso de análisis forense digital también implica evaluar e interpretar las pruebas digitales (fase de análisis) y comunicar los resultados del análisis (fase de presentación de informes). Durante la fase de análisis, se extraen las pruebas digitales del dispositivo, se analizan los datos y se reconstruyen los eventos. Antes del análisis de pruebas digitales, se debe informar al analista forense digital en el laboratorio de los objetivos de la investigación, y se le debe proporcionar los antecedentes del caso y cualquier otra información que se haya obtenido durante la investigación y que pueda ayudar al analista forense en esta fase (p. ej., la dirección IP o las direcciones MAC). Se realizan diversos tipos de análisis en función del tipo de pruebas digitales buscadas, como el análisis de redes, sistemas de archivos, aplicaciones, vídeos, imágenes y medios (es decir, el análisis de los datos en el dispositivo de almacenamiento) (Grance et al., 2005; Carrier, 2005; Red Europea de Institutos de Ciencias Forenses, 2015; Mejores prácticas para la autenticación de imágenes del SWGDE, 2018; Mejores prácticas para el análisis de contenido de imágenes del SWGDE, 2017; Directrices para el análisis forense de imágenes del SWGDE, 2017; Mejores prácticas para la obtención de datos recuperados de grabadoras de video digital del SWGDE, 2018; Mejores prácticas para la obtención de pruebas de video digital y multimedia recuperadas de almacenamiento en la nube del SWGDE, 2018). Se analizan los archivos para determinar su origen, y cuándo y dónde se crearon, modificaron, accedieron, descargaron o cargaron los datos, así como la posible conexión de estos archivos en los dispositivos de almacenamiento con, por ejemplo, un almacenamiento remoto, como el almacenamiento en la nube (Carrier, 2005). El tipo de pruebas digitales (p. ej., correos electrónicos, mensajes de texto, geolocalización, documentos de procesamiento de textos, imágenes, videos y registros de conversaciones) buscadas depende del caso de delito cibernético.

Generalmente, existen cuatro tipos de análisis que pueden realizarse en computadoras: análisis de tiempo, análisis de propiedad y posesión, análisis de aplicaciones y archivos, y análisis de ocultación de datos. El análisis de tiempo busca crear una línea de tiempo o una secuencia de acciones mediante el uso de marcas de tiempo (fecha y hora) que condujeron a un evento, o para determinar la hora y la fecha en que un usuario realizó alguna acción (Instituto Nacional de Justicia de los Estados Unidos, 2004b). Este análisis se realiza para atribuir un delito a un delincuente o, por lo menos, atribuir un acto que llevó a un individuo en particular a cometer un delito (Instituto Nacional de Justicia de los Estados Unidos, 2004b); sin embargo, existen retos en la validación de los resultados del análisis de tiempo (consulte el recuadro Nota).

El análisis de propiedad y posesión se usa para determinar la persona que creó, accedió o modificó los archivos en un sistema informático (Instituto Nacional de Justicia de los Estados Unidos, 2004b). Por ejemplo, este análisis puede revelar una imagen de material de abuso sexual infantil (es decir, la «representación, por cualquier medio, de un menor que participa en actividades sexuales explícitas reales o simuladas o la representación de las partes íntimas de un menor con fines principalmente sexuales»; artículo 2, Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de menores, la prostitución infantil y la pornografía infantil de las Naciones Unidas de 2000) en el dispositivo del sospechoso. Esta información por sí sola no es suficiente para probar la propiedad del material de abuso sexual infantil. Se necesitan más pruebas para demostrarlo, como el uso exclusivo de la computadora donde se encontró el material. El análisis de aplicaciones y archivos se realiza para examinar las aplicaciones y los archivos de un sistema informático para determinar el conocimiento, la intención y las capacidades del perpetrador para cometer un delito cibernético (por ejemplo, el etiquetado o el nombre del archivo puede indicar el contenido del mismo; p. ej., el nombre del archivo puede ser el nombre de la víctima del delito cibernético) (Instituto Nacional de Justicia de los Estados Unidos, 2004b).

Nota

Los datos de la marca de tiempo pueden ser modificados. Por consiguiente, no se debe llegar a una conclusión basada solo en dicha evidencia. Lo mismo aplica para otros datos. Por ejemplo, el historial del navegador web muestra que se ha accedido a los sitios y las horas en que se ha accedido a ellos. Se necesitan más pruebas para demostrar que la persona cuya prueba digital se utilizó para acceder a estos sitios web era el propietario o el sospechoso usuario del dispositivo.

También se puede realizar un análisis de ocultación de datos. Como su nombre lo indica, el análisis de ocultación de datos busca datos ocultos en un sistema. Los delincuentes utilizan varias técnicas de ocultación de datos para ocultar sus actividades ilícitas y la información de identificación, como el uso del cifrado (discutido en Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención de delitos cibernéticos: aplicaciones y medidas prácticas, así como en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos), de dispositivos de protección de contraseñas y de contenidos específicos (p. ej., archivos), cambiando las extensiones de los archivos y ocultando particiones (Instituto Nacional de Justicia de los Estados Unidos, 2004b; Casey, 2011; Maras, 2014; Nelson et al., 2015). Durante la fase de análisis, el investigador necesita abordar las técnicas de ocultación de datos que los delincuentes podrían haber utilizado para ocultar sus identidades y actividades. Los datos ocultos pueden revelar «el conocimiento [de un delito], la propiedad [del contenido] o la intención [de cometer un delito]» (Instituto Nacional de Justicia de los Estados Unidos, 2004b, p. 17).

Nota

Cuando se borra un archivo en una computadora, se reubica en la papelera o papelera de reciclaje. Si se vacía la papelera o papelera de reciclaje (es decir, mediante el borrado de contenido), los archivos borrados se eliminan de la tabla de asignación de archivos, que archiva los nombres de los archivos y las ubicaciones en los discos duros (Maras, 2014). El espacio donde se encuentra el archivo se marca como espacio libre (es decir, espacio no asignado) después de ser borrado, pero el fichero sigue ubicado en ese espacio (al menos hasta que se sobrescribe total o parcialmente con nuevos datos) (Maras, 2014).

Como concluyó el Instituto Nacional de Justicia de los Estados Unidos, «por sí solos, los resultados obtenidos de cualquiera de estos (...) [análisis] pueden no ser suficientes para llegar a una conclusión. Sin embargo, cuando se consideran en conjunto, las conexiones entre los resultados individuales pueden proporcionar una imagen más completa» (p. 18).

El propósito de estos análisis es la reconstrucción del delito (o la reconstrucción del evento). La reconstrucción de eventos busca determinar quién fue responsable del evento, qué ocurrió, dónde ocurrió el evento, cuándo tuvo lugar y cómo se desarrolló el evento, a través de la identificación, recopilación y vinculación de datos (revelando el «panorama general» o esencia de un evento). La reconstrucción de eventos puede implicar un análisis temporal (es decir, la determinación de los eventos de tiempo que ocurrieron y la secuencia de dichos eventos), un análisis relacional (es decir, la determinación de los individuos involucrados y lo que hicieron, y la conexión y relaciones entre estos individuos) y un análisis funcional (es decir, la evaluación de rendimiento y capacidades de los sistemas y dispositivos involucrados en los eventos) (Casey, 2010; Casey, 2011; Kao, 2016). En términos generales, se realiza la reconstrucción del evento para probar o refutar una hipótesis de trabajo relativa al caso (es decir, una conjetura fundada relativa a la secuencia de actos que condujeron a un evento) (ENFSI, 2015).

En última instancia, la reconstrucción del evento para la fase de análisis utiliza un conocimiento imperfecto para sacar conclusiones sobre un caso basado en las pruebas disponibles y en los análisis de las pruebas. Por este motivo, es importante que los investigadores de delitos cibernéticos y los analistas forenses digitales reconozcan estas limitaciones y eviten interpretaciones sesgadas de los resultados de estos análisis, como las que resultan del sesgo de confirmación, donde los individuos buscan y apoyan resultados que respaldan sus hipótesis de trabajo y descartan los resultados que entran en conflicto con ella (Kassin et al., 2013; Boddington, 2016).

Nota

Los investigadores deben participar en actividades reconstructivas preliminares en las etapas de identificación y recolección de la investigación. Estas tareas ayudan a los investigadores a identificar nuevas fuentes potenciales de pruebas digitales.

Los resultados del análisis se documentan en un informe. Los informes deben ser tan claros y precisos como sea posible. Se debe incluir material demostrativo (como cifras, gráficos, resultados de herramientas) y documentos de apoyo, como la documentación sobre la cadena de custodia, junto con una explicación detallada de los métodos utilizados y los pasos dados para examinar y extraer los datos (Instituto Nacional de Justicia de los Estados Unidos, 2004b). Los hallazgos deberán explicarse a la luz de los objetivos del análisis (es decir, el propósito de la investigación y el caso que se está investigando). El informe también debe incluir la información sobre las limitaciones de los hallazgos. El contenido del informe varía según la jurisdicción en función de las políticas nacionales (cuando existan) relativas a las investigaciones y al análisis forense digital. Para evitar la mala interpretación o la atribución de un peso inadecuado a las pruebas digitales, el informe debe comunicar los errores conocidos y la incertidumbre de los resultados (Red Europea de Institutos de Ciencias Forenses, 2015, p. 39).

Admisibilidad de pruebas digitales

Deben cumplirse ciertos requisitos legales y técnicos para garantizar la admisibilidad de las pruebas digitales en un tribunal de justicia (Antwi-Boasiako y Venter, 2017). En cuanto a los requisitos legales, el tribunal evalúa la autorización legal para llevar a cabo registros e incautaciones de los datos provenientes de las tecnologías de la información y la comunicación y otros relacionados, y la pertinencia, autenticidad, integridad y fiabilidad de las pruebas digitales (Antwi-Boasiako y Venter, 2017). Con respecto a este último aspecto, el tribunal evalúa de manera crítica los procedimientos e instrumentos de análisis forense digital utilizados para extraer, conservar y analizar las pruebas digitales; los laboratorios digitales donde se realizan los análisis; los informes de los analistas forenses digitales, y las calificaciones técnicas y académicas de dichos analistas y de los testigos periciales (si fuese necesario) (Antwi-Boasiako y Venter, 2017). Antwi-Boasiako y Venter (2017) desarrollaron un marco, el Modelo armonizado para la evaluación de la admisibilidad de las pruebas digitales (HM-DEAA), que contiene los requisitos técnicos y legales esenciales que determinan la admisibilidad de dichas pruebas. En particular, el HM-DEAA propone un modelo de tres fases para evaluar la admisibilidad de las pruebas, el cual incluye la evaluación, consideración y determinación de dichas pruebas digitales. El marco del HM-DEAA se utiliza en la siguiente sección de este módulo para destacar los requisitos legales y técnicos utilizados mayormente en todas las jurisdicciones para garantizar la admisibilidad de las pruebas digitales en los tribunales nacionales.

Deben cumplirse ciertos requisitos legales y técnicos para garantizar la admisibilidad de las pruebas digitales en un tribunal de justicia (Antwi-Boasiako y Venter, 2017). En cuanto a los requisitos legales, el tribunal evalúa la autorización legal para llevar a cabo registros e incautaciones de los datos provenientes de las tecnologías de la información y la comunicación y otros relacionados, y la pertinencia, autenticidad, integridad y fiabilidad de las pruebas digitales (Antwi-Boasiako y Venter, 2017). Con respecto a este último aspecto, el tribunal evalúa de manera crítica los procedimientos e instrumentos de análisis forense digital utilizados para extraer, conservar y analizar las pruebas digitales; los laboratorios digitales donde se realizan los análisis; los informes de los analistas forenses digitales, y las calificaciones técnicas y académicas de dichos analistas y de los testigos periciales (si fuese necesario) (Antwi-Boasiako y Venter, 2017). Antwi-Boasiako y Venter (2017) desarrollaron un marco, el Modelo armonizado para la evaluación de la admisibilidad de las pruebas digitales (HM-DEAA), que contiene los requisitos técnicos y legales esenciales que determinan la admisibilidad de dichas pruebas. En particular, el HM-DEAA propone un modelo de tres fases para evaluar la admisibilidad de las pruebas, el cual incluye la evaluación, consideración y determinación de dichas pruebas digitales. El marco del HM-DEAA se utiliza en la siguiente sección de este módulo para destacar los requisitos legales y técnicos utilizados mayormente en todas las jurisdicciones para garantizar la admisibilidad de las pruebas digitales en los tribunales nacionales.

Manejo de pruebas digitales

En esta fase, los tribunales determinan si se utilizó la autorización legal apropiada para registrar e incautar los datos provenientes de las tecnologías de la información y la comunicación (TIC) y aquellos relacionados. Los tipos de autorización legal incluyen una orden de registro, una orden judicial o una citación. La orden legal necesaria para obtener datos sobre los datos de las TIC y aquellos relacionados varía según la jurisdicción y está determinado por las leyes nacionales (consulte Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos). Sin embargo, la orden legal que los países utilizan predominantemente para incautar las TIC es una orden de registro. No obstante, las leyes nacionales difieren en los requisitos para obtener las órdenes legales en función de las circunstancias del caso, las circunstancias que rodean el registro y la incautación, y las credenciales de quienes realizan el registro (consulte Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos para obtener más información sobre las órdenes legales necesarias para acceder a los datos en todas las jurisdicciones).

Nota

Las pruebas digitales pueden revelar el comportamiento característico de los delincuentes cibernéticos, como los desarrolladores de programas maliciosos y los hackers (Casey, 2011). Un comportamiento característico es un patrón reconocible y distinguible de actividades (p. ej., técnicas, instrumentos y apodo específicos) que puede atribuirse a una fuente y proporciona algún tipo de beneficio psicológico o emocional (p. ej., gratificación y reconocimiento por parte de pares) al delincuente cibernético (Casey, 2011).

La relevancia forense de las pruebas digitales también se evalúa en esta fase. La pertinencia forense se determina según si las pruebas digitales vinculan o descartan una conexión entre el autor del delito y el objetivo (p. ej., la víctima, el dispositivo digital, el sitio web, etc.) o la escena del delito (el lugar donde se produjo el delito o el delito cibernético); 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 (modus operandi o MO) del autor del delito (es decir, los hábitos, técnicas y características singulares del comportamiento del delincuente) y si demuestran que se produjo un delito (corpus delicti) (Maras, 2014; Maras y Miranda, 2014).

Análisis y presentación de informes

En esta fase se evalúa la integridad de las pruebas digitales examinando los procedimientos y las herramientas forenses digitales utilizadas para obtener dichas pruebas, la competencia y las cualificaciones de los expertos forenses digitales que las han obtenido, conservado y analizado (la competencia y las cualificaciones de los expertos varían según cada país, consulte Delitos Cibernéticos-Módulo 5: Investigaciones de delitos cibernéticos) y los laboratorios forenses digitales en los que se manejaron y examinaron las pruebas (Instituto Nacional de Justicia de los Estados Unidos; 2004a; Maras, 2014). En esencia, esta evaluación busca determinar si se utilizaron principios científicos para conservar, obtener y analizar las pruebas digitales, y si se cumplieron los estándares para gestionar y examinar las pruebas digitales (p. ej., si las herramientas de análisis forense digital fueron validadas, actualizadas, mantenidas adecuadamente y probadas antes de su uso, para garantizar su funcionamiento correcto).

Los expertos en análisis forense digital testifican ante los tribunales para explicar sus cualificaciones; cómo funcionan los dispositivos digitales, las plataformas en línea y otras fuentes relacionadas con las TIC; el proceso del análisis forense digital; por qué se utilizó una herramienta de análisis forense digital específica y no otras; cómo se conservaron, obtuvieron y analizaron las pruebas digitales; la interpretación y los hallazgos de los análisis realizados, así como la exactitud de estas interpretaciones y cualquier alteración que pueda haberse producido en los datos y por qué se produjeron estas alteraciones (Instituto Nacional de Justicia de los Estados Unidos; 2004a; Maras, 2014).

También se examinan las cualificaciones de los expertos en análisis forense digital para determinar la competencia de los individuos que manejan y analizan las pruebas digitales. Esta competencia es esencial para garantizar la calidad de los productos de trabajo y la confianza en los resultados producidos (Resumen del proceso de acreditación de laboratorios forenses digitales y multimedia del SWGDE, 2017). No obstante, no existen estándares universales de competencias para los expertos en análisis forense digital. Las cualificaciones de los expertos en análisis forense digital varían en función del país (UNODC, 2013). La certificación de los expertos en análisis forense digital puede o no ser necesaria, dependiendo de la jurisdicción (UNODC, 2013). Por consiguiente, esta fase evalúa si los expertos tienen las cualificaciones necesarias para actuar como testigos periciales o realizar los exámenes requeridos de las TIC y los datos relacionados con dichas TIC. Lo que también se determina es si la competencia de estos expertos y analistas fue verificada y puesta a prueba.

Nota

El Daubert Tracker, llamado así por el caso estadounidense Daubert contra Merrell Dow Pharmaceuticals Inc. (1993), que establece los criterios que las cortes de los Estados Unidos utilizan para determinar la confiabilidad de una evaluación forense presentada en la corte, mantiene un registro de los casos legales denunciados y no denunciados en los que los métodos y cualificaciones de los expertos han sido cuestionados (Maras, 2014).

También se examinan las normas y protocolos del laboratorio de análisis forense digital para determinar la competencia del laboratorio en el manejo y análisis de las pruebas digitales y la producción de resultados fiables. Lo que se examina en particular es si «el laboratorio utiliza métodos fiables, equipos y programas informáticos adecuados, personal competente y si llega a conclusiones razonables» (Resumen del proceso de acreditación de laboratorios forenses digitales y multimedia del SWGDE, 2017, p. 4). La acreditación ayuda en este empeño «proporcionando un medio para mejorar la calidad, evaluar el desempeño, dar una revisión independiente, cumplir con las normas establecidas y servir para asegurar la promoción, el fomento y mantenimiento de los estándares más altos de la práctica forense» (Barbara, 2012). Aunque la ISO/IEC 17025 «se esfuerza por estandarizar los laboratorios en todo el mundo en términos de pruebas, control de calidad y calibración», el apoyo que le brinda la comunidad del análisis forense digital es diverso (Merriott, 2018). Además, aunque la acreditación proporciona los mecanismos de supervisión y responsabilidad necesarios para garantizar que se cumplen las normas de la práctica forense (Mitos y verdades sobre la acreditación de laboratorios de pruebas digitales y multimedia del SWGDE, 2017), no se practica de manera universal. En los Estados Unidos, por ejemplo, la acreditación es requerida por algunos estados, pero no por todos (Barbara, 2012). En el Reino Unido, el Regulador de las Ciencias Forenses acredita a las organizaciones que participan en el análisis forense digital (Forensic Access, 2017), mientras que, en Sudáfrica, la agencia nacional designada para la acreditación es el Sistema Nacional de Acreditación de Sudáfrica (SANAS, 2016; consulte la Ley N.º 19 de 2006, es decir, la Ley de Acreditación para la Evaluación de Conformidad, Calibración y Buenas Prácticas de Laboratorio de 2006).

Determinación de pruebas digitales

Esta fase evalúa la autenticidad, integridad y fiabilidad de las pruebas digitales en función de los resultados de la evaluación del proceso de análisis forense digital realizada en la fase anterior (es decir, la fase de consideración de las pruebas digitales), como el uso de métodos y herramientas forenses sólidos para obtener pruebas digitales y el testimonio de testigos periciales y analistas forenses digitales para corroborar la autenticidad, integridad y fiabilidad de dichas pruebas (Antwi-Boasiako y Venter, 2017; Instituto Nacional de Justicia de los Estados Unidos, 2004a). Una prueba digital es admisible si establece algún hecho alegado en el caso, si se mantuvo inalterada durante el proceso del análisis forense digital y si los resultados del análisis son válidos, fiables y sometidos a revisión por pares (Brezinski y Killalea, 2002; Instituto Nacional de Justicia de los EE. UU., 2004a; Red Europea de Institutos de Ciencias Forenses, 2015). Para ser admisibles, los hallazgos deben ser interpretados de manera imparcial, y deben revelarse los errores e incertidumbres en estos, así como las limitaciones en la interpretación de dichos hallazgos (Brezinski y Killalea, 2002; Red Europea de Institutos de Ciencias Forenses, 2015).

Por último, este modelo de tres fases consolida los requisitos legales y técnicos comunes para la admisibilidad de pruebas en todas las jurisdicciones (Antwi-Boasiako y Venter, 2017). La estandarización de las prácticas del análisis forense digital es fundamental para garantizar la admisibilidad de las pruebas digitales en todas las jurisdicciones. Dada la naturaleza transnacional del delito cibernético, la armonización de las prácticas del análisis forense digital no solo es de suma importancia para la investigación de los delitos cibernéticos, sino que también es esencial para la cooperación internacional al respecto (discutido en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos).

¿Sabían que...?

Al igual que el análisis forense digital, el e-discovery es un proceso mediante el cual los datos digitales «se buscan, localizan, aseguran e investigan con la finalidad de utilizarlos como pruebas en un caso legal» (Lawton et al., 2014, p. 4). Sin embargo, existen diferencias clave entre el análisis forense digital y el *e-discovery*. A diferencia del análisis forense digital, el *e-discovery* se enfoca principalmente en la conservación de datos con fines de registro (de la manera más rentable) y con la finalidad de cumplir los requisitos legales para producir pruebas digitales en los procedimientos judiciales cuando un tribunal así lo ordena.

¿Desean saber más?

Lawton, D., Stacey, R. & Dodd, G. (2014). eDiscovery in digital forensic investigations. UK Home Office. CAST Publication Number 32/14.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf

Referencias

- ***Antwi-Boasiako, A. & Venter, H. (2017).*** A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). Advances in Digital Forensics (pp. 23-38).

- ***Barbara, J. (2012).*** ISO/IEC 17025:2005 Accreditation of the Digital Forensics Discipline in Perspective. Forensic Magazine.

- ***Boddington, R. (2016).*** A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial. Annual ADFSL Conference on Digital Forensics, Security and Law.

- ***Brezinski, D. & Killalea, T. (2002).*** Guidelines for Evidence Collection and Archiving. Request for Comments: 3227.

- ***Carrier, B. (2005).*** File System Forensic Analysis. Pearson.

- ***Casey, E. (2011).*** Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd Edition). Academic Press.

- ***Casey, E. (2010).*** Handbook of digital forensics and investigation. Elsevier.

- ***Cloud Security Alliance. (2013).*** Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing.
  • *https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf*

- ***Conlan, K., Baggili, I. & Breitinger, F. (2016).*** Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18, 66-75.

- ***Data Security Council of India. (2011).*** Cyber Crime Investigation Manual.

- ***European Network of Forensic Science Institute. (2015).*** Best practice manual for the forensic examination of digital technology. ENFSI-BPM-FIT-01.

- ***Finklea, K. (2017).*** Law Enforcement Using and Disclosing Technology Vulnerabilities Specialist in Domestic Security. Congressional Research Service, R44827.

- ***Forensic Access. (2017).*** Forensic Services. United Kingdom.
  • *https://www.forensic-access.co.uk/forensic-services/*

- ***Grance, T., Chevalier, S., Kent, K. & Dang, H. (2005).*** Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, Special Publication 800-86.

- ***ISFCE. (n.d.).*** Code of Ethics and Professional Responsibility.

- ***ISO/IEC 17025. (2017).*** Testing and calibration laboratories.
  • *https://www.iso.org/home/standards/popular-standards/isoiec-17025-testing-and-calibra.html*

- ***ISO/IEC 27037. (2012).*** Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.

- ***Kao, DY. (2016).*** Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments. The Journal of Supercomputing, 72(1), 141-160.

- ***Kizza, J.M. (2013).*** Computer Crime Investigations and Ethics. In: Ethical and Social Issues in the Information Age (Fifth Edition). Springer; Chapter 15.

- ***Lawton, D., Stacey, R. & Dodd, G. (2014).*** eDiscovery in digital forensic investigations. UK Home Office. CAST Publication Number 32/14.

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett.

- ***Merriott, R. (2018).*** ISO 17025 For Digital Forensics - Yay or Nay. Forensic Focus.

- ***Nelson, B., Phillips, A. & Steuart, C. (2016).*** Guide to Computer Forensics and Investigations (5th Edition). Cengage Learning.

- ***NIST. (n.d.).*** Computer Forensics Tool Testing Program (CFTT).

- ***Police Service of Scotland. (2018).*** Digitally Stored Evidence Standard Operating Procedure, Version 2.

- ***Quick, D., Martini, B. & Choo, R. (2014).*** Cloud Storage Forensics. Elsevier.

- ***Roux, B. & Falgoust, M. (2012).*** Ethical issues raised by data acquisition methods in digital forensics research. Journal of Information Ethics, 21(1), 40-60.

- ***Sammons, J. (2012).*** The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

- ***SANAS. (2016).*** Criteria For Laboratory Accreditation in the Field of Forensics. TG 01-02.
  - *http://www.sanas.co.za/manuals/pdfs/TG%2001-02.pdf?manualsOrder=Sorter_doc_title&manualsDir=ASC&manualsPage=4*

- ***Seigfried-Spellar, K.C., Rogers, M. & Crimmins, D.M. (2017).*** Development of A Professional Code of Ethics in Digital Forensics. Annual ADFSL Conference on Digital Forensics, Security and Law, 135-144.

- ***Sharevski, F. (2015).*** Rules of professional responsibility in digital forensics: A comparative analysis. Journal of Digital Forensics, Security and Law, 10(2), 39-54.

- ***SWGDE. (2018).*** SWGDE Best Practices for Computer Forensic Acquisitions.
  - *https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Acquisitions*

- ***SWGDE. (2018).*** SWGDE Best Practices for Computer Forensic Examination.
  - *https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Examination*

- ***SWGDE. (2018).*** SWGDE Best Practices for Data Acquisition from Digital Video Recorders.
  - *https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Data%20Acquisition%20from%20Digital%20Video%20Recorders*

- ***SWGDE. (2018).*** SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage.
  - *https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Digital%20and%20Multimedia%20Evidence%20Video%20Acquisition%20from%20Cloud%20Storage*

- ***SWGDE. (2018).*** SWGDE Best Practices for Image Authentication.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Image%20Authentication

- ***SWGDE. (2017).*** SWGDE Best Practices for Image Content Analysis.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Image%20Content%20Analysis

- ***SWGDE. (2018).*** SWGDE Best Practices for Mobile Device Evidence Collection and Preservation, Handling and Acquisition (Draft).
  • https://www.swgde.org/documents/Released For Public Comment/SWGDE Best Practices for Mobile Device Evidence and Collection, Preservation, and Acquisition

- ***SWGDE. (2013).*** SWGDE Best Practices for Mobile Phone Forensics.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics

- ***SWGDE. (2018).*** SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20the%20Acquisition%20of%20Data%20from%20Novel%20Digital%20Devices

- ***SWGDE. (2014).*** SWGDE Capture of Live Systems.
  • https://www.swgde.org/documents/Current%20Documents/SWGDE%20Capture%20of%20Live%20Systems

- ***SWGDE. (n.d.).*** SWDGE Drafts For Public Comment.
  • https://www.swgde.org/documents/draftsForPublicComment

- ***SWGDE. (2017).*** SWGDE Guidelines for Forensic Image Analysis.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Guidelines%20for%20Forensic%20Image%20Analysis

- ***SWGDE. (2017).*** SWGDE Myths and Facts about Accreditation for Digital and Multimedia Evidence Labs.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Myths%20and%20Facts%20about%20Accreditation%20for%20Digital%20and%20Multimedia%20Evidence%20Labs

- ***SWGDE. (2017).*** SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Overview%20of%20the%20Accreditation%20Process%20for%20Digital%20and%20Multimedia%20Forensic%20Labs

- ***SWGDE. (2014).*** SWGDE Recommended Guidelines for Validation Testing.
  •https://www.swgde.org/documents/Current%20Documents/SWGDE%20Recommended%20Guidelines%20for%20Validation%20Testing

- ***UNODC. (2013).*** Draft Comprehensive Study on Cybercrime.

- ***US National Institute of Justice. (2004a).*** Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors.

- ***US National Institute of Justice. (2008).*** Electronic Crime Scene Investigation: A Guide for First Responders (Second Edition).

- ***US National Institute of Justice. (2004b).*** Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

- ***US National Institute of Justice. (2007b).*** Investigative Uses of Technology: Devices, Tools, and Techniques.
- ***US National Institute of Justice. (2007a).*** Investigations Involving the Internet and Computer Networks.

Casos

- ***Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993).***

Leyes

- ***Accreditation for Conformity Assessment, Calibration and Good Laboratory Practice Act of 2006 (South Africa).***
  - *https://www.thedti.gov.za/business_regulation/acts/accreditation_act.pdf*
- ***Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography of 2000 (United Nations).***
  - *https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx*

Lecturas principales

- ***Antwi-Boasiako, A. and Venter, H. (2017).*** A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). Advances in Digital Forensics (pp. 23-38).

- ***Casey, E. (2011).*** Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd Edition). Academic Press.

- ***European Network of Forensic Science Institute. (2015).*** Best practice manual for the forensic examination of digital technology. ENFSI-BPM-FIT-01.

- ***European Union Agency for Network and Information Security. (2014).*** Electronic Evidence - A Basic Guide for First Responders Good Practice Material for CERT First Responders.
  • *https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders*

- ***European Union Agency for Network and Information Security. (2016).*** Forensic Analysis Network Incident Response Toolset (Document for Students).

- ***European Union Agency for Network and Information Security. (2013).*** Identification and Handling of Electronic Evidence Handbook (Document for Teachers).

- ***Kao, D.Y. (2016).*** Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments. The Journal of Supercomputing, 72(1), 141-160.

- ***Kizza, J.M. (2013).*** Computer Crime Investigations and Ethics. In: Ethical and Social Issues in the Information Age (Fifth Edition). Springer; Chapters 4 and 15.

- ***Maras, M.H. (2014).*** Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett. Chapters 9-14.

- ***Nelson, B., Phillips, A. & Steuart, C. (2016).*** Guide to Computer Forensics and Investigations (5th Edition). Cengage Learning.

- ***Sammons, J. (2012).*** The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

Lecturas avanzadas

Se recomiendan las siguientes lecturas a los interesados en investigar los temas de este módulo en detalle:

- ***Boddington, R. (2016).*** A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial. Annual ADFSL Conference on Digital Forensics, Security and Law.

- ***Casey, E. (2010).*** Handbook of digital forensics and investigation. Elsevier.

- ***Choo, K.K.R. & Dehghantanha, A. (2017).*** Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Elsevier.

- ***EC-Council. (2017).*** Computer Forensics: Investigating Network Intrusions and Cybercrime (2nd Edition). Cengage.

- ***Grance, T., Chevalier, S., Kent, K. & Dang, H. (2005).*** Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, Special Publication 800-86.

- ***Kizza, J.M. (2013).*** Computer Crime Investigations and Ethics. In: Ethical and Social Issues in the Information Age (Fifth Edition). Springer.

- ***Lawton, D., Stacey, R. & Dodd, G. (2014).*** eDiscovery in digital forensic investigations. UK Home Office. CAST Publication Number 32/14.

- ***Ligh, M.H., Case, A., Levy, J. & Walters, A. (2014).*** The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons.

- ***Malin, C.H., Casey, E. & Aquilina, J.M. (2008).*** Malware Forensics: Investigating and Analyzing Malicious Code. Syngress.

- ***Messier, R. (2017).*** Network Forensics. John Wiley & Sons.

- ***Quick, D., Martini, B. & Choo, R. (2014).*** Cloud Storage Forensics. Elsevier.

- ***SWGDE. (2018).*** SWGDE Best Practices for Computer Forensic Acquisitions.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Acquisitions*

- ***SWGDE. (2018).*** SWGDE Best Practices for Computer Forensic Examination.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Examination*

- ***SWGDE. (2018).*** SWGDE Best Practices for Data Acquisition from Digital Video Recorders.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Data%20Acquisition%20from%20Digital%20Video%20Recorders*

- ***SWGDE. (2018).*** SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Digital%20and%20Multimedia%20Evidence%20Video%20Acquisition%20from%20Cloud%20Storage*

- ***SWGDE. (2018).*** SWGDE Best Practices for Image Authentication.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Image%20Authentication*

- ***SWGDE. (2017).*** SWGDE Best Practices for Image Content Analysis.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Image%20Content%20Analysis*

- ***SWGDE. (2018).*** SWGDE Draft Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition.
  •*https://www.swgde.org/documents/Released For Public Comment/SWGDE Best Practices for Mobile Device Evidence and Collection, Preservation, and Acquisition*

- ***SWGDE. (2018).*** SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20the%20Acquisition%20of%20Data%20from%20Novel%20Digital%20Devices*

- ***SWGDE. (2014). SWGDE Capture of Live Systems.***
  • *https://www.swgde.org/documents/Current%20Documents/SWGDE%20Capture%20of%20Live%20Systems*

- ***SWGDE. (n.d.).*** SWDGE Drafts For Public Comment.
  • *https://www.swgde.org/documents/draftsForPublicComment*

- ***SWGDE. (2017).*** SWGDE Guidelines for Forensic Image Analysis.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Guidelines%20for%20Forensic%20Image%20Analysis*

- ***SWGDE. (2017).*** SWGDE Myths and Facts about Accreditation for Digital and Multimedia Evidence Labs.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Myths%20and%20Facts%20about%20Accreditation%20for%20Digital%20and%20Multimedia%20Evidence%20Labs*

- ***SWGDE. (2017).*** SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Overview%20of%20the%20Accreditation%20Process%20for%20Digital%20and%20Multimedia%20Forensic%20Labs*

- ***SWGDE. (2014).*** SWGDE Recommended Guidelines for Validation Testing.
  •*https://www.swgde.org/documents/Current%20Documents/SWGDE%20Recommended%20Guidelines%20for%20Validation%20Testing*

- ***US National Institute of Justice. (2004a).*** Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors.

- ***US National Institute of Justice. (2008).*** Electronic Crime Scene Investigation: A Guide for First Responders (Second Edition).

- ***US National Institute of Justice. (2004b).*** Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

- ***US National Institute of Justice. (2007b).*** Investigative Uses of Technology: Devices, Tools, and Techniques.

- ***US National Institute of Justice. (2007a).*** Investigations Involving the Internet and Computer Networks.

Herramientas complementarias

Casos en los medios de comunicación

Estos casos pueden ser utilizados para estimular el debate:

- **NPR. (n.d.). FBI-Apple Encryption Dispute. NPR.**
  https://www.npr.org/series/469827708/the-apple-fbi-debate-over-encryption

- **Statt, N. (2016m April 14).** Canadian police have had master key to BlackBerry's encryption since 2010. The Verge.
  https://www.theverge.com/2016/4/14/11434926/blackberry-encryption-master-key-broken-canada-rcmp-surveillance

Ejercicios de simulación

Los especialistas pueden utilizar la siguiente información para crear ejercicios que simulan la obtención de datos forenses:

Existen varios tipos de imágenes de datos, como las basadas en unidades estáticas (ColdSnap), en sistemas en vivo (HotSnap) y en redes, etc. Para crear la imagen de la unidad o la red, existen soluciones de bloqueo de escritura basadas en *hardware* y *software*. En el siguiente enlace se puede encontrar una guía de muestra sobre los bloqueos de escritura: https://www.cru-inc.com/data-protection-topics/write-blockers/

El siguiente es un ejemplo de solución basada en *hardware*: Tableau Forensic Imager TX1:

Figura 1

Tableau Forensic Imager TX1

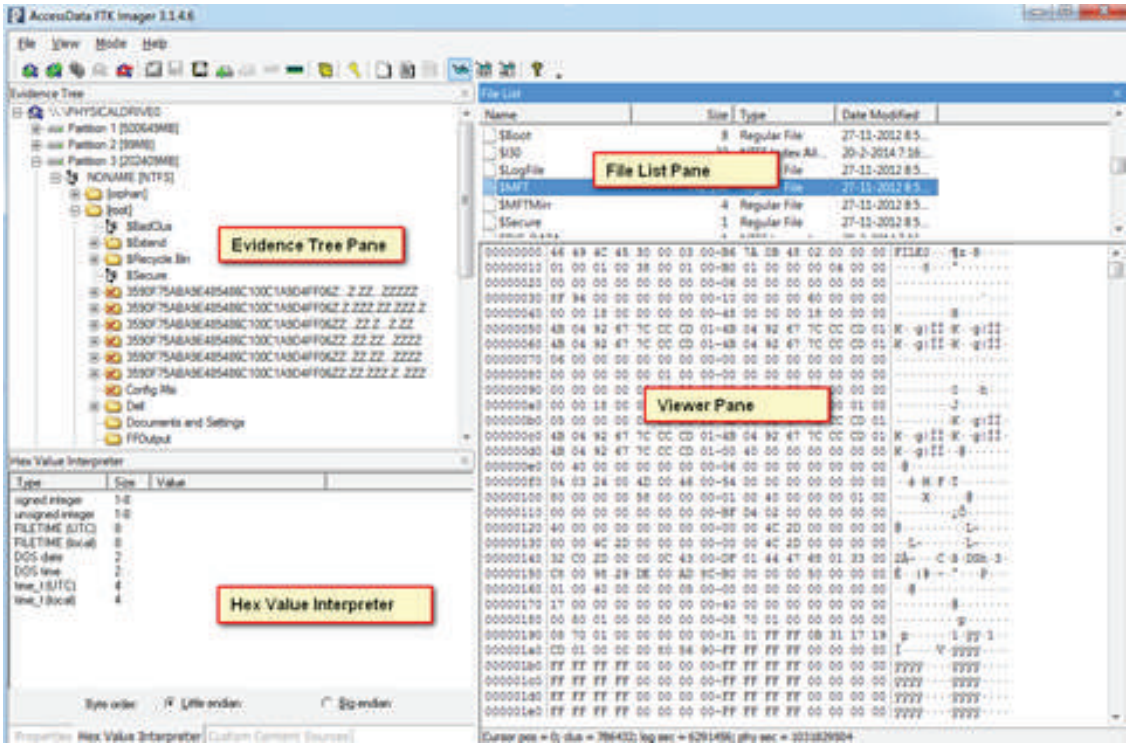
Nota

La imagen muestra el *hardware* Tableau Forensic Imager TX1. Tomado de Tableau Forensic Imager TX1, por Catalog, n.d., Forensic Computers. *https://www.forensiccomputers.com/media/catalog/product/t/x/tx1-05_1.jpg*

Guía de fuente: https://www.guidancesoftware.com/document/user-guide/tx1-forensic-imager-user-guide

Figura 2

FTK Imager



Los especialistas pueden utilizar la siguiente información para crear ejercicios que simulan la obtención de datos forenses:

Existen varios tipos de imágenes de datos, como las basadas en unidades estáticas (ColdSnap), en sistemas en vivo (HotSnap) y en redes, etc. Para crear la imagen de la unidad o la red, existen soluciones de bloqueo de escritura basadas en *hardware* y *software*. En el siguiente enlace se puede encontrar una guía de muestra sobre los bloqueos de escritura:
https://www.cru-inc.com/data-protection-topics/write-blockers/

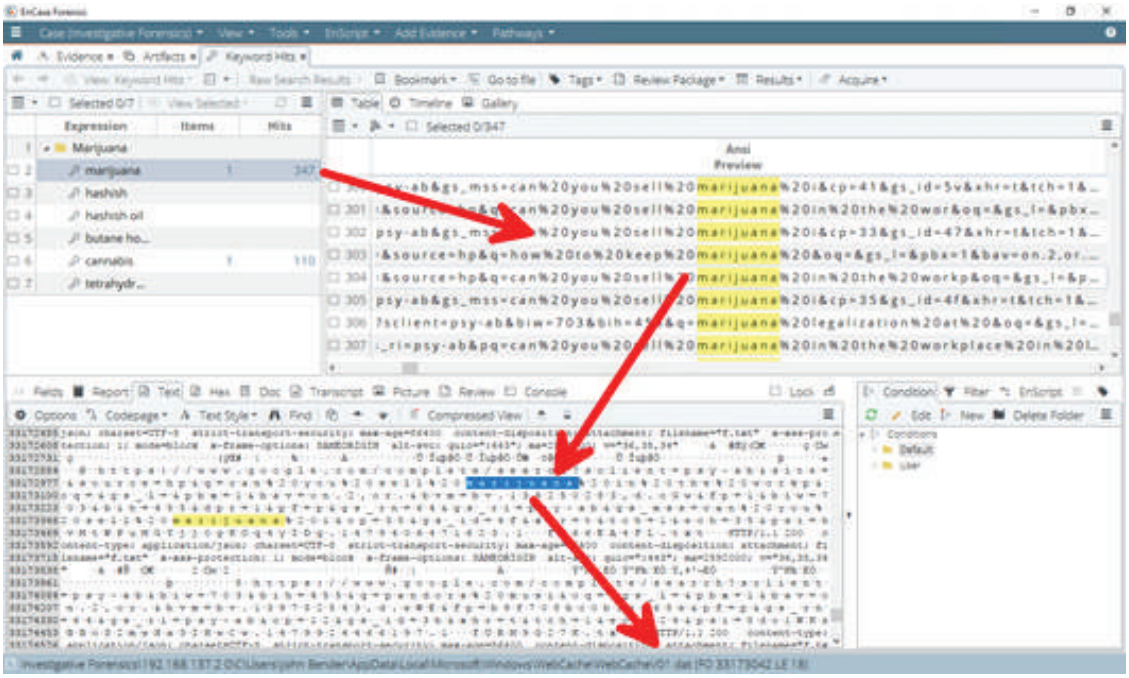
Nota

La imagen muestra el *software* FTK Imager. Tomado de FTK Imager, por eForensics Magazine, 2014, eForensics Magazine. *https://eforensicsmag.com/wp-content/uploads/2014/04/m1.png*

Un ejemplo de herramienta de ***análisis forense digital es EnCase.***

Figura 3

EnCase



En el siguiente enlace se puede encontrar una guía de muestra, a partir de la cual se puede crear un ejercicio de simulación utilizando esta herramienta:

https://www.digitalforensics.com/blog/how-to-use-the-encase-processor/

Nota

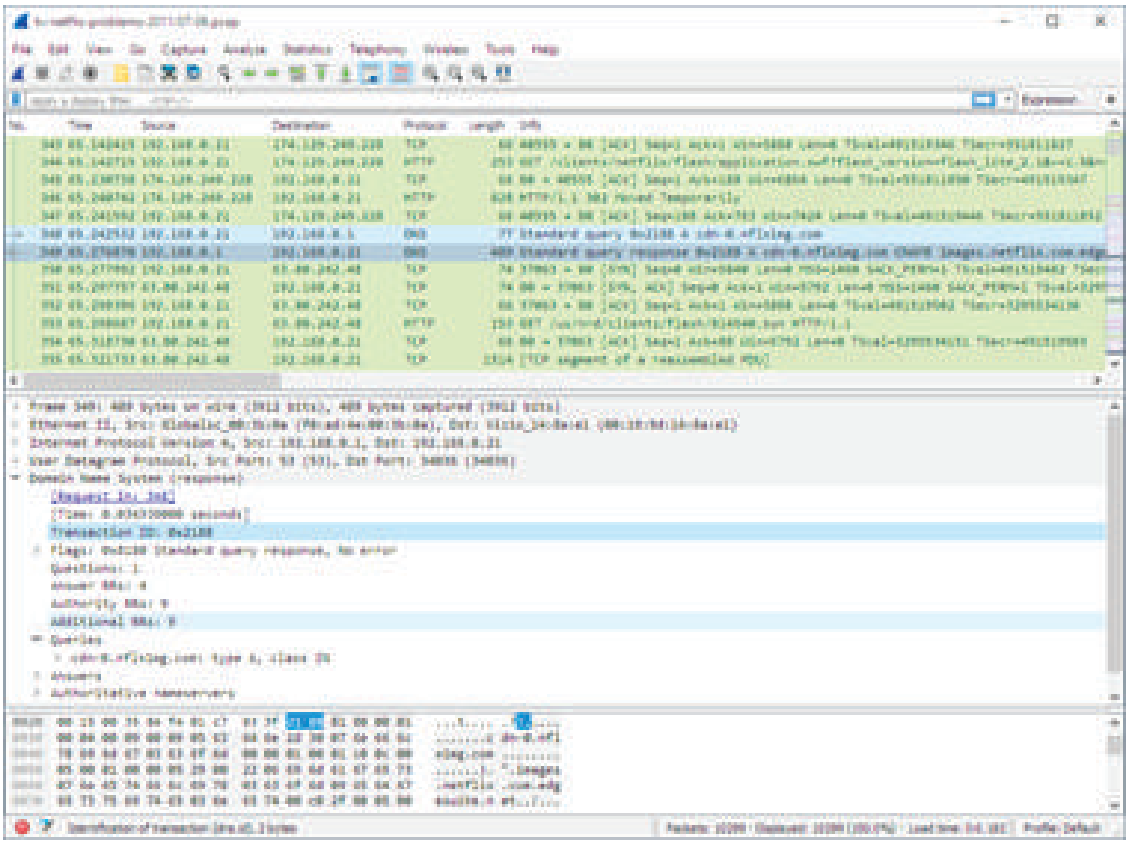
La imagen muestra la herramienta de análisis forense EnCase. Tomado de En Case, por Open Text Blogs, n.d., Open Text Blogs.

https://5wbts45dnuj11q6172p5dkzf-wpengine.netdna-ssl.com/wp-content/uploads/Figure-2.png

Un ejemplo de herramienta de ***análisis forense digital es EnCase.***

Figura 4

Wireshark



En el siguiente enlace se puede encontrar una guía de muestra, a partir de la cual se puede crear un ejercicio de simulación utilizando esta herramienta:

https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

Nota

La imagen muestra la herramienta basada en la red Wireshark. Tomado de Wireshark, por Wireshark, n.d., Wireshark. *https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html*

Sitios web

- ***DFIR Science, Digital Forensic Science.***

- ***European Cybercrime Training and Education Group (ECTEG).***

- ***European Union Agency for Law Enforcement Training (CEPOL).***
  - *https://www.cepol.europa.eu/*

- ***SWGDE. (n.d.).*** SWDGE Drafts For Public Comment.
  - *https://www.swgde.org/documents/draftsForPublicComment*

Videos

- ***ABA Criminal Justice Section. (2016, June 13).*** Forensics 2016: Issues in Accreditation (Part 1) (duración: 42:24) [Video] YouTube.
  - *https://www.youtube.com/watch?v=d5IU55OJfTg*

  Este video incluye la primera parte de un panel de debate del Colegio de Abogados de Estados Unidos, el cual otorga la acreditación para el análisis forense digital en los Estados Unidos.

- ***ABA Criminal Justice Section. (2016, June 13).*** Forensics 2016: Issues in Accreditation (Part 2) (duración: 32:22) [Video] YouTube.
  - *https://www.youtube.com/watch?v=Dz79m-J3K78*

  Este video incluye la segunda parte de un panel de debate del Colegio de Abogados de Estados Unidos, el cual otorga la acreditación para el análisis forense digital en los Estados Unidos.

- ***DFIR Science. (2016, December 9).*** Beginner Introduction to The Sleuth Kit (command line) (duración: 22:54) [Video] YouTube.
  - *https://www.youtube.com/watch?v=R-IE2j04Chc.*

  Videotutorial que presenta las imágenes forenses de discos y el análisis del sistema de archivos usando SleuthKit en un sistema operativo Linux.

- ***DFIR Science. (2016, October 2).*** Forensic Data Acquisition - Hardware Write Blockers (duración: 7:59) [Video] YouTube.
  - *https://www.youtube.com/watch?v=7eT8KSHMGFw&t=112s.*

  Este video trata sobre los bloqueos de escritura y lo que estos hacen, así como muestra un proceso, paso a paso, sobre cómo utilizarlos.

- ***DFIR Science. (n.d.).*** Forensic Acquisition in Windows - FTK Imager (duración: 29:02) [Video] YouTube.
  - *https://www.youtube.com/watch?v=TkG4JqUcx_U*

  Este video muestra un proceso, paso a paso, de la obtención forense en un sistema operativo Windows.

- ***DFIR Science. (2017, September 3).*** [How to] Identify File Types in Windows (duración: 6:34) [Video] YouTube.
  - *https://www.youtube.com/watch?v=-vsfm1IqmWA*

  Este video presenta un tutorial, paso a paso, sobre cómo identificar los tipos de archivos en un sistema operativo Windows.

Cooperación internacional contra los delitos cibernéticos

Módulo 7

Módulo 7: Cooperación internacional contra los delitos cibernéticos

Introducción

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 estos delitos 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 sobre delincuencia organizada, particularmente 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 mercados negros), como Darkode (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 registro de los 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.

Objetivos

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

"Un delito cibernético lo puede cometer un delincuente en cualquier parte del mundo con conexión a internet".

Cuestiones clave

Se pueden encontrar pruebas de delitos cibernéticos en fragmentos en varios dispositivos (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital), sistemas y servidores digitales de todo el mundo. La naturaleza y el alcance transnacional de los delitos cibernéticos y la existencia de pruebas digitales extraterritoriales exigen la cooperación nacional, regional e internacional en las investigaciones de delitos cibernéticos. Este módulo hace una exploración profunda de la cooperación internacional en la medida en que se relaciona con los delitos cibernéticos, particularmente con los temas de soberanía y jurisdicción, factores que influencian la cooperación internacional, mecanismos formales e informales de cooperación internacional, recopilación de pruebas extraterritoriales y déficit nacional en la capacidad para realizar investigaciones de delitos cibernéticos. Para más información sobre la cooperación internacional para combatir la delincuencia organizada transnacional, consulte la serie de módulos sobre delincuencia organizada (especialmente el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional).

Soberanía y jurisdicción

La soberanía territorial se refiere al ejercicio completo y exclusivo de autoridad y poder que ejerce el Estado sobre su territorio geográfico. La protección de la soberanía considera preponderantemente los instrumentos internacionales y regionales sobre delitos cibernéticos (discutido en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos). Un ejemplo de ello es la Convención Árabe para el Combate de los Delitos con Tecnología de la Información de 2010 de la Liga de los Estados Árabes. Específicamente, el artículo 4 de esta Convención sostiene que:

> “**Cada Estado parte se comprometerá,** con sujeción a sus propias leyes o principios constitucionales, a cumplir con las obligaciones que le incumban en virtud de la aplicación de la presente Convención de forma compatible con los dos principios de igualdad de la soberanía regional de los Estados y de la no injerencia en los asuntos internos de los demás Estados.”

La soberanía territorial se puede aplicar al ciberespacio, en especial a la infraestructura de tecnología de la información y la comunicación (TIC) de los Estados. Se puede infringir la soberanía del Estado cuando terceros tienen acceso no autorizado a la TIC en países extranjeros, sin el conocimiento o el permiso del país anfitrión o de sus agentes del orden público. Esta transgresión ocurre incluso si este acceso no autorizado es consecuencia de la investigación de un delito cibernético cometido en un país diferente, en un esfuerzo por encontrar el origen del ataque cibernético o por impedir que este se produzca (una táctica conocida como *hackback* o *hacking back*, [identificación del origen de los ataques]) (Wrange, 2014).

La jurisdicción, que está vinculada a la soberanía (UNODC, 2013, nota 9, p. 184), le otorga a los Estados el poder y la autoridad para definir y mantener los deberes y derechos de las personas en su territorio, y para hacer cumplir las leyes y sancionar las infracciones (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos). Los Estados demandan principalmente su jurisdicción sobre los delitos cometidos dentro de su territorio (principio de territorialidad). El apartado 2 del artículo 22 del Convenio sobre Delitos Cibernéticos del Consejo de Europa de 2001 establece que «cada parte adoptará las medidas legislativas y de otra índole que sean necesarias para establecer su jurisdicción sobre cualquier delito (...) [incluido en] el presente Convenio, cuando el delito se cometa (...) en su territorio». Sin embargo, como sostienen Brenner y Koops (2004), «el hecho de que se haya “cometido” o no un delito (...) en el territorio de una nación no es, sin embargo, una tarea sencilla cuando esta perpetración implica el uso del ciberespacio» (p. 10).

La jurisdicción sobre los delitos cibernéticos se establece por otros factores, como la nacionalidad del infractor (principio de nacionalidad, principio de personalidad activa), la nacionalidad de la víctima (principio de nacionalidad, principio de personalidad pasiva) y las repercusiones de los delitos cibernéticos en los intereses y la seguridad del Estado (principio de protección) (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos), siempre y cuando [se pueda mostrar] «una "conexión suficiente" o un "vínculo genuino" entre (...) el [delito cibernético] y el Estado que ejerce la jurisdicción» (Epping y Gloria, 2004, como se citó en UNODC, 2013, pp. 184-185). En el Reino Unido, por ejemplo, el Tribunal de Apelaciones en el caso R versus Sheppard and Anor (2010) aplicó la Ley del Orden Público del Reino Unido de 1986 a un material racista publicado en un sitio web que estaba alojado en un servidor de Estados Unidos y condenó a dos residentes del Reino Unido por haberlo publicado.

Las legislaciones nacionales sobre delitos cibernéticos establecen su jurisdicción sobre los delitos cibernéticos. Por ejemplo, en Malasia, la Ley de Delitos Informáticos de 1997 estableció su jurisdicción sobre delitos cibernéticos. En particular, el artículo 9 de esta ley establece que:

> "**Las disposiciones de la presente ley,** en relación con cualquier persona, independientemente de su nacionalidad o ciudadanía, tendrán efecto tanto fuera como dentro de Malasia, y si una persona comete un delito según la presente ley en cualquier lugar fuera de Malasia, podrá ser tratada como responsable de ese delito como si lo hubiera cometido en Malasia."

En comparación, Tanzania demanda jurisdicción sobre un delito cibernético cuando:

> Un acto u omisión que constituye un delito se comete total o parcialmente (...) dentro de la República Unida de Tanzania; (...) en un barco o una aeronave registrados en la República Unida de Tanzania; (...) por un ciudadano de la República Unida de Tanzania; (...) por un ciudadano de la República Unida de Tanzania que reside fuera del país solo si el acto u omisión constituye igualmente un delito en la legislación de ese país; o (...) por cualquier persona, independientemente de su nacionalidad, ciudadanía o ubicación, cuando el delito sea (...) cometido usando un sistema, dispositivo o datos informáticos ubicados en la República Unida de Tanzania; o (...) dirigido contra un sistema, dispositivo o datos informáticos o por una persona ubicada en la República Unida de Tanzania. (artículo 30, Ley de Delitos Cibernéticos de 2015)

En cambio, Kenia establece jurisdicción sobre delitos cibernéticos de la siguiente manera:

> Se considera que un acto u omisión cometido fuera de Kenia, que de haberse cometido en Kenia constituiría un delito según la presente ley, se ha cometido en Kenia si (...) la persona que lo comete es (...) un ciudadano de Kenia; o (...) reside habitualmente en Kenia; y (...) si el acto u omisión se comete (...) contra un ciudadano de Kenia; (...) contra bienes pertenecientes al Gobierno de Kenia fuera de Kenia; o (...) para obligar al Gobierno de Kenia a hacer o abstenerse de realizar cualquier acto; o (...) si la persona que comete el acto u omisión está, después de la perpetración u omisión, presente en Kenia. (artículo 66 de la Ley sobre el Uso Indebido de Computadoras y Delitos Cibernéticos de Kenia de 2018)

Dentro de estas y otras leyes nacionales sobre delitos cibernéticos, la jurisdicción se determina principalmente por la ubicación de los infractores, víctimas y las repercusiones de los delitos cibernéticos.

Mecanismos formales de cooperación internacional

La cooperación internacional depende de leyes nacionales sustantivas sobre delitos cibernéticos armonizadas, que penalizan el delito cibernético, y de las leyes nacionales procesales sobre delitos cibernéticos que establecen las normas que rigen la práctica de la prueba y los procedimientos penales (discutido en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos). También se puede facilitar la cooperación internacional armonizando, donde sea necesario, los instrumentos bilaterales, regionales y multilaterales sobre delitos cibernéticos. Igualmente, es necesario adherirse o ratificar los instrumentos regionales y multilaterales sobre delitos cibernéticos para hacer que sean jurídicamente vinculantes. Para más información sobre la cooperación internacional para combatir la delincuencia organizada transnacional, consulte la serie de módulos sobre delincuencia organizada (especialmente el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional).

La cooperación internacional se facilita con tratados bilaterales, regionales y multilaterales sobre delitos cibernéticos (discutidos en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos), siempre y cuando exista una doble incriminación (es decir, una cláusula en los tratados que exija que la conducta alegada se considere ilegal en los países cooperantes). Sin la doble incriminación y sin leyes armonizadas, se crean refugios seguros para los delitos cibernéticos en los que no se puede procesar a los autores del delito. Esto se observó en el ahora infame caso del virus Love Bug del 2000, cuyo creador y distribuidor no pudo ser procesado porque sus actos no se consideraban delito en su país (Filipinas) en el momento del incidente.

Sin embargo, la cooperación internacional puede seguir siendo posible incluso sin una interpretación estricta del requisito de la doble incriminación. Además:

> **Cuando la doble incriminación se considera un requisito**, se estimará cumplida independientemente de si las leyes del Estado parte requerido lo incluye en la misma categoría de delitos o lo denomine con la misma terminología del Estado parte requirente si la conducta que subyace al delito por el que se solicita asistencia es un delito penal según las leyes de ambos Estados parte. (apartado 2 del artículo 43, Convención de las Naciones Unidas contra la Delincuencia Organizada de 2003)

Sin embargo, hay excepciones para el requisito de la doble incriminación. Por ejemplo, el apartado 3 del artículo 29 del Convenio sobre Delitos Cibernéticos de 2001 del Consejo de Europa no exige la doble incriminación para la «conservación rápida de datos informáticos almacenados»:

> Por medio de un sistema informático, situado en el territorio de la otra Parte, en cuanto la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua para el registro o un acceso similar, para la incautación o un aseguramiento similar, o para la divulgación de los datos en casos de delitos sustantivos incluidos en el presente Convenio. (artículos 2 a 11)

El apartado 4 del artículo 29 establece el derecho de los Estados a rechazar las solicitudes de conservación si requieren de la doble incriminación para la asistencia mutua por delitos que no están incluidos en el Convenio.

Además de la doble incriminación, otro requisito sustantivo para la cooperación internacional es que se respeten las obligaciones internacionales en asuntos de derechos humanos (UNODC, 2013, p. 205). Se pueden rechazar las solicitudes de cooperación internacional si la solicitud tiene como resultado que el Estado viole sus obligaciones internacionales en asuntos de derechos humanos al responder a la solicitud.

¿Sabían que...?

El repositorio de delitos cibernéticos de la UNODC tiene una opción de «Lecciones aprendidas», que abarca temas relacionados con la prevención, la investigación (facultades de investigación, obtención de datos de los proveedores de servicios y otras medidas de investigación), las pruebas y el procedimiento (práctica judicial, pruebas digitales, jurisdicción y otras prácticas procesales), la cooperación internacional (cooperación rápida, extradición, cooperación internacional y asistencia judicial recíproca), la asistencia técnica y el enjuiciamiento. En el repositorio se puede buscar por tema o país.

Los mecanismos formales para la cooperación internacional incluyen tratados bilaterales, regionales y multilaterales sobre delitos cibernéticos. De hecho, la cooperación considera de manera preponderante estos tratados. Por ejemplo, el Acuerdo sobre Cooperación para Combatir Delitos Informáticos de la Comunidad de Estados Independientes del 2001 incluye varios artículos dedicados a la cooperación internacional (artículos 5-7), que abarcan los tipos de cooperación incluidos en el presente Acuerdo (es decir, intercambio de información, prestación de asistencia jurídica de conformidad con los instrumentos internacionales, y prevención, detección, represión e investigación de los delitos cibernéticos, por citar algunos), así como la manera en que los Estados Miembros pueden solicitar asistencia y las directrices sobre cómo ejecutar estas solicitudes. El artículo 8 de este Acuerdo incluye las circunstancias en las que se puede denegar una solicitud de asistencia (es decir, cuando la solicitud infringe la legislación nacional del Estado), y el requisito de notificar por escrito al Estado requirente que su solicitud fue denegada y las razones por las que se denegó.

¿Sabían que...?

El Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Delitos Cibernéticos (Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Delitos Cibernéticos) también busca promover la cooperación entre los signatarios con respecto a la recopilación de pruebas y su conservación en casos de delitos cibernéticos.

Además, los artículos 32 y 34 de la Convención Árabe para el Combate de los Delitos con Tecnología de la Información de 2010 de la Liga de los Estados Árabes incluyen las disposiciones y las solicitudes de asistencia mutua y los procedimientos para la cooperación. Además, en el Convenio de la Unión Africana sobre Seguridad Cibernética y Protección de Datos Personales de 2014, el artículo 28 incluye las disposiciones sobre la armonización, la asistencia judicial recíproca en asuntos de delitos cibernéticos y el intercambio de información. La última insta a los Estados a establecer instituciones que puedan facilitar el intercambio de información sobre las amenazas y las vulnerabilidades de la seguridad cibernética, como el Equipo Informático de Respuesta de Emergencia (CERT) o el Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) (consulte Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención de delitos cibernéticos: aplicaciones y medidas prácticas). En el apartado 2 del artículo 28, se les indica a los Estados que «usen los medios disponibles para la cooperación internacional», que pueden incluir «asociaciones internacionales, intergubernamentales, regionales o (...) público-privadas» para responder a los delitos cibernéticos.

"Los mecanismos formales para la cooperación internacional incluyen tratados bilaterales, regionales y multilaterales sobre delitos cibernéticos".

Otros mecanismos que facilitan la cooperación internacional en la investigación y en el enjuiciamiento de los delincuentes cibernéticos son los tratados de asistencia judicial recíproca y de extradición. Los tratados de asistencia judicial recíproca (MLAT) son acuerdos entre países que se aplican a una lista de delitos y que definen el tipo de asistencia que presta cada país (p. ej., pruebas) en las investigaciones (Maras, 2016, p. 78) (consulte el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional, de la serie de módulos sobre delincuencia organizada, para más información sobre la asistencia judicial recíproca). El enfoque de la lista es bastante desactualizado y no considera la naturaleza evolutiva de los delitos cibernéticos. Al entender la naturaleza cambiante de los delitos (y de los delitos cibernéticos), en algunos MLAT, en vez de tener una lista de delitos, las partes acuerdan cooperar en la investigación y el enjuiciamiento de todos los delitos proscritos en sus respectivas legislaciones nacionales (con algunas excepciones) (García y Doyle, 2010). Las solicitudes de asistencia mutua se deben presentar por escrito (consulte la figura 1, en la que se muestra una solicitud de MLAT entre un país de la Unión Europea y un país que no pertenece a la UE) y deben incluir información sobre la autoridad requirente, el motivo de la solicitud, la descripción de la solicitud, la investigación o los procedimientos judiciales a la que se refiere la solicitud de asistencia, la descripción del delito o delitos y las leyes infringidas, toda solicitud relativa a los procedimientos a seguir para obtener, conservar y, por último, transferir las pruebas físicas y digitales (discutido en Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital) a la autoridad requirente, los plazos para las solicitudes de conservación de datos y para ejecutarlas, y cualquier otra información que ayude al Estado que recibe la solicitud a realizarla (consulte, por ejemplo, el artículo 5 del Convenio de Asistencia Judicial en Materia Penal de 1992 de la Comunidad Económica de los Estados de África Occidental o ECOWAS).

Figura 1

Solicitud de MLAT entre un país de la Unión Europea y un país que no pertenece a la UE

Tomado de Security Union: Facilitating Access to Electronic Evidence, por European Commission, 2018, European Union. http://europa.eu/rapid/attachment/IP-18-3343/en/Factsheet E-evidence.pdf.

Las solicitudes de asistencia mutua se pueden negar en ciertas circunstancias. Por ejemplo, si la solicitud «perjudica la soberanía, la seguridad y el orden público» (artículo 4 del Convenio de Asistencia Judicial en Materia Penal del ECOWAS; consulte también el artículo 2 del Convenio Europeo de Asistencia Judicial en Materia Penal de 1959, el apartado 4 del artículo 25 del Convenio sobre Delitos Cibernéticos del Consejo de Europa y el artículo 18 de la Ley N.º 09-04 de Argelia del 14 de Shaabán de 1430 que corresponde al 5 de agosto de 2009, el cual contiene normas específicas sobre la prevención y la lucha contra los delitos relacionados con las tecnologías de la información y la comunicación). Se pueden negar las solicitudes de asistencia judicial recíproca si, por ejemplo, «están relacionadas con (...) delito(s) que la Parte requerida considere (...) delito(s) político(s) o (...) delito(s) conectados con (...) delito(s) político(s)» (apartado 4 del artículo 25 del Convenio sobre Delitos Cibernéticos). También se pueden denegar las solicitudes de datos si la asistencia o la divulgación que se pide resulta en la violación de las obligaciones internacionales en asuntos de derechos humanos del Estado que responde (UNODC, 2013, p. 204) (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos).

Algunos países (p. ej., Brasil, Japón y Ucrania) brindan asistencia judicial recíproca si se garantiza la reciprocidad (es decir, si el Estado requirente honra una solicitud del mismo tipo del Estado que responde en el futuro). Además, el Convenio sobre Delitos Cibernéticos del Consejo de Europa de 2001 actúa como un MLAT para los países que no tienen uno con el país que solicita la asistencia. En ausencia de tratados y acuerdos, se pueden usar las comisiones rogatorias (es decir, solicitudes escritas por tribunales nacionales que incluyen «información sobre el caso, descripción de la prueba necesaria y por qué se necesita y un compromiso de reciprocidad para futuros casos»; Maras, 2016, 78-79; Bell, 2007) para obtener apoyo en asuntos relacionados con delitos cibernéticos (consulte el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional, de la serie de módulos sobre delincuencia organizada, para más información sobre comisiones rogatorias).

También se producen importantes retrasos (es decir, un plazo de meses) con otros mecanismos formales de cooperación (es decir, la asistencia judicial recíproca y la extradición) (UNODC, 2013, p. 207; Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional, de la serie de módulos sobre delincuencia organizada). Estos retrasos son particularmente problemáticos debido a la volatilidad de las pruebas digitales (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital).

Redacción de la solicitud de asistencia judicial recíproca

Si bien algunos países incluyen directrices para las solicitudes de asistencia judicial recíproca y las comisiones rogatorias, e incluso proporcionan modelos, esta práctica no es universal. Para ayudar a los países con las solicitudes de asistencia mutua, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) creó el programa para redactar solicitudes formales de asistencia judicial recíproca, en un esfuerzo por optimizar el proceso armonizando los formatos de las solicitudes y, así, facilitar el rápido envío y entrega de las solicitudes de asistencia.

Los tratados de extradición, como el Convenio de Extradición Europeo de 1957 y el Convenio de Extradición Interamericano de 1981 de la OEA, son acuerdos para arrestar o extraditar a individuos al país requirente si se cumplen los castigos para los delitos extraditables (consulte Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional, de la serie de módulos sobre delincuencia organizada, para más información sobre tratados de extradición). Por ejemplo, el artículo 3 del Convenio de Extradición del ECOWAS de 1994 lista los castigos con un «periodo mínimo de dos años». Las órdenes de detención en las regiones, como la orden de detención europea, permiten arrestar a los infractores por delitos relacionados con la informática, los cuales son «punibles en el Estado Miembro emisor con una pena privativa de libertad o con una orden de detención por un periodo máximo de al menos tres años (...) sin la verificación de la doble incriminación del acto» (apartado 2 del artículo 2, Decisión Marco 2002/584/JHA del 13 de junio de 2002 de la orden de detención europea y los procedimientos de entrega entre los Estados Miembros - Declaraciones hechas por Estados Miembros sobre la adopción de la Decisión Marco).

La existencia de un tratado de extradición no asegura que una persona sea extraditada al país requirente. Esto se pudo observar en el caso de Lauri Love, un *hacker* británico, cuya extradición a Estados Unidos fue negada (Parkin, 2017), a pesar de la existencia del Tratado de Extradición entre Reino Unido y Estados Unidos de 2003.

"La existencia de un tratado de extradición no asegura que una persona sea extraditada al país requirente".

Además, los tratados de extradición incluyen condiciones en las que no se concederá la extradición. Por ejemplo, el Convenio de Extradición Interamericana de la OEA niega las solicitudes de extradición cuando el castigo por el delito es cadena perpetua o pena de muerte (artículo 9). También se niega la extradición en casos donde la persona que será extraditada será sometida a tratos o a castigos inhumanos o degradantes (p. ej., el artículo 5 del Convenio de Extradición del ECOWAS y el artículo 9 del Convenio de Extradición Interamericana de la OEA). Las solicitudes de extradición también se pueden denegar por otras razones, como la falta de pruebas para justificar la extradición (p. ej., la Ley de Extradición de Botsuana de 1990), cuando la solicitud implica un delito no extraditable (p. ej., un delito militar, el artículo 7 del Convenio de Extradición del ECOWAS), o cuando el sujeto que pide la extradición es ciudadano del país que recibe la solicitud (p. ej., el artículo 698 del Código de Procedimiento Penal de Argelia y el artículo 5 (LI) de la Constitución de Brasil). Respecto a este último, el principio de la no extradición de ciudadanos está consagrado en la constitución y en los instrumentos regionales e internacionales. Independientemente de este principio, «el derecho internacional público dicta que los Estados tienen la obligación legal de extraditar o procesar (aut dedere aut judicare) a personas que cometen delitos internaciones graves» (Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional). Algunos tratados de órdenes de detención también pueden excluir delitos específicos, como ciertos delitos políticos (p. ej., consulte el artículo 3 de la Comunidad del Caribe o el Tratado de Orden de Detención de la CARICOM de 2008).

Mecanismos informales de cooperación internacional

Los mecanismos informales para la cooperación internacional, como compartir información entre los organismos encargados de hacer cumplir la ley (es decir, la cooperación entre policías; para más información consulte la serie de módulos sobre delincuencia organizada, en especial el Módulo 8: Seguridad cibernética y prevención de delitos cibernéticos), se usan también en las investigaciones de delitos cibernéticos (James y Gladyshev, 2016). El tipo de información compartida entre los organismos encargados de hacer cumplir la ley que usan canales informales cambia según el Estado. En Australia:

> "Las autoridades pueden prestar los siguientes tipos de asistencia entre los organismos: tomar declaraciones voluntarias a los testigos, realizar entrevistas voluntarias a los testigos, tomar declaraciones voluntarias a los testigos mediante un servicio de video, acoger a la policía extranjera que realiza investigaciones en Australia, intercambiar información de inteligencia, realizar vigilancia física, obtener antecedentes penales u obtener material de acceso público. (UNODC, «Informal cooperation channels: Australia»)"

¿Sabían que...?

Existe un mecanismo informal para la cooperación internacional con respecto al enjuiciamiento de delitos cibernéticos: la Red Mundial de Fiscales contra la Delincuencia Electrónica (GPEN) de la Asociación Internacional de Fiscales.

Los canales de cooperación informal se usan principalmente para obtener asistencia y asesoramiento jurídico y técnico en casos de delitos cibernéticos en lugar de solicitar la recolección de pruebas digitales (UNODC, 2013, p. 214). En Japón, por ejemplo, solo se puede solicitar información mediante un canal informal cuando el país requirente no tiene la intención de usar la información como prueba (UNODC, «International cooperation: Japan»). Si el país planea usar la información como prueba, se requiere de una solicitud formal de asistencia judicial recíproca (consulte el Módulo 11: Cooperación internacional para combatir la delincuencia organizada internacional). Las pruebas digitales obtenidas de estos canales pueden considerarse inadmisibles en los tribunales nacionales del Estado requirente si no se mantiene una cadena de custodia (consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos, Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital y Delitos Cibernéticos-Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital para más información). Si la información se comparte de forma informal entre las autoridades de Estados Unidos, Paraguay y Argentina (por mencionar algunos), los países requirentes deben hacer seguimiento por canales formales (UNODC, «Police to Police Cooperation: United States»; UNODC, «Informal cooperation: Paraguay»; y UNODC, «Channels for urgent requests for MLA in cybercrime cases: Argentina»).

Las organizaciones internacionales y regionales también facilitan la cooperación internacional informal. Por ejemplo, se pueden hacer solicitudes urgentes a la Organización de los Estados Americanos (UNODC, «Channels for urgent requests»). También se pueden realizar mediante la Interpol (UNODC, «Channels for urgent requests for MLA in cybercrime cases: Liechtenstein»), la organización policial internacional más grande del mundo, a través de su red I-24/7 en más de 190 países. Los organismos nacionales encargados de hacer cumplir la ley que forman parte de esta red comparten conocimientos especializados, tecnología y recursos para luchar contra los delitos transnacionales.

La Interpol actúa como un centro de comunicación entre países, al difundir información, como notas, e incluso al ayudar en operaciones coordinadas entre países. Por ejemplo, en 2012, la Interpol ayudó a las autoridades locales de España, Argentina, Chile y Colombia a arrestar a los 25 miembros de Anonymous (Operación «Desenmascaramiento»), un grupo internacional de hackers (Whiteman, 2012; Interpol, «Operation Unmask»). En 2017, «la INTERPOL condujo una operación (...) [que involucraba] a Indonesia, Malasia, Birmania, Filipinas, Singapur, Tailandia y Vietnam», así como a China y a las organizaciones del sector privado, lo que llevó a la «identificación de casi 9 000 servidores de mando y control (C2) y cientos de sitios web expuestos, incluyendo los portales del Gobierno» (Interpol, 2017).

El artículo de Whiteman (2012) dice que la Interpol detuvo a los sospechosos. Este es un error. La Interpol no tiene la autoridad para arrestar a un delincuente. La Interpol puede ayudar a crear algo similar al Equipo Conjunto de Investigación (Europol, s.f.), que ayuda en las investigaciones penales, pero solo los investigadores locales tienen la autoridad para arrestar. Desafortunadamente, los medios de comunicación muestran, a menudo de forma incorrecta, a la Interpol como una fuerza policial internacional que tiene autoridad local. En vez de que la Interpol tenga la autoridad para realizar detenciones en un país, cada Estado crea su propia Oficina Central Nacional (OCN) (Interpol, 2018). La sede de la Interpol puede brindar información y recomendaciones a las OCN, pero no puede obligarlos a actuar. Además, los miembros de la OCN son, a veces, aunque no siempre, policías o fiscales con juramentos locales.

De acuerdo con el Proyecto del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC de 2013, los países informaron que la cooperación informal sigue dependiendo en gran medida de la existencia de instrumentos bilaterales y regionales, de las redes interconectadas de organizaciones regionales e internacionales y de las relaciones y asociaciones de los organismos encargados de hacer cumplir la ley (UNODC, 2013, p. 210). Las asociaciones también desempeñan un papel crucial para la cooperación entre los organismos encargados de la aplicación de la ley y el sector privado durante las investigaciones de delitos cibernéticos (consulte Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos, para más información sobre las asociaciones entre el sector público y el privado). La cooperación entre el equipo de investigación de delitos cibernéticos de Microsoft y los organismos encargados de hacer cumplir la ley en Estados Unidos, en Marruecos y en Turquía condujo a la detección y eventual arresto de los creadores y distribuidores de Zotob, un programa parásito (FBI, 2006).

Retención, conservación y acceso de datos

También se pueden denegar las solicitudes de cooperación internacional debido a los requisitos de procedimiento. Por ejemplo, consideremos las prácticas de retención, conservación y acceso de datos. Los datos retenidos por Internet y por los proveedores de servicios de comunicación (discutido en Delitos Cibernéticos-Módulo 1: Introducción al delito cibernético) depende de los términos de servicio de los proveedores, de las políticas de privacidad y de las prácticas comerciales (Westmoreland y Kent, 2015). Por esta razón, existe una variación entre los proveedores no solo con respecto al tipo de datos retenidos (p. ej., registro de IP o información sobre cuentas desactivadas), sino también al periodo de retención (días, semanas, meses o años) (consulte, p. ej., las «Directrices para la aplicación de la ley» de Twitter y la «Política de datos» de Facebook para más información). La retención de datos, así como el acceso, también varía según las leyes nacionales, regionales e internacionales de protección de datos (descrito en detalle en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos).

Los organismos encargados de hacer cumplir la ley solicitan la conservación de datos a los proveedores de servicios, en un esfuerzo por retener los datos antes de que se eliminen o se alteren de alguna manera (Sutton, 2016). La legislación nacional prescribe el acceso a los datos conservados. Las órdenes judiciales (p. Ej., órdenes de registro) necesarias para obtener diversas formas de datos de los proveedores de servicios, si los hubiera, son diferentes según el país. Por ejemplo, mientras que en Estados Unidos se necesita la citación de un testigo y una orden judicial para los datos sin contenido (o metadatos; p. ej., datos de abonados y direcciones IP) y una orden de registro para los datos de contenido (p. ej., el texto en correos electrónicos u otros mensajes) (la Ley de Comunicaciones Almacenadas de los Estados Unidos de 1986; el Título II de la Ley de Privacidad de las Comunicaciones Electrónicas de 1986), en Turquía, las autoridades no necesitan una orden judicial para acceder a los datos sin contenido ni a los de contenido (Ley de Internet 5651) (discutido en Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos).

¿Sabían que...?

Las redes sociales y otras plataformas en línea tienen informes de transparencia (consulte, p. ej., los informes de Pinterest, Tumblr, Twitter, LinkedIn, y Facebook, por nombrar algunos), que incluyen la información sobre el número de solicitudes realizadas para acceder a los datos de los usuarios en sus sitios, sobre las partes nacionales o internacionales que solicitan esta información, sobre qué mecanismos jurídicos se usaron para solicitar o acceder a los datos y si la plataforma cumplió con la solicitud.

Soberanía y jurisdicción

Incluso con los mecanismos formales e informales de cooperación internacional establecidos, surgen desafíos en la identificación y recopilación de pruebas digitales del almacenamiento en la nube y otros proveedores de servicio. El problema con la informática en la nube es que es difícil saber dónde se almacenan los datos. Sin este conocimiento, no se puede identificar «la jurisdicción relevante a la que se debe dirigir la solicitud de cooperación para obtener la prueba [digital]» (UNODC, 2013, p. 216).

Los datos en la nube pueden fragmentarse y ser almacenados en múltiples lugares y múltiples países. Esta fragmentación se muestra en United States v. Microsoft (2018). En este caso, el Gobierno estadounidense emitió una orden de registro en cumplimiento con la Ley de Comunicaciones Almacenadas de los Estados Unidos (SCA) de 1986 para obtener las pruebas para un caso de tráfico de drogas. En respuesta, Microsoft cumplió con este pedido al transferir los datos relevantes sin contenido que estuvieron almacenados en los servidores estadounidenses (p. ej., la libreta de direcciones del sospechoso); sin embargo, no le dio los datos relevantes de contenido (p. ej., el contenido de sus correos electrónicos) porque estos estaban almacenados en un centro de datos de Microsoft en Dublín, Irlanda.

La controversia en el fondo de United States v. Microsoft (2018) era si las disposiciones de la SCA permiten el acceso a los datos localizados en los servidores de otro país o si este acceso constituía un alcance extraterritorial no justificado legalmente. Ahora el asunto es irrelevante con el fragmento de la Ley de Clarificación del Uso Legítimo de los Datos fuera de los Estados Unidos (Ley de la Nube) de 2018. La Ley de la Nube modificó la sección 18 U.S.C. § 2713 de la SCA y se puede resumir de la siguiente manera:

> **Un proveedor de servicios de comunicaciones electrónicas o de computación remota** (en la nube) deberá cumplir con las obligaciones de este capítulo de conservar, hacer una copia de seguridad o revelar el contenido de una comunicación electrónica o por cable y cualquier registro u otra información perteneciente a un cliente o suscriptor en posesión, custodia o control de dicho proveedor, independientemente de si dicha comunicación, registro u otra información se encuentra dentro o fuera de los Estados Unidos.

La Ley de la Nube da acceso directo a datos extraterritoriales. Sin embargo, hasta 2018 todavía no se han establecido «normas y salvaguardas comunes con respecto a las circunstancias, si las hubiera, en las cuales los agentes de la ley pueden tener acceso directo a datos extraterritoriales» (UNODC, 2013, p. 216).

La Ley de la Nube y el Reglamento General de Protección de Datos

Han surgido preocupaciones ya que la Ley de la Nube socavará el Reglamento General de Protección de Datos (RGPD) (Vogel, 2018), un reglamento completo sobre protección de datos que entró en vigencia el 25 de mayo de 2018 (el RGPD se analiza en detalle en Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos). Las empresas se enfrentan a elevadas multas y sanciones si no cumplen con el RGPD. Las empresas que necesitan cumplir con la Ley de la Nube y el RGPD necesitan equilibrar el requisito de la Ley de la Nube de dar acceso a los datos con el requisito de la RGPD de proteger los derechos de datos del sujeto implicado (consulte Delitos Cibernéticos-Módulo 10: Privacidad y protección de datos), y garantizar que se establezcan las salvaguardas necesarias y que se cumplan los requisitos de los artículos 44-49 del RGPD cuando se transfieren los datos a terceros o a organizaciones internacionales.

Capacidad nacional y cooperación internacional

La cooperación internacional depende de la capacidad de los Estados de procesar las solicitudes de una forma que garantice la admisibilidad de las pruebas en un tribunal. Para lograr dicho objetivo, es necesario que los profesionales cualificados en materia de delitos cibernéticos aseguren que la prueba se obtenga de acuerdo con las normas que rigen la práctica de la prueba y el procedimiento penal (para más información consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital y Delitos Cibernéticos-Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). Sin embargo, estos profesionales no abundan. De hecho, los países de todo el mundo sufren de un déficit de capacidad nacional para lidiar con los delitos cibernéticos (UNODC, 2013).

La cooperación internacional depende de la capacidad de los Estados de procesar las solicitudes de una forma que garantice la admisibilidad de las pruebas en un tribunal. Para lograr dicho objetivo, es necesario que los profesionales cualificados en materia de delitos cibernéticos aseguren que la prueba se obtenga de acuerdo con las normas que rigen la práctica de la prueba y el procedimiento penal (para más información consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital y Delitos Cibernéticos-Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital). Sin embargo, estos profesionales no abundan. De hecho, los países de todo el mundo sufren de un déficit de capacidad nacional para lidiar con los delitos cibernéticos (UNODC, 2013).

Para lidiar con el déficit de capacidad nacional, se han y se siguen realizando asociaciones con organizaciones nacionales, regionales e internacionales (p. ej., el Departamento de Justicia de los Estados Unidos, la Organización de los Estados Americanos y la Unión Internacional de las Telecomunicaciones), así como con las empresas privadas, para brindarle a los países necesitados la asistencia financiera, humanitaria y técnica en materia de delitos cibernéticos y apoyar sus esfuerzos para desarrollar su propia capacidad nacional para lidiar con estos delitos.

En cumplimiento con la resolución 65/230 (A/RES/65/230) de la Asamblea General de las Naciones Unidas, con la resolución 22/7 sobre el fortalecimiento de la cooperación internacional para combatir el delito cibernético y la resolución 22/8 sobre el fomento de la asistencia técnica y la creación de capacidad para fortalecer las medidas nacionales y la cooperación internacional contra el delito cibernético de la Comisión de Prevención del Delito y Justicia Penal de las Naciones Unidas, la UNODC tiene la obligación de ayudar a los Estados a combatir el delito cibernético al facilitar la capacitación técnica para la mejora de la capacidad, y al implementar programas de prevención y de educación de delitos cibernéticos, y campañas de sensibilización. Estas capacitaciones, programas y campañas son particularmente importantes, dado que brindan soluciones a largo plazo al déficit actual de capacidad nacional, pues proporcionan el conocimiento, las aptitudes y las habilidades necesarias para realizar investigaciones de delitos cibernéticos.

"Los países de todo el mundo sufren de un déficit de capacidad nacional para lidiar con los delitos cibernéticos".

Referencias

- ***Bell, A. E. (2007).*** Investigating International Cybercrimes. Police Chief Magazine, 74(3).
  - *http://www.policechiefmagazine.org/investigating-international-cybercrimes/*
- ***Brenner, S.W. & Koops, B.J. (2004).*** Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1), 1-46.
- ***Epping, V. and Gloria, C. (2004).*** Der Staat im Völkerrecht. En: Knut Ipsen (ed.). Völkerrecht (5th ed). Munich: C.H. Beck.
- ***Europol. (n.d.).*** Joint Investigation Teams - JITS.
  - *https://www.europol.europa.eu/activities-services/joint-investigation-teams*
- ***FBI. (2006).*** Moroccan Authorities Sentence Two in Zotob Computer Worm Attack.
  - *https://archives.fbi.gov/archives/news/pressrel/press-releases/moroccan-authorities-sentence-two-in-zotob-computer-worm-attack*
- ***Interpol. (2017).*** INTERPOL-led cybercrime operation across ASEAN unites public and private sectors.
  - *https://www.interpol.int/News-and-media/News/2017/N2017-051*
- ***Interpol. (n.d.).*** Operation Unmask.
  - *https://www.interpol.int/en/Crime-areas/Cybercrime/Operations/Operation-Unmask*
- ***Interpol. (n.d.).*** Red Notices.
  - *https://www.interpol.int/INTERPOL-expertise/Notices/Red-Notices*
- ***James, J. & Gladyshev, P. (2016).*** A survey of mutual legal assistance involving digital evidence. Digital Investigation, 18, 23-32.
- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press.
- ***Parkin, S. (2017, September 8).*** Keyboard warrior: the British hacker fighting for his life. The Guardian.
  - *https://www.theguardian.com/news/2017/sep/08/lauri-love-british-hacker-anonymous-extradition-us*
- ***Sutter, D. (2016).*** Guide to Obtaining Communication Service Provider Evidence from the United States. I.R.I.S. LLC.
  - *http://www.irisinvestigations.com/wordpress/wp-content/uploads/2016/12/Toolbox/12-SUBPOENA%20GUIDE-SAMPLES/Communication%20Service%20Providers%20Guidance%202015.pdf*
- ***UNODC. (n.d.).*** Channels for urgent requests for MLA in cybercrime cases: Argentina.
  - *https://www.unodc.org/cld/lessons-learned/arg/channels_for_urgent_requests_for_mla_in_cybercrime_cases.html?&tmpl=cyb*
- ***UNODC. (n.d.).*** Channels for urgent requests for MLA in cybercrime cases: Liechtenstein.
  - *https://www.unodc.org/cld/lessons-learned/lie/specific_channels_for_urgent_requests_for_mla_in_cybercrime_cases.html?&tmpl=cyb*
- ***UNODC. (2013).*** Comprehensive Study on Cybercrime. Draft–February 2013. UNODC.
  - *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*
- ***UNODC. (2017).*** Global Programme on Cybercrime.
  - *https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.*
- ***UNODC. (n.d.).*** Informal cooperation: Paraguay.
  - *https://www.unodc.org/cld/lessons-learned/pry/informal_cooperation.html?&tmpl=cyb*

- ***UNODC. (n.d.).*** Informal cooperation channels: Australia.
  - *https://www.unodc.org/cld/lessons-learned/aus/informal_cooperation_channels.html?&tmpl=cyb*

- ***UNODC. (n.d.).*** International cooperation: Japan.
  - *https://www.unodc.org/cld/lessons-learned/jpn/informal_cooperation.html?&tmpl=cyb*

- ***UNODC. (n.d.).*** Mutual Legal Assistance Request Writer Tool.
  - *https://www.unodc.org/mla/*

- ***UNODC. (n.d.).*** Police to Police Cooperation: United States of America.
  - *https://www.unodc.org/cld/lessons-learned/usa/police-to-police_cooperation.html?&tmpl=cyb*

- ***US Department of Justice. (2017).*** Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy.
  - *https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible*

- ***Vogel, P. (2018, June 7).*** The Cloud Act's Dramatic Impact on International Privacy Law. National Law Review.
  - *https://www.natlawreview.com/article/cloud-act-s-dramatic-impact-international-privacy-laws*

- ***Westmoreland, K. & Kent, G. (2015).*** International Law Enforcement Access to User Data: A Survival Guide and Call for Action. Canadian Journal of Law and Technology, 13(2), 225-254.

- ***Whiteman, H. (2012, February 29).*** Interpol arrests suspected 'Anonymous' hackers. CNN.
  - *https://edition.cnn.com/2012/02/29/world/europe/anonymous-arrests-hacking/index.html*

- ***Wrange, P. (2017).*** Intervention in national and private cyberspace and international law. En Ebbesson, Jonas, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds), International Law and Changing Perceptions of Security (pp. 307-326). Brill/Nijhoff.

Casos

- ***R v. Sheppard and Anor [2010] EWCA Crim 65.***

- ***United States v. Microsoft, 584 U.S. (2018).***

Leyes

- ***African Union. (2014).*** Convention on Cyber Security and Personal Data Protection.
  - *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

- ***Algeria. (2009).*** Law No. 09-04 of 14 Sha'ban 1430 Corresponding to 5 August 2009 Containing Specific Rules on the Prevention and Fight Against Information Technologies and Communications Crimes.
  - *http://www.wipo.int/wipolex/en/details.jsp?id=14778*

- ***Algeria. (n.d.).*** Code of Criminal Procedure.
  - *http://www.wipo.int/wipolex/en/details.jsp?id=14775*

- ***Botswana. (1990).*** Extradition Act. IMOLIN.
  - *https://www.imolin.org/doc/amlid/Botswana_Extradition_Act18of1990.pdf*

- ***Caribbean Community (CARICOM). (2008).*** Arrest Warrant Treaty. OAS.
  - *http://www.oas.org/juridico/mla/en/treaties/en_caricom_arrest_warrant_treaty_2008.pdf*

- ***Commonwealth of Independent States. (2001).*** Agreement on Cooperation in Combating Offences related to Computer Information.
  - *https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth*

- ***Council of Europe. (1957).*** European Convention on Extradition.
  - *https://rm.coe.int/1680064587*

- ***Council of Europe. (1959).*** European Convention on Mutual Assistance in Criminal Matters.
  - *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016800656ce*

- ***Council of Europe. (2001).*** Convention on Cybercrime.
  - *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561*

- ***Economic Community of West African States (ECOWAS). (1992).*** Convention on Mutual Assistance in Criminal Matters. ECOWAS Documentation on-line.
  - *http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Mutual%20Assistance%20in%20Criminal%20Matters.pdf*

- ***ECOWAS. (1994).*** Convention on Extradition. ECOWAS Documentation on-line.
  - *http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Extradition.pdf*

- ***European Union. (2002).*** Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002F0584*

- ***Jamaica. (2015).*** Cybercrimes Act. Jamaica Houses of Parliament.
  - *http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf*

- ***Kenya. (2018).*** Computer Misuse and Cybercrimes Act. Kenya Law.
  - *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf*

- ***League of Arab States. (2010).*** Arab Convention on Combating Information Technology Offences.
  - *http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences*

- ***Malaysia. (1997).*** Computer Crimes Act. University of Oxford. Said Business School.
  - *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2014_Act_563_-_Computer_Crimes_Act_1997.pdf*

- ***Organization of American States (OAS). (1981).*** Inter-American Convention on Extradition.
  - *http://www.oas.org/juridico/english/treaties/b-47.html*

- ***Tanzania. (2015).*** Cybercrimes Act. Reporters Sans Frontieres.
  - *https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf*

- ***Turkey. (n.d.).*** Internet Law 5651.
  - *http://www.wipo.int/wipolex/en/details.jsp?id=11035*

- ***United Kingdom. (1986).*** Public Order Act.
  - *https://www.legislation.gov.uk/ukpga/1986/64/contents*

- ***United Nations. (2003).*** Convention against Corruption. Ministerio de Educación y Cultura de Uruguay.
  - *https://www.mec.gub.uy/innovaportal/file/52706/1/ciber_convenio.pdf*

- ***United Nations. (2010).*** General Assembly Resolution 65/230.
  - *http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230*

- ***United Nations, Commission on Crime Prevention and Criminal Justice. (2013).*** Resolution 22/7: Strengthening international cooperation to combat cybercrime. UNODC.
  - *https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf*

- ***United Nations, Commission on Crime Prevention and Criminal Justice. (2013).*** Resolution 22/8: Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime. UNODC.
  - *https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf*

- ***United States. (1986).*** Stored Communications Act.
  - *https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121*

- ***United States. (2018).*** Clarifying Lawful Overseas Use of Data Act. CONGRESS.GOV.
  - *https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf*

Lecturas principales

- ***Brenner, S.W. (2007).*** Private-Public Sector Cooperation in Combating Cybercrime: En Search of a Model. Journal of International Commercial Law and Technology. 2(2), 58-67.

- ***Brenner, S.W. & Koops, B.J. (2004).*** Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1), 1-46.

- ***International Telecommunication Union (ITU). (2012).*** Understanding cybercrime: Phenomena, challenges and legal response (pp. 266-280). ITU.
  • *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

- ***Maras, M.H. (2016).*** International Cybercrime Investigations and Prosecutions: Cutting the Gordian Knot. Pandora's Box2016: Law and Technology, 107-112.

- ***Mulligan, S.P. (2018, April 23).*** Cross-Border Data Sharing Under the CLOUD Act. Congressional Research Service.
  • *https://fas.org/sgp/crs/misc/R45173.pdf*

- ***Svantesson, D. & Gerry, F. (2015).*** Access to extraterritorial evidence: The Microsoft cloud case and beyond. Computer Law & Security Review, 31(4), 478-489.

- ***UNODC. (2013).*** Comprehensive Study on Cybercrime. Draft–February 2013 (Chapter 7, pp. 183-223). UNODC.
  • *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

Lecturas avanzadas

Se recomienda las siguientes lecturas a los interesados en investigar los temas de este módulo con más detalle:

- ***Economic Crime Division. (2009).*** The functioning of 24/7 points of contact for cybercrime. Council of Europe Project on Cybercrime.

- ***ENISA. (2013).*** Cooperation in the Area of Cybercrime: Toolset, Documents for students. ENISA.
  • *https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/cooperation-in-the-area-of-cybercrime-toolset.pdf/view*

- ***Finklea, K.M. (2013).*** The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement. CRS Report for Congress. Congressional Research Service.
  • *https://fas.org/sgp/crs/misc/R41927.pdf*

- ***Kleijssen, J. & Perri, P. (2016).*** Cybercrime, Evidence and Territoriality: Issues and Options. En Martin and Wouter Werner. Netherlands Yearbook of International Law 2016. Springer.

- ***Maillart, J.B. (2018).*** The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum, 1-16, publicado en línea el 3 de septiembre de 2018.

- ***Spoenle, J. (2010).*** Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Council of Europe Project on Cybercrime.
  • *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df*

- ***U.S. Department of Justice. (2019).*** Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. White Paper. April 2019. U.S. Department of Justice.
  • *https://www.justice.gov/dag/page/file/1153436/download*

- ***Von Heintschel, W. (2013).*** Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, 89, 123-156.

Herramientas complementarias

Documentos

- ***UNODC.*** Basic Tips for Investigators and Prosecutors for Requesting Electronic/Digital Data/Evidence from Foreign Jurisdictions. Global Programme for Strengthening the Capacities of Member States to Prevent and Combat Serious and Organized Crime (GPTOC – GLOT32). UNODC.
  - *http://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf*

- ***UNODC.*** Практические советы/рекомендации для следователей и прокуроров о подготовке и направлении запросов (поручений) о взаимной правовой помощи (ВПП), касающихся предоставления информации/доказательств, расположенных на электронных носителях в иностранных государства. Глобальная программа «Укрепление потенциала государств в целях предупреждения и борьбы с тяжкими преступлениями и преступлениями транснационального характера» (GLOT32). UNODC
  - *http://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Rus_logo.pdf*

- ***UNODC/UNSC CTED/IAP (2019).*** Practical Guide for Requesting Electronic Evidence Across Borders. SHERLOC.
  - *https://sherloc.unodc.org/cld/secured/18-05840_Practical_Guide_Electronic_Evidence_ebook.pdf*

- ***U.S. Department of Justice, Office of International Affairs Criminal Division. (2016).*** Obtaining Electronic Evidence from the United States [Power Point slides]. IAP.
  - *https://www.iap-association.org/getattachment/Conferences/Regional-Conferences/North-America-and-Caribbean/4th-North-American-and-Caribbean-Conference/Conference-Documentation/4NACC_Jamaica_P6_ppt_Magdalene_Boynton-(1).pdf.aspx*

Sitios web

- ***Council of Europe. (n.d.).*** International Cooperation against Cybercrime.
  - *https://www.coe.int/en/web/cybercrime/international-cooperation*

- ***Interpol. (n.d.).*** International Cooperation Agreements.
  - *https://www.interpol.int/About-INTERPOL/Legal-materials/International-Cooperation-Agreements*

Seguridad cibernética y prevención del delito cibernético:

estrategias, políticas y programas

Módulo

Módulo 8: Seguridad cibernética y prevención del delito cibernético: *estrategias, políticas y programas*

Introducción

La tecnología de la información y las comunicaciones (TIC) es parte integral del desarrollo nacional y mundial, debido a que facilita la innovación y el crecimiento económico. La dependencia de los Gobiernos, organizaciones, empresas y particulares de las TIC, junto con la creciente interdependencia de los dispositivos digitales en los países y las crecientes conexiones de red con los sistemas digitales de otros países, ha hecho que los países sean vulnerables al delito cibernético. En vista de ello, la delincuencia cibernética puede tener un impacto negativo en la seguridad nacional, la seguridad internacional y la economía mundial. Debido a su impacto en la seguridad y la economía, la protección de las TIC se considera de suma 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 frente al delito cibernético y los delincuentes cibernéticos. Este módulo examina críticamente estas estrategias y las herramientas utilizadas para evaluarlas, así como los esfuerzos de los países en relación con la seguridad cibernética y prevención del delito cibernético.

Objetivos

- Discutir la gobernanza de internet e identificar y evaluar los principios de internet, las tensiones en la realización de estos principios y los obstáculos para la gobernanza universal de internet.

- Describir las características básicas de las estrategias de seguridad cibernética, y diferenciar entre las estrategias de seguridad cibernética y las de prevención del delito cibernético.

- Explicar y evaluar los objetivos y el ciclo de vida de las estrategias nacionales de seguridad cibernética.
  Identificar, examinar y evaluar los marcos para la cooperación internacional en asuntos de seguridad cibernética.

- Evaluar los esfuerzos nacionales e internacionales para mejorar la postura de los países en seguridad cibernética.

Cuestiones clave

La seguridad cibernética hace referencia a «la actividad o proceso, capacidad o habilidad, o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos se protegen o defienden contra los daños, la utilización, modificación o la explotación no autorizada» (US National Initiative for Cybersecurity Career and Studies, s.f.). La seguridad cibernética abarca un conjunto de estrategias, marcos y medidas destinadas a: identificar las amenazas (es decir, una circunstancia que podría causar daño) y las vulnerabilidades (es decir, la exposición al daño) de sistemas, redes, servicios y datos frente a estas amenazas; prevenir la explotación de las vulnerabilidades; mitigar el daño causado por amenazas materializadas y salvaguardar a las personas, los bienes, las tecnologías de la información y la comunicación (TIC) (ITU, 2008; Maras, 2014). La seguridad cibernética busca fortalecer la resiliencia (es decir, la habilidad para soportar interrupciones, adaptarse a condiciones cambiantes y recuperarse de incidentes) de las TIC y proteger la confidencialidad (es decir, impedir el acceso no autorizado), la integridad (es decir, preservar la exactitud y fiabilidad de los datos) y la disponibilidad (es decir, garantizar la accesibilidad) de sistemas, redes, servicios y datos (consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos para obtener información sobre confidencialidad, integridad y disponibilidad en relación con el delito cibernético). En este módulo, se analizan de forma crítica las estrategias de seguridad cibernética que utilizan los países para proteger las TIC, las características y ciclos vitales de dichas estrategias, los marcos utilizados para evaluarlas, y la naturaleza y alcance de las capacidades de los países para proteger las TIC (las medidas prácticas de seguridad cibernética se analizan en Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención del delito cibernético: aplicaciones y medidas prácticas).

Gobernanza de internet

Según Kerr (2003), existen «dos perspectivas dominantes sobre internet» (como se citó en Frischmann, 2003, p. 205): por un lado, internet es vista como «una meta-red global que sirve como una plataforma abierta para la transmisión de información entre los usuarios finales que conectan las computadoras a la red»; por otro lado, internet es vista «en términos de las aplicaciones que habilita y las formas en las que estas afectan a los usuarios finales» (Frischmann, 2003; pp. 205-206; consulte también Kerr, 2003, pp. 359-360). Es esta última concepción de internet «la que lleva a concebir el ciberespacio como una especie de realidad virtual» (o entorno) en la que se desarrollan las actividades en línea (Frischmann, 2003, p. 206).

La bibliografía sobre las teorías de regulación relativas a la gobernanza de internet y del ciberespacio se centran en qué individuos, grupos, empresas, organizaciones y organismos públicos regulan internet y el ciberespacio, y en cómo se regulan el ciberespacio e internet (Chang y Grabosky, 2017, p. 535; para más información sobre las teorías de regulación, consulte Drahos, 2017). Este punto de vista se apoya en la bibliografía, que sostiene que el ciberespacio e internet están regulados, por ejemplo, por leyes, códigos de programación informática, arquitectura de sistemas y arquitectura de internet (Lessig, 2006); personas, empresas y organizaciones con o sin alguna forma de participación gubernamental (es decir, un tipo de autorregulación; consulte Braithwaite, 1982), y personas, empresas y organizaciones que comparten la responsabilidad de la gobernanza (es decir, la seguridad distribuida; consulte Brenner, 2005) (para más información, consulte Chang & Grabosky, 2017, pp. 535-542).

Según la Cumbre Mundial sobre la Sociedad de la Información (CMSI), un foro mundial organizado por las Naciones Unidas, la gobernanza de internet hace referencia al «desarrollo y aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivas funciones, de principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos que moldean la evolución y utilización de internet» (CMSI, 2005, p. 4; consulte también Kurbalija, 2014, p. 5). Mueller (2010) afirma que la gobernanza de internet no recae principalmente en «instituciones formales que elaboran las políticas», en cambio:

> “La mayor parte de la gobernanza de internet en el mundo real es descentralizada y emergente (...) proviene de las interacciones de decenas de miles de operadores de redes y proveedores de servicios, y a veces de los propios usuarios, que están conectados a través de internet. (p. 9)”

Internet tiene impacto en los intereses globales y su gobernanza:

> “Incluye más que nombres y direcciones de internet, temas tratados por la Corporación de Internet para la Asignación de Nombres y Números (ICANN); también cubre otros temas importantes de política pública, como los recursos críticos de internet, la seguridad y protección de internet y los aspectos y temas de desarrollo relativos al uso de internet. (WGIG, 2005, p. 4)”

Por estos motivos, una sola entidad no puede ser y no ha sido designada como un organismo de gobernanza internacional (Reich et al., 2014). En cambio, múltiples partes interesadas que rigen internet a nivel internacional (los Gobiernos, el sector privado, el mundo académico y la sociedad civil) se encargan de una serie de temas técnicos y no técnicos. No obstante, los países varían en cuanto a sus puntos de vista sobre qué partes interesadas deberían desempeñar un papel primordial en la gobernanza de internet. Mientras que algunos países creen que múltiples partes interesadas deberían ser responsables de la gobernanza de internet, otros países creen que la gobernanza de internet debería ser el dominio exclusivo del Estado (para más información, consulte Masters, 2014; Chang y Grabosky, 2017).

¿Sabían que...?

El Foro para la Gobernanza de Internet (FGI) contiene recursos para temas relacionados con la gobernanza de internet.

¿Desean saber más?

Foro para la Gobernanza de Internet. (n.d.). Publications & Reports.

https://www.intgovforum.org/multilingual/content/publications-reports

Incluso si los países se ponen de acuerdo sobre las partes interesadas responsables de la gobernanza de internet, existen otras barreras para la gobernanza universal de internet debido a las diferencias en los sistemas y leyes de justicia penal de los países (consulte Delitos Cibernéticos-Módulo 3) y en las posturas sobre cuestiones culturales, religiosas, sociales y políticas (consulte Delitos Cibernéticos-Módulos 2, 3 y 10) (Chang, 2012; Chang, 2011; Whitmore et al., 2009). Si bien el objetivo general de la gobernanza de internet es que los países configuren juntos la internet, la realidad es que los países difieren en cuanto a cómo debe darse esta configuración. Esto se observa en las diferencias de los países en cuanto al respeto de algunos principios subyacentes de internet, como la libertad (es decir, que se puede acceder a la información y compartirla «sin restricciones razonables»), la apertura (es decir, un flujo de información en línea sin obstáculos), la interoperabilidad (es decir, la capacidad de los diferentes dispositivos digitales y sistemas informáticos para conectarse, comunicarse e intercambiar datos), la seguridad (es decir, proteger la confidencialidad, integridad y disponibilidad de los sistemas, redes, servicios y datos) y la resiliencia (es decir, el mantenimiento de las operaciones durante las interrupciones y condiciones cambiantes) (Negroponte et al., 2013; Principios para la Formulación de Políticas de Internet de la OCDE de 2014; Declaración Africana sobre los Derechos y las Libertades en internet de 2014; UNESCO, 2015; Morgus y Sherman, 2018, pp. 10-13). Internet ha pasado de ser una plataforma para intercambiar y compartir información, conforme al principio de apertura, a ser una plataforma para interactuar socialmente, comercializar y prestar servicios gubernamentales (Lessig, 1999; Chang y Grabosky, 2017). Al mismo tiempo, internet y las TIC han sido, y siguen siendo, objeto de mal uso y abuso por parte de agentes amenazantes y actores malintencionados que permiten el crecimiento de los delitos cibernéticos y, por consiguiente, la necesidad de seguridad.

Algunos países no se adhieren ni promueven algunos de estos principios (Morgus y Sherman, 2018). Por ejemplo, algunos países enfatizan y dan prioridad a la seguridad a expensas de los principios de libertad y apertura (Morgus y Sherman, 2018, p. 14). Otros países no suscriben la apertura, lo que priva a los ciudadanos del acceso a la información proveniente de fuera de sus países. Además, los países, que por lo demás apoyan los principios de internet, participan en acciones que entran en conflicto con uno o más de estos principios. Por ejemplo, la neutralidad de la red, que promueve la apertura requiriendo que todos los datos, independientemente de la fuente, sean tratados por igual (consulte las definiciones en los marcos jurídicos; p. ej., el artículo 3 de la Ley Federal 12,965 de Brasil de 2014), no puede aplicarse, lo que permite a los proveedores de servicios de internet bloquear o controlar los datos, así como ofrecer vías rápidas para los datos (es decir, priorización pagada) (Shepardson, 2018). Además, existen tensiones en la ejecución de estos principios o en la adhesión a ellos. Los casos en cuestión son la apertura y la seguridad; un cortafuegos, una medida de seguridad que restringe el libre flujo de información —es decir, la apertura— bloqueando el tráfico de datos no autorizados. En este caso, el bloqueo del tráfico de red no autorizado (flujo de información entrante) mediante el cortafuego se produce para garantizar la seguridad del sistema y de la red.

¿Sabían que...?

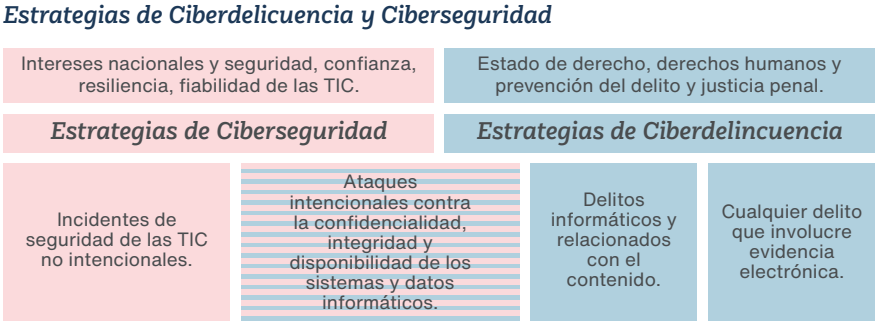
Freedom House tiene un mapa interactivo en línea (Mapa de la libertad en internet 2018) que muestra qué países tienen acceso «libre», parcialmente libre o acceso restringido a internet.

Estrategias de seguridad cibernética: características básicas

Las estrategias de seguridad cibernética y las estrategias contra el delito cibernético (o prevención del delito cibernético) son términos que se han utilizado de manera intercambiable. Si bien las estrategias de seguridad cibernética y contra el delito cibernético se complementan entre sí e incluyen algunas áreas de superposición, estas no son idénticas (Seger, 2012) (ver figura 1). Las estrategias de prevención del delito cibernético plantean los esfuerzos para combatir directa e indirectamente el delito cibernético, tales como las respuestas de las fuerzas del orden y la promoción de la cooperación nacional e internacional entre Gobiernos, empresas, instituciones académicas, organizaciones y el público, con el fin de controlar o reducir el delito cibernético (Seger, 2012). En palabras simples, las estrategias contra el delito cibernético se enfocan exclusivamente en la prevención del delito y las políticas, programas y prácticas de la justicia penal (Seger, 2012). Por el contrario, las estrategias de seguridad cibernética proporcionan orientación en asuntos de seguridad cibernética (pudiendo incluir la prevención del delito cibernético) y mapean objetivos, planes de acción, medidas y las responsabilidades de las instituciones en el cumplimiento de estos objetivos. Estas estrategias incluyen medidas legales, procedimentales, técnicas e institucionales diseñadas para salvaguardar los sistemas, redes, servicios y datos.

Figura 1

Estrategias de seguridad cibernética y estrategias contra el delito cibernético



Adaptado de Seger, A., 2011. *Estrategias de Ciberdelincuencia. Conferencia Octopus 2011.*

Tomado de Comprehensive Study on Cybercrime Draft–February 2013 (p. 228), por UNODC, 2013, UNODC. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Las estrategias nacionales de seguridad cibernética esclarecen las aspiraciones de los países en términos de seguridad cibernética y prevención del delito a nivel nacional e internacional. Estas estrategias resumen los principios en los que se basa la estrategia, prescriben los intereses que esta estrategia intenta proteger, identifican las herramientas utilizadas para promover y proteger estos intereses, identifican las amenazas cibernéticas y los obstáculos que esas amenazas representan para la seguridad nacional y económica, delinean las prioridades de la política de seguridad cibernética y asignan recursos a estas prioridades (Lindstrom y Luiijf, 2012, p. 44). Estas estrategias «motivan (...) a los responsables de las políticas a identificar objetivos estratégicos [«fines»] a precisar los recursos disponibles para alcanzar los objetivos [«medios»] y a proporcionar una guía sobre cómo deben aplicarse esos recursos para alcanzar los objetivos establecidos [«formas»]» (Lindstrom y Luiijf, 2012, p. 46).

Las estrategias de seguridad cibernética detallan por qué la estrategia es importante y por qué es necesaria (contexto), qué hace (objetivos), qué cubre y qué y a quién afecta (alcance) (UIT, 2018, p. 30). Los componentes clave de estas estrategias son los objetivos, las acciones prioritarias, los resultados esperados y los mecanismos de evaluación.

Los objetivos de las estrategias de seguridad cibernética incluyen objetivos relacionados con la seguridad nacional y con las tecnologías de la información y la comunicación. Por ejemplo, la estrategia de seguridad cibernética de Suecia:

> “**Se basa en los objetivos de la seguridad de Suecia:** proteger de la vida y la salud de la población, el funcionamiento de la sociedad y (...) [su] capacidad para defender valores fundamentales como la democracia, el Estado de derecho, los derechos humanos y las libertades. (...) La estrategia también se basa en el objetivo político general [de las tecnologías de la información (IT)] (...) para que Suecia se convierta en el líder mundial del aprovechamiento de las oportunidades de la transformación digital. (Ministerio de Justicia de Suecia, 2017, p. 1; consulte también Ministerio de Justicia de Suecia, «Estrategia Nacional de Seguridad Cibernética)”

En Nigeria, los objetivos de su Estrategia de Seguridad Cibernética (2014) son los siguientes (Sección 3.3.2):

"

I Una legislación integral sobre el delito cibernético y las medidas para contrarrestar las amenazas cibernéticas que se puedan adoptar a nivel nacional, regional y mundial en el contexto de asegurar el ciberespacio de la nación.

II Provisión de medidas que protejan la infraestructura de la información crucial, así como la reducción de nuestras vulnerabilidades nacionales a través de un marco de garantía de la seguridad cibernética.

III Articular una capacidad de respuesta eficaz a las emergencias informáticas.

IV Los mecanismos nacionales de desarrollo de capacidades, concientización del público y empoderamiento de las habilidades son necesarias para ayudar a fortalecer nuestra capacidad de responder con prontitud y eficacia a los ataques cibernéticos.

V Un mecanismo fiable para lograr que las múltiples partes interesadas a nivel nacional y los socios internacionales aborden colectivamente las amenazas cibernéticas.

VI Disuadir y proteger al Gobierno de todas las formas de ataques cibernéticos.

VII Coordinar las iniciativas de seguridad cibernética en todos los niveles de Gobierno en el país.

VIII Crear capacidades nacionales contra las amenazas cibernéticas con una cooperación coherente, a través de la asociación entre el sector público y privado, y la participación de múltiples partes interesadas.

IX Promover la visión nacional sobre la seguridad cibernética mediante la concientización, la asociación a través de responsabilidades compartidas y una comunidad de partes interesadas en la que se confíe.

X Promover la coordinación, cooperación y colaboración de las partes interesadas regionales y mundiales en seguridad cibernética "

Las acciones prioritarias están diseñadas para alcanzar los objetivos. Por ejemplo, en la Unión Europea, la mayoría de las estrategias nacionales de seguridad cibernética identifican como acciones prioritarias la creación de estándares, normas y leyes de seguridad cibernética (siempre que sea necesario), el fomento de una cultura de seguridad cibernética no solo entre las partes interesadas (es decir, organismos públicos, instituciones académicas, empresas y organizaciones), sino también entre el público en general, y el cultivo de la cooperación nacional e internacional y la colaboración entre las partes interesadas pertinentes (ENISA, 2014). Algunas acciones prioritarias enumeradas en la Estrategia Cibernética Nacional de 2018 de los Estados Unidos son «dar prioridad a la innovación», «fomentar la adherencia universal a las normas en materia cibernética», «dirigir con inteligencia objetiva y colaborativa» y «mejorar la detención de delincuentes ubicados en el extranjero» (por nombrar algunos).

Los mecanismos de evaluación incluyen herramientas que pueden utilizarse para determinar lo que se ha logrado (y por extensión, cómo se compara con los resultados esperados). También se incluyen los indicadores clave de rendimiento (KPI), que son medidas que se utilizan para determinar el progreso de la realización de los objetivos estratégicos de la estrategia nacional de seguridad cibernética (ENISA, s.f., anexo B). Sobre la base de esta evaluación, se modifican las estrategias nacionales de seguridad y se revisan las acciones prioritarias (ITU, 2018).

Entre los ejemplos de las estrategias de seguridad cibernética están los instrumentos de política adecuados (p. ej. normas, políticas, leyes, programas educativos, etc.) necesarios para alcanzar los objetivos de dichas estrategias (ITU, 2018, p. 33), así como los responsables de supervisar la implementación de los instrumentos. Por ejemplo, en la Política Nacional de Seguridad Cibernética 2017-2022, Chile incluye las medidas que deben implementarse en función de los objetivos estratégicos específicos y los organismos responsables de aplicar o ayudar en la implementación de las medidas. Asimismo, en el Plan Nacional de Seguridad Cibernética 2022 de Filipinas, se identifican las medidas para alcanzar los objetivos estratégicos y las funciones y responsabilidades de las principales partes interesadas.

Estrategias nacionales de seguridad cibernética: ciclos de vida, buenas prácticas y repositorios

El ciclo de vida de la estrategia nacional de seguridad cibernética incluye cinco fases (ITU, 2018, pp. 16-27):

La primera fase (fase 1) es la fase de iniciación, que incluye la identificación de las partes interesadas pertinentes, así como sus funciones en el proceso de desarrollo, y la creación de un plan para el desarrollo de la estrategia.

La segunda fase (fase 2), inventario y análisis, incluye una evaluación de la postura del país con respecto a la seguridad cibernética, la identificación de las amenazas a la seguridad cibernética y la evaluación de los riesgos actuales y futuros para la seguridad cibernética.

La tercera fase (fase 3) es la elaboración de la estrategia de seguridad cibernética. Esta fase implica la redacción de la estrategia, la obtención de retroalimentación de las partes interesadas pertinentes, la finalización de la estrategia basada en la retroalimentación y la publicación de esta.

La cuarta fase (fase 4), ejecución, consiste en la elaboración de un plan de acción, la determinación de las iniciativas basadas en los objetivos de la estrategia que se aplicarán, la identificación de los recursos necesarios para aplicar esas iniciativas, la determinación de las medidas concretas que se adoptarán y los plazos para completar esas medidas. En esta fase también se especifican las métricas y los indicadores clave de rendimiento para determinar la eficiencia (es decir, la oportunidad) y la eficacia (es decir, los buenos resultados) de las iniciativas.

En general, los planes de acción incluyen las soluciones (o medidas) que se pueden ejecutar para alcanzar los objetivos, las partes interesadas responsables de las tareas, las métricas que se utilizarán para determinar el plazo para completar la tarea y si se logró el resultado deseado. Los planes de acción se han ejecutado a nivel nacional (p. ej., la Autoridad de Seguridad Nacional, Plan de Acción para la Implementación del Concepto de Seguridad Cibernética de la República Eslovaca para 2015-2020) y a nivel regional (p. ej., el Plan de Acción sobre Seguridad Cibernética y Delito Cibernético de Caricom).

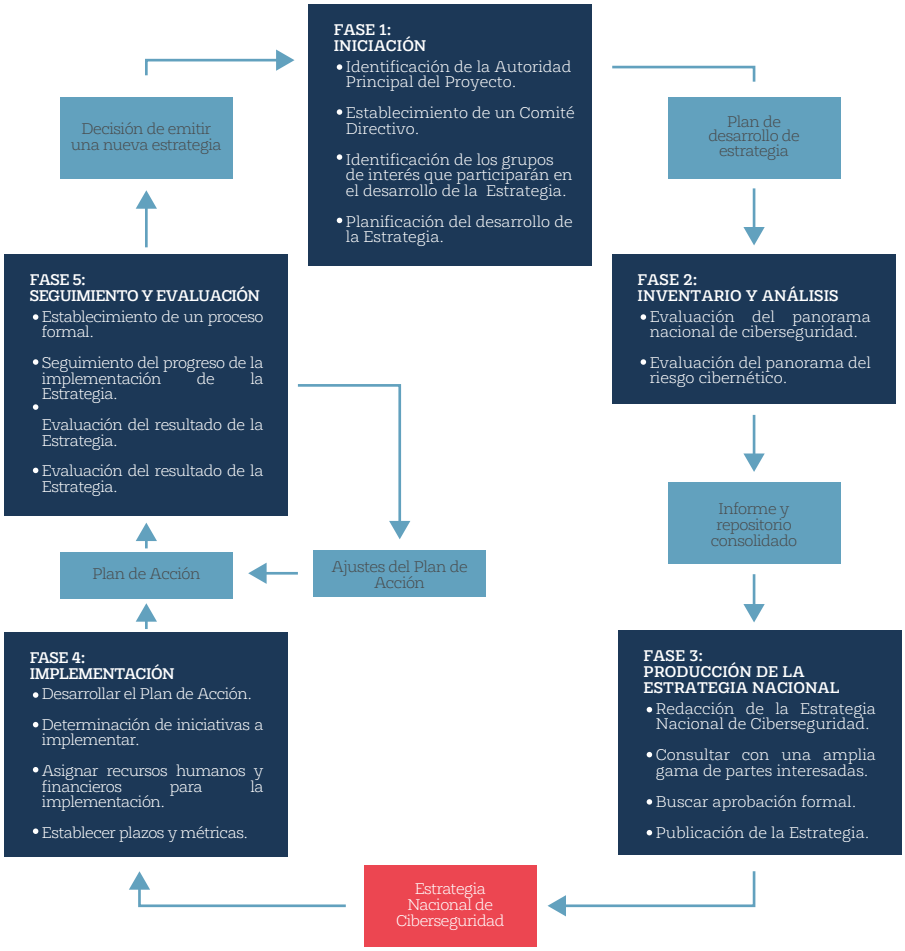
La quinta fase (fase 5), supervisión y evaluación, busca determinar si el plan de acción está acorde con los objetivos de la estrategia de seguridad cibernética, y evalúa la estrategia y el plan de acción para determinar si están actualizados, si cumplen con las necesidades de seguridad cibernética del país y si pueden lidiar con la evolución de los riesgos de seguridad cibernética. Si el plan de acción no cumple con los objetivos de la estrategia de seguridad cibernética, se harán cambios al plan. También se harán cambios en la estrategia, en caso de que sea obsoleta o no se pueda aplicar a las amenazas de seguridad cibernéticas nuevas o emergentes.

¿Sabían que...?

Las nuevas tecnologías (p. ej., cadena de bloques, inteligencia artificial, computación cuántica) se mencionan en algunas estrategias cibernéticas nacionales (consulte, p. ej., la Estrategia Cibernética Nacional de los Estados Unidos y la Estrategia Cibernética Nacional del Reino Unido 2016-2021).

Figura 2

Ciclo de vida de la estrategia nacional de seguridad cibernética



Tomado de A Guide to Developing a National Cybersecurity Strategy (p. 17), por ITU, 2018, ITU https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

La Guía de buenas prácticas de la estrategia nacional de seguridad cibernética (2016) de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) incluye ejemplos de objetivos estratégicos y tareas que deben cumplirse para lograr estos objetivos y proporcionar orientación sobre cómo desarrollar una estrategia nacional de seguridad cibernética (pp. 14-21). La ENISA (2014) también enfatizó la necesidad de crear estrategias nacionales de seguridad cibernética basadas en evidencias, mediante la realización de evaluaciones puntuales y periódicas de dichas estrategias (es decir, examinando los resultados basados en métricas de evaluación predefinidas) y utilizando los resultados de estas evaluaciones para modificar las estrategias y los planes de acción para la ejecución de las estrategias (pp. 9-10).

Las estrategias nacionales de seguridad cibernética pueden incluirse en un solo documento o se pueden distribuir partes de la estrategia en diferentes instrumentos que cubran alguna faceta de la seguridad cibernética (UIT, s.f.). La Unión Internacional de Telecomunicaciones (UIT) tiene un repositorio de estrategias nacionales de seguridad cibernética que incluye políticas, planes y otros documentos nacionales relacionados con la seguridad cibernética (es decir, el Repositorio de Estrategias Nacionales de Seguridad Cibernética). Además, el Centro de Excelencia de Defensa Cibernética Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) alberga en su sitio web las estrategias de seguridad cibernética de los Estados Miembro y de los Estados no Miembro de la OTAN y documentos relacionados. Asimismo, la ENISA ha elaborado un mapa interactivo que incluye las estrategias nacionales de seguridad cibernética de los Estados Miembro de la Unión Europea y los objetivos de sus estrategias (p. ej., abordar el delito cibernético, establecer una capacidad de respuesta a los incidentes, participar en la cooperación internacional, establecer requisitos básicos de seguridad y establecer asociaciones entre el sector público y privado, entre otras).

"Las estrategias nacionales de seguridad cibernética esclarecen las aspiraciones de los países en términos de seguridad cibernética y prevención del delito a nivel nacional e internacional".

Cooperación internacional en asuntos de seguridad cibernética

La Unión Internacional de Telecomunicaciones (UIT), un organismo de las Naciones Unidas que es considerado el «principal foro mundial a través del cual las partes trabajan para alcanzar un consenso sobre una amplia variedad de cuestiones que afectan a la futura dirección de la industria de las TIC» (UIT, s.f.), lanzó la Agenda Global sobre Seguridad Cibernética, que es «un marco para la cooperación internacional destinada a aumentar la confianza y la seguridad en la sociedad de la información» (UIT, s.f.). La Agenda Global sobre Seguridad Cibernética identifica cinco pilares estratégicos: legal, técnico, organizacional, creación de capacidades y cooperación (consulte la figura 3).

Figura 3

Pilares estratégicos de la Agenda Global sobre Seguridad Cibernética

Tomado de Global Cybersecurity Index Overview. International Telecommunication Union, 2nd Annual Meeting of Community of Practice on Composite Indicators and Scoreboards (9-10 November 2017, Ispra, Italy) (diapositiva 5), por Grace Acayo, 2017, ITU

https://composite-indicators.jrc.ec.europa.eu/sites/default/files/02%20-%20Global%20Cybersecurity%20Index%20-%20Grace%20Acayo_0.pdf

El pilar legal se centra en la armonización de los reglamentos y las leyes relacionadas con la seguridad cibernética y a los delitos dependientes de la cibernética y propiciados a través de ella. Los casos en cuestión son las leyes sobre delito cibernético (consulte Delitos Cibernéticos-Módulos 2 y 3), las leyes y regulaciones sobre protección de datos (consulte Delitos Cibernéticos-Módulo 10), las leyes de seguridad cibernética y otras leyes relacionadas (p. ej., Ley Danesa de Protección de Datos de 2018, Dinamarca; Decreto sobre Delitos de 2009, Fiyi: División 6-Delitos Informáticos; Ley Federal N.° (1) de 2006 sobre Comercio y Transacciones Electrónicas, Arabia Saudita; Ley sobre el Uso Indebido de la Informática de 1990 y Ley de Protección de Datos de 2018, Reino Unido. Para más información sobre este pilar, consulte UIT, 2015; UIT, 2017).

El pilar técnico abarca las instituciones técnicas existentes, las normas y protocolos de seguridad cibernética y las medidas necesarias para combatir las amenazas contra la seguridad cibernética. Un ejemplo de institución técnica es un Equipo de Respuesta ante Emergencias Informáticas (CERT), definido como «una organización o equipo que proporciona, a una circunscripción bien definida, servicios y apoyo tanto para prevenir como para responder a incidentes de seguridad informática» (Wahid, 2016). Las capacidades de los CERT varían según el rango y combinación de servicios reactivos, proactivos o de gestión de la calidad de la seguridad ofrecidos (CMU-SEI, 2006). Por ejemplo, estos servicios pueden incluir la respuesta oportuna a un incidente para que el ataque pueda ser contenido e investigado rápidamente y facilitar la rápida recuperación a un estado anterior al incidente (Borodkin, 2001). Además de la respuesta a incidentes, un CERT puede realizar otras actividades como llevar a cabo una evaluación de vulnerabilidades y proporcionar sesiones informativas de seguridad; estas actividades adicionales dependen de la organización (Proffitt, 2007). Los países pueden tener CERT y Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT) nacionales, gubernamentales y sectoriales, o una combinación de todos o algunos de ellos (para más información sobre este pilar, consulte UIT, 2015; UIT, 2017). Los CERT y CSIRT también han creado grupos dentro de sus regiones para compartir información y coordinar actividades, entre otros (p. ej., el CERT de Asia Pacífico o APCERT; el CERT de África o AfricaCERT).

¿Sabían que...?

CERT® es una marca registrada del Software Engineering Institute of Carnegie Mellon University. Los CSIRT pueden solicitar autorización para utilizar la marca registrada CERT. El siguiente sitio web incluye los pasos que un CSIRT debe seguir a fin de recibir la autorización para utilizar la marca registrada CERT:

https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/

El pilar organizacional incluye estructuras y políticas organizacionales de seguridad cibernética y organismos responsables de la coordinación de la política de seguridad cibernética. Este pilar incluye las estrategias nacionales de seguridad cibernética y los marcos nacionales de seguridad cibernética, así como los organismos reguladores que supervisan la implementación de estas estrategias y marcos (p. ej., el Consejo de Seguridad Cibernética de Islandia, la Oficina Federal para la Seguridad de la Información en Alemania, la Oficina de Seguridad Cibernética y Aseguramiento de la Información del Reino Unido, el Ministerio de Ciencia, TIC y Planificación del Futuro en la República de Corea, y el Departamento Nacional de Planeación y el Ministerio de Tecnologías de la Información y Comunicaciones en Colombia, por nombrar algunos [para más información sobre este pilar, consulte UIT, 2015; UIT, 2017]).

El pilar de creación de capacidades abarca los esfuerzos para promover la concientización, educación y capacitación sobre seguridad cibernética. Algunos ejemplos incluyen campañas públicas de concientización, investigación y desarrollo en seguridad cibernética, formación profesional y programas nacionales de educación y planes de estudios. Por ejemplo, en República Dominicana:

> **La Comisión Nacional para la Sociedad de la Información y el Conocimiento (CNSIC)** tiene un programa nacional de concientización oficialmente reconocido que promueve normas, valores y comportamientos sociales que contribuyen a la integridad, la creatividad y la innovación en la navegación por el ciberespacio. (UIT, 2015, p. 171; para más información sobre este pilar, consulte UIT, 2015; UIT, 2017).

Otros países también han lanzado campañas de concientización y educación sobre seguridad cibernética (consulte el recuadro sobre Ejemplos de campañas nacionales e internacionales de concientización y educación sobre seguridad cibernética). Además de estas campañas de concientización y educación sobre seguridad cibernética, la UIT brinda herramientas para ayudar a los países en sus esfuerzos de creación de capacidades. Estas herramientas están diseñadas para «capturar información sobre amenazas específicas que afectan al país» (Redes de Investigación Honeypot o HORNET) y «agregar y difundir datos relevantes sobre incidentes» (Motor de Alerta e Informes de Vigilancia de Abuso o AWARE) (UIT, s.f.).

Ejemplos de campañas nacionales e internacionales de concientización y educación sobre seguridad cibernética

Australia

Australia tiene una campaña, Stay Smart Online, que brinda a las personas y a las pequeñas empresas información sobre cómo protegerse de las amenazas a la seguridad cibernética y reducir su riesgo. Además, el sitio web de la Oficina de la Comisión de Seguridad Electrónica de Australia promueve la seguridad en línea, proporcionando recursos educativos para niños, padres y otros, informándolos sobre las diversas formas de delitos cibernéticos (en particular, los delitos cibernéticos interpersonales, tratados en Delitos Cibernéticos-Módulo 12) y las formas en que pueden protegerse en línea, y ofreciendo a los usuarios la opción de denunciar ciertos delitos cibernéticos a través del sitio web. Por ejemplo, la Oficina tiene un portal de denuncias en línea contra el abuso mediante el uso de imágenes, donde las víctimas pueden denunciar los casos en que sus imágenes sexuales o de desnudos han sido compartidas (cargadas o distribuidas) sin su consentimiento. La Oficina se esfuerza para localizar las imágenes y trabaja con las redes sociales o los intermediarios de internet pertinentes (y, en algunos casos, con los agresores) para que las imágenes sean retiradas y eliminadas (Flynn y Henry, por publicar).

Canadá

En Canadá, Get Cyber Safe brinda a las personas y empresas información sobre los riesgos de seguridad cibernética y las formas en las que las personas y las empresas pueden protegerse de las amenazas a la seguridad cibernética.

Reino Unido

La campaña GetSafeOnline del Reino Unido es una iniciativa de concientización sobre seguridad cibernética, que ofrece a las personas información sobre prácticas seguras en el hogar y en el lugar de trabajo.

Estados Unidos

La iniciativa StaySafeOnline de la Alianza Nacional de Seguridad Cibernética ofrece a las personas información sobre prácticas seguras en internet, delitos cibernéticos, seguridad de cuentas clave en línea y dispositivos digitales, así como sobre gestión de la privacidad. El Mes de Concientización Nacional sobre Seguridad Cibernética (NCSAM), que se celebra cada mes de octubre, fue lanzado por una asociación público-privada (es decir, la Alianza Nacional de Seguridad Cibernética y el Departamento de Seguridad Nacional de los Estados Unidos), cuyo objetivo es brindar los recursos que las personas necesitan para navegar por internet y utilizar los dispositivos digitales de forma segura. Asimismo, el Mes Europeo de Seguridad Cibernética (ECSM), una campaña de concientización sobre seguridad cibernética que se celebra de forma similar cada mes de octubre, pretende informar a las personas sobre el delito cibernético y seguridad cibernética en un esfuerzo por modificar las prácticas inseguras de internet. Además, en febrero de cada año se celebra en todo el mundo el Día Internacional de la Internet Segura, para promover la seguridad y fomentar comunidades en línea sanas y felices.

El Departamento de Seguridad Nacional de los Estados Unidos (DHS) también creó una campaña internacional de educación y concientización conocida como PARA. PIENSA.CONÉCTATE.™ Las empresas, los ministerios de los Gobiernos nacionales y las ONG de ámbito nacional, por ejemplo, de Bolivia, Panamá, Mongolia, Tonga, Nigeria, Trinidad y Tobago, Antigua y Barbuda, Jamaica, India y Japón (por mencionar algunos) han adoptado e implementado este tipo de campaña de concientización (Anti-Phishing Working Group, s.f.). El Departamento de Seguridad Nacional de los Estados Unidos creó un paquete informativo para su campaña PARA. PIENSA. CONÉCTATE.™, para permitir que otros países lancen campañas nacionales similares en sus propios países. Este paquete incluye una lista de comprobación de las mejores prácticas, un ejemplo de plan de comunicaciones y una métrica de la campaña de concientización sobre seguridad cibernética (Mes Europeo de Seguridad Cibernética, s.f.).

Sudáfrica

Sudáfrica ha desplegado varias campañas de concientización sobre seguridad cibernética dirigidas exclusivamente por la academia, las organizaciones privadas y los organismos públicos (Dlamini y Modise, 2012). Además, el Departamento de Telecomunicaciones y Servicios Postales de Sudáfrica creó un Centro de Seguridad Cibernética, que incluye información y recursos sobre medidas de protección contra el delito cibernético y campañas de concientización sobre seguridad cibernética. Al igual que los Estados Unidos y otros países, Sudáfrica tiene una campaña de concientización sobre seguridad cibernética que se celebra anualmente en octubre (Pazvakavambwa, 2016).

Myanmar

En 2018, se lanzó CyberBayKin, una campaña de seguridad cibernética de Myanmar, para concientizar sobre la seguridad y el riesgo cibernético en Myanmar. La Universidad de Monash (Australia) y Kernellix Co., Ltd. (Myanmar) iniciaron la campaña, en colaboración con el Centro Nacional de Seguridad Cibernética del Ministerio de Transporte y Comunicaciones de Myanmar. En el lanzamiento se presentaron seis personajes de cómic de este país que fueron diseñados para la campaña. En la campaña de un año de duración, se publicaron ilustraciones de cómic de concientización sobre la seguridad cibernética cada quince días en la plataforma de Facebook. El Departamento de Relaciones Exteriores y Comercio de Australia, en el marco de la Estrategia Internacional de Participación Cibernética y la Facultad de Ciencias Sociales de la Universidad de Monash, apoya y financia la campaña (CyberBayKin, 2018).

El pilar de la cooperación se centra en las asociaciones interinstitucionales y público-privadas, las redes de intercambio de información y los acuerdos de cooperación. Un ejemplo de ello es la Estrategia Internacional de Compromiso Cibernético para mejorar la colaboración público-privada y la cooperación entre países. Otros ejemplos incluyen asociaciones entre países e intercambio de información con la UIT, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), la Organización para la Seguridad y la Cooperación en Europa (OSCE), y la Organización del Tratado del Atlántico Norte (OTAN), y acuerdos de cooperación, como el Convenio sobre Delitos Cibernéticos de 2001 del Consejo de Europa, el Acuerdo sobre Cooperación en la Lucha contra los Delitos Relacionados con la Informática de 2001 de la Comunidad de Estados Independientes, el Convenio Árabe sobre la Lucha contra los Delitos Relacionados con la Tecnología de la Información de 2010 de la Liga de Estados Árabes y el Convenio de la Unión Africana sobre Seguridad Cibernética y Protección de los Datos Personales de 2014, por nombrar algunos (para más información sobre este pilar, consulte UIT, 2015; UIT, 2017).

Un análisis comparativo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2012) de las estrategias nacionales de seguridad cibernética en diez países (Australia, Canadá, Finlandia, Francia, Alemania, Japón, Países Bajos, España, Estados Unidos y Reino Unido) reveló diferencias en las definiciones de seguridad cibernética, pero similitudes en los enfoques de los países para abordar la seguridad cibernética de manera integral, incluyendo en diversos grados los contenidos de cada pilar legal, técnico, organizacional, creación de capacidades y cooperación.

Para crear una estrategia nacional de seguridad cibernética integral y eficaz, la Guía para la elaboración de una estrategia nacional de ciberseguridad de 2018 de la UIT propone la inclusión de las siguientes áreas temáticas en la estrategia: gobernanza (tratada en este módulo), gestión de riesgos (es decir, el proceso de identificación, evaluación y control o eliminación de amenazas, tratados en Delitos Cibernéticos-Módulo 9), preparación y resistencia (tratados en Delitos Cibernéticos-Módulo 9); servicios críticos de infraestructura y servicios esenciales (tratados en Delitos Cibernéticos-Módulo 14); capacidad, creación de capacidades y concientización (tratados en este módulo y en Delitos Cibernéticos-Módulo 7); legislación y regulación (tratados en Delitos Cibernéticos-Módulos 2, 3 y 10) y cooperación internacional (tratados en Delitos Cibernéticos-Módulo 7). Otras organizaciones también han proporcionado orientación sobre el desarrollo de la política de seguridad cibernética y los marcos reguladores, las medidas técnicas y organizacionales, la creación de capacidades y la cooperación (p. ej., el Modelo de gobernanza cibernética de la Mancomunidad de 2014 de la Organización de Telecomunicaciones de la Mancomunidad).

Postura de seguridad cibernética

Postura de seguridad cibernética es un término utilizado para describir las capacidades de seguridad cibernética de un país, organización o empresa. Se han utilizado varias herramientas para evaluar la postura de seguridad cibernética. Un ejemplo de esta herramienta es el Índice global de seguridad cibernética (GCI) de la Unión Internacional de Telecomunicaciones. Según la UIT (s.f.), el Índice global de seguridad cibernética (GCI) es una herramienta de creación de capacidades que evalúa el compromiso de los países con la seguridad cibernética, identifica su postura respecto a ella y los aspectos que deben mejorarse. Se puede evaluar la postura de seguridad cibernética de los países en función de su desarrollo en los cinco pilares (legal, técnico, organizacional, creación de capacidades y cooperación) encontrados en la Agenda Global sobre Seguridad Cibernética de la UIT. En particular, los países reciben puntajes de dicho índice basados en su nivel de compromiso con los cinco pilares. Estos puntajes incluyen la iniciación (es decir, pasos iniciales que demuestren el compromiso con los pilares), la madurez (es decir, compromisos hechos con los pilares) y el liderazgo (es decir, un alto compromiso con los pilares) (UIT, 2017, p. 13).

Los resultados de la encuesta del Índice global de seguridad cibernética de 2017 revelaron que la mitad de los países que respondieron no tenían una estrategia de seguridad cibernética (UIT, 2017). Los resultados de la encuesta del Índice global de seguridad cibernética de 2017 también revelaron una gran variación en los compromisos de seguridad cibernética entre los Estados dentro y fuera de sus regiones. Los resultados revelaron, además, que la solidez de los compromisos de seguridad cibernética de los países variaba según el pilar (es decir, los países obtuvieron una puntuación alta en algunos pilares y media o baja en otros) (UIT, 2017; para información detallada de los resultados, consulte UIT, 2017). Sin embargo, para que los esfuerzos sean efectivos, se necesitan compromisos de seguridad cibernética en todos los pilares.

El Centro Mundial de Capacidad en Seguridad Cibernética (GCSCC) de la Universidad de Oxford desarrolló un Modelo del estado de desarrollo de capacidad en seguridad cibernética (CMM) para evaluar la postura de seguridad cibernética de los países (es decir, la madurez de la capacidad de seguridad cibernética), examinando los esfuerzos de los países en «políticas y estrategias de seguridad cibernética», «cultura y sociedad cibernética», «educación, capacitación y habilidades en seguridad cibernética», «marcos regulatorios y legales» y «normas, organizaciones y tecnologías» (Centro Mundial de Capacitación en Seguridad Cibernética, 2016, pp. 10-13). Esta evaluación informa a los países en qué estado de madurez se encuentran: fase inicial (es decir, sin seguridad cibernética o empezando a desarrollarse), formativa (es decir, con cierta seguridad cibernética), consolidada (es decir, con seguridad cibernética en funcionamiento; con una consideración mínima de la asignación de recursos), estratégica (es decir, con elecciones deliberadas y calculadas sobre seguridad cibernética) y dinámica (es decir, se adapta la seguridad cibernética a los cambios del entorno y de las necesidades) (Centro Mundial de Capacitación en Seguridad Cibernética, 2016, p. 7). Se ha utilizado el CMM para evaluar numerosos países de todo el mundo de forma individual o como parte de un estudio regional (Centro Mundial de Capacitación en Seguridad Cibernética, 2018). Además del CMM, el Centro Mundial de Capacitación en Ciberseguridad desarrolló el Portal de Capacidad para la Seguridad Cibernética, que incluye material de creación de capacidades y mejores prácticas de seguridad cibernética, y facilita el intercambio de información, con el fin de ayudar a los países a mejorar su postura de seguridad cibernética.

Los países también han implementado marcos para ayudar a los sectores público y privado a mejorar su postura de seguridad cibernética. Un ejemplo de ello es el Marco para mejorar la infraestructura crítica de seguridad cibernética del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) (publicado en 2014, revisado en 2017 y 2018), el cual proporciona lineamientos, normas y mejores prácticas para ayudar a los sectores público y privado a mejorar su postura de seguridad cibernética. En 2017, se aprobó el Decreto Ejecutivo sobre el Fortalecimiento de la Seguridad Cibernética de las Redes Federales y la Infraestructura Crítica de los Estados Unidos, en el que se ordenaba a las organizaciones federales a utilizar este marco para mejorar su postura de seguridad cibernética. También se ha adoptado o adaptado este marco por parte de empresas y organizaciones dentro de los Estados Unidos y algunos otros países (p. ej., Italia, Uruguay y Bermudas) (NIST, 2018). La Asociación de Auditoría y Control en Sistemas de Información (ahora solo conocida por su acrónimo ISACA) desarrolló un programa de auditoría para comprobar la eficacia de las medidas de seguridad cibernética que implementaron las empresas, organizaciones y agencias utilizando el marco del NIST (ISACA, 2017). Del mismo modo, las regulaciones del Gobierno chino, como el Reglamento Especial sobre Divulgación de Información de Bancos Comerciales y la Medida de Notificación de Incidentes de Seguridad de la Información en Internet, y la normativa de Taiwán, como la Guía de Notificación de Incidentes Importantes de Bancos y las Medidas sobre Notificación y Respuesta a los Incidentes de Seguridad de la Información y la Comunicación a Nivel Nacional, son normas destinadas a facilitar la colaboración entre los sectores público y privado sobre la seguridad cibernética (Chang, 2012; Chang et al., 2018).

Reconociendo que la postura de seguridad cibernética depende de la cantidad y calidad de la fuerza laboral en seguridad cibernética, Estados Unidos también implementó en 2017 el Marco para el personal de seguridad cibernética de la Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE). Este marco forma parte de los objetivos estratégicos de la NICE para desarrollar una fuerza laboral en seguridad cibernética, a través de la identificación de los conocimientos, habilidades y destrezas necesarias para los diferentes puestos de trabajo en seguridad cibernética, y para proporcionar orientación a la academia y a los empleadores sobre la creación e implementación de programas académicos y de formación profesional. El déficit mundial en cantidad y calidad de profesionales en seguridad cibernética explica el hecho de que es necesario prestar atención al desarrollo de la fuerza laboral en seguridad cibernética en la mayoría de los países (Frost y Sullivan Executive Briefing, 2017).

Referencias

- ***African Declaration on Internet Rights and Freedoms of 2014. (n.d.).*** Freedom of expression.
  - *https://africaninternetrights.org/en/principles/3#principle*

- ***Anti-Phishing Working Group. (n.d.).*** Twenty-Three National Campaigns Deployed Since 2010 - Join Us
  - *http://education.apwg.org/safety-messaging-convention/*

- ***Borodkin, M. (2001).*** Computer Incident Response Team. SANS.
  - *https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641*

- ***Braithwaite, J. (1982).*** Enforced self-regulation: A new strategy for corporate crime control. Michigan Law Review, 80(7), 1466-1507.

- ***Brenner, S.W. (2005).*** Distributed security: Moving away from reactive law enforcement. International Journal of Communication Law & Policy, 9, 1-42.

- ***Caricom. (2016).*** Cyber Security and Cybercrime Action Plan.

- ***Carnegie Mellon University-Software Engineering Institute (CMU-SEI). (2016).*** CSIRT Services. Carnegie Mellon University-Software Engineering Institute.
  - *https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf*

- ***Chang, L.Y.C. (2011).*** Cyber-conflict between Taiwan and China. Strategic Insight, 10(1), 26-35.

- ***Chang, L.Y.C. (2012).*** Cybercrime in the Greater China Region:Regulatory Responses and Crime Prevention Across the Taiwan Strait. Cheltenham: Edward Elgar.

- ***Chang, L.Y.C., Zhong, L.Y. & Grabosky, P.N. (2016).*** Citizen co-production of cyber security: Self-Help, Vigilantes, and Cybercrime. Regulation & Governance, 12: 101-114.

- ***Chang, L.Y.C. & Grabosky, P. (2017).*** The governance of cyberspace. In Peter Drahos (ed.). Regulatory Theory: Foundations and Applications (pp. 533-551). ANU Press.

- ***Commonwealth Telecommunications Organisation. (2014).*** Commonwealth ICT Ministers Forum 2014 (Marlborough House, London). CCDCOE.
  - *https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf*

- ***Cyber Security Agency of Singapore. (2016).*** Singapore's Cybersecurity Strategy.

- ***CyberBayKin. (2018).*** About the Campaign. https://en.cyberbaykin.org/#about-the-campaign

- ***Dlamini, Z. y Modise, M. (2012).*** Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. 7th International Conference on Information Warfare and Security (ICIW), University of Washington, Seattle, United States (March 22-23, 2012).

- ***Drahos, P. (ed.). (2017).*** Regulatory Theory: Foundations and Applications. ANU Press.

- ***ENISA. (2014).*** Appendix A: Mapping of Cybersecurity Strategies.

- ***ENISA. (2014).*** An Evaluation Framework for National Cyber Security Strategies.

- ***ENISA. (n.d.).*** ENISA and Cyber Security Strategies.

- ***ENISA. (n.d.).*** Annex B - Methodology. ENISA.
  •*https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies-1/annex-b-methodology/view*

- ***European Cyber Security Month. (n.d.).*** International Cyber Awareness Programs New Campaign Packet.
  • *https://cybersecuritymonth.eu/news/international-cyber-awareness-programs-new-campaign-packet*

- ***Frischmann, B.M. (2003).*** The Prospect of Reconciling internet and Cyberspace. Loyola University Chicago Law Journal, 35(1), 205-234.

- ***Flynn, A. & Henry, N. (por publicar).*** Image-Based Sexual Abuse. En Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press.

- ***Frost & Sullivan Executive Briefing. (2017).*** 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk.

- ***Global Cyber Security Capacity Centre. (2018).*** CMM Assessments Around the World.

- ***Global Cyber Security Capacity Centre. (2016).*** Cybersecurity Capacity Maturity Model for Nations (Revised Edition). University of Oxford.

- ***Government of Chile. (2017).*** National Cybersecurity Policy 2017-2022.

- ***Internet Society. (n.d.).*** World Summit on the Information Society.
  • *https://www.internetsociety.org/issues/internet-governance/wsis/*

- ***ISACA. (2017).*** ISACA Produces New Audit Program Based on NIST Framework.
  •*https://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/ISACA-Produces-New-Audit-Program-Based-on-NIST-Framework.aspx*

- ***ITU. (2018).*** A Guide to Developing A National Cybersecurity Strategy.

- ***ITU. (2017).*** Global Cybersecurity Index (GCI) 2017.

- ***ITU. (2015).*** Global Cybersecurity Index & Cyberwellness Profiles. ITU.
  • *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf*

- ***ITU. (2014).*** Understanding cybercrime: Phenomena, challenges and legal response. ITU.
  • *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf*

- ***ITU. (2008).*** Overview of cybersecurity. Recommendation ITU-T X.1205. Series X: Data Networks, Open System Communications And Security.
  • *https://www.itu.int/rec/T-REC-X.1205-200804-I*

- ***ITU. (n.d.).*** Cyberthreat Insight.
  • *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberthreat_Insight.aspx*

- ***ITU. (n.d.).*** Global Cybersecurity Agenda.
  • *https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx*

- ***ITU. (n.d.).*** National Strategies.

- ***ITU. (n.d.).*** National Cybersecurity Strategies Repository.

- ***Kerr, O.S. (2003).*** The Problem of Perspective in internet Law, Georgetown Law Journal, 91, 357-377.

- ***Kurbalija, J. (2014).*** An Introduction to internet Governance. 6th edition. DiploFoundation.

- ***Lessig, L. (1999).*** Code and Other Laws of Cyberspace. Basic Books.

- ***Lessig, L. (2006).*** Code: Version 2.0. Basic Books.

- ***Lindstrom, G. & Luiijf, E. (2012).*** Political Aims & Policy Methods. En Alexander Klimburg (Ed.). National Cyber Security Framework Manual (pp. 44-65). NATO CCD COE Publication, Tallinn.

- ***Maras, M.H. (2014).*** Transnational Security. CRC Press.

- ***Masters, J. (2014).*** What is internet Governance? Council on Foreign Relations.

- ***Morgus, R. and Sherman, J. (2018).*** The Idealized internet vs. internet Realities: Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global internet (Version 1.0).

- ***Mueller, M. (2010).*** Networks and states: The global politics of internet governance. MIT Press.

- ***National Security Authority (Slovakia). (2015).*** Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020. ENISA.
  •*https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ActionPlanforthe ImplementationoftheCyberSecurityConceptoftheSlovakRepublicfor20152020_3_.pdf*

- ***NATO CCD COE. (n.d.).*** Cyber Security Strategy Documents.
  • *https://ccdcoe.org/library/strategy-and-governance/*

- ***Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017).*** National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. NIST Special Publication 800-181.

- ***Nigeria, National Cybersecurity Strategy. (2014).*** ITU.
  •*https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf*

- ***Negroponte, J.D., Palmisano, S.J. & Segal, A. (2013).*** Defending an Open, Global, Secure, and Resilient internet. Council on Foreign Relations. Independent Task Force Report No. 70.

- ***NIST. (2018).*** Path Forward to Support Adaption and Adoption of Cybersecurity Framework: The Framework for Improving Critical Infrastructure Cybersecurity.

- ***OECD. (2012).*** Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the internet Economy, OECD Digital Economy Papers, No. 211.

- ***OECD. (2014).*** OECD Principles for Internet Policy Making of 2014. OECD.
  • *https://www.oecd.org/internet/ieconomy/oecd-principles-for-internet-policy-making.pdf*

- ***Pazvakavambwa, R. (2016, October 17).*** Government to promote cyber security awareness. ITWeb.
  • *https://www.itweb.co.za/content/3mYZRX79OmXqOgA8*

- ***Proffitt, T. (2007).*** Creating and Managing an Incident Response Team for a Large Company. SANS.
  •*https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821*

- ***Reich, P., Anand, P., Mittal, V., Kiran, A., Osula, A.M. & Weinstein, S. (2014).*** Internet governance: International law and global order in cyberspace. En Manfred Steger, Paul Battersby, and Joseph Siracusa. (eds.). The SAGE Handbook of Globalization (pp. 592-620), Sage.

- ***Seger, A. (2012).*** Cybercrime strategies. Global Project on Cybercrime.

- ***Shepardson, D. (2018, October 12).*** U.S. defends FCC's repeal of net neutrality rules. Reuters.
  • *https://www.reuters.com/article/us-usa-internet/u-s-defends-fccs-repeal-of-net-neutrality-rules-idUSKCN1MM242*

- ***Swedish Ministry of Justice. (2016).*** A national cyber security strategy. Government Offices of Sweden.
  •*https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213*

- ***UK Centre for the Protection of National Infrastructure. (n.d.).*** Security Awareness Campaigns
  • *https://www.cpni.gov.uk/security-awareness-campaigns*

- ***UNESCO. (2015).*** Principles for governing the internet: A comparative analysis. UNESCO.
  • *http://unesdoc.unesco.org/images/0023/002344/234435e.pdf*

- ***UNODC. (2013).*** Draft Comprehensive Study on Cybercrime.

- ***US National Initiative for Cybersecurity Career and Studies (NICCS).*** Glossary.
  • *https://niccs.us-cert.gov/about-niccs/glossary*

- ***US White House. (2018).*** National Cyber Strategy 2018. White House.
  • *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf*

- ***Wahid, A. (2016).*** Introduction to Computer Security Incident Response Team (CSIRT). Asia Pacific Network Information Centre. APNIC.
  - *ftp://ftp.apnic.net/apnic/training/eLearningHandouts/2017/20171004/02%20Introduction%20to%20CSIRT.pdf*

- ***Whitmore, A., Choi, N. & Arzrumtsyan, A. (2009).*** One Size Fits All? On the Feasibility of International internet Governance. Journal of Information Technology & Politics, 6:1, 4-11.

- ***Working Group on Internet Governance. (2005).*** Report of the Working Group on internet Governance. Working Group on Internet Governance.
  - *https://www.wgig.org/docs/WGIGREPORT.pdf*

Legislaciones y convenciones nacionales e internacionales

- ***African Union. (2014).*** African Union Convention on Cyber Security and Personal Data Protection.
  - *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

- ***Commonwealth of Independent States. (2001).*** Agreement on Cooperation in Combating Offences related to Computer Information.
  - *https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth*

- ***Council of Europe. (2001).*** Convention on Cybercrime.
  - *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561*

- ***Denmark. (2018).*** Data Protection Act.
  - *https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf*

- ***Fiji. (2009).*** Crimes Decree 2009: Division 6 – Computer Offences.
  - *https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=86223&p_country=FJI&p_count=296*

- ***League of Arab States. (2010).*** Arab Convention on Combating Information Technology Offences.
  - *http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences*

- ***Saudi Arabia. (2006).*** Federal Law No. (1) on Electronic Commerce and Transactions.
  - *http://www.wipo.int/wipolex/en/text.jsp?file_id=316895*

- ***United Kingdom. (1990).*** Computer Misuse Act.
  - *https://www.legislation.gov.uk/ukpga/1990/18/contents*

- ***United Kingdom. (2018).*** Data Protection Act.
  - *http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted*

Lecturas principales

- ***Benoliel, D. (2015).*** Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study. North Carolina Journal of Law & Technology, 16(3).

- ***Carr, M. (2016).*** Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.

- ***ENISA. (2014).*** An Evaluation Framework for National Cyber Security Strategies.

- ***Henschke, A. & Ford, S.B. (2017).*** Cybersecurity, trustworthiness and resilient systems: guiding values for policy. Journal of Information Technology & Politics, 2:1, 82-95.

- ***Internet Society. (2016).*** Internet Governance – Why the Multistakeholder Approach Works.

- ***ITU. (2018).*** A Guide to Developing A National Cybersecurity Strategy.

- ***Lindstrom, G. & Luiijf. (2012).*** Political Aims & Policy Methods. En Alexander Klimburg (Ed.). National Cyber Security Framework Manual (pp. 44-65). NATO CCD COE Publication, Tallinn.
  • *https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf*

- ***Morgus, R. & Sherman, J. (2018).*** The Idealized internet vs. internet Realities: Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global internet (Version 1.0).

- ***Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017).*** National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. NIST Special Publication 800-181.

- ***Reich, P., Anand, P., Mittal, V., Kiran, A., Osula, A.M. & Weinstein, S. (2014).*** Internet governance: International law and global order in cyberspace. En Manfred Steger, Paul Battersby, and Joseph Siracusa. (eds.). The SAGE Handbook of Globalization (pp. 592-620), Sage.

- ***Seger, A. (2012).*** Cybercrime strategies. Global Project on Cybercrime.

- ***Whitmore, A., Choi, N. & Arzrumtsyan, A. (2009).*** One Size Fits All? On the Feasibility of International internet Governance. Journal of Information Technology & Politics, 6:1, 4-11..

Lecturas avanzadas

Se recomiendan las siguientes lecturas a los interesados en investigar los temas de este módulo en más detalle:

- ***Azmi, R., Tibben, W. & Win, K.T. (2018).*** Review of cybersecurity frameworks: context and shared concepts. Journal of Information Technology & Politics, 3:2, 258-283.

- ***Finnemore, M. & Hollis, D. (2016).*** Constructing Norms for Global Cybersecurity. American Journal of International Law, 110(3), pp. 425-479.

- ***Jardine, E. (2018).*** Mind the denominator: towards a more effective measurement system for cybersecurity. Journal of Information Technology & Politics, 3:1, 116-139.

- ***Lacy, M. & Prince, D. (2018).*** Securitization and the global politics of cybersecurity. Global Discourse: An Interdisciplinary Journal of Current Affairs and Applied Contemporary Thought, 8(1), 100-115.

- ***Malone, E.F. & Malone, M.J. (2013).*** The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response. Journal of Information Technology & Politics, 19:2, 158-177.

- ***Sexton, M. (2016).*** U.K. cybersecurity strategy and active cyber defence – issues and risks. Journal of Information Technology & Politics, 1:2, 222-224.

- ***Shackelford, S.J. & Craig, A.N. (2014).*** Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. Stanford Journal of International Law, 50(1), 119-184.

- ***Shackelford, S.J. & Kastelic, A. (2016).*** Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity. N.Y.U. Journal of Legislation and Public Policy, 119, 895-984.

- ***Thomas, T. (2014).*** Creating Cyber Strategists: Escaping the 'DIME' Mnemonic. Defence Studies, 14(4), 370-393.

- ***Van der Berg, B. & Keymolen, E. (2017).*** Regulating security on the Internet: control versus trust. International Review of Law, Computers & Technology, 31(2), 158-177.

Herramientas complementarias

Sitios web

- ***Australian Cyber Security Centre. (n.d.).*** Stay Smart Online campaign (Australia).
  - *https://www.staysmartonline.gov.au/about-us*

- ***eSafety Commissioner. (n.d.).*** Office of the eSafety Commissioner (Australia).
  - *https://www.esafety.gov.au/*

- ***European Comission. (n.d.).*** Safer Internet Day (SID).
  - *https://ec.europa.eu/digital-single-market/en/safer-internet-day-sid*

- ***European Cyber Security Month. (n.d.).*** What is ECSM?
  - *https://cybersecuritymonth.eu/about-ecsm/whats-ecsm*

- ***European Union Agency for Network and Information Security. (n.d.).*** National Cybersecurity Strategies (NCSSs) Map.
  - *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncssmap#b*

- ***Europol. (n.d.).*** Mobile Malware: Public Awareness and Prevention.
  - *https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/mobile-malware*

- ***France Diplomatie. (2018).*** France-Singapore Road Map for deepening cooperation in digital innovation, internet governance and cybersecurity.
  - *https://www.diplomatie.gouv.fr/en/country-files/singapore/events-2630/article/france-singapore-road-map-for-deepening-cooperation-in-digital-innovation*

- ***Get Safe Online. (n.d.).*** Get Safe Online (United Kingdom).
  - *https://www.unodc.org/e4j/data/_secondary_lower_s_secondary_upper_s_university_uni_/get_safe_online.html?lng=en&match=get safe online*

- ***Global Cyber Security Capacity Centre. (n.d.).*** Cybersecurity Capacity Maturity Model.
  - *https://www.unodc.org/e4j/data/_university_uni_/cybersecurity_capacity_maturity_model_for_nations.html?lng=en*

- ***Global Cyber Security Capacity Centre. (n.d.).*** Global Cyber Security Capacity Centre.
  - *https://www.unodc.org/e4j/data/_university_uni_/global_cyber_security_capacity_centre.html?lng=en*

- ***Government of Canada. (n.d.).*** Get Cyber Safe (Canada).
  - *https://www.unodc.org/e4j/data/_university_uni_/get_cyber_safe.html?lng=en*

- ***International Telecommunication Union (ITU). (n.d.).*** Cyberthreat Insight.
  - *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberthreat.aspx*

- ***International Telecommunication Union (ITU). (n.d.).*** National Cybersecurity Strategies Repository.
  - *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx*

- ***International Telecommunication Union (ITU). (n.d.).*** Global Cybersecurity Index.
  - *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*

- ***National Cyber Security Alliance. (n.d.).*** StaySafeOnline.
  - *https://staysafeonline.org/*

- ***National Cyber Security Alliance. (n.d.).*** National Cybersecurity Awareness Month.
  - *https://staysafeonline.org/ncsam/about-ncsam/*

- ***National Cyber Security Alliance. (n.d.).*** STOP. THINK. CONNECT.
  - *https://staysafeonline.org/stop-think-connect/*

- ***North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence. (n.d.).*** Cyber Security Strategy documents.
  - *https://ccdcoe.org/cyber-security-strategy-documents.html*

- ***Safernet. (n.d.).*** Safernet (Brazil).
  - *https://new.safernet.org.br*

- ***UK Centre for the Protection of National Infrastructure. (n.d.).*** Security Awareness Campaigns.
  - *https://www.cpni.gov.uk/security-awareness-campaigns*

- ***United Nations Institute for Disarmament Research (UNIDIR). (n.d.).*** Cyber Policy Portal.
  - *https://cyberpolicyportal.org/en/*

- ***US National Initiative for Cybersecurity Education. (n.d.).*** National Initiative for Cybersecurity Education (NICE).
  - *https://www.nist.gov/itl/applied-cybersecurity/nice*

- ***US National Institute of Standards and Technology. (n.d.).*** National Institute of Standards and Technology.
  - *https://www.nist.gov/*

Videos

- ***ISIF Asia Information Society Innovation Fund. (2017, July 25).*** What is CERT? (duración: 3:20) [Video] YouTube.
  - *https://www.youtube.com/watch?v=eBJDKBFSLqs*

  Este video presenta una breve visión general de los CERT.

- ***ITU. (2018, October 10).*** #ICT4SDG: How can tech save the world? (duración: 2:04) [Video] YouTube.
  - *https://www.youtube.com/watch?v=JsmPWgWVGdg*

  Este video cubre la importancia de la tecnología de la información y la comunicación y su impacto.

- ***ITU. (n.d.).*** ITU and Cybersecurity: Building confidence in the use of ICT (duración: 1:29) [Video] YouTube.
  - *https://www.youtube.com/watch?v=RyPf2XizQOg*

  En este video se examinan las amenazas a la seguridad cibernética y la importancia de la seguridad de las TIC.

- ***ITU. (2016, May 25).*** ITU Standardization - The technical foundations of the Information Society (duración: 3:31) [Video] YouTube.
  - *https://www.youtube.com/watch?v=hgP4IyY33iI*

  Este video animado ofrece una breve historia de la tecnología de la información y la comunicación, y del papel de la UIT en la creación de normas internacionales, así como de la importancia y las repercusiones de la estandarización de la UIT.

- ***UN Geneva. (2010, October 14).*** ITU - Cyber Security (duración: 3:24) [Video] YouTube.
  - *https://www.youtube.com/watch?v=8JCdW8HA2Ms*

  Este video discute la apertura de internet y los impactos de esta apertura.

Seguridad cibernética y prevención del delito cibernético:

aplicaciones y medidas prácticas

Módulo

9

Módulo 9: Seguridad cibernética y prevención del delito cibernético: *aplicaciones y medidas prácticas*

Introducción

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, propiedades e información. Sobre la base del Módulo 8: Seguridad cibernética y prevención de delitos cibernéticos: estrategias, políticas y programas, este módulo 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.

Objetivos

- Definir, discutir y evaluar los activos, amenazas, vulnerabilidades y riesgos.
- Identificar y evaluar las maneras en las que se exponen las vulnerabilidades.
- Describir y criticar las relaciones entre seguridad cibernética y usabilidad.
- Discutir sobre la prevención situacional de delitos y aplicarla a la prevención y reducción de delitos cibernéticos.
- Discutir y analizar la detección de incidentes, así como las respuestas, recuperación y preparación para enfrentarlos.

Cuestiones clave

Las medidas de seguridad cibernética se diseñan para salvaguardar, por lo general, a las personas y las propiedades, pero también a los sistemas, servicios e información, en particular. La protección de sistemas, redes, servicios y datos requiere un enfoque multifacético con sólidas estrategias, políticas y programas generales de seguridad cibernética (discutido en el Módulo 8: Seguridad cibernética y prevención de delitos cibernéticos: estrategias, políticas y programas) y medidas útiles de seguridad cibernética para identificar amenazas y vulnerabilidades, y para prevenir, detectar, responder y recuperarse de amenazas materializadas. Estas últimas medidas serán exploradas en este módulo, junto con conceptos vinculados al riesgo, investigaciones sobre seguridad cibernética y divulgación de vulnerabilidades, y estrategias y técnicas de prevención situacional de delitos. Los conceptos y enfoques básicos sobre la prevención de delitos se abordan con mayor detalle en la serie de módulos sobre la prevención del delito y justicia penal, particularmente en el Módulo 1: Normas y estándares de las naciones unidas para la prevención del delito y la justicia penal y en el Módulo 2: Prevención de delitos cibernéticos.

Activos, vulnerabilidades y riesgos

Las medidas de seguridad cibernética se implementan para proteger los activos, que se definen como «elementos de importancia o valor, que pueden ser personas, propiedades, información, sistemas o equipos» (Maras, 2014b, p. 21), como empleados de una organización, dispositivos digitales, programas de computadora y datos (ITU, 2008). Los activos son susceptibles (es decir, vulnerables) a varias formas de daño. Los activos tienen vulnerabilidades internas (intrínsecas) o externas (extrínsecas). Por ejemplo, en materia de las tecnologías de la información y comunicación (TIC), pueden encontrarse vulnerabilidades intrínsecas dentro del diseño del sistema, de las configuraciones, del *hardware* y del *software*, entre otras áreas (ENISA, 2017). Un caso particular es el de un error de programa. En 2018, se reveló un error de programa en el monedero de la criptomoneda Monero, lo que les permitió a algunas personas aprovecharse de esta vulnerabilidad para duplicar ilegalmente las cantidades en sus transferencias con criptomoneda (Barth, 2018) (para más información sobre criptomonedas, consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos). En contraste, las vulnerabilidades extrínsecas no se encuentran dentro de los activos, como las TIC. Un ejemplo de ello es el propio usuario de las TIC. El usuario puede involucrarse en acciones que exponen su dispositivo a infecciones de programas maliciosos (p. ej., al abrir archivos adjuntos en correos electrónicos que provienen de remitentes desconocidos). Las propiedades intrínsecas y extrínsecas hacen que los activos sean vulnerables a amenazas (es decir, a cualquier elemento que podría causar un efecto adverso). Estas amenazas pueden causar daño intencional o involuntario. Por ejemplo, el *hardware* de un dispositivo digital podría funcionar mal o ser dañado intencionalmente por una persona que se aprovecha de algunas vulnerabilidades del *firmware* (soporte lógico inalterable) del programa (ENISA, 2017).

Riesgo

Las decisiones para salvaguardar los activos se hacen en condiciones de incertidumbre; es decir, se hacen en ausencia de un conocimiento absoluto sobre las potenciales amenazas, vulnerabilidades y aprovechamiento de esas vulnerabilidades (Knight, 1921). Originalmente, la definición del riesgo se limitaba a la probabilidad (o posibilidad) de una amenaza y su impacto (o consecuencias) en caso de materializarse la amenaza (Dali y Lajtha, 2012). Este concepto de riesgo se representa en la siguiente fórmula:

Se utilizan fórmulas, como la presentada arriba, para cuantificar los riesgos (para obtener información sobre la manera de cuantificar la seguridad cibernética y las limitaciones de estos esfuerzos, consulte Freund y Jones, 2015; Hubbard y Seiersen, 2016).

En 2009, la Organización Internacional de Normalización (ISO, por sus siglas en inglés), una organización internacional no gubernamental que desarrolla y publica normas internacionales para armonizar las prácticas entre países, propuso una definición diferente, con la intención de que sirva como referencia para promocionar el entendimiento mutuo y la consistencia en el uso de términos clave relativos al riesgo (Luko, 2013; Dali & Lajtha, 2012). De manera puntual, la Guía ISO 73 (2009) define riesgo como el «efecto de la incertidumbre sobre el logro de los objetivos» (consulte 3.1 de la Guía ISO 73 (2009)) que se presenta, por ejemplo, en las metas financieras a corto y largo plazo. En esta definición de riesgo, la incertidumbre se refiere al «estado, incluso parcial, de deficiencia de información, entendimiento o conocimiento de un evento (...)» [(es decir, una «ocurrencia o cambio de un conjunto de circunstancias en particular», Sección 3.5.1.3 de la Guía ISO 73)], (...) de su consecuencia (...) [(«resultado de un evento que afecta los objetivos», Sección 3.6.1.3 de la Guía ISO 73)], (...) o de su probabilidad [(la «posibilidad de que ocurra algo, ya sea definida, medida o determinada de manera objetiva o subjetiva, y descrita matemáticamente o en términos generales (como por ejemplo, una probabilidad matemática o la frecuencia durante un periodo de tiempo determinado)», notas de la Sección 3.6.1.1 de la Guía ISO 73)]» (consulte las notas 3.1 de la Guía ISO 73; para obtener un análisis más detallado de la terminología relativa al riesgo, consulte Hoyle, 2018).

Figura 3

Gestión de los riesgos para la seguridad - Metodología

Tomado de Gestión de los riesgos para la seguridad - Metodología, por Grupo de Análisis de Amenazas, s.f., Grupo de Análisis de Amenazas.
https://www.threatanalysis.com/security-risk-management/

Las evaluaciones de riesgo (descritas en la figura 1) identifican las vulnerabilidades de los activos, identifican o se basan en la información acerca de las amenazas internas y externas que dan los medios de comunicación u organizaciones asociadas del sector público o privado e identifican los impactos y probabilidad de las amenazas (NIST, 2018). El propósito de una evaluación de riesgos es «identificar (...) amenazas; (...) daños (impactos adversos) que puedan ocurrir a causa de las potenciales amenazas de aprovechamiento de vulnerabilidades y (...) la probabilidad de que ocurran daños» (NIST, 2012; para obtener información sobre las limitaciones y dificultades de las evaluaciones de riesgo en materia de seguridad cibernética y sobre lo que puede hacerse para superar esas limitaciones y dificultades, consulte Hubbard y Seiersen, 2016).

Después de evaluar los riesgos, se identifican las respuestas (tratamiento de riesgos) y se priorizan sobre la base de los recursos (p. ej., financieros) y necesidades. Luego, se implementan medidas para eliminar, reducir o mitigar el riesgo (Maras, 2014b).

Divulgación de las vulnerabilidades

Las frases seguridad de la información y seguridad cibernética se han utilizado de manera intercambiable, aunque de manera incorrecta (Von Solms y Van Niekerk, 2013). Si bien no existe una definición consensuada de seguridad de la información, la definición incluida en la ISO/IEC 27002 ha sido una de las más utilizadas. La ISO/IEC 27002 define la seguridad de la información como la «preservación de [la] confidencialidad, integridad y disponibilidad de la información». Así como todavía no existe una definición universal para seguridad de la información, tampoco la hay aún para seguridad cibernética. De acuerdo con la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), la «seguridad cibernética busca garantizar la obtención y el mantenimiento de las propiedades de seguridad de la organización y de los activos de los usuarios frente a los riesgos de seguridad relevantes en el entorno cibernético» (ITU-T X.1205). La seguridad cibernética no solo protege el ciberespacio, «sino que (...) protege a [aquellos] que operan en el ciberespacio y cualquiera de sus activos que pudieran ser alcanzados a través del ciberespacio» (Von Solms y Van Niekerk, 2013, p. 101).

¿Sabían que...?

La ISO/IEC 27002 contiene 14 dominios de control de seguridad de la información, así como orientación y requerimientos para la implementación de cada uno de esos controles. Dichos dominios son los siguientes: políticas de seguridad para la información; seguridad para la organización de la información; seguridad de recursos humanos; gestión de activos; control de acceso; criptografía; seguridad física y ambiental; seguridad para las operaciones; seguridad para las comunicaciones; adquisición, desarrollo y mantenimiento de sistemas; relaciones con proveedores; gestión de incidentes relativos a la seguridad de la información; aspectos vinculados con la gestión de continuidad empresarial y la seguridad de la información, y cumplimiento.

¿Desean saber más?

Para más información sobre estos controles, consulte: https://www.iso.org/obp/ui/#iso:std:iso-ie-c:27002:ed-1:en

La seguridad de la información y la seguridad cibernética están determinadas por la divulgación de las vulnerabilidades. Cuando los investigadores y profesionales en el campo descubren vulnerabilidades, tienen dos opciones: divulgarlas completamente (divulgación masiva) o con responsabilidad (divulgación responsable) (Trull, 2015). La divulgación masiva involucra publicar las vulnerabilidades del software o hardware en línea (p. ej., en un sitio web) antes de tener una solución disponible (Trull, 2015). En contraste, la divulgación responsable se refiere a la práctica de no revelar la vulnerabilidad hasta que la organización a cargo del *hardware* o *software* haya encontrado una solución para la vulnerabilidad (Trull, 2015). Para proceder con la divulgación responsable, el investigador o profesional se contacta con la organización afectada y espera hasta que la organización publique una solución para la vulnerabilidad identificada. Una vez que se publica una solución, el investigador o profesional puede divulgar oficialmente la información sobre la vulnerabilidad y recibir crédito por haberla identificado. Al utilizar este método de divulgación, el investigador o profesional puede pedir lo que se conoce como un identificador de Vulnerabilidades y Exposiciones Comunes (CVE). El CVE, «una lista de identificadores comunes para vulnerabilidades de seguridad cibernética ya publicadas y conocidas por el público» (CVE, s.f.), se usa para rastrear las vulnerabilidades en programas importantes, así como a aquellos que encuentran esas vulnerabilidades. Además de las opciones de divulgación masiva y responsable, el investigador o profesional también puede optar por no revelar la vulnerabilidad (Cencini et al., 2005). Otro método de revelación es la divulgación coordinada de vulnerabilidades (CVD), que se refiere al «proceso de recabar información de los rastreadores de vulnerabilidades, coordinando la publicación de esa información entre las partes involucradas y revelando la existencia de las vulnerabilidades de software y sus soluciones a diversos actores, incluyendo al público» (Householder et al., 2017).

Los delincuentes cibernéticos atentan contra los clientes de cirugía plástica

Se encuentran disponibles directrices de mejores prácticas para la divulgación y el manejo de vulnerabilidades. Algunos casos puntuales son las directrices de mejores prácticas que desarrollaron y publicaron la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) (para obtener más información sobre estas organizaciones, consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital) sobre divulgación de vulnerabilidades (ISO/IEC 29147) y procesos de manejo de vulnerabilidades (ISO/IEC 30111).

Medidas de seguridad cibernética y usabilidad

Idealmente, las respuestas a los riesgos deberían diseñarse para proteger la confidencialidad, integridad y disponibilidad de los sistemas, redes, servicios y datos, así como garantizar la usabilidad de estas medidas (NIST, 2018). La usabilidad de dispositivos digitales (es decir, la facilidad de uso), a menudo, tiene prioridad sobre la seguridad de estos dispositivos y sus contenidos (Whitten y Tygar, 1999). Sin embargo, la seguridad y la usabilidad no necesariamente son mutuamente excluyentes (Sherwood et al., 2005). Las medidas de seguridad cibernética pueden ser ambas cosas: seguras y usables.

Las medidas de seguridad cibernética incluyen aquellas que buscan establecer la identidad del usuario para prevenir el acceso no autorizado a los sistemas, servicios y datos. Estas medidas de autenticación incluyen «lo que uno sabe» (p. ej., contraseñas y códigos PIN), «lo que uno tiene» (p. ej., tarjetas inteligentes y *tokens*) y «lo que uno es» (p. ej., información biométrica, como las huellas digitales) (Lehtinen et al., 2006; Griffin, 2015). La autenticación de múltiples factores (AMF) requiere dos o más de estos métodos de autenticación para establecer la identidad del usuario (Andress, 2014).

Otro tipo de medida de seguridad cibernética es el control del acceso. Los controles de acceso, que establecen privilegios, determinan el acceso autorizado y previenen el acceso no autorizado, incluyen medidas de autenticación, y otras medidas diseñadas para proteger las contraseñas y los inicios de sesión a los sistemas, aplicaciones, sitios web, redes sociales (y otras plataformas) y dispositivos digitales (Lehtinen et al., 2006). Una medida puntual sería, por ejemplo, limitar el número de intentos permitidos para ingresar una contraseña en un teléfono inteligente. Existe una opción en los teléfonos inteligentes que permite a los usuarios borrar todos los datos en el dispositivo después de un cierto número de intentos fallidos para ingresar la contraseña. Esta característica se creó para permitir que los usuarios protejan los datos en sus dispositivos, en caso el dispositivo digital haya sido robado o que alguien intente acceder sin autorización.

Otros ejemplos de controles de acceso incluyen aumentar progresivamente el plazo de espera cada vez que la contraseña sea mal ingresada o limitar el número diario de intentos de digitación con contraseñas erradas, lo que también podría impedir el acceso del usuario a la cuenta durante un periodo de tiempo determinado (Lehtinen et al., 2006). Los controles que regulan los inicios de sesión están diseñados a manera de protección contra los intentos de acceso no autorizado a las cuentas del usuario. Los retrasos de tiempo se diseñan como protección contra los ataques de fuerza bruta.

¿Sabían que...?

La prueba de Turing completamente automática y pública para diferenciar computadoras de humanos (CAPTCHA, por sus siglas en inglés) se ha empleado para prevenir ataques de fuerza bruta. Sin embargo, los estudios demuestran que las imágenes de CAPTCHA también pueden evadirse (p. ej., Bursztein et al., 2014; Sivakorn et al., 2016; Gao et al., 2014).

Un ataque de fuerza bruta es el uso de un *script* (es decir, programa informático) o *bot* (discutido en Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos) para adivinar (por ensayo y error) las credenciales de los usuarios (como sus nombres de usuario o contraseña) (para obtener más información sobre los ataques de fuerza bruta, consulte Knusden y Robshaw, 2011, 95-108). Los ataques de fuerza bruta utilizan, entre otras cosas, contraseñas comunes o detalles filtrados de inicio de sesión. En 2018, se reveló que la opción de contraseña maestra, que permitía a los usuarios encriptar las contraseñas que estuvieran guardadas en el buscador de Mozilla Firefox (un buscador web), podía ser fácilmente expuesta utilizando un ataque de fuerza bruta (Trend Micro, 2018).

¿Sabían que...?

Los *hackers* o *script-kiddies* hábiles (individuos sin mayores habilidades técnicas) pueden ejecutar ataques de fuerza bruta.

¿Desean saber más?

INFOSEC Institute. (2018). Popular Tools for Brute-force Attacks.
https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref

Los usuarios o los sistemas pueden generar contraseñas (Adams et al., 1997). Las contraseñas generadas por sistemas (es decir, una contraseña creada por un programa) son difíciles de adivinar y podrían resistir a los crackers (descifradores) de contraseñas (aunque esto dependerá de la longitud de las contraseñas). El problema con las contraseñas generadas por sistemas es que son difíciles de recordar. Esto lleva a los individuos a guardar su contraseña, por ejemplo, escribiéndola o guardándola en su buscador, aplicación o dispositivo digital. Por este motivo, se prefiere el uso de contraseñas generadas por el usuario. No obstante, las contraseñas generadas por el usuario también podrían ser difíciles de recordar. Los sistemas, aplicaciones y plataformas en línea, a menudo, tienen reglas de creación de contraseñas que son difíciles de cumplir por los usuarios porque requieren, por ejemplo, que las contraseñas tengan un mínimo de longitud e incluyan combinaciones de mayúsculas con minúsculas, números y símbolos. Por ese motivo, al igual que las contraseñas generadas por sistemas, las contraseñas generadas por el usuario también suelen ser difíciles de recordar.

También se anima a las personas a tener una contraseña distinta para cada cuenta (Información del Consumidor de la Comisión Federal de Comercio de los Estados Unidos, 2017). Esta recomendación tiene como objetivo minimizar el daño causado a los individuos en caso las credenciales de una de sus cuentas sean expuestas. En 2017, una compañía de investigación encontró un archivo en línea con 1400 millones de usuarios y contraseñas de individuos, provenientes de una variedad de redes sociales, sitios de transmisión de juegos, televisión y películas y otros sitios en línea (Matthews, 2017). Si algunas de estas personas reciclan sus contraseñas, esta filtración pone en peligro sus otras cuentas (aquellas con los mismos usuarios o contraseñas) también. Si bien el uso de contraseñas complejas y distintas para cada cuenta brinda cierto grado de seguridad a las personas, también impacta la usabilidad de las contraseñas (es decir, la facilidad para recordarlas). Como bien sostienen Adams et al. (1997), «más restricciones en los mecanismos de autenticación generan más problemas en la usabilidad» (p. 3).

Se han propuesto opciones de autenticación distintas a las contraseñas. El uso de mecanismos de autenticación alternativos, como la información biométrica, también trae consigo consecuencias adversas de tipo social, legal y hasta de seguridad (Greenberg, 2017a; Greenberg, 2017b). Un caso conocido es el de los iPhones de Apple que vienen con un TouchID, que permite a los usuarios desbloquear sus dispositivos con su huella dactilar, y un FaceID, que con su tecnología de reconocimiento facial permite a los usuarios desbloquear sus dispositivos mostrando el rostro. En Estados Unidos, los agentes de justicia penal no pueden obligar a una persona a compartir sus contraseñas; la misma protección no se ha extendido todavía para las huellas dactilares y demás información biométrica (consulte, por ejemplo, Virginia v. Baust, 2014 y State v. Diamond, 2018, donde los tribunales sostuvieron que las personas pueden ser obligadas a usar sus huellas dactilares para desbloquear un teléfono) (para obtener más información sobre esta práctica en Estados Unidos y las prácticas en otros países como India, Australia y Nueva Zelanda, consulte el siguiente recuadro sobre La biométrica y el privilegio contra la autoincriminación).

La biométrica y el privilegio contra la autoincriminación

De acuerdo con la Quinta Enmienda a la Constitución de los Estados Unidos: «Ninguna persona estará obligada a responder por un delito castigado con la pena capital, o con cualquier otra pena, salvo en la presencia o acusación de un gran jurado, a excepción de los casos que se presenten en los territorios de las fuerzas armadas navales o terrestres o en la milicia, cuando se encuentre en servicio activo, en tiempo de guerra o peligro público; ni ninguna persona estará sujeta, por la misma ofensa, a ser puesta dos veces en peligro de perder la vida o la integridad física; ni se le forzará a declarar contra sí misma en ningún juicio penal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará su propiedad privada para uso público sin una justa indemnización».

Uno de los derechos provistos bajo la Quinta Enmienda fue el privilegio contra la autoincriminación (también conocida como el derecho contra la autoincriminación forzada). En Schmerber v. California (1966), la corte sostuvo que «el privilegio protege a un acusado solo de ser obligado a testificar contra sí mismo, o de brindar al Estado evidencia de naturaleza testimonial o comunicativa» (761). En contraste, la Quinta Enmienda a la Constitución de los EE. UU. «no ofrece protección contra la imposición de entregar huellas dactilares, fotografías o medidas, (...) comparecer ante el tribunal, pararse, adoptar una postura, caminar, o hacer algún gesto particular» (United States v. Wade, 1967, 223). De hecho, los tribunales en los Estados Unidos pueden obligar a los acusados a entregar una muestra de sangre o saliva, una muestra de voz en audio, entre otras (Schmerber v. California, 1966; U.S. v. Dionisio, 1973; People v. Smith, 1982).

Tomando United States v. Wade (1967) como precedente, el juez a cargo del caso Virginia v. Baust (2014) concluyó que como la huella dactilar no requiere una comunicación de conocimiento del acusado, tampoco está bajo protección de la Quinta Enmienda; lo mismo aplica para las llaves y el ADN del acusado (3). Por eso, mientras que las contraseñas están protegidas en la Quinta Enmienda, esa misma protección no se extiende para las huellas dactilares (y, por extensión, a las demás muestras de información biométrica). La falta de protección de la información biométrica bajo la Quinta Enmienda se reafirmó en State v. Diamond (2018).

Por último, en Estados Unidos, «lo que uno es» puede ser impuesto (es decir, que puede obligarse a los individuos a brindar sus huellas dactilares y, por extensión, a desbloquear teléfonos inteligentes con la tecnología de reconocimiento facial), mientras que «lo que uno sabe» generalmente no puede recabarse de manera forzada, de acuerdo con la Quinta Enmienda a la Constitución de EE. UU. (por el privilegio contra la autoincriminación). De manera similar, otros países (p. ej., Australia, Nueva Zelanda, India, por mencionar algunos) y los tribunales de derechos humanos (p. ej., el Tribunal Europeo de Derechos Humanos) no consideran la imposición de mostrar el rostro, huellas dactilares, u otra información biométrica (como las huellas de los pies) como una violación al privilegio contra la autoincriminación (consulte, p. ej., Sorby v. Commonwealth, 1983; Nueva Zelanda, King v. McLellan, 1974; India, State of U.P. v. Sunil, 2017 y Saunders v. United Kingdom, 1996).

Los seres humanos son el eslabón más débil en la cadena de la seguridad cibernética (Crossler et al., 2013; Grossklags y Johnson, 2009; Sasse et al., 2001; Schneier, 2000). De hecho, múltiples estudios han demostrado que los incidentes relacionados con la seguridad cibernética (como filtraciones o ataques en las redes, sistemas, servicios o datos) son el resultado del error y fracaso del ser humano en la implementación de medidas de seguridad (Safa y Maple, 2016; Pfleeger, Sasse y Furnham, 2014; Crossler et al., 2013). Si bien se presta mucha atención al papel que juegan los seres humanos en los incidentes relacionados con la seguridad cibernética, las medidas de seguridad cibernética que están implementadas al momento del problema pueden jugar un papel importante durante el incidente. La realidad es que las medidas de seguridad cibernética (lo que en verdad pueden hacer) y las expectativas que tienen los usuarios sobre el desempeño de esas medidas (lo que piensan que hacen), a menudo, no son iguales (Ur et al., 2016; Gunson et al., 2011; Furnell, 2005).

La literatura y las investigaciones sobre las interacciones entre los humanos y las computadoras proponen que la seguridad de los dispositivos, sistemas, programas, aplicaciones y plataformas digitales en línea, entre otros, deberían desarrollarse pensando en los usuarios (es decir, la seguridad en el diseño; consulte Eloff & Eloff, 2002; Cranor & Garfinkel, 2005; Sasse y Flechais, 2005; Karat et al., 2005; Dix et al., 2004; Balfanz et al., 2004). Esto, sin embargo, no es una práctica común. La práctica común es construir sistemas y después intentar modificar las interacciones del usuario con el sistema, para llegar a cumplir los requerimientos de seguridad (Nurse et al., 2011; Yee, 2004).

¿Sabían que...?

En la Unión Europea, la Ley de Seguridad Cibernética de 2018 creó un «marco para certificaciones europeas de seguridad cibernética para productos, procesos y servicios», con el fin de promocionar la seguridad en el diseño, a través de la «incorporación de las características de seguridad en las etapas tempranas del (...) diseño y desarrollo técnico» de los dispositivos digitales (Comisión Europea, 2018).

¿Desean saber más?

Comisión Europea. (2018). Ley de Seguridad Cibernética.

https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Prevención situacional de delitos

La prevención situacional de delitos (SCP, por sus siglas en inglés) se enfoca en las maneras en las que se podrían prevenir y reducir los delitos (Clarke, 1980; la SCP se examina con mayor detalle en el Módulo 2: Prevención del delito de la serie de módulos universitarios sobre la prevención del delito y justicia penal). La SCP se considera una parte esencial de las Directrices para la prevención del delito (resolución 2002/13) del Consejo Económico y Social de las Naciones Unidas (ECOSOC, por sus siglas en inglés) (consulte UNODC, 2010).

Si bien la SCP es un concepto aplicado a la prevención del delito en el mundo real, también puede utilizarse como una medida de prevención para los delitos cibernéticos en el contexto de la seguridad cibernética. Cuando se aplica a los delitos cibernéticos, las medidas de la SCP se enfocan en reducir, negar o limitar las oportunidades y habilidades de los delincuentes para cometer sus delitos. Las medidas técnicas para la prevención de delitos cibernéticos son una forma de prevención situacional de delitos. Un ejemplo de estas medidas técnicas son los programas cortafuego para la detección de programas maliciosos, que ayudan a prevenir accesos no autorizados, examinando y bloqueando el tráfico. Otro ejemplo son los sistemas de detección de intrusos, que permiten la detección de ataques cibernéticos, así como el acceso y el uso no autorizado de sistemas, redes, datos, servicios y recursos afines (Maras, 2014a, p. 311).

Cornish y Clarke (2003) propusieron estrategias y técnicas para prevenir y reducir los delitos (consulte la figura 2). Las cinco estrategias propuestas para prevenir o reducir los delitos involucran incrementar el esfuerzo requerido para delinquir, aumentar los riesgos de detección y captura, disminuir las ganancias que se obtienen al delinquir, reducir las provocaciones que devienen en delitos y eliminar las excusas para delinquir. No todas las estrategias y técnicas de esta lista pueden aplicarse a todos los delitos (Clarke, 2004). Además, las técnicas y estrategias pueden superponerse, y una técnica puede servir para más de una estrategia (Clarke, 2004). Para obtener más información sobre las técnicas y estrategias de prevención de delitos, consulte la serie de módulos sobre prevención del delito y justicia penal.

Figura 2

25 técnicas de prevención situacional

VEINTICINCO TÉCNICAS DE PREVENCIÓN SITUACIONAL

Aumentar el esfuerzo	Aumentar los riesgos	Reducir las recompensas	Reducir provocaciones	Eliminar excusas
1) Refuerzo de la seguridad. • Bloqueo de la columna de dirección e inmovilizadores. • Barreras antirrobo. • Empaquetado a prueba de manipulaciones.	**6) Ampliar la vigilancia.** • Tomar rutinas de precaución: salir de noche en grupo, llevar teléfono móvil, dejar señales de estar en casa. • Vigilancia del vecindario.	**11) Oculte objetivos.** • Aparcamientos en la calle. • Directorios telefónicos de género neutro. • Camiones blindados sin identificación	**16) Reducir frustraciones y estrés.** • Colas eficientes y un servicio atento/ cortés. • Aumentar cantidad de asientos. • Música tranquila y luces tenues.	**21) Establecer reglas.** • Contratos de arrendamiento. • Código contra el acoso. • Registro de hotel.
2) Control de acceso a instalaciones. • Intercomunicador. • Tarjeta de acceso electrónica. • Control visual de equipaje.	**7) Ayudar en la vigilancia natural.** • Mejorar el alumbrado de las calles. • Diseño de espacios defensivos. • Apoyar a los informantes / denunciantes.	**12) Retirar objetivos.** • Auto radio removible. • Refugio de mujeres. • Tarjetas prepagadas para teléfonos prepago.	**17) Evitar conflictos.** • Recintos separados para aficionados equipos de fútbol • rivales. • Reducir amontonamientos en bares. Mejorar tarifas de taxis.	**22) Letreros fijos con instrucciones.** • "No estacionar". • "Propiedad privada". • "Apagar la fogata".
3) Pantallas de salida. • Boleto necesario para salida. • Exportar documentos. • Etiquetas de mercancía electrónica.	**8) Reducir el anonimato.** • Identificaciones para taxistas. • Calcomanías de "¿Qué tal conduzco?" • Uniformes escolares.	**13) Identificar propiedad.** • Marca de propiedad. • Licencia de vehículos y marcado de piezas. • Marca de ganado.	**18) Reducir incitadores emocionales.** • Controlar la pornografía violenta. • Hacer cumplir el buen comportamiento en los estadios de fútbol. • Prohibir las ofensas racistas.	**23) Recomendaciones.** • Letreros de control de velocidad en autopistas. • Firmas para declaración de aduanas. • "Llevarse cosas de la tienda sin pagar es robo".
4) Desviar a los infractores. • Cierre de calles. • Baños separados para mujeres. • Dispersar bares.	**9) Utilice agentes que prevengan el delito.** • Circuito cerrado de televisión en buses de dos pisos. • Dos empleados por tienda de conveniencia. • Vigilancia remunerada.	**14) Interrumpir los mercados.** • Monitorear casas de empeño. • Controlar avisos clasificados. • Licencia para venderos callejeros.	**19) Neutralizar la presión de grupo.** • "Los idiotas beben y conducen". • "Está bien decir que no". • Dispersar alborotadores en las escuelas.	**24) Ayudar al cumplimiento.** • Devoluciones fáciles en bibliotecas. • Lavatorios públicos. • Tachos de basura.
5) Control de herramientas/armas • Armas "inteligentes". • Inutilizar teléfonos móviles robados. • Restringir la venta de pintura en aerosol a jóvenes.	**10) Fortalezca la vigilancia formal.** • Cámaras de tránsito. • Alarmas contra robos. • Guardias de seguridad.	**15) Disminuir ventajas** • Etiquetas de mercancía con tapón de seguridad. • Limpiadores de grafitis. • Rompemuelles	**20) Desalentar imitaciones.** • Reparación inmediata de actos vandálicos. • V-chip en televisores. • Censurar detalles del modus operandi.	**25) Controlar las drogas y el alcohol.** • Alcoholímetros en bares. • Monitoreo de consumo de alcohol en establecimientos. • Eventos con cero alcohol.

Tomado de 25 técnicas de prevención situacional, por el Centro de Vigilancia Policial Orientada a los Problemas, s.f., Centro de Vigilancia Policial Orientada a los Problemas. **https://popcenter.asu.edu/sites/default/files/library/25%20techniques%20grid.pdf**

Las medidas de SCP son, han sido y serán utilizadas para prevenir y reducir los delitos cibernéticos (Maras, 2016). Por ejemplo, una de las técnicas de la lista de Cornish y Clarke (2003), propuesta para la estrategia SCP de aumentar el riesgo de detección y captura, es la de «utilizar gestores de sitios» (consulte la figura 2). En materia de delitos cibernéticos, los gestores de sitios, que controlan los comportamientos en un área designada, pueden ser los proveedores del servicio de internet (consulte Delitos Cibernéticos-Módulo 1: Introducción al delito cibernético) o administradores y moderadores de plataformas en línea (Maras, 2016, 52). Se han empleado gestores de sitios para lidiar con delitos cibernéticos en plataformas de redes sociales. Por ejemplo, Facebook aumentó la cantidad de moderadores e intensificó la vigilancia para contenido violento en su plataforma después de que Steven Stephens transmitiera su video asesinando a un hombre vía Facebook Live (Isaac y Mele, 2017; Guynn, 2017) Algunas de estas técnicas de SCP implementadas para lidiar con delitos cibernéticos podrían infringir los derechos humanos (p. ej., el bloqueo o eliminación de contenido) (para obtener más información sobre las restricciones a los derechos humanos y las circunstancias limitadas en las se justifican ciertas restricciones proporcionales a algunos derechos humanos de acuerdo con el derecho internacional de los derechos humanos, consulte Delitos Cibernéticos-Módulo 3: Marcos jurídicos y derechos humanos).

El desplazamiento de delitos ocurre cuando un delito que fue pensado para un objetivo inicial se comete contra un objetivo distinto, como consecuencia de las medidas de seguridad adoptadas. A pesar de lo que suele pensarse, las investigaciones demuestran que la prevención situacional de delitos no necesariamente provoca un desplazamiento de delitos (Clarke, 1997; Hesseling, 1994; para discutir la literatura y las conclusiones generales sobre el desplazamiento de delitos, consulte Prevención del Delito y Justicia Penal-Módulo 2: Prevención del delito). Un estudio acerca del uso que dan los proxenetas a los sitios web de anuncios clasificados Backpage y Craiglist reveló que los esfuerzos de los organismos encargados de hacer cumplir la ley no desplazaron el uso de los proxenetas de estos sitios para promocionar el trabajo sexual (Finn y Stalans, 2016).

La SCP se centra en la posibilidad de que en algún punto las amenazas contra la seguridad cibernética se materialicen. Entonces, estas medidas se implementan porque se da por hecho que las amenazas sí van a materializarse y que deben tomarse acciones para combatirlas. Si bien la SCP se enfoca (aunque no exclusivamente) en prevenir los delitos, la realidad es que, incluso adoptando esas medidas, es probable que se cometan los delitos. A partir de ello, se adoptan medidas para detectar, enfrentar y recuperarse de incidentes de seguridad cibernética.

Detección, respuestas, recuperación y preparación para incidentes

La detección de incidentes es el proceso de identificar amenazas por medio de un intenso monitoreo de los activos y una búsqueda de actividad anómala (NIST, 2018). Una vez que la amenaza ha sido detectada, se toman las acciones necesarias para neutralizarla (si es una amenaza activa al momento de la respuesta) y para investigar el incidente. Después de responder al incidente, el primer paso en el proceso de recuperación es el de restaurar el acceso y disponibilidad de los sistemas, redes, servicios y datos al estado previo al incidente (NIST, 2018).

La recuperación también involucra un elemento de planificación que requiere la identificación, creación e implementación de las medidas de resistencia que permitan restaurar los sistemas, redes, servicio y datos que estaban inaccesibles, modificados, dañados o afectados durante el incidente. Un elemento vital para asegurar esa resistencia es tener un plan de continuidad de las operaciones o un plan de gestión de emergencias actualizado (Maras, 2014b), que indica las instrucciones que deben seguirse y acciones que deben tomarse en caso de producirse un incidente de seguridad cibernética. En palabras simples, este plan incluye información detallada sobre las maneras de enfrentar un incidente y sobre cómo recuperarse de él. Todos los involucrados en las respuestas y recuperación en la esfera de la seguridad cibernética deben estar informados del plan de gestión de emergencias. Para ello, necesitan capacitarse con ejercicios destinados a probar la eficacia y eficiencia de esos planes. Un ejemplo de este tipo de ejercicios son los Ejercicios de Cyber Storm del Departamento de Seguridad Nacional de los Estados Unidos, que involucran participantes de agencias privadas y estatales, así como agencias de otros países (p. ej., Australia, Canadá, Dinamarca, Finlandia, Francia, Alemania, Hungría, Italia, Japón, Nueva Zelanda, Holanda, Suecia, Suiza y el Reino Unido), para probar las prácticas actuales de intercambio de información entre agencias, así como su preparación, protección y capacidad de respuesta en materia de seguridad cibernética (DHS, s.f.).

Referencias

- ***Adams, A., Sasse, M.A. & Lunt, P. (1997).*** Making passwords secure and usable. En: People and Computers XII - Proc. of the 7th International Conference on Human-Computer Interaction (HCI'97). Springer.
  • *https://pdfs.semanticscholar.org/5781/15f73bf80798d859106a035466fecc77b209.pdf*

- ***Balfanz, D., Durfee, G., Smetters, D.K. & Grinter, R.E. (2004).*** In search of usable security: Five lessons from the field. Security & Privacy, IEEE, 2(5), 19-24.

- ***Barth, B. (2018, August 3).*** Monero bug that doubled coin transfer amounts allowed attackers to steal from Altex.exchange. SC magazine.
  •*https://www.scmagazine.com/monero-bug-that-doubled-coin-transfer-amounts-allowed-attackers-to-steal-from-altexexchange/article/785998/*

- ***Broodkin, M. (2001).*** Computer Incident Response Team. SANS Institute.

- ***Bursztein, E., Aigrain, J., Moscicki, A. & Mitchell, J.C. (2014).*** The end is nigh: Generic solving of text-based CAPTCHAs. En: Proceedings of the 8th USENIX Workshop on Offensive Technologies.

- ***Cavusoglu Hu., Raghunathan, S. & Cavusoglu, Ha. (2009).***Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. Information Systems Research, 20(2), 198-217.

- ***Cencini, A., Yu, K. & Chan, T. (2005).*** Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure. University of Washington Computer Science & Engineering.
  •*https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf*

- ***Clarke, R.V.G. (2004).*** 25 Techniques of Situational Crime Prevention Presentation at Problem-Oriented Policing Conference (Charlotte, 28-30 October 2004).

- ***Clarke, R.V.G. (1980).*** Situational crime prevention: Theory and practice. British Journal of Criminology, 20(1), 136-147.

- ***Cornish, D.B. & Clarke, R.V.G. (2003).*** Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. En: Martha J. Smith y Derek B. Cornish (Guest Eds.). Theory for practice in situational crime. Willan.

- ***Cranor, L.F. & Garfinkel, S.L. (2005).*** Security and Usability: Designing Secure Systems That People Can Use. O'Reilly.

- ***CVE. (n.d.).*** About CVE.
  • *https://cve.mitre.org/about/index.html*

- ***Dali, A. y Lajtha, C. (2012).*** ISO 31000 Risk Management - "The Gold Standard." EDPACS, 45(5), 1-8.

- ***Dix, A., Finlay, J. Abowd, G.D. & Beale, R. (2004).*** Human-Computer Interaction (3rd ed.). Prentice Hall.

- ***Eloff, M.M. & Eloff, J.H.P. (2002).*** Human Computer Interaction: An Information Security Perspectives. In M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi and Heba K. Aslan. Security in the Information Society: Visions and perspectives. Springer.

- ***ENISA. (2017).*** Hardware Threat Landscape and Good Practice Guide (Version 1). ENISA.
  • *https://www.enisa.europa.eu/publications/hardware-threat-landscape/at_download/fullReport*

- ***Finn, M.A. & Stalans, L.J. (2016).*** How Targeted Enforcement Shapes Marketing Decisions of Pimps: Evidence of Displacement and Innovation. Victims and Offenders, 11(4), 578-599.

- ***Freund, J. & Jones, J. (2015).*** Measuring and managing information risk: A FAIR approach. Butterworth-Heinemann.

- ***Furnell, S. (2005).*** Why users cannot use security. Computers & Security, 24(4), 274-279.

- ***Gao, S., Mohamed, M., Saxena, N. & Zhang, C. (2014).*** Gaming the game: defeating a game CAPTCHA with efficient and robust hybrid attacks. 2014 IEEE International Conference on Multimedia and Expo, 1-6.

- ***Greenberg, A. (2017, December 11).*** Hackers Say they've broken FaceID a week after iPhone X release. Wired.
  • *https://www.wired.com/story/hackers-say-broke-face-id-security/*

- ***Greenberg, A. (2017, December 9).*** How secure is the iPhone X's FaceID? Here's what we know? Wired.
  • *https://www.wired.com/story/iphone-x-faceid-security/*

- ***Grossklags, J. and Johnson, B. (2009).*** Uncertainty in the weakest-link security game. International Conference on Game Theory for Networks (13-15 de mayo de 2009).
  • *http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags-Gamenets2009.pdf*

- ***Gunson, N., Marshall, D., Morton, H. & Jack, M. (2011).*** User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208-220.

- ***Guynn, J. (2017, May 3).*** Facebook Live violence horrifies users, who say Facebook's still not doing enough. USA Today.
  •*https://www.usatoday.com/story/tech/news/2017/05/03/facebook-live-violence-not-enough-mark-zuckerberg-users/101247030/*

- ***Householder, A.D., Wassermann, G., Manion, A. & King, C. (2017).*** The CERT Guide to Coordinated Vulnerability Disclosure. Software Engineering Institute. Carnegie Mellon University.
  • *https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf*

- ***Hoyle, D. (2018).*** ISO 9000 Quality Systems Handbook-updated for the ISO 9001: 2015 standard (7th edition). Routledge.

- ***Hubbard, D.W. & Seiersen, R. (2016).*** How to Measure Anything in Cybersecurity Risk. Wiley.

- ***Isaac, M. & Mele, C. (2017, April 17).*** A murder posted on Facebook prompts outrage and questions over responsibility. New York Times.
  • *https://www.nytimes. com/2017/04/17/technology/facebook-live-murder-broadcast.html*

- ***ITU. (2008).*** Overview of cybersecurity. Recommendation ITU-T X.1205. Series X: Data Networks, Open System Communications and Security.

- ***Karat, C.M., Karat, J. & Brodie, C. (2005).*** Usability Design and Evaluation for Privacy and Security Solutions. En: Lorrie Faith Cranor y Simon L. Garfinkel (eds), Designing Secure Systems That People Can Use. O'Reilly & Associates.

- ***Knight, F. (1921).*** Risk, Uncertainty, and Profit. University of Chicago Press.
- ***Lehtinen, R., Russell, D. & Gangemi Sr., G.T. (2006).*** Computer Security Basics. O'Reilly Media.
- ***Luko, S.N. (2013).*** Risk Management Terminology. Quality Engineering, 25(3), 292-297.
- ***Maras, M.H. (2014a).*** Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett.
- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press.
- ***Maras, M.H. (2014b).*** Transnational Security. CRC Press.
- ***Matthew, L. (2017, December 11).*** File with 1.4 Billion Hacked and Leaked Passwords Found on the Dark Web. Forbes.
  • *https://www.forbes.com/sites/leemathews/2017/12/11/billion-hacked-passwords-dark-web/#272c6cfc21f2*
- ***NIST. (2018).*** Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
- ***NIST. (2012).*** Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. National Institute of Standards and Technology.
  • *https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf*
- ***Nurse, J.R.C., Creese, S., Goldsmith, M. & Lamberts, K. (2011).*** Guidelines for Usable Cybersecurity: Past and Present. Third International Workshop on Cyberspace Safety and Security.
- ***Pfleeger, S.L., Sasse, M.A. & Furnham, A. (2014).*** From Weakest Link to Security Hero: Transforming Staff Security Behavior. Homeland Security & Emergency Management, 11(4), 489-510.
- ***Proffitt, T. (2007).*** Creating and Managing an Incident Response Team for a Large Company. 35. SANS.
  •*https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821*
- ***Sasse, M.A., & Flechais, I. (2005).*** The Case for Usable Security. En: Lorrie Faith Cranor y Simon L. Garfinkel (eds), Designing Secure Systems That People Can Use. O'Reilly & Associates.
- ***Sasse, M.A., Brostoff, S. & Weirich, D. (2001).*** Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.
- ***Schneier, B. (2000).*** Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons, Inc.
- ***Shaw, M. (2010).*** Handbook on the crime prevention guidelines: Making them work. UNODC.
- ***Sherwood, J., Clark, A. & Lynas, D. (2005).*** Enterprise security architecture: a business-driven approach. CMP Books.
- ***Sivakorn, S., Polakis, I. & Keromytis, A.D. (2016).*** I Am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs. En: Proceedings of the 1st IEEE European Symposium on Security and Privacy, Saarbrucken, Germany (21-24 de marzo de 2016), 388-403.
- ***Stalans, L.J. and Finn, M.A. (2016).*** Consulting legal experts in the real and virtual world: Pimps' and johns' cultural schemas about strategies to avoid arrest and conviction. Deviant Behavior, 37(6), 644-664.

- ***Trull, J. (2015, February 26).*** Responsible Disclosure: Cyber Security Ethics. CSO.
  - *https://www.csoonline.com/article/2889357/security0/responsible-disclosure-cyber-security-ethics.html*

- ***Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N. & Cranor, L.F. (2016).*** Do users' perceptions of password security match reality? En: Proceedings of the 2016 CHI conference on human factors in computing systems. ACM, 3748–3760.

- ***US Department of Homeland Security (DHS) (n.d.).*** Cyber Storm: Securing Cyber Space. US Department of Homeland Security (DHS).

- ***US Federal Trade Commission Consumer Information. (2017).*** Computer Security.
  - *https://www.consumer.ftc.gov/articles/0009-computer-security#passwords*

- ***Venter, H.S. & Eloff, J.H. (2003).*** A taxonomy for information security technologies. Computers & Security, 22(4), 299-307.

- ***Von Solms, Rossouw and Johan van Niekerk. (2013).*** From information security to cyber security. Computers and Security, 38, 97-102.

- ***Whitten, A. & Tygar, J.D. (1999).*** Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Paper presented at the Proceedings of the 8th USENIX Security Symposium, Washington D.C., America.

- ***Yee, K.P. (2004).*** Aligning security and usability. Security & Privacy, 2(5), 48-55.

Casos

- ***Fisher v. United States, 96 S.Ct. 1569 (1976)***

- ***King v. McLellan [1974] VR 773***

- ***People v. Smith, 86 AD2d 251 (NY App Div 3d Dept 1982)***

- ***Saunders v. United Kingdom (Application no. 19187/91) (1996) 23 EHRR 313***

- ***Schmerber v. California, 384 U.S. 757 (1966)***

- ***Sorby v Commonwealth (1983) 152 CLR 281***

- ***State v. Diamond, 2018 WL 443356 (Minn. 2018)***

- ***State of U.P. v. Sunil el 2 de mayo, 2017, judgment of Supreme Court (India)***

- ***United States v. Wade, 388 U.S. 218 (1967)***

- ***U.S. v. Dionisio, 410 U.S. 1 (1973)***

- ***Virginia v. Baust, No. CR14-1439 (Va. Cir. 28 de octubre, 2014)***

Lecturas principales

- ***Adams, A., Sasse, M.A. & Lunt, P. (1997).*** Making passwords secure and usable. En: People and Computers XII - Proc. of the 7th International Conference on Human-Computer Interaction (HCI'97), Springer.
  • *https://pdfs.semanticscholar.org/5781/15f73bf80798d859106a035466fecc77b209.pdf*

- ***Arora, A., Nandkumar, A. & Telang, R. (2006).*** Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. Information Systems Frontiers, 8(5), 350-362.

- ***Beebe, N.L. & Rao, V.S. (2005).*** Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security. Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, Dec 2005.
  • *https://pdfs.semanticscholar.org/34b5/d16969c46561ebdacf40cdf6c39194059d93.pdf*

- ***Collins, J.D., Sainato, V.A. & Khey, D.N. (2011).*** Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. International Journal of Cyber Criminology, 5(1), 794-810.

- ***Cornish, D.B. & Clarke, R.V.G. (2003).*** Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. En: Martha J. Smith y Derek B. Cornish (Guest Eds.). Theory for practice in situational crime. Willan.

- ***Dali, A. & Lajtha, C. (2012).*** ISO 31000 Risk Management - "The Gold Standard." EDPACS, 45(5), 1-8.

- ***Eloff, M.M. & Eloff, J. H. P. (2002).*** Human Computer Interaction: An Information Security Perspectives. In M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi and Heba K. Aslan. Security in the Information Society: Visions and perspectives. Springer.

- ***ENISA. (2017).*** Hardware Threat Landscape and Good Practice Guide (Version 1). ENISA.
  • *https://www.enisa.europa.eu/publications/hardware-threat-landscape/at_download/fullReport*

- ***Luko, S.N. (2013).*** Risk Management Terminology. Quality Engineering, 25(3), 292-297.

- ***NIST. (2018).*** The Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
  • *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*

- ***Shaw, M. (2010).*** Handbook on the crime prevention guidelines: Making them work. UNODC.
  • *https://www.unodc.org/pdf/criminal_justice/Handbook_on_Crime_Prevention_Guidelines_-_Making_them_work.pdf*

Lecturas avanzadas

- ***Antonucci, D. (2017).*** The Cyber Risk handbook: Creating and Measuring Effective Cybersecurity Capabilities. Wiley.

- ***Brown, M.W., Stikvoort, D., Kossakowski, K.P., Killcrece, G., Ruefle, R. & Zajicek, M. (2003).*** Handbook for Computer Security Incident Response Teams (CSIRTS). Software Engineering Institute. Carnegie Mellon University.
  - *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305*

- ***Garfinkel, S. & Cranor, L. (2008).*** Security and Usability: Designing Secure Systems That People Can Use. O'Reilly Media.

- ***Householder, A., Wassermann, G., Manion, A. & King, C. (2017).*** The CERT Guide to Coordinated Vulnerability Disclosure. Software Engineering Institute. Carnegie Mellon University.
  - *https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf*

- ***Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET). (2018).*** La cyber resilience: Thème d'approfondissement 2017 de la section sécurité et risques. 30 janvier 2018, n° 2017/02/CGE/SR. République Francaise.
  - *https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2017_02_CGE_SR_Rapport.pdf*

- ***Luttgens, J., Pepe, M. & Mandia, K. (2014).*** Incident Response & Computer Forensics (Third Edition). McGraw-Hill.

- ***Sanders, C. & Smith, J. (2013).*** Applied Network Security Monitoring: Collection, Detection and Analysis (1st edition). Syngress.

- ***Schaake, M., Pupillo, L., Ferreira, A. & Varisco, G. (2018).*** Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges. Report of a CEPS Task Force. Centre for European Policy Studies (CEPS) Brussels.
  - *https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf*

Herramientas complementarias

Sitios web

- ***NIST. (n.d.).*** Back to Basics: Multi-factor Authentication (MFA).
  - *https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication*

- ***The Conversation. (n.d.).*** Cybersecurity - News, Research and Analysis.
  - *https://theconversation.com/us/topics/cybersecurity-535*

- ***US NIST. (n.d.).*** Cybersecurity.
  - *Cybersecurity.*

Videos

- ***Artificial Intelligence - All in One. (2016, May 15).*** Lecture 1 — Human Computer Interaction | Stanford University (duración: 4:18) [Video]. YouTube.
  - *https://www.youtube.com/watch?v=WW1g3UT2zww&list=PLLssT5z_DsK_nusHL_Mjt87THSTlgrsyJ*

  Este video incluye una de una serie de charlas disponibles sobre varias facetas de la interacción entre el ser humano y la computadora.

- ***Coursera. (n.d.).*** Network Security Considerations (duración: 8:49) [Video] Coursera.
  - *https://www.coursera.org/lecture/it-security/network-hardening-best-practices-T3lID*

  Este video trata sobre las maneras de fortalecer las redes, la protección de la seguridad de las redes, y el monitoreo y análisis de redes.

- ***RSA Conference. (2018, August 23).*** Passwords and Fingerprints and Faces—Oh My! Comparing Old and New Authentication (duración: 46:14) [Video] YouTube.
  - *https://www.youtube.com/watch?v=DReQdq9E4bY*

  Este video cubre varias medidas de autenticación (desde antaño hasta el presente), en particular, las contraseñas y las medidas biométricas.

- ***USENIX Enigma Conference. (2016, January 29).*** USENIX Enigma 2016 Conference Why Is Usable Security Hard, and What Should We Do About it? (duración: 20:56) [Video] YouTube.
  - *https://www.youtube.com/watch?v=XfFjde0UPbY*

  Este video describe lo que significa la seguridad de fácil uso, sus desafíos y lo que puede hacerse con esos desafíos.

Privacidad y protección de datos

Módulo 10

Módulo 10: Privacidad y protección de datos

Introducción

Tanto delincuentes como delincuentes cibernéticos buscan datos personales para usarlos en la comisión de delitos y delitos cibernéticos. Estos datos personales se pueden obtener de varias fuentes (las cuales se tratan 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, *hobbies*, historia y preocupaciones médicas, desórdenes psicológicos, profesión, situación de empleo, servicio militar, afiliaciones, relaciones, geolocalización, hábitos, rutinas y otras actividades de una persona, entre otros datos (consulte Delitos Cibernéticos-Módulo 4: Introducción al análisis forense digital). Cuando se acumulan dichos datos personales, estos pueden proporcionar una idea casi completa de la vida personal y profesional de las personas.

El presente módulo examina críticamente el impacto de la acumulación de datos, así como el impacto que la recolección, almacenamiento, análisis, uso y divulgación de datos tiene sobre la privacidad y seguridad. En particular, este módulo aborda 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 los datos y las leyes de notificación de filtraciones. Además, se abordan las maneras en las que se protegen (o pueden ser protegidos) los datos, a fin de que las personas, propiedades e información estén seguras.

Nota

Las maneras en las que las investigaciones de delitos cibernéticos pueden impactar la privacidad, especialmente con respecto al monitoreo de sospechosos, la vigilancia encubierta y retención de datos, se tratan en diferentes módulos. Estos son: Módulo 3: Marcos jurídicos y derechos humanos; Delitos Cibernéticos-Módulo 5: Investigación de delitos cibernéticos; Delitos Cibernéticos-Módulo 6: Aspectos prácticos de las investigaciones de delitos cibernéticos y análisis forense digital, y Delitos Cibernéticos-Módulo 7: Cooperación internacional contra el delito cibernético.

Objetivos

- Debatir sobre la privacidad y su importancia como derecho humano.
- Identificar y evaluar el impacto de los delitos cibernéticos sobre la privacidad.
- Evaluar críticamente la relación entre la seguridad y privacidad.
- Evaluar críticamente las leyes sobre la protección de datos y las notificaciones sobre la filtración, así como las prácticas en diferentes países.
- Evaluar críticamente las prácticas de aplicación de la protección de datos y recomendar maneras efectivas para protegerlos.

Cuestiones clave

La proliferación de las tecnologías digitales conectadas a internet y su adopción alrededor del mundo han permitido la recolección, almacenamiento, análisis y divulgación de una gran cantidad de datos personales. Los hábitos de búsqueda en internet, el historial de navegación y los datos de ubicación (de la dirección IP y las aplicaciones y servicios basados en la localización, facturaciones y etiquetas de ubicación en sitios web, plataformas de redes sociales y aplicaciones) de las personas se registran, así como su información personal, debido a la necesidad de rellenar formularios en línea para varios propósitos (p. ej., trabajo, educación, la recepción de servicios gubernamentales como beneficios de jubilación, etc.), o de registrarse en aplicaciones, sitios web y otras plataformas en línea y a la disponibilidad de sitios web que consolidan la información de los usuarios. También pueden existir imágenes personales y grabaciones de video y audio en línea o en aplicaciones que hayan sido subidas por usuarios, amigos, familiares, conocidos, compañeros de clase, colegas, empleadores, organizaciones, agencias de Gobierno, los medios de comunicación y hasta extraños. A la acumulación de estos datos, entre otros, que crea «conjuntos de datos extremadamente grandes que se pueden analizar para revelar patrones, tendencias y asociaciones, especialmente relacionados con el comportamiento e interacciones humanas», se le conoce como *big data* (Maras y Wandt, 2018; Maras y Wandt, 2019).

La internet de las cosas (IdC) es un término que se usa para describir una red interconectada e interoperable de dispositivos con conexión a internet que facilitan el monitoreo de objetos, personas, animales y plantas, así como la vasta recolección, almacenamiento, análisis y difusión de datos sobre ellos (Maras, 2015). La IdC se suma a los datos de las personas que se recolectan, almacenan, analizan, comparten y ponen a disposición de alguna otra manera. Los dispositivos de la IdC van desde cosas que se llevan puestas (relojes, accesorios de ropa) y recogen información sobre la actividad física y datos sobre el sueño y la salud (p. ej., pulsímetro), pasando por electrodomésticos, muebles, productos y objetos personales (p. ej., refrigeradoras, hornos, lavadoras, televisores, aspiradoras, camas, balanzas, sistemas de alarmas y seguridad, luz, etc.) que rastrean y recogen información sobre su uso en los hogares, registrando preferencias, hábitos y rutinas, hasta ciudades inteligentes (ciudades intercomunicadas) que rastrean la ubicación, movimiento, rutinas, hábitos y otras actividades de las personas dentro de estas ciudades (Maras y Wandt 2018; Maras y Wandt, 2019). Como estos datos pueden revelar mucho sobre los usuarios, es necesario protegerlos. Esta protección es esencial, no solo para salvaguardar la privacidad de las personas, sino también para minimizar la vulnerabilidad ante los delitos cibernéticos.

En lo que sigue, el presente módulo cubrirá la privacidad como derecho humano, el impacto de los delitos cibernéticos en la privacidad, la relación entre la privacidad y la seguridad, la legislación sobre la protección de datos, las leyes sobre la notificación, la filtración de datos y el cumplimiento de la legislación sobre datos privados.

Privacidad: ¿Qué es y por qué es importante?

La privacidad es un derecho humano fundamental. El derecho a la privacidad «constituye una necesidad absoluta para (...) las persona[s]» (Eissen, 1967, como se citó en De Meyer, 1973) y está consagrado en tratados internacionales de derechos humanos, como el artículo 8 de la Convención Europea de Derechos Humanos de 1950, el artículo 11 de la Convención Americana sobre Derechos Humanos de 1969, el artículo 12 de la Declaración Universal de Derechos Humanos de 1948 y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966. Este derecho también se reconoce en el artículo 17 de la Convención sobre los Derechos del Niño de 1989, en el artículo 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares de 1990, en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea del 2000 y en el artículo 22 de la Convención Internacional sobre los Derechos de las Personas con Discapacidad de 2006. Los conceptos de privacidad varían e incluyen el derecho a no ser observado; el derecho a la intimidad; la capacidad de mantener en secreto pensamientos, creencias, identidad y comportamiento propios y el derecho a escoger y controlar cuándo, qué, por qué, dónde, cómo y a quién se le revela información sobre uno, y hasta qué extremo esa información es revelada (Cooley, 1907; Fried, 1970; Janis et al., 2000; Maras, 2009; para un análisis más detallado de estos y otros conceptos de privacidad, consulte Koops et al., 2017). El último concepto de privacidad (p. ej., el derecho a elegir y controlar la información sobre uno mismo) vincula la privacidad con la protección de información (o datos).

La privacidad facilita el cumplimiento de otros derechos humanos y está muy relacionada con ellos. La privacidad es una condición necesaria para la libertad de expresión, pensamiento, religión, reunión y asociación (consulte A/HRC/39/29; A/HRC/23/40 y A/HRC/29/32, párr. 15; A/HRC/31/66, párrs. 73-78 y A/72/135, párrs. 47-50). El derecho a la privacidad también está vinculado con el derecho a la libre determinación. El apartado 1 del artículo 20 de la Comisión Africana de Derechos Humanos y de los Pueblos de 1981 sostiene que «todos los pueblos deben tener el derecho a existir. Todos tienen el derecho incuestionable e inalienable a la libre determinación. Pueden determinar libremente su estado político y buscar su desarrollo económico y social de acuerdo con la política que ellos hayan elegido libremente.» Un aspecto esencial de la libre determinación es la habilidad de tomar decisiones y actuar de la forma que ellos escojan, libres de coerción (autonomía personal).

Esta elección se extiende más allá de las acciones físicas e incluye acciones en línea. Un aspecto inherente de la privacidad de una persona es la autonomía personal y el derecho a la libre determinación. Este derecho a la libre determinación permite que las personas lleven una vida auténtica al ser libres de tomar decisiones, y escoger y controlar la información sobre ellos a la que se puede acceder, divulgar y compartir.

Nota

Según un Informe de 2018 de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «[las regulaciones excesivas de privacidad también pueden resultar en limitaciones excesivas para otros derechos, en particular la libertad de expresión, por ejemplo, cuando una regulación desproporcionada interfiere con la divulgación legítima de noticias, expresión artística o investigaciones científicas» (A/HRC/39/29).

Otro aspecto inherente de la privacidad de una persona es la dignidad humana, un concepto controvertido (Rodríguez, 2015) que se refiere al «sentimiento de autoestima, (...) [de una persona] que tenemos el deber de desarrollar y respetar en (...) [uno mismo] y el deber de protegerlo en los otros» (Schroeder, 2017). La dignidad humana es considerada la base de los derechos humanos y está incluida en los preámbulos de numerosos instrumentos internacionales de derechos humanos, como la Declaración (DUDH) de 1948, el Pacto Internacional de Derechos Civiles y Políticos de 1966, el Pacto Internacional de Derechos Económicos, Sociales y Culturales (ICESCR) de 1966, la Carta Africana de Derechos Humanos y de los Pueblos de 1981, la Convención de las Naciones Unidas sobre los Derechos del Niño (UNCRC) de 1989, la Convención de 1963 y la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer de 1979. Aunque no esté explícitamente incluido en la Convención Europea sobre Derechos Humanos de 1950, se ha descrito en jurisprudencia como la «esencia» de los instrumentos de derechos humanos (Pretty versus United Kingdom, 2002). La dignidad humana también es considerada un principio esencial en muchas constituciones en el mundo (Shultztiner y Carmi, 2014).

Privacidad y seguridad

El control y la elección por sobre la divulgación de información están vinculados a la libertad de las personas a identificarse, a ellos mismos y sus acciones, a su propio criterio, elección y voluntad (Maras, 2012). Por tanto, el derecho a la privacidad está vinculado a la libertad de no tener que identificarse. El anonimato permite a los usuarios tomar parte de actividades sin revelar su identidad o sus acciones (Maras, 2016). En línea, el anonimato «proporciona a las personas y grupos una zona de privacidad en línea para expresar opiniones y ejercer la libertad de expresión sin interferencias o ataques arbitrarios e ilegales» (A/HRC/29/32, párr. 16). En vista de esto, la privacidad permite que los usuarios accedan a una tecnología de la información y comunicación con un espacio libre de intimidación, venganza y otras formas de coerción o sanción por la expresión de pensamientos, opiniones, vistas e ideas, sin ser obligados a identificarse. En ese sentido, «las soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones digitales, en particular las medidas de [anonimato] (...), pueden ser importantes para garantizar el disfrute de los derechos humanos, en particular los derechos a la privacidad, a la libertad de expresión y a la libertad de reunión pacífica y de asociación» (A/HRC/RES/38/7). A la luz de ello, «los Estados no deben interferir en el uso de tales soluciones técnicas, sin restricción alguna y, por lo tanto, cumplir las obligaciones de los Estados según la legislación internacional de derechos humanos» (A/RES/72/175, párr. 14; consulte también A/HRC/RES/39/6, párr. 14).

Se cree que este derecho al anonimato alienta a algunas personas a expresarse de formas dañinas y crueles, discriminatorias, racistas y llenas de odio hacia otros, lo cual no harían si sus identidades se supieran (este tipo de comportamientos se exploran con más detalle en Delito Cibernético-Módulo 12: Delito cibernético interpersonal). Aunque esto sea cierto para algunas personas, existen otras que se sienten animadas a revelar sus identidades cuando hacen estos comentarios. discurso de odio (Fleishman, 2018; Maras, 2016).

Mapa mundial de leyes y políticas de codificación

Global Partners Digital publicó un mapa interactivo en línea con leyes y políticas de codificación en el mundo que se encuentra disponible aquí:
https://www.gp-digital.org/world-map-of-encryption/

Esta identificación se da para ser reconocidos por individuos que piensan del mismo modo y para convocar seguidores a fin de actuar (Haines et al., 2014; Douglas y McGarty, 2001; Rost et al., 2016). Milos Yiannopoulos, un exescritor para una fuente de noticias sensacionalista de extrema derecha (*Breitbart*), es conocido por hacer comentarios racistas, misóginos, antiinmigrantes y antimusulmanes y hacer otros discursos de odio, a fin de ganar popularidad entre quienes piensan de manera similar dentro de los movimientos de extrema derecha y derecha alternativa o entre sus seguidores, y para movilizar a otros a participar en actos similares al hacer blanco de aquellos que fueron el objeto de su discurso de odio (Fleishman, 2018; Maras, 2016).

La identidad de la persona y su ubicación pueden ser difíciles de determinar por el anonimato y el uso de tecnologías que facilitan la privacidad, como Tor (discutida en Delito Cibernético-Módulo 5: Delito cibernético interpersonal). Otro ejemplo de una tecnología que facilita la privacidad es la codificación. La codificación bloquea el acceso a la información y las comunicaciones de los usuarios a terceros. Los Gobiernos en el mundo han argumentado a favor de la necesidad de acceder a comunicaciones e información codificada para combatir delitos serios como el terrorismo, la delincuencia organizada y la explotación sexual infantil (Markoff, 1996; MacFarquhar, 2018; Meyer, 2018; Hawkins, 2018; para más información sobre terrorismo, delincuencia organizada y explotación sexual infantil, consulte la serie de módulos sobre la lucha contra el terrorismo y crimen organizado, así como Delito Cibernético-Módulo 12: Delito cibernético interpersonal). Por estas razones, los servicios de mensajería encriptados son considerados ilegales en algunos países (MacFarquhar, 2018; Meyer, 2018).

Telegram, una aplicación de mensajería encriptada que tiene más de 200 millones de usuarios, ha sido bloqueada por orden judicial en algunos países porque la compañía rehusaba dar las claves de descifrado a estos Gobiernos para monitorear las comunicaciones de los usuarios vía la app (MacFarquhar, 2018; Meyer, 2018). Algunos países han ordenado que se creen puertas traseras y se proporcionen claves de descifrado, mientras otros han pedido que se creen puertas traseras y se proporcionen claves de descifrado para combatir delitos serios, como el terrorismo (Global Partners Digital, 2017; consulte, p.ej., debate sobre el cifrado Apple-FBI). Sin embargo, estas puertas traseras y la provisión de claves de descifrado podrían conducir al abuso del acceso a los datos (es decir, los Gobiernos podrían usar los datos de maneras no previstas, más allá de la autorización inicial en un caso específico), y a su uso por parte de los delincuentes para obtener acceso a esta información para visualizarla, copiarla, borrarla o alterarla.

¿Sabían que...?

Se puede acceder a la información y comunicaciones cifradas si el almacenamiento en la nube está habilitado en dispositivos digitales. La investigación en EE. UU. a Paul Manafort, el exdirector de campaña de Donald Trump, por cargos de fraude bancario y lavado de dinero, reveló que los fiscales podían acceder a sus mensajes cifrados vía Telegram y WhatsApp, los cuales se almacenaban en su cuenta de iCloud.

¿Desean saber más sobre este caso?

Bump, P. (2018, June 9). Don't be Paul Manafort: How to make your online communications more secure. The Washington Post.
https://www.washingtonpost.com/news/politics/wp/2018/06/09/dont-be-paul-manafort-how-to-protect-your-online-communications-more-securely/?noredirect=on&utm_term=.e8b919ed5fc4

Aunque la codificación dificulte responsabilizar a los delincuentes cibernéticos y puede ser aprovechada para cometer delitos cibernéticos, su prohibición y restricción es infundada y legalmente injustificada. La completa prohibición de la codificación limita la privacidad de una persona de manera arbitraria y, por lo tanto, contraviene el derecho internacional de derechos humanos (consulte A/HRC/29/32). La Corte Interamericana de Derechos Humanos ha descrito la privacidad como «ser exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública» (Ituango Massacres versus Colombia, 2006, párr. 192), y sostuvo que los Estados tienen:

> **La obligación de garantizar el derecho a la privacidad** mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar la vida privada, protegiéndola de las interferencias de las autoridades públicas así como también de las personas o instituciones privadas, incluyendo los medios de comunicación. (Fontevecchia y D'Amico versus Argentina, 2011)

Riesgos de seguridad no previstos

Strava permite que los usuarios de esta aplicación para monitorear la actividad física compartan las rutas por las que corren con otros usuarios de estos dispositivos (Berlinger y Vazquez, 2018). En 2018, Strava publicó un mapa de preferencias en línea con las rutas por las que corren los usuarios. Aunque la información publicada no se pudo rastrear hasta usuarios individuales, el mapa de preferencias reveló movimientos sobre y alrededor de bases militares de EE. UU. remotas en otros países (Hern, 2018; Berlinger y Vazquez, 2018). El uso de esta aplicación y de aplicaciones similares en teléfonos inteligentes, así como el uso de dispositivos de la IdC para medir la actividad física, puede ser particularmente problemático para quienes trabajan en las bases militares o en puestos y áreas en las que el monitoreo de sus movimientos los podría poner a ellos, su organización u otros en peligro.

Las medidas implementadas en respuesta a las amenazas de seguridad que tienen consecuencias adversas significativas para el ejercicio de los derechos humanos crean inseguridad. Es importante señalar que la seguridad y la privacidad son interdependientes: la seguridad proporciona a las personas la libertad de vivir sus vidas con dignidad y autonomía personal y de tomar decisiones libres de miedo y coerción, mientras que la privacidad permite a las personas «alcanzar la libre determinación y desarrollar su[s] personalidad[es] sin coerción» (Maras, 2009, p. 79). La privacidad es, por tanto, un medio para lograr la seguridad. De hecho, proteger la privacidad de las personas es importante para proteger los datos y para asegurar los sistemas que contienen estos datos y las redes por las que estos circulan. Estas protecciones y salvaguardas minimizan las vulnerabilidades ante las amenazas de seguridad y mitigan el daño causado por el acceso, recopilación, eliminación, modificación y divulgación de datos no autorizados.

Delitos cibernéticos que comprometen la privacidad

Los delitos cibernéticos violan la privacidad de las personas y la seguridad de sus datos, particularmente, la piratería, los programas maliciosos, el hurto de identidad, el fraude financiero y médico y ciertos delitos contra las personas que involucran el revelar información personal, mensajes, imágenes y grabaciones de audio y video sin el consentimiento o permiso de ellas (es decir, acoso, hostigamiento e intimidación cibernéticos, los cuales son tratados en Delito Cibernético-Módulo 12: Delito cibernético interpersonal).

Los actores legales e ilegales consideran que los datos son un producto básico, tanto en línea como fuera de ella (Maras, 2016). Por esta razón, los datos son el primer blanco de los delincuentes cibernéticos. Los datos también desempeñan un papel importante en la comisión de muchos delitos cibernéticos, principalmente, porque no están protegidos de manera adecuada y se puede acceder a ellos y obtenerlos ilícitamente. Las filtraciones de datos son el resultado de memorias portátiles cifradas y otros dispositivos de almacenamiento (generalmente laptops y teléfonos inteligentes) extraviados o robados, una seguridad de sistema y datos deficiente, el acceso no autorizado a la base de datos o el exceso de acceso no autorizado a una base de datos y la divulgación, lanzamiento o publicación accidental de datos. Algunos ejemplos notables de filtración de datos incluyen los siguientes:

"**La base de datos de identificación** del Gobierno centralizado nacional de India (Aashaar), el cual almacena los datos biométricos (p. ej., huellas dactilares y escaneo de iris) y los datos de identidad de 1200 millones de indios y se usa para verificar identidades en los servicios financieros, del Gobierno, servicios básicos y otros, fue objeto de una filtración de bases de datos en 2018 y puso en riesgo los datos de identidad, como el acceso a nombres, números de identificación de doce dígitos, números de teléfono, direcciones de correo electrónico y códigos postales, pero no los datos biométricos (Safi, 2018; Doshi, 2018).

La información de aproximadamente 30 millones de sudafricanos se filtró en línea en 2017, incluidos sus nombres, género, ingresos, historial de empleo, números de identidad, números de teléfono y direcciones domiciliarias, por la filtración de datos que sufrió una de las principales empresas inmobiliarias en el país, Jigsaw Holdings (Fihlani, 2017; Gous, 2017).

Los datos de más de tres mil millones de usuarios de Yahoo! se vieron comprometidos en 2013, incluidos nombres, direcciones de correo electrónico, contraseñas (con cifrados que podían saltarse con facilidad) y fechas de nacimiento (Newman, 2017).

Se accedió a Deloitte, una firma consultora mundial, a través de una cuenta no asegurada, comprometiendo los nombres de usuario y contraseñas, entre otros datos, de aproximadamente 350 clientes (Hopkins, 2017).

Los datos personales (p. ej., identificación nacional, nombre, género, nombres de los padres, dirección domiciliaria, fecha y ciudad de nacimiento) de más de 49 millones de turcos se puso a disposición en 2016 mediante una base de datos en línea consultable (Greenberg, 2016).

En 2016, se pusieron en riesgo los datos personales y biométricos de más de 55 millones de votantes en Filipinas, luego de que unos piratas informáticos de sombrero negro (para más información sobre la distinción entre los de sombrero negro, blanco y gris, consulte Delitos Cibernéticos-Módulo 2: Tipos generales de delitos cibernéticos; también consulte Radziwill et al., 2015; Chatelain, 2018b) pudieron acceder sin autorización al sitio web de la Comisión de Elecciones (COMELEC) (Tan, 2016)."

¿Sabían que...?

Las contraseñas robadas no solo ponen en riesgo las cuentas comprometidas, pues las personas a menudo reciclan contraseñas y las usan (las mismas o partes de estas contraseñas; p.ej., ciertos números) en más de un sitio web, dirección de correo electrónico o plataforma en línea.

Los actores legales e ilegales consideran que los datos son un producto básico, tanto en línea como fuera de ella (Maras, 2016). Por esta razón, los datos son el primer blanco de los delincuentes ciberméticos. Los datos también desempeñan un papel importante en la comisión de muchos delitos ciberméticos, principalmente, porque no están protegidos de manera adecuada y se puede acceder a ellos y obtenerlos ilícitamente. Las filtraciones de datos son el resultado de memorias portátiles cifradas y otros dispositivos de almacenamiento (generalmente *laptops* y teléfonos inteligentes) extraviados o robados, una seguridad de sistema y datos deficiente, el acceso no autorizado a la base de datos o el exceso de acceso no autorizado a una base de datos y la divulgación, lanzamiento o publicación accidental de datos. Algunos ejemplos notables de filtración de datos incluyen los siguientes:

Además de revelar estos datos con propósitos financieros, los datos comprometidos pueden ser (y han sido) revelados para humillar a las personas y exponer sus acciones y comportamientos reales o considerados inmorales. Un caso puntual es la publicación de información personal (como nombres y direcciones de correo electrónico) de aproximadamente 37 millones de usuarios de Ashley Madison, un sitio web que conectaba usuarios en busca de relaciones extramatrimoniales en línea (Zetter, 2015).

El peso de asegurar los datos, mayormente, recae sobre las personas que sufren del robo de sus datos. A estas personas se les informa que deben minimizar su «huella digital» actualizando configuraciones de seguridad en aplicaciones, sitios web, redes sociales y otras plataformas en línea y eliminando o reduciendo la cantidad de datos sobre ellos que ponen a disposición de otros (Maras, 2016). Este enfoque centrado en la víctima hace que la responsabilidad de protección recaiga sobre las víctimas del delito cibernético y no sobre los delincuentes y las empresas cuyos sistemas fueron filtrados. La realidad es que las víctimas no pueden proteger sus datos personales cuando estos están «almacenados en bases de datos de terceros y son el objeto del robo de estos, muy lejos de (...) [su] control» (Maras, 2016, 289). Es también cada vez más difícil minimizar la «huella digital» propia actualmente. Existen menos alternativas, si es que las hay, disponibles para las personas que optan por que no se recojan, analicen ni usen sus datos. Por ejemplo, una persona que usa redes sociales tiene una de dos opciones: proporcionar el mínimo de información requerida para usar la plataforma social (lo cual es, en esencia, por lo que la persona «paga» para usar el dispositivo) o no proporcionar la información y no usar la plataforma. No se ofrece otra alternativa. Los dispositivos del internet de las cosas (IdC) (discutidos en la sección introductoria de este módulo) también requieren información personal para su uso. Cada vez más, los nuevos dispositivos que entran al mercado —hasta aquellos que no venían con conexión a internet, como electrodomésticos, joyas, ropa y juguetes— ahora tienen conexión a internet (Maras, 2015) y dejan a los clientes con menos opciones, en caso elijan no comprar un dispositivo que no tenga estas opciones.

Leyes sobre la protección de datos

Los datos personales están protegidos de acuerdo con el derecho a la privacidad en instrumentos internacionales de derechos humanos. Por ejemplo, el Tribunal Europeo de Derechos Humanos sostuvo que los datos de teléfono, correos electrónicos y uso de internet (Copland versus the United Kingdom, 2007 §§ 41-42) y los datos almacenados en servidores de computadora (Wieser and Bicos Beteiligungen GmbH versus Austria, § 45) encajan en el alcance de la protección estipulada en el apartado 1 del artículo 8 de la Convención Europea de Derechos Humanos. El mero almacenamiento de datos personales puede violar el derecho a la privacidad de un usuario. La violación depende del contexto en que se recogieron los datos, cómo se recogieron, trataron y usaron, y el resultado de este tratamiento (S. and Marper versus the United Kingdom, 2008). Además, en Tristán Donoso versus Panama and Escher et al. versus Brazil (2009), el Tribunal Interamericano de Derechos Humanos sostuvo que los datos que se recogen y transmiten vía las nuevas tecnologías digitales e internet están contemplados en el artículo 11 de la Convención Americana de Derechos Humanos de 1969. Además, el artículo 8 de la Personales de 2014 contempla el derecho al «respeto de los datos personales». Por otra parte, el apartado 1 del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea del 2000 y el apartado 1 del artículo 16 del Tratado de Funcionamiento de la Unión Europea de 1957 (también conocido como el Tratado de Roma) consideran la protección de los datos personales como un derecho humano fundamental.

La protección de los datos cubre la generación, recojo, almacenamiento, análisis, uso y divulgación de información personal. La protección de los datos cubre la generación y recojo de datos personales porque «el derecho a la privacidad no solo sufre el impacto del análisis o uso de la información sobre una persona por parte de un humano o un algoritmo (…) [(Bernal, 2016) sino también] (…) la mera generación y recojo de datos en relación a la identidad, familia o vida de una persona (…) (consulte A/HRC/27/37, párr. 20 (…) [; Rotaru v. Romania, 2000; Kopp versus Switzerland, 1998; y Roman Zakharov versus Russia, 2015)]» (A/HRC/39/29, párr. 7).

Los organismos públicos y privados pueden consultar, buscar, editar, actualizar y acceder a las bases de datos que contienen datos personales en los mismos países o entre ellos. La gobernanza del recojo, almacenamiento, uso y divulgación de la información por parte de los organismos privados y públicos varía de país en país. De acuerdo con un informe de la Oficina del Alto Comisionado para los Derechos Humanos de 2018, «la mayor interconexión entre el tratamiento de datos públicos y privados y los antecedentes a la fecha que señalan un mal uso masivo y recurrente de información personal por parte de empresas comerciales confirman que se necesitan medidas legislativas para lograr un nivel adecuado de protección de la privacidad» (cita de A/HRC/RES/34/7, párr. 5(f) y A/HRC/RES/38/7, párr. A/HRC/39/29, párr. 27). Los datos personales podrían ser procesados por países con leyes para la protección de los datos fuertes o débiles, o por países que no cuentan con leyes para la protección de los datos. Por ejemplo, en Ghana, la sección 60 del Acta de Protección de Datos de 2012 permite que el Gobierno acceda a los datos personales sin alguna autorización u otra orden legal (es decir, orden judicial) en beneficio de la seguridad nacional.

Las prácticas de protección de los datos también varían entre las autoridades públicas y privadas. En los Estados Unidos, por ejemplo, solo ciertos tipos de datos que las empresas privadas recogen, almacenan, analizan y comparten están regulados (p. ej., datos financieros, de salud, educativos y de niños; Matas y Wandt, 2019). Además, en ciertos países, la protección varía dependiendo del tipo de datos (p. ej., al contenido del correo electrónico se le otorga más protección que a la dirección de correo electrónico del emisor o remitente). Las leyes de protección de datos varían dependiendo de los tipos y fuentes de datos (p. ej., datos por sectores, datos en línea, datos fuera de línea y datos sensibles) y temas de datos (p. ej., adultos y niños). México tiene dos leyes para la protección de datos: una que regula el sector privado, la Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010, y otra que regula el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017. México también tiene algunas disposiciones en la ley que regulan los datos privados en relación con los servicios en la nube, incluyendo la regulación del acceso de las fuerzas del orden a datos almacenados en la nube y el manejo de los datos después de la finalización de los servicios en la nube.

La naturaleza transfronteriza de internet requiere una regulación transnacional de protección de datos que se extienda más allá de los marcos y leyes nacionales. Algunos ejemplos incluyen la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014 y la Comunidad Económica de Estados de África Occidental (ECOWAS) Ley Suplementaria A/SA.1/01/10 sobre la Protección de Datos Personales dentro de la ECOWAS. Estas leyes y marcos regionales recibieron la influencia de la Directiva de Protección de Datos de la UE (Directiva 1995/46/EC) (Greenleaf, 2011; Orji, 2017; Makulilo, 2013a; Makulilo, 2013b). La Directiva 1995/46/EC fue reemplazada por el Reglamento General de Protección de Datos de la UE (RGPD) el 25 de mayo de 2018. Esta única ley de protección de los datos rige el tratamiento, almacenamiento, uso e intercambio de datos en los Estados miembro de la UE y otros países, organismos y organizaciones privadas fuera de la UE que le proporcionan bienes y servicios y procesan los datos de sus residentes. El RGPD busca armonizar el tratamiento, almacenamiento, uso e intercambio seguro de datos de información personal. Esta ley minimiza la huella digital de los usuarios y la manera en que las aplicaciones, tecnología y servicios y plataformas de internet explotan esta huella. El RGPD fortalece los derechos de privacidad de las personas y mejora la libre circulación de datos personales a través de las fronteras al armonizar las prácticas de protección de datos. El RGPD aclaró lo que constituye datos personales, estableció reglas para manejar los datos, designó funciones y responsabilidades para quienes controlan y procesan datos personales, creó mayores sanciones por incumplimiento e impuso que las notificaciones de filtración de datos se den dentro de las 72 horas a partir del incidente.

Este reglamento impone nuevas obligaciones para quienes controlan los datos (es decir, la entidad que determina las razones para el tratamiento de datos y los métodos usados para procesarlos) y los procesadores de datos (es decir, la entidad responsable por el tratamiento de datos basado en métodos identificados por quien controla los datos). El RGPD regula el acceso a los datos y la rectificación, eliminación y transparencia de los procesadores y controladores de datos; brinda el derecho a oponerse a prácticas de segmentación de mercado; impone obligaciones de seguridad de datos para las empresas que los procesan; proporciona mayores poderes a las autoridades encargadas de proteger los datos y facilita la coordinación y cooperación para el tratamiento y la protección de datos. Este reglamento también contempla multas elevadas y sanciones por incumplimiento.

Los usuarios tienen el derecho a estar informados sobre el tratamiento de datos; el derecho a acceder a los datos procesados; el derecho a rectificar los datos procesados; el derecho a la supresión («derecho a ser olvidado»; el titular de los datos tiene el derecho a pedir y exigir que sus datos se borren de los historiales, y a prevenir un mayor uso y transferencia de sus datos personales por parte de terceros); el derecho a oponerse al tratamiento de datos; el derecho a restringir el tratamiento de datos; el derecho a la portabilidad de datos (es decir, dicho titular tiene el derecho a pedir sus datos personales al controlador de datos y transferirlos a otro controlador) y el derecho a no ser sujeto a una decisión basada exclusivamente en un tratamiento automático (p. ej., segmentación).

¿Sabían que...?

Las contraseñas robadas no solo ponen en riesgo las cuentas comprometidas, pues las personas a menudo reciclan contraseñas y las usan (las mismas o partes de estas contraseñas; p.ej., ciertos números) en más de un sitio web, dirección de correo electrónico o plataforma en línea.

El derecho a ser olvidado

En Google Spain SL, Google Inc. versus Agencia Española de Protección de Datos, Mario Costeja González (2014), el Tribunal de Justicia de la Unión Europea interpretó que la Directiva 1995/46/EC permite a los usuarios pedir que sus datos personales dejen de indexarse en motores de búsqueda y navegadores. Específicamente, el tribual sostuvo que las personas tienen el derecho a pedir que los controladores de datos (p. ej., navegadores y motores de búsqueda, como Google) que borren los enlaces a sitios web que incluyan información incorrecta, incompleta, irrelevante o que ya no sea pertinente o válida sobre ellos. En particular, la persona puede pedir que se borren los enlaces que aparecen por las búsquedas del nombre del usuario relacionada a este contenido. Esta desindexación se limita al contenido que se ha indexado bajo el nombre del usuario. Esta desindexación no prohibiría la disponibilidad de este contenido indexado bajo un término de búsqueda diferente basado en el contenido, publicación u otra fuente o editor o autor del contenido.

El RGPD aplica para instituciones de la UE, lo cual el Tribunal de Justicia de la Unión Europea ha interpretado como una organización que procesa datos en el contexto de sus actividades, aún si estas actividades son mínimas (Weltimmo versus NAIH, 2014). Mientras ocurran en el contexto de algún acuerdo que exista en la Unión Europea, este tratamiento de datos está contemplado por el RGPD. Las organizaciones con oficinas en la UE y aquellas que promueven o venden servicios de marketing o publicidad que tienen como objetivo a los residentes de la UE también están sujetas al RGPD. Incluso algunas instituciones que no son de la UE están sujetas al RGPD si procesan datos personales con el fin de ofrecer bienes y servicios a residentes de la UE y de monitorear el comportamiento del consumidor en la UE para segmentar el mercado, identificar patrones y predecir preferencias personales de los usuarios.

El RGPD no aplica al tratamiento de los datos personales por razones de seguridad nacional y de conformidad a las políticas extranjeras y de seguridad comunes de la UE (es decir, por temas de defensa y seguridad). El RGPD tampoco aplica a los datos procesados por instituciones de la UE, lo que está regido por el Reglamento (EC) 45/2001 del Parlamento Europeo y del Consejo del 18 de diciembre del 2000 «sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos». El RGPD tampoco aplica a los datos procesados por autoridades públicas en el curso de la prevención, detección, investigación y enjuiciamiento del delito, lo cual está regido por la Directiva (EU) 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016

> “Sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y sobre la libre circulación de dichos datos.”

El Convenio de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981 (ETS No. 108) del Consejo de Europa es un tratado internacional legalmente vinculante sobre la protección de datos personales. Un protocolo adicional opcional al Convenio, el Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, respecto a las autoridades supervisoras y los flujos transfronterizos de datos de 2001, pidió el establecimiento de autoridades supervisoras para asegurar la protección de los datos y el respeto a la privacidad en la divulgación de datos. Otro protocolo (CETS No. 223) enmendó y actualizó el Convenio de 1981 (es decir, el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 2018). De acuerdo con el Consejo de Europa (s.f.), la modernización del Convenio «apuntó a dos objetivos principales: lidiar con los desafíos resultantes del uso de nuevas tecnologías de información y comunicación y reforzar la efectiva implementación del Convenio» (para las principales novedades del Convenio modernizado, consulte: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8; y para una tabla comparativa entre el Convenio de 1981 y el modernizado, consulte: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958).

Además de las leyes de protección de datos nacionales, regionales e internacionales, existen directrices y principios que algunos países y organizaciones intergubernamentales han creado y que sectores públicos y privados en todo el mundo ha implementado, como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) con sus Directrices para la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (1980; 2013).

Las Directrices de la OCDE sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 2013 son las siguientes:

Principio de limitación del recojo de datos
Deben establecerse límites para el recojo de datos personales. Cualquiera de estos datos debe obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del titular de los datos.

Principio de calidad de datos
Los datos personales deben ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, deben ser exactos, estar completos y actualizados.

Principio de especificación del propósito
Se deben especificar los propósitos del recojo de datos, a más tardar, en el momento en que se produce dicho recojo. Su uso será limitado al cumplimiento de los objetivos u otros que no sean incompatibles con los propósitos originales, especificando en cada momento si hubiera un cambio de objetivo.

Principio de limitación de uso
No se deberán divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el párrafo 9, excepto:

a) si se tiene el consentimiento del titular de los datos o
b) por imposición legal de las autoridades.

Principio de medidas de seguridad
Se emplearán medidas razonables de seguridad para proteger los datos personales contra riesgos, tales como la pérdida, el acceso no autorizado, la destrucción, el uso, la modificación o la divulgación de estos.

Principio de transparencia
Debe existir una política general sobre transparencia en cuanto a la evolución, prácticas y políticas relativas a los datos personales. Se debe contar con medios fácilmente disponibles para establecer la existencia y la naturaleza de datos personales, el propósito principal para su uso, y la identidad y lugar de residencia habitual de quien controla esos datos.

Principio de participación individual

Toda persona tiene derecho a:

a) que el controlador de datos u otra fuente le confirme si tiene datos sobre su persona;
b) que se le comuniquen los datos relativos a su persona en un tiempo razonable y a un precio, si lo hubiera, que no sea excesivo, de forma razonable y de manera fácilmente inteligible;
c) que se le expliquen las razones por las que una solicitud suya según los subapartados (a) y (b) ha sido denegada, así como a poder cuestionar tal denegación y
d) expresar dudas sobre los datos relativos a su persona y, si su reclamo tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan

Principio de responsabilidad

Todo controlador de datos debe rendir cuentas acerca del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Se han adoptado principios similares en legislaciones nacionales. Consulte, por ejemplo, la Ley de Privacidad de Nueva Zelanda de 1993 y la Ley de Privacidad de Australia de 1988.

Leyes sobre la notificación de filtración de datos

Según el Borrador del Estudio Exhaustivo sobre el Delito Cibernético de la UNODC Aunque muchos países tengan leyes que exigen notificaciones sobre la filtración de datos (p. ej., Filipinas, Ley de Privacidad de Datos de 2012 e Indonesia, norma legal n.° 82 de 2012 sobre las Disposiciones de Sistemas Electrónicos y Transacciones y su reglamento de implementación, norma legal n.° 20 de 2016 sobre la Protección de Datos Personales en un Sistema Electrónico), estas no son obligatorias en la mayoría de países (p. ej., Argentina, Bielorrusia, Costa Rica, Egipto, Japón, Macao, Malasia, Madagascar, Mauricio, Panamá, Rusia, y Arabia Saudita) o son obligatorias para el sector privado y no para el público en otros países, o solo para ciertos sectores de la sociedad (p. ej., Angola y Serbia). En Argentina, aunque no se requiere la notificación sobre la filtración de datos, se solicita a los organismos que lleven registros de filtraciones de datos en caso se los soliciten durante una investigación o auditoría.

¿Sabían que...?

DLA Piper ha hecho un mapa mundial interactivo de leyes sobre la protección de datos, así como una base de datos consultable sobre leyes nacionales sobre la protección de datos y notificaciones de filtración de datos:

https://www.dlapiperdataprotection.com/index.html?c=IL&c2=&t=breach-notification

Actos informáticos que causan daños personales

Las leyes sobre la notificación de filtraciones de datos incluyen disposiciones con relación a la aplicación de estas leyes, como las personas, organismos o autoridades a las que las leyes aplican y qué está considerado una filtración según estas leyes. Estas leyes requieren que las entidades que hayan sido objeto de una filtración (y están contempladas por la ley) contacten a las personas u otras partes cuyos datos se han filtrado y les informen sobre el incidente.

Particularmente, estas leyes consideran la manera en la que se da una notificación, el tiempo límite para esta notificación y las personas, organismos o autoridades que se necesitan contactar por motivos de la filtración. El RGPD, por ejemplo, establece que el aviso sobre la filtración de datos debe darse obligatoriamente dentro de las 72 horas por acceso no autorizado a sistemas y datos, así como por el uso y distribución de los datos (artículo 33). Se requiere que los procesadores de datos notifiquen a los controladores sobre alguna filtración dentro de las 72 horas, y que los controladores notifiquen a la autoridad supervisora de protección de datos del Estado miembro de la UE que se haya visto afectado dentro del mismo periodo de tiempo.

Las leyes sobre la notificación de filtraciones de datos también incluyen excepciones al requerimiento de notificación. Por ejemplo, de acuerdo con el RGPD, la notificación al titular de los datos depende de la gravedad de la filtración de datos (artículo 34). Algunas leyes sobre la notificación de filtraciones de datos no requieren notificación si se determina que no es probable que dañe a las partes afectadas. En otras leyes, la notificación ocurre cuando una filtración alcanza un umbral específico. En los Estados Unidos, la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA) requiere que la notificación a las partes afectadas se dé dentro de 60 días desde la filtración. Sin embargo, en casos donde se ha accedido a los datos sobre la salud de más de 500 individuos, se debe contactar a la Oficina para los Derechos Civiles del Departamento de Salud y Servicios Humanos y a los medios de comunicación dentro de los 60 días desde la filtración, mientras que cuando se filtra la información personal de salud de menos de 500 personas, los medios de comunicación no necesitan ser notificados y la Oficina para los Derechos Civiles del Departamento de Salud y Servicios Humanos debe ser contactada en un plazo máximo de 60 días después del inicio del siguiente año calendario (Revista HIPPA, 2015).

Las leyes de notificación de filtraciones de datos de otros países también requieren que las entidades que procesan los datos implanten medidas de seguridad para proteger los datos o acciones por parte de la entidad filtrada a fin de corregir la situación o remediar el daño (p. ej., Canadá, Indonesia y los Estados Unidos).

Generalmente, las dificultades que enfrentan los países con leyes adecuadas para hacer cumplir la protección de los datos incluyen problemas de financiamiento, incapacidad de hacer cumplir estas leyes adecuadamente (p. ej., restricciones de recursos humanos y técnicos), infraestructura TIC inadecuada y no poder o querer manejar pedidos transfronterizos de datos (UCTAD, 2016, p. 9).

La aplicación de los principios y leyes sobre la protección de datos y privacidad varía entre los sectores público y privado, y dentro de los países. El RGPD, por ejemplo, se estableció para armonizar y reforzar las facultades de las autoridades encargadas de la protección de datos para asegurar la aplicación efectiva de la ley. Además de las leyes de protección de datos, a fin de contribuir a los esfuerzos de protección, las organizaciones internacionales y regionales han desarrollado e implementado un reglamento de protección de datos. Por ejemplo, el Foro de Cooperación Económica Asia Pacífico (APEC) desarrolló el Marco de Privacidad, el cual incluye principios y directrices para proteger los datos de una manera que evite obstáculos para el flujo de la información entre miembros. También desarrolló las Reglas de Privacidad Transfronteriza, un mecanismo autorregulador voluntario que determina estándares de protección de datos para el intercambio transfronterizo de datos entre los miembros. Es importante resaltar que las leyes nacionales de protección de datos y privacidad tienen prioridad sobre estas normas.

¿Sabían que...?

La Asociación Internacional de Profesionales de la Privacidad (IAPP) puso a disposición un cuadro que resalta las similitudes y diferencias entre el Marco de Privacidad de la APEC y el RGPD con respecto a los siguientes aspectos: propósito, ámbito material y territorial, información personal, controladores de datos, procesadores de datos, información de dominio público, variaciones de países miembros permitidas (derogaciones), prevención del principio de no maleficencia, avisos, límite de recojo, límite de uso, elección y consentimiento, integridad de datos, medidas de seguridad, acceso y corrección, rendición de cuentas, transferencia de datos personales a otra persona o país, definición de filtración, notificación y atenuación de filtraciones. Dicho cuadro se puede encontrar aquí:

https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/

Además de la aplicación de estas normas por parte de una autoridad, las tecnologías pueden imponer la protección de los datos. Un caso puntual es la tecnología garante de la privacidad (PET). El objetivo de la tecnología garante de la privacidad es proteger y preservar la privacidad de las personas. Por esta razón, la tecnología garante de la privacidad se puede usar para implementar y hacer cumplir las leyes sobre la protección de datos. Estas tecnologías se usan principalmente para proteger la confidencialidad (es decir, los datos se protegen y solo los usuarios autorizados pueden acceder a ellos) y la integridad de los datos (es decir, los datos no se han modificado y son lo que deben ser). Un ejemplo de tecnología garante de la privacidad es el cifrado. Otro ejemplo es la gestión de la identidad, la cual se refiere al proceso de autenticar las identidades de usuarios, identificando privilegios asociados y garantizando el acceso a los usuarios sobre la base de estos privilegios. La gestión de la identidad apoya los principios de seguridad y proporcionalidad al restringir el acceso y uso de los datos.

Las leyes de protección de datos también se pueden aplicar mediante la protección de datos desde el diseño. El artículo 25 del RGPD ordena la «protección de datos desde el diseño», por lo que los controladores y procesadores de datos incorporan las PET y otras medidas de seguridad en el diseño de sistemas y tecnologías. Estas funciones de diseño requieren de controles y políticas técnicas y organizacionales para asegurar los datos personales y la provisión de medidas de seguridad diseñadas para asegurar la confidencialidad, integridad y disponibilidad (es decir, accesible a pedido) de sistemas, redes, servicios y datos (p. ej., control de acceso, cifrado, cortafuegos, monitoreo del uso de la computadora y políticas de seguridad de la información, abordados en Delitos Cibernéticos-Módulo 9: Seguridad cibernética y prevención del delito cibernético: aplicaciones y medidas prácticas).

Otra medida de protección de datos desde el diseño (o privacidad desde el diseño) implica no tener la información de identificación a plena vista, mediante el anonimización y seudonimización. Según el apartado 5 del artículo 4 del RGPD, la seudonimización se refiere al:

> “Tratamiento de datos personales de manera tal que ya no puedan atribuirse al titular de los datos sin utilizar información adicional, siempre que dicha información adicional se guarde por separado y esté sujeta a medidas técnicas y organizacionales destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.”

La seudonimización ocurre cuando se reemplaza la identificación de datos en un registro por identificadores artificiales. Esta es una forma de enmascaramiento de datos, pues protege la confidencialidad de los datos para prevenir la identificación del titular. Además de las medidas de protección de datos desde el diseño, se pueden implementar medidas de protección de datos por defecto. Un ejemplo de esta medida es la práctica de solo procesar datos personales, lo cual es necesario para lograr el objetivo planteado de la actividad (siguiendo los principios de minimización de datos y limitación de propósito).

Referencias

- ***Berlinger, J. & Vazquez, M. (2018, January 29).*** US military reviewing security practices after fitness app reveals sensitive info. CNN.
  • *https://edition.cnn.com/2018/01/28/politics/strava-military-bases-location/index.html*

- ***Bernal, P. (2016).*** Data gathering, surveillance and human rights: recasting the debate. Journal of Information Technology & Politics, 1(2), 243-264.

- ***Chatelain, Y. (2018a, July 5).*** Darknet: faut-il démanteler la revente illégale de la liberté de s'exprimer et de s'informer? The Conversation.
  •*https://theconversation.com/darknet-faut-il-demanteler-la-revente-illegale-de-la-liberte-de-sexprimer-et-de-sinformer-97993*

- ***Chatelain, Y. (2018b, May 15).*** Principles of hacktivism and hackers: ignorance and prejudices! The Conversation.
  • *https://theconversation.com/principles-of-hacktivism-and-hackers-ignorance-and-prejudices-96514*

- ***Cooley, T. (1907).*** A Treatise on the Law of Torts. Callaghan and Company.

- ***Council of Europe. (n.d.).*** Modernisation of Convention 108.
  • *https://www.coe.int/en/web/data-protection/convention108/modernised*

- ***De Meyer, J. (1973).*** The Right to Respect for Private and Family Life, Home, and Communications in relations between individuals, and the Resulting Obligations for States Parties to the Convention. En A. H. Robertson, ed. Privacy and Human Rights. Manchester University Press.

- ***Douglas, K.M. & McGarty, C. (2001).*** Identifiability and Self-Presentation: Computer-Mediated Communication and Intergroup Interaction. British Journal of Social Psychology, 40(3), 399-416.

- ***Eissen, M.A. (1967).*** La protection internationale des droits de l'homme dans le cadre Européen. Dalloz.

- ***Fihlani, P. (2017, October 20).*** Millions caught in South Africa's 'worst data breach'. BBC News.
  • *http://www.bbc.com/news/world-africa-41696703*

- ***Finklea, K. (2017).*** Dark Web. Congressional Research Service.
  • *https://fas.org/sgp/crs/misc/R44101.pdf*

- ***Fleishman, G. (2018, June 26).*** Milos Yiannopoulos Jokes of Death Squads Murdering Journalists. Fortune.
  • *http://fortune.com/2018/06/26/milo-yiannopoulos-jokes-of-death-squads-murdering-journalists/*

- ***Fried, C. (1970).*** An Anatomy of Values. Harvard University Press.

- ***Global Partners Digital. (2017).*** Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders.
  • *https://www.gp-digital.org/wp-content/uploads/2017/09/TRAVELGUIDETOENCRYPTIONPOLICY.pdf*

- ***Gous, N. (2017, October 18).*** Top real estate company admits to being unwitting source of country's largest personal data breach. Sunday Times.
  •*https://www.timeslive.co.za/news/south-africa/2017-10-18-top-real-estate-company-admits-to-being-unwitting-source-of-countrys-largest-personal-data-breach/*

- ***ENISA. (2017).*** Hardware Threat Landscape and Good Practice Guide (Version 1). ENISA.
  • *https://www.enisa.europa.eu/publications/hardware-threat-landscape/at_download/fullReport*

- ***Greenberg, A. (2016, April 5).*** Hack brief: Turkey breach spills info on more than half its citizens. Wired.
  • *https://www.wired.com/2013/11/open-market-trial-begins/*

- ***Greenleaf, G. (2011).*** The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108. International Data Privacy Law, 2(2), 68-92.

- ***Haines, R., Hough, J., Cao, L. & Haines, D. (2014).*** Anonymity in computer-mediated communication: More contrarian ideas with less influence. Group Decision and Negotiation, 23(4), 765-786.

- ***Hern, A. (2018, January 28).*** Fitness tracking app Strava gives away location of secret army bases. The Guardian.
  • *https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases*

- ***HIPAA Journal. (2015).*** Summary of the HIPAA breach notification rule.
  • *https://www.hipaajournal.com/summary-of-the-hipaa-breach-notification-rule-101/*

- ***Hopkins, N. (2017, October 10).*** Deloitte hack hit server containing emails from across US government. The Guardian.
  •*https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government*

- ***Janis, M., Kay, R. & Bradley, A. (2000).*** European Human Rights Law: Text and Materials (2nd edition). Oxford University Press.

- ***Koops B.J., Newell, B.C., Timan, T., Škorvánek, I., Chokrevski, T. & Galič, M. (2017).*** A typology of privacy. University of Pennsylvania Journal of International Law, 38(2), 483-575.

- ***MacFarquhar, N. (2018, April 13).*** Russian court bans Telegram app after 18-minute hearing. The New York Times.
  • *https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html*

- ***Makulilo, A.B. (2013a).*** Data Protection Regimes in Africa: too far from the European 'adequacy' standard? International Data Privacy Law, 3(1), 42-50.

- ***Makulilo, A.B. (2013b).*** Mauritius Data Protection Commission: an analysis of its early decisions. International Data Privacy Law, 3(2), 131-139.

- ***Maras, M.H. (2016).*** Cybercriminology. Oxford University Press.

- ***Maras, M.H. (2009).*** From Targeted to Mass Surveillance: Is the EU Data Retention Directive a Necessary Measure or an Unjustified Threat to Privacy? En Ben Goold and Daniel Neyland, eds. New Directions in Surveillance and Privacy (pp. 74-103). Willan.

- ***Maras, M.H. (2014).*** Inside Darknet: The Takedown of Silk Road. Criminal Justice Matters, 98(1), 22-23.

- ***Maras, M.H. (2015).*** The Internet of Things: Security and Privacy Implications. International Data Privacy Law, 5(2), 99-104.

- ***Maras, M.H. (2012).*** The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the "Others"? International Journal of Law, Crime and Justice, 40(2), 65-81.

- ***Maras, M.H. & Wandt, A. (2019).*** Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things. Journal of Cyber Policy.

- ***Maras, M.H. & Wandt, A. (2018).*** IoT Data Collection and Analytics. Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York (2 de mayo de 2018).

- ***Meyer, D. (2018, May 1).*** Iran Bans Telegram, an App Used By Half the Country. Fortune.
  - *http://fortune.com/2018/05/01/iran-bans-telegram-secure-app/*

- ***Newman, L.H. (2017, October 3).*** Yahoo's 2013 email hack actually compromised three billion accounts. Wired.
  - *https://www.wired.com/story/yahoo-breach-three-billion-accounts/*

- ***Orji, U.J. (2017).*** Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. International Data Privacy Law, 7(3), 179-189.

- ***Radziwill, N., Romano, J., Shorter, D. & Benton, M. (2015).*** The Ethics of Hacking: Should It Be Taught? arXiv.
  - *https://arxiv.org/pdf/1512.02707.pdf*

- ***Rodriguez, P.A. (2015).*** Human dignity as an essentially contested concept. Cambridge Review of International Affairs, 28(4), 743-756.

- ***Rost, K., Stahel, L. & Frey, B.S. (2016).*** Digital Social Norm Enforcement: Online Firestorms in Social Media. PLOS One, 11(6).
  - *http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155923*

- ***Safi, M. (2018, January 4).*** Personal data of a billion Indians sold online for £6, report claims. The Guardian.
  - *https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar*

- ***Schroeder, D. (2017, August 9).*** How to define dignity and its place in human rights – a philosopher's view. The Conversation.
  - *https://theconversation.com/how-to-define-dignity-and-its-place-in-human-rights-a-philosophers-view-81785*

- ***Shultztiner, D. & Carmi, G.E. (2014).*** Human Dignity in National Constitutions: Functions, Promises and Dangers. The American Journal of Comparative Law, 62(2), 461-490.

- ***Tan, L. (2016, April 8).*** 55M Filipino voters open to fraud after Comelec hack – int'l tech security firm. CNN Philippines.
  - *http://cnnphilippines.com/news/2016/04/08/Comelec-hack-fraud-data-breach-security.html*

- ***United Nations Conference on Trade and Development. (2016).*** Data protection regulations and international data flows: Implications for trade and development.
  - *http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf*

- ***Vidhi, D. (2018, January 4).*** A security breach in India has left a billion people at risk of identity theft. The Washington Post.
  - *https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?noredirect=on&utm_term=.770f96a565e0*

- ***Zetter, K. (2015, August 18).*** Hackers finally post stolen Ashley Madison data. Wired.
  - *https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/*

Casos

- *Escher et al. V. Brazil. Inter-American Court of Human Rights (Preliminary Objections, Merits, Reparations, and Costs). Judgment of 6 July 2009. Series C No. 200 (2009).*
- *Fontevecchia and D'Amico v. Argentina. Inter-American Court of Human Rights (Merits, Reparations and Costs). Judgment, I/A Court H.R., Series C No. 238 (2011).*
- *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja*
- *González Case C-131/12 [ECR, 13 de mayo de 2014].*
- *Ituango Massacres v. Colombia. Inter-American Court of Human Rights (Preliminary Objections, Merits, Reparations and Costs). Judgment of 1 July 2006. Series C No. 148 (2006).*
- *Kopp v. Switzerland (App No. 23224/94) [1998] ECHR 18.*
- *Pretty v. United Kingdom (App 2346/02) [2002] ECHR 423.*
- *Roman Zakharov v. Russia (App No. 47143/06) [2015] ECHR 1065.*
- *Rotaru v. Romania (App No. 28341/95) [2000] ECHR 192.*
- *S and Marper v United Kingdom (App nos. 30562/04 and 30566/04) [2008] ECHR 1581.*
- *Tristán Donoso v. Panama. Inter-American Court of Human Rights (Preliminary objection, merits, reparations and costs). Judgment of 27 January 2009. Series C No. 193 (2009).*
- *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság (Weltimmo v. Hungarian Data Protection Authority) Case C-230/14 [ECR, 30 de octubre de 2015].*
- *Wieser and Bicos Beteiligungen GmbH v Austria (App no. 74336/01) [2007] ECHR 815.*

Legislaciones y convenciones nacionales e internacionales

- ***African Charter on Human and Peoples Rights (1981).*** Instruments.
  - *http://www.achpr.org/instruments/achpr/*
- ***African Union. (2014).*** African Union Convention on Cyber Security and Personal Data Protection.
  - *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*
- ***Council of Europe. (1950).*** European Convention on Human Rights.
  - *https://www.echr.coe.int/Documents/Convention_ENG.pdf*
- ***Council of Europe. (1981).*** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
  - *https://rm.coe.int/1680078b37*

- ***ECOWAS. (2010).*** Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.
  - *http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf*

- ***European Union. (2000).*** Charter of Fundamental Rights.
  - *http://www.europarl.europa.eu/charter/pdf/text_en.pdf*

- ***European Union. (2016).*** Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG*

- ***European Union. (1995).***Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046*

- ***European Union. (2000).*** Regulation (EC) no 45/2001 of the of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.
  - *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045*

- ***European Union. (1957).*** Treaty on the Functioning of the European Union.
  - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT*

- ***Inter-American Commission on Human Rights. (1969).*** American Convention on Human Rights.
  - *https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm*

- ***Intersoft Consulting. (n.d.).*** General Data Protection Regulation (GDPR).
  - *https://gdpr-info.eu/*

Materiales de las Naciones Unidas

- ***General Assembly.***

  Resolution (A/RES/72/175).
  - *https://undocs.org/A/RES/72/175*

  Resolution (A/72/135).
  - *https://undocs.org/A/72/135*

- ***General Assembly, Human Rights Council.***

  Resolution (A/HRC/RES/34/7).
  - *https://undocs.org/A/HRC/RES/34/7*

  Resolution (A/HRC/RES/38/7).
  - *https://undocs.org/A/HRC/RES/38/7*

Resolution (A/HRC/RES/39/6).
• *https://undocs.org/A/HRC/RES/39/6*

Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies (A/HRC/31/66).
• *https://undocs.org/A/HRC/31/66*

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40).
• *https://undocs.org/A/HRC/23/40*

The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (A/HRC/39/29).
• *https://undocs.org/A/HRC/39/29*

- ***UN Documents. (1963).*** United Nations Declaration on the Elimination of All Forms of Racial Discrimination.
  • *http://www.un-documents.net/a18r1904.htm*

- ***UN General Assembly. (1990).*** International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families.
  • *https://www.refworld.org/docid/3ae6b3980.html*

- ***UN Women. (1979).*** Convention on the Elimination of All Forms of Discrimination against Women.
  • *http://www.un.org/womenwatch/daw/cedaw/text/econvention.htm*

- ***United Nations. (1948).*** Universal Declaration on Human Rights.
  • *http://www.un.org/en/universal-declaration-human-rights/*

- ***United Nations. (2006).*** Convention on the Rights of Persons with Disabilities (CRPD).
  • *https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html*

- ***United Nations Human Rights. (1966).*** International Covenant on Civil and Political Rights.
  • *https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx*

- ***United Nations Human Rights. (1966).*** International Covenant on Economic, Social and Cultural Rights.
  • *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx*

- ***United Nations Human Rights. (1989).*** Convention on the Rights of a Child.
  • *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx*

Legislación nacional

- ***Australia. Privacy Act (1988).***
  • *https://www.legislation.gov.au/Series/C2004A03712*

- ***Ghana. Data Protection Act (2012).***
  •*https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf*

- ***Indonesia. Regulation No. 20 regarding the Protection of Personal Data in an Electronic System (2016).***

- ***Indonesia. Regulation No. 82 concerning Electronic System and Transaction Operation (2012).***
  - *http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html*

- ***Mexico. Federal Law on Protection of Personal Data Held by Private Parties (2010).***
  - *https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf*

- ***Mexico. General Law for the Protection of Personal Data in Possession of Obliged Subjects (2017).***
  - *http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26%2F01%2F2017*

- ***Philippines. Data Privacy Act (2012).***
  - *https://privacy.gov.ph/data-privacy-act/*

- ***United States of America. Health Insurance Portability and Accountability Act (HIPAA) (1996).***
  - *https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf*

- ***New Zealand. Privacy Act (1993).***
  - *http://www.legislation.govt.nz/act/public/1993/0028/232.0/DLM296639.html*

Lecturas principales

- ***Bambauer, D.E. (2013).*** Privacy versus Security. Journal of Criminal Law and Criminology, 103(3), 667-684.

- ***European Union Agency for Fundamental Rights and Council of Europe. (2018).*** Handbook on European data protection law 2018 edition.
  - *https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law*

- ***Maras, M.H. & Wandt, A. (2019).*** Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things. Journal of Cyber Policy.

- ***Schartum, D.W. (2016).*** Making privacy by design operative. International Journal of Law and Information Technology, 24(2), 151-175.

- ***United Nations Conference on Trade and Development. (2016).*** Data protection regulations and international data flows: Implications for trade and development.
  - *https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf*

Lecturas avanzadas

Se recomienda las siguientes lecturas a los interesados en investigar los temas de este módulo con más detalle:

- ***Brunton, F. & Nissbaum, H. (2015).*** Obfuscation: A User's Guide for Privacy and Protest. MIT Press.

- ***Chatelain, Y. (2018, July 5).*** Darknet: faut-il démanteler la revente illégale de la liberté de s'exprimer et de s'informer? The Conversation.
  •*https://theconversation.com/darknet-faut-il-demanteler-la-revente-illegale-de-la-liberte-de-sexprimer-et-de-sinformer-97993*

- ***Gerry, F., Muraszkiewicz, J. & Vavoula, N. (2016).*** The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. Computer Law & Security Review, 32(2), 205-217.

- ***Joyce, D. (2015).*** Privacy in the Digital Era: Human Rights Online? Melbourne Journal of International Law, 16, 270-285.

- ***Koops, B.J., Newell, B.C., Timan, T., Škorvánek, I., Chokrevski, T. & Galič, M. (2017).*** A typology of privacy. University of Pennsylvania Journal of International Law, 38(2), 483-575.

- ***McCallister, E., Grance, T. & Scarfone, K.A. (2010).*** Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). NIST.
  • *https://www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii*

- ***NIST. (2017).*** Security and Privacy Controls for Information Systems and Organizations. Draft NIST Special Publication 800-53.
  • *https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf*

- ***Stewart, K. (n.d.).*** Looking Backward, Moving Forward: What Must be Remembered When Resolving the Right to be Forgotten. Brooklyn Journal of International Law, 42(2), 843-886.

- ***Summers, S.J., Schwarzenegger, C., Ege, G. & Young, F. (2014).*** The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society. Hart.

- ***Tikkinen-Piri, C., Rohunen, A. & Markula, J. (2018).*** EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

- ***Vaciago, G. (2012).*** ISPs and Civil Liberties: The "Reasonable Expectation of Privacy" of Twitter's User from People v. Harris. Computer Law Review International, 13(5), 137-141.

Herramientas complementarias

Estudio de caso

Cambridge Analytica

- ***Hern, A. & Pegg, D. (2018, July 10).*** Facebook fined for data breaches in Cambridge Analytica scandal. The Guardian.
  •*https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal*

- ***Solon, O. (2018, May 16).*** Cambridge Analytica whistleblower says Bannon wanted to suppress voters. The Guardian.
  •*https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony*

- ***Granville, K. (2018, March 19).*** Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. New York Times.
  • *https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html*

- ***NPR. (n.d.).*** Stories about Cambridge Analytica. NPR.
  • *https://www.npr.org/tags/467415574/cambridge-analytica*

- ***Wired. (n.d.).*** Cambridge Analytica. Wired.
  • *https://www.wired.com/tag/cambridge-analytica/*

Sitios web

- ***The Conversation. (n.d.).*** Articles on Data Protection. The Conversation.
  • *https://theconversation.com/us/topics/data-protection-36720*

- ***The Conversation. (n.d.).*** Articles on Privacy. The Conversation.
  • *https://theconversation.com/us/topics/privacy-111*

Videos

- ***Karagiannis, K. [Black Hat]. (2015, April 3).*** Quantum Key Distribution and the Future of Encryption. (duración: 27:05) [Video] YouTube.
  • *https://www.youtube.com/watch?v=RrdTAURD1rI*
  Este video describe el cálculo cuántico y su impacto en la seguridad de datos y privacidad.

- ***Mueller, E. & Mueller, M. (2017, December 29).*** Clase: How Alice and Bob meet if they don't like onions. Survey of Network Anonymisation Techniques. 34th Chaos Communication Congress (duración: 61:52) [Video] Media.ccc.de.
  • *https://media.ccc.de/v/34c3-9104-how_alice_and_bob_meet_if_they_don_t_like_onions#t=34*
  Este video define qué es el anonimato, lo analiza, evalúa varias redes de comunicación anónimas e investigaciones actuales sobre esta área.

- ***NIST. (2018, May 18).*** Assessing Privacy Controls Workshop (duración: 57:17) [Video] NIST.
  • *https://www.nist.gov/news-events/events/2018/05/assessing-privacy-controls-workshop.*
  Este video incluye un panel del NIST que aborda la ingeniería privada y problemas de la gestión de riesgo, particularmente aquellos que se relacionan con controles de privacidad.

- ***NIST. (n.d.).*** What is the Internet of Things (IoT) and How Can we Secure it? (duración: 7:53) [Video] NIST.
  • *https://www.nist.gov/topics/internet-things-iot*
  Este video aborda la IdC y lo que se puede hacer para asegurarla.

- ***Privacy International. (2015, May 12).*** Big Data (duración: 4:48) [Video] YouTube.
  • *https://www.youtube.com/watch?v=HOoKhnvoYkU*
  Este video brinda una visión general sobre la big data, la manera en la que se recoge y analiza, por qué se busca, sus consecuencias y lo que se puede hacer con respecto a ella.

- ***Privacy International. (2015, May 12).*** Data Protection Explained (duración: 3:06) [Video] YouTube.
  • *https://www.youtube.com/watch?v=VUae3XgIZVU*
  Este video habla de lo que son los datos, por qué tienen valor, quiénes los controlan, cómo los controladores de datos los obtienen, qué es la legislación de protección de datos y qué hace, la variación en la legislación de protección de datos y por qué dicha legislación es importante.

- ***Privacy International. (2015, May 12).*** What is Privacy? (duración: 3:11) [Video] YouTube.
  • *https://www.youtube.com/watch?v=zsboDBMq6vo*
  Este video analiza qué es la privacidad, por qué es importante, cómo se recolectan los datos, cómo impacta la privacidad y qué se puede hacer para protegerla.

Conclusiones

Módulos del 6 al 10

Módulo 6: Aspectos prácticos de investigaciones de delitos cibernéticos y análisis forense digital

Los investigadores de delitos cibernéticos y los expertos en análisis forense digital manejan o, de alguna otra manera, procesan las pruebas digitales. Estos profesionales deben cumplir con las políticas nacionales y las directrices de mejores prácticas para garantizar la admisibilidad de las pruebas digitales en los tribunales. Dichas políticas incluyen los requisitos técnicos y legales necesarios para garantizar la admisibilidad de las pruebas. Además de estos requisitos, resulta esencial la armonización transfronteriza de la investigación de los delitos cibernéticos y las prácticas del análisis forense digital para las investigaciones, que a menudo implican a más de una jurisdicción (la cooperación internacional en asuntos de delitos cibernéticos se trata en Delitos Cibernéticos-Módulo 7: Cooperación internacional contra los delitos cibernéticos).

Módulo 7: Cooperación internacional contra los delitos cibernéticos

La doble incriminación y la armonización de las leyes de delitos cibernéticos nacionales, bilaterales, regionales y multilaterales son esenciales para la cooperación internacional. Incluso con la doble incriminación y las leyes armonizadas, la cooperación internacional para las investigaciones de delitos cibernéticos puede representar un problema. Lo que complica el asunto es la falta de recopilación, conservación e intercambio oportunos de pruebas digitales entre países mediante mecanismos formales de cooperación (p. ej., MLAT). Los países en el mundo también sufren un déficit de capacidad nacional para investigar delitos cibernéticos en términos de recursos humanos, financieros y técnicos (UNODC, 2013). Además de la ausencia o insuficiencia de fondos necesarios, también falta personal cualificado, equipos técnicos y herramientas para investigar delitos cibernéticos, realizar análisis forenses digitales universales, y establecer estándares y protocolos de pruebas que aseguren la admisibilidad de la prueba digital en los tribunales nacionales de los países cooperantes. Solo una intervención multidimensional dirigida a las áreas mencionadas anteriormente puede mejorar la cooperación internacional en asuntos de delitos cibernéticos.

Módulo 8: Seguridad cibernética y prevención del delito cibernético: estrategias, políticas y programas

Los Gobiernos, las organizaciones no gubernamentales, las instituciones académicas, las empresas y las personas usan ampliamente las tecnologías de la información y la comunicación (TIC). La actual interdependencia de los dispositivos y sistemas en todo el mundo, sumada a la importancia de las TIC para la seguridad económica y nacional de los países, y para el desarrollo nacional y mundial, exige una respuesta colectiva y armonizada de los países en todo el mundo. Las estrategias nacionales de seguridad cibernética se aplican para esbozar la forma en que se produce esta protección, incluidas las medidas que deben adoptarse y las organizaciones responsables de supervisar estas medidas. Existen métricas que pueden utilizarse para evaluar la eficacia de estas estrategias. Además, se dispone de herramientas y recursos que permiten a los países evaluar su postura de seguridad cibernética y ayudarlos a mejorar su postura en este ámbito.

Módulo 9: Seguridad cibernética y prevención del delito cibernético: aplicaciones y medidas prácticas

Las medidas de seguridad cibernética están diseñadas para proteger a las personas, propiedades, sistemas, redes, datos y recursos relacionados ante las amenazas. Estas medidas incluyen la prevención, identificación, respuesta y recuperación de los incidentes de seguridad cibernética. Se identifican los activos y se evalúan las amenazas, vulnerabilidades y riesgos antes de desarrollar e implementar las medidas de seguridad cibernética. Las investigaciones en materia de seguridad pueden ayudar a informar sobre el desarrollo de las medidas de seguridad cibernéticas nuevas y mejoradas. Las medidas de seguridad cibernética, a menudo, no consideran a las personas que las utilizan. Los seres humanos pueden facilitar o interferir con los esfuerzos de seguridad cibernética. Por esta razón, las medidas y los sistemas de seguridad cibernética efectivos necesitan ser creados de la mano de los individuos que los emplearán.

Módulo 10: Privacidad y protección de datos

Los datos juegan un papel importante en la comisión de muchos delitos cibernéticos y en las vulnerabilidades frente a los delitos cibernéticos. Aunque los datos brinden a sus usuarios (personas, empresas privadas, organizaciones y gobiernos) innumerables oportunidades, estos beneficios pueden ser (y han sido) explotados para algunos propósitos delictivos. Específicamente, la recolección, almacenamiento, análisis y difusión de datos permiten que se cometan muchos delitos cibernéticos, al igual que la gran recolección, almacenamiento, uso y distribución de datos sin el consentimiento informado de los usuarios ni las medidas legales y de protección necesarias. Es más, la acumulación, el análisis y la transferencia de datos ocurren en magnitudes para las que los Gobiernos y organizaciones no están preparados, lo que crea una serie de riesgos para la seguridad cibernética. La privacidad, la protección de datos y los sistemas de seguridad, redes y datos son interdependientes. Por lo tanto, para protegernos frente a los delitos cibernéticos, se necesitan medidas de seguridad que estén diseñadas para proteger los datos y la privacidad de los usuarios.

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Federal Ministry
Republic of Austria
European and International Affairs

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

UPC
Universidad Peruana de Ciencias Aplicadas