Número 10
Enero - Junio 2024
Publicación Semestral

ISSN 2992-7404

Universidad Veracruzana 1944 2024 80 Aniversario

Revista de la

# FACULTAD DE DERECHO
# UNIVERSIDAD VERACRUZANA


Universidad Veracruzana

U V FACULTAD DE DERECHO

# REVISTA DE LA FACULTAD DE DERECHO
# DE LA UNIVERSIDAD VERACRUZANA

Número 10, Enero- Junio de 2024



La Revista de la Facultad de Derecho de la Universidad Veracruzana, Año 6, número 10, Enero-Junio, de 2024 es una publicación semestral editada y distribuida por la Universidad Veracruzana a través de la Facultad de Derecho, Circuito Gonzalo Aguirre Beltrán S/N, Zona Universitaria, C.P. 91090, Xalapa-Enríquez, Veracruz, México. Con certificado de reserva de derechos al Uso Exclusivo, No. 04-2018050209552200-203, de fecha 2 de mayo de 2018, con certificado de reserva de derechos al Uso Exclusivo No. 04-2022-040514214800-102, de fecha 5 de abril de 2022, ambos otorgados por el Instituto Nacional del Derecho de Autor. La Revista de la Facultad de Derecho de la Universidad Veracruzana, es una publicación electrónica, que se rige por la política de libre acceso a la ciencia jurídica. ISSN 2992-7404, correo electrónico: rmonroy@uv.mx y página web: https://www.uv.mx/derecho/revista-de-la-facultad-de-derecho-de-la-universidad-veracruzana/. Coordinador del Comité editorial de la Facultad de Derecho y Coordinador responsable de la edición: Dr. Roberto Monroy García. Las opiniones expresadas por los autores no reflejan necesariamente la postura del Comité editorial de la Facultad de Derecho, ni del Consejo editorial de la Revista. Cada autor se hace responsable de la originalidad de los contenidos y de las opiniones sustentadas en cada uno de los artículos. Se prohíbe la reproducción en cualquier forma de los contenidos en texto o en imágenes de esta publicación sin la autorización expresa del Comité editorial de la Facultad de Derecho de Universidad Veracruzana. La consulta de esta publicación es gratuita.

# CIBERSEGURIDAD

Esperanza Sandoval Pérez[1]

Natalia Rayón Tenorio[**]

***RESUMEN:*** En este trabajo, se aborda el problema generado por el daño a los equipos informáticos al introducir un código malicioso llamado *malware* que incluye virus, gusanos o troyanos; con el propósito de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o el sistema operativo; con la finalidad de establecer medidas preventivas para evitar un ciberataque, aunado a que el Estado Mexicano carece de una legislación precisa en materia de ciberseguridad.

***Palabras clave***: ciberdelitos, ciberataque, ciberseguridad, delitos informáticos, *malware.*

***ABSTRACT:*** In this work, the problem generated by the damage to computer equipment by introducing a malicious code called malware that includes viruses, worms or Trojans is addressed; for the purpose of compromising the confidentiality, integrity or availability of data, applications or the operating system; with the purpose of establishing preventive measures to avoid a cyberattack, coupled with the fact that the Mexican State lacks precise legislation on cybersecurity.

***Keywords:*** cybercrime, cyberattack, cybersecurity, computer crime, malware.

[1]Licenciada en Derecho, especializada en Derecho Penal por el Instituto de Iberoamérica y Portugal de Salamanca-España, y en Delitos en Especial por la misma Universidad; Maestra en Ciencias Penales y Doctorada en Derecho Público por la Universidad Veracruzana; Doctora en Derecho Procesal por el Centro Mexicano de Estudios de Posgrado. Forma parte del SNI. Correo perasandoval@gmail.com, https://orcid.org/0000-0002-65 06-2507

** Cursante del 7°Semestre de la Licenciatura en Derecho de la U.V. Auxiliar de investigador Nacional, con NP. 57090, Diplomada Tecnologías de la Información y la Comunicación, Diplomada en Informática Forense, Participante en el Congreso CEEAD2024, sobre Educación Jurídica. Actualmente realiza investigación sobre la *Inseguridad de datos personales en posesión de terceros.* Correo natalia.rayon0411@gmail.com.

***SUMARIO***: Introducción. Aspectos generales y marco jurídico de la ciberseguridad; Amenazas; Investigación de delitos; El perito en informática forense; Toma de decisiones con base en evidencia. Conclusiones. Referencias.

## Introducción

A partir de la firma y ratificación del Convenio de Budapest (2001) hasta la época actual se busca por un lado armonizar las leyes nacionales y mejorar las técnicas de investigación de conductas criminales que para su comisión requieren el uso de herramientas digitales (computadora, celulares y otros dispositivos electrónicos que guardan la información, datos personales y las aplicaciones que el usuario elige, entre otras cosas. Todo experto en conocimientos técnicos e informáticos puede actuar de diferente forma, por ejemplo, quien utilice esos equipos como *medio* de comisión de un delito, que generalmente son de carácter patrimonial, deberá responden ante la Ley Penal, para el caso las entidades federativas los agrupan bajo el bien jurídico como delitos informáticos. En este trabajo, se aborda el problema generado por el daño a los equipos informáticos al introducir un código malicioso llamado *malware* que incluye virus, gusanos o troyanos; con el propósito de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o el sistema operativo; con el propósito de establecer medidas preventivas para evitar un *ciberataque,* aunado a que el Estado mexicano carece de una legislación precisa en materia de ciberseguridad.

En cuanto a la estructura de esta investigación primero se abordan los aspectos generales y marco jurídico de la ciberseguridad; en segundo lugar se determina la descripción del tipo penal requerido para sancionar al responsable del hecho criminal; en tercer lugar se analiza el procedimiento que deberá seguirse para la recolección de indicios, siguiendo las disposiciones de la cadena de custodia con la finalidad de obtener evidencia útil para que el Ministerio Publico cuente con el dato de prueba; en cuarto lugar se expone la intervención del experto en informática forense y el valor de su dictamen; en quinto lugar se explicar la determinación del Ministerio Publico conforme a lo dispuesto al Código Nacional

de Procedimientos Penales. Por último, se plantean las conclusiones y se enlistan las referencias.

## Aspectos generales y marco jurídico de la ciberseguridad

El mundo de la informática invita a conocer las Tecnologías de la información, la computación, el uso del internet y los dispositivos electrónicos; como la herramienta o medio a través del cual se facilitan las tareas de diversa naturaleza lo que se evidenció en la etapa de la pandemia que entre otros efectos despertó el interés de explorar el surgimiento, la evolución y el estado actual de estas herramientas, así como demás dispositivos electrónicos que en su aspecto negativo son el medio de comisión de ilícitos penales. Lo anterior reviste especial importancia en el ámbito jurídico ya que no obstante que los Códigos y Leyes penales sistematizan estas conductas atendiendo al bien jurídico tutelado como delitos informáticos.

En trabajos anteriores, Sandoval Pérez (2012) se introduce al estudio de la informática forense, el número creciente de usuarios, la frágil seguridad del sistema que da soporte electrónico a la custodia y generación de datos que se almacenan, difunden y distribuyen a través de medios electrónicos; que facilitan el acceso ilícito a bandejas de entrada y de salida, chats, videos pornográficos, extorciones, fraudes, secuestros; entre muchas otras conductas ya consideradas como delitos. Incursionando también en temas básicos para abordar la ciberseguridad, como es la trilogía investigadora del delito informático, nombre más común para referirse a estas conductas criminales; el perito informático y el subsecuente informe pericial y oros tópicos. Mientras que Muñoz Torres (2009) aborda la distinción del delito informático, telemático, computacional, cibernético y electrónicos.

Para abordar el tema es necesario primero hacer referencia artículo 16, párrafo segundo, de la Constitución Federal que establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición, en los términos que fija la *ley Federal de protección de datos personales en posesión de sujetos obligados*

(2017), en la cual se prevén supuestos de excepción a los principios que rigen el tratamiento de datos por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros. Derecho que se ha vulnerado por el uso indebido de la tecnología de la información y la comunicación (Tics), utilizada para atacar las redes, sistemas, datos, sitios web; entre otros, medios para la comisión de un hecho previsto en la ley como delito, surgiendo así los delitos informáticos que, en su descripción, identifican las herramientas tecnológicas como *medio de comisión* del delito.

Sin embargo, existen otras conductas antisociales graves, que se enfocan a la afectación de dichas herramientas a través de un malware para obtener un beneficio personal o directo, dañar los equipos de personas colectivas, empresas elegidas al azar que no obstante su gravedad no se encuentran elevadas a la calidad de delito, por lo que no es posible perseguir, procesar y sancionar al o los responsables como autores o participes del hecho criminal, independientemente de que exista una denuncia o una querella; por lo que su conducta queda impune y la víctima no recibe el resarcimiento de los daños causados a sus bienes jurídicos, en consecuencia es relevantemente indagar sobre la protección de una red informática de todo intruso, atacantes o programa malignos, oportunistas, para mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

En consecuencia, es necesario establecer que la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y datos de ataques maliciosos. También se conoce como seguridad de la información electrónica. El termino se aplica en diferentes contextos, desde los negocios hasta la informática móvil y puede dividirse en algunas categorías comunes como la seguridad de red, seguridad de aplicaciones y la seguridad de la información; orientada hacia la *prevención* general de las conductas (acciones u omisiones) que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como la

afectación del derecho previsto en el artículo constitucional, ya citado; con la pretensión de que las conductas criminales se tipifiquen en el derecho penal domestico facilitando la detección, investigación y sanción, tanto a nivel nacional como internacional, estableciendo disposiciones materiales que permitan una cooperación internacional rápida, fiable, reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.

El convenio sobre la ciberdelincuencia elaborado por el Consejo de Europa en Estrasburgo (Budapest, 2001) es el instrumento jurídico que sienta las bases para la lucha efectiva contra la ciberdelincuencia que exige la cooperación internacional reforzada, rápida y eficaz en materia penal, ante la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional, ya que surgieron profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas, causado el riesgo de que estas fueran utilizadas para cometer delitos y de que las pruebas relativas a dichos delitos fueran almacenadas y transmitidas por medio de dichas redes.

Este documento representa para México el compromiso de adecuar la normativa penal para evaluar y sintonizar la normatividad interna con las tendencias internacionales, tanto como de compartir nuestras mejores prácticas en este ámbito. El cuanto al marco jurídico se tiene como antecedentes las leyes, reglamentos y normativas vigentes en el Estado mexicano que son:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Telecomunicaciones y Radiodifusión.
- Normal Federal de Transparencia y Acceso a la Información Pública.
- Ley Federal del Derecho de Autor.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Ley General de Títulos y Operaciones de Crédito

- Código Penal Federal.
- Estrategia Nacional de Ciberseguridad 2017.
- Estrategia Nacional de Seguridad 2014-2018.

A partir de 2018, se han presentado diferentes iniciativas de leyes sobre ciberseguridad, ninguna ha llegado a concretarse, actualmente existe un proyecto de Ley Federal de Ciberseguridad propuesta por la Comisión de Ciencia y Tecnología e Innovación del Senado de la Republica que busca crear un criterio unificado y claro sobre ciberseguridad, que tiene cuatro planteamientos centrales:

1. Garantizar la seguridad nacional mediante la defensa del espacio digital;
2. Crear un marco legal que permita sancionar o tipificar los ciberataques;
3. La realización de pruebas de penetración o *pentesting* anualmente a las instituciones públicas y privadas; y,
4. Crear Agencia Nacional de Ciberseguridad controlada por el Ejecutivo, similar a los modelos seguidos por la Unión Europea, Estados Unidos y Brasil.

Recientemente, el gobierno federal anuncio la creación de una Comisión Intersecretarial de Tecnologías de Información y Comunicación (TIC), y de la Seguridad de la Información para sustituir la Comisión para el Desarrollo del Gobierno Electrónico creada en el 2005, con la finalidad de establecer cómo deben coordinarse e implementarse las políticas federales en materia de TICs y de seguridad de la información, impulsando actividades y estrategias para su aprovechamiento. Por ello, es probable que sus decisiones tengan impacto en el contenido precisa de la nueva ley de ciberseguridad.

## Amenazas

Una de las principales amenazas para los dispositivos tecnológicos utilizados para el teletrabajo es el *malware*, también conocido como código malicioso. Éste se define como cualquier programa informático que se coloca de forma oculta en un

dispositivo, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo.

Los tipos más comunes de amenazas de *malware* incluyen virus, gusanos, troyanos, rootkits y spyware, que pueden infectar cualquier dispositivo por medio del correo electrónico, los sitios web, las descargas y el uso compartido de archivos, el software punto a punto y la mensajería instantánea. Además, existen amenazas relacionadas con la ingeniería social como el *phishing, Smishing* y *Vishing*, por medio de las cuales los atacantes intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos:

a. El *Phishing* es un método de ataque a través del correo electrónico enviado por un delincuente pretendiendo ser otra persona, compañía o sitio de confianza, para robar la contraseña o información sensible. Este tipo de amenazas también pueden buscar tomar el control del dispositivo o computadora.
b. El *Smishing* ocurre cuando se recibe un mensaje de texto corto (SMS) al teléfono celular, por medio del cual se solicita al usuario llamar a un número de teléfono o ir a un sitio web.
c. El *Vishing* es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima.

Para la protección de la red Wi-Fi, la Secretaria de Comunicaciones y Tecnología, en la Guía sobre Ciberseguridad (2020), hace referencia a los expertos en informática forense quienes se han ocupado de la seguridad de esta red que es una importante medida de seguridad de las redes en el hogar. Es cada vez más común que los usuarios cuenten en casa con un ruteador inalámbrico para conectar sus dispositivos a Internet sin necesidad de cables. Para evitar que usuarios no autorizados se conecten de forma inalámbrica al ruteador y tengan la posibilidad de acceder a la conexión, e incluso al resto de los dispositivos

conectados y a la información que se transmite, es importante asegurar que la red cuente con contraseña que el usuario debe introducir al conectar por primera vez un dispositivo. Los ruteadores ofrecen varios tipos de contraseñas y cifrados (que codifican los datos del usuario, usando un valor o clave secreta y los hace incomprensibles para terceros), como los siguientes:

a) Las redes sin cifrado, o abiertas, son aquéllas que no tienen ninguna contraseña o cifrado y permiten a cualquier usuario conectarse. Una red con estas características no es recomendable.
b) El cifrado Wired Equivalent Privacy (WEP, por sus siglas en inglés) es considerado, hoy en día, un sistema poco seguro y no se aconseja su utilización ya que, con las herramientas y conocimientos adecuados, se puede llegar a conseguir la clave de acceso a la red Wi-Fi en pocos minutos.
c) El cifrado Wi-Fi Protected Access (WPA, por sus siglas en inglés), específicamente en su versión 2 (WPA2) o más actualizada, es considerado seguro y se recomienda comprobar que esté habilitado como parte de las medidas de seguridad de la red.

Para comprobarlo, es necesario entrar desde la computadora a las propiedades de la red, para ver el tipo de seguridad de la conexión. Se recomienda tener habilitada alguna de las variantes de WPA2, al menos. Puedes solicitar apoyo a tu proveedor de servicios de Internet para más orientación. Por lo que recomiendan cambiar las contraseñas predeterminadas en el ruteador por unas de elección del usuario, utilizando una contraseña robusta para la red *Wi-Fi*, también incluir incluya mayúsculas, minúsculas, números y símbolos. Cuanto mayor sea la longitud de la contraseña, más difícil será que un atacante pueda descubrirla.

Es importante evitar compartir la clave de la red Wi-Fi con otras personas, pues quien tenga acceso a tu red inalámbrica podría tener acceso a todos los dispositivos conectados a ella. Evitar la conexión a redes públicas abiertas (o *hotspots Wi-Fi*). Estas redes son totalmente inseguras ya que permiten que cualquier dispositivo se conecte al ruteador sin ningún tipo de seguridad, por lo que

cualquier usuario podría capturar la información se transmita a través de dicha conexión.

Las contraseñas protegen la información que contienen los dispositivos y cuentas de los usuarios. No obstante, ante la cantidad de claves y combinaciones que cotidianamente se deben utilizar, la mayoría de las personas opta por contraseñas fáciles de recordar por la comodidad que esto implica, o bien, por la falta de conocimiento de lo fácil que puede ser para un ciberdelincuente obtenerlas.

Para asegurar la efectividad de las contraseñas y evitar el robo de éstas, es recomendable poner en práctica las siguientes acciones:

1. Al generar las contraseñas de los dispositivos y cuentas se deben utilizar claves largas y únicas para cada caso, evitando utilizar la misma contraseña para diferentes dispositivos o cuentas.
2. Se deben evitar las combinaciones sencillas como fechas de nacimiento, secuencias consecutivas, repeticiones de un mismo dígito o palabras simples como *"password"* o "contraseña".
3. La mayor longitud de la contraseña, así como la incorporación de mayúsculas, minúsculas, números y caracteres especiales, contribuyen a que ésta sea más segura y difícil de vulnerar.
4. Se debe evitar escribir contraseñas en papeles o tener archivos con esa información que sean fácilmente accesibles para otros.
5. Habilitar el doble factor de autenticación o verificación en dos pasos. Esta medida es una capa adicional de seguridad disponible para cada vez más servicios en la que, además de la contraseña, durante el inicio de sesión se solicita información sobre otro medio al que sólo el usuario autorizado tiene acceso (por ejemplo, verificación para entrar al correo electrónico mediante la recepción de un código vía SMS, llamada o mensaje de WhatsApp).
6. Es importante no facilitar a nadie, aunque así lo solicite, por ningún medio, contraseñas y/o códigos para el inicio de sesión.
7. Es recomendable cambiar con frecuencia las contraseñas a efecto de evitar accesos no autorizados.

**Investigación de delitos**

Es importante recordar el término de trilogía investigadora que se refiere a la coordinación entre el Ministerio Público como investigador jurídico, a la policía como investigador fático y los peritos como investigadores técnicos; lo anterior para comprender la función de cada uno de ellos en materia de ciberseguridad; es decir que a partir de la noticia criminal informada al ministerio público, este debe dirigir la investigación con el apoyo de las policías y los servicios periciales, tal y como lo establece el artículo 21 constitucional que en parte relativa al tenor siguiente:

La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función. Entre las diligencias que lleva a cabo el ministerio público, es informar a la policía científica para que aplique sus conocimientos y lleve a cabo las acciones pertinentes en materia de investigación cibernética. Cuando se tiene que trabajar con evidencias y verificar que estas no hayan sido comprometidas física o lógicamente, se debe establecer una serie de cuidados y establecer lo que se conoce como cadena de custodia. Estos mecanismos van a permitir conservar las garantías de confiabilidad de una evidencia, ya que si una de estas no presenta las seguridades necesarias y sufre cambios del estado original como se recogió, pondrá en duda las futuras conclusiones que se extraigan de ella y así no tendrán la validez suficiente cuando vayan a ser incluidas como parte del procedimiento penal.

La cadena de custodia debe estar formada por varias etapas, bien descritas y con una correcta documentación desde el origen hasta el punto de llegada de dicha evidencia, las cuales se las puede detallar a continuación:

1. La identificación, extracción y registro de la evidencia. La evidencia debe ser bien identificada, indiferente del lugar de donde venga, sea un equipo informático llevado a un laboratorio, una escena de un delito, etc.

2. La preservación y almacenamiento de la evidencia. Se deben aplicar medidas de preservación de una determinada evidencia, garantizando la seguridad y el correcto almacenamiento de esta.

3. Los traslados a los que se vea sometida a la prueba, indicando tiempos, origen y destino para cada desplazamiento, así como, los posibles incidentes que puedan darse durante los mismos.

Los traspasos de posesión, qué son los cambios en la titularidad de la responsabilidad de la conservación de una evidencia, por ejemplo, si se entrega una evidencia a un compañero para que haga copias , la almacene o la traslade, dichos traspasos tienen que registrar cuando y donde tuvieron lugar, quién entregaba la evidencia y quién la recibida y el receptor deberá encargarse a partir de ese momento, tanto de la evidencia, como de su cadena de custodia y como no podía ser de otra forma las medidas de custodia y preservación de la evidencia que se apliquen también deben documentarse en la cadena de custodia, al fin y al cabo, la cadena de custodia es un registro cronológico de actividades, incidentes y responsabilidades respecto de cada evidencia.

Cada entrada en el registro, debe indicar quién tiene la evidencia, quién se la entregó cuando se la entregó, cómo y dónde se almacenó y que se hizo con ella, además, puede ser positivo, cuando se trate de evidencias físicas, adjuntar fotografías o incluso videos de los procesos en los que esta información multimedia puede aportar valor, como por ejemplo, durante la adquisición para mostrar el estado de las evidencias y durante los procesos a los que la sometan para demostrar que no varía su estado.

También es importante el llenado del formulario de cadena de custodia en el que se debe identificar, etiquetar y catalogar todos los dispositivos, involucrados real o potencialmente en el incidente, esto incluye:

I. Ordenadores.
II. Portátiles.
III. Tabletas.
IV. Smartphones.
V. Impresoras y otros dispositivos.

Estos dispositivos se pueden encontrar en dos situaciones: encendidos o apagados. Se denomina coloquialmente análisis postmortem al que se practica sobre equipos que se encuentran apagado, tradicionalmente se apagaban los equipos para preservar las evidencias y eliminar riesgo de modificación, pero entonces, se podía perder información volátil. El objetivo principal de este tipo de análisis es la recuperación de datos de las unidades de memoria como discos duros o memoria USB. Se llama e-Discovery al proceso de capturar y analizar grandes cantidades de datos para descubrir evidencias entre ellos, al ser una forma de adquisición masiva de datos, suele darse en incidentes graves y grandes o relacionados con grandes infraestructuras, puede involucrar decenas o cientos de equipos, sistemas raid, etc., el objetivo no es tanto localizar información oculta, cómo detectar información relevante entre la masa total de datos disponibles, este trabajo puede gestionarse mediante técnicas de Big Data.

El análisis de equipos en vivo es el que se practica cuando se encuentra con una computadora o un servidor encendido, en lugar de apagado. Es típico de respuestas a brechas de seguridad en redes o equipos y busca la captura de datos reales en vivo, tiene ciertas ventajas sobre los escenarios postmortem, como el acceso a disco cifrados, el volcado de memoria RAM, el acceso archivos temporales, etc.,

## El perito en informática forense

El objetivo principal de la informática forense es generar evidencias licitas para el procedimiento penal, las evidencias desde el punto de vista que ocupa, son el conjunto de recursos y datos a los que ha tenido acceso un perito para extraerlos, analizarlos, verificar su autenticidad y poder así responder a las cuestiones técnicas planteadas por la parte que le contrate o por un tribunal. La informática forense permite dar solución a problemas relacionados con la seguridad de la información, con el objetivo de salvaguardar la información digital, en el caso de haber ocurrido un delito, utilizando como medio al computador o algún equipo digital.

Fases de peritaje

1. Adquisición.
2. Análisis.
3. Presentación.

Cada fase podría extenderse agrupando las actividades en cinco etapas que se detallan a continuación:

*Preparación*. La primera es prepararse para una investigación, que empieza incluso antes de ser contratados o de que ocurra un incidente, ya que la preparación incluye formación, mantenimiento de equipos, recursos, reciclaje, además de preparación específica en función del incidente a atender.

*Adquisición*. La segunda fase es la de adquisición de datos, que se realizan bien en la escena del incidente, en el laboratorio, si es allí donde llevan los equipos afectados o involucrados en un incidente.

*Análisis*. El análisis de datos es el siguiente paso, consiste en indexar, dar forma y comprender la información pertinente para la investigación de entre todo el conjunto de datos adquiridos en la fase previa.

*Identificación de evidencias*. La identificación de evidencias es la cuarta etapa y consiste en señalar de todo lo adquirido y analizado, que es lo relevante para el caso en el que se trabaja, lo que, en caso de declaración ante un tribunal, se tendría que explicar y defender.

Por último, está la generación del informe de conclusiones o informe pericial, en el que se detallan todas las actividades del proceso de investigación y las conclusiones obtenidas respecto a la información disponible y a las preguntas que el contratista formulase. El trabajo forense o peritaje, tiene que ser de carácter científico, no subjetivo, el perito debe responder a preguntas de tipo técnico planteadas por su contratista, sea una parte involucrada en un incidente o por un tribunal.

El perito no debe valorar, por ejemplo, si la acción de una persona es constitutiva de delito, sino, localizar o verificar las evidencias que permitan a los juristas comprender los aspectos de la tecnología que escapan a su conocimiento y así poder tomar esa decisión de forma razonada. Al fin y al cabo, la ciencia forense es la aplicación de conocimientos, métodos y técnicas de investigación científica

que buscan determinar la veracidad de unos hechos, su origen y su autoría. En informática forense una gran parte del trabajo consiste en verificar la veracidad de la información, ya que las evidencias digitales son fácilmente modificables, incluso pueden ser evidencias totalmente inventadas, confirmada la veracidad objetiva de una evidencia, el trabajo consiste en el cómo y cuándo es posible en el quién y cuándo se habla de quién, se puede referir no sólo a personas, quizá sea a equipos, a cuentas de servicios online, etc., que otros profesionales deberán vincular con una persona.

La prueba pericial es el testimonio del perito en la audiencia del juicio oral, esto implica que esta es la información que proporciona la persona experta; la simple presencia o existencia de un perito no origina prueba, son los datos sobre el peritaje que realizo lo que ayuda al órgano jurisdiccional a generar convicción para efecto de la sentencia (Romero, 2014).

**Toma de decisiones con base en evidencia**

De acuerdo con el Código Nacional de Procedimientos Penales el Ministerio Público podrá abstenerse de investigar, cuando los hechos relatados en la denuncia, querella o acto equivalente no fueren constitutivos de delito o cuando los antecedentes y datos suministrados permitan establecer que se encuentra extinguida la acción o la responsabilidad penal del imputado, lo cual deberá fundar y motivar. Las maneras de abstención de la investigación son:

1. Archivo temporal. El Ministerio Público podrá archivar temporalmente aquellas investigaciones en fase inicial en las que no se encuentren antecedentes, datos suficientes o elementos de los que se puedan establecer líneas de investigación que permitan realizar diligencias tendentes a esclarecer los hechos que dieron origen a la investigación. El archivo subsistirá en tanto se obtengan datos que permitan continuarla a fin de ejercitar la acción penal (artículo 254).

2. No ejercicio de la acción. Antes de la audiencia inicial, el Ministerio Público previa autorización del Procurador o del servidor público en quien se delegue la facultad, podrá decretar el no ejercicio de la acción penal cuando de los antecedentes del caso le permitan concluir que en el caso concreto se actualiza

alguna de las causales de sobreseimiento previstas en este Código. La determinación de no ejercicio de la acción penal, para los casos del artículo 327 del presente Código, inhibe una nueva persecución penal por los mismos hechos respecto del indiciado, salvo que sea por diversos hechos o en contra de diferente persona (artículo 255).

Por otra parte, si el ministerio público reúne los suficientes datos de prueba tendrá la oportunidad para formular la imputación a personas detenidas. La formulación de la imputación es la comunicación que el Ministerio Público efectúa al imputado, en presencia del Juez de control, de que desarrolla una investigación en su contra respecto de uno o más hechos que la ley señala como delito.

En el caso de detenidos en flagrancia o caso urgente, después que el Juez de control califique de legal la detención, el Ministerio Público deberá formular la imputación, acto seguido solicitará la vinculación del imputado a proceso sin perjuicio del plazo constitucional que pueda invocar el imputado o su Defensor. En el caso de que el Ministerio Público o la víctima u ofendido o el Asesor jurídico solicite una medida cautelar y el imputado se haya acogido al plazo constitucional, el debate sobre medidas cautelares sucederá previo a la suspensión de la audiencia.

El imputado no podrá negarse a proporcionar su completa identidad, debiendo responder las preguntas que se le dirijan con respecto a ésta y se le exhortará para que se conduzca con verdad. Se le preguntará al imputado si es su deseo proporcionar sus datos en voz alta o si prefiere que éstos sean anotados por separado y preservados en reserva. Si el imputado decidiera declarar en relación con los hechos que se le imputan, se le informarán sus derechos procesales relacionados con este acto y que lo que declare puede ser utilizado en su contra, se le cuestionará si ha sido asesorado por su Defensor y si su decisión es libre. Si el imputado decide libremente declarar, el Ministerio Público, el Asesor jurídico de la víctima u ofendido, el acusador privado en su caso y la defensa podrán dirigirle preguntas sobre lo que declaró, pero no estará obligado a responder las que puedan ser en su contra. En lo conducente se observarán las reglas previstas en este Código para el desahogo de los medios de prueba (artículo 309).

## Conclusiones

La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito;

La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos.

De la breve explicación que se hace en este trabajo a la luz de los conocimientos adquiridos durante el diplomado en ciberseguridad, en el cual la participación de los cursantes aportaron sus conocimientos prácticos, de la doctrina consultada se concluye que hasta ahora no existe un proyecto consolidado para crear y determinar, con base en la problemática actual que se expone un tipo que haga referencia al bien jurídico tutelado, los sujetos (activo y pasivo), el nexo causal, resultado y circunstancias de modo y tiempo para sancionar estas conductas que hasta ahora solo quedan en el espacio socio- criminal y la victima en estado vulnerable, sin derecho a obtener la reparación integral del daño que le ha causado la conducta (acción u omisión) del responsable en términos de los que disponen tanto las leyes sustantivas como adjetivas penales.

## Referencias

Centeno *Dabya.* (2018) México y el Convenio de Budapest: Posibilidades Incompatibilidades. México, Derechos digitales.

Código Nacional de Procedimientos Penales.

Constitución Política de los Estados Unidos Mexicanos.

Convenio de Ciberseguridad. (2001). Serie de Tratados Europeos- No. 185. Budapest. Disponible en:

https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Muñoz. T. I. (2009). Delitos informáticos. México: UBIJUS.

Romero, C. et al. (2020). La informática forense desde un enfoque práctico. Ecuador: UNESUM.

Romero, G. A. (2014). Estudios sobre la prueba pericial en el juicio oral mexicano. México: Instituto de Investigaciones jurídicas UNAM.

Sandoval, P. E. (2015). Ciencias forenses (especialidades científicas). México: Porrúa.

SCT. (2020). Guía de Ciberseguridad. México: SEGOB.