
VI
CONGRESO
INTERNACIONAL
EN INVESTIGACIÓN
CRIMINAL
Tendencias de la
Investigación Criminal
en la era digital 4.0
25 NOV
2022

MEMORIAS DEL VI CONGRESO EN INVESTIGACIÓN CRIMINAL:
TENDENCIAS DE LA INVESTIGACIÓNCRIMINAL EN LA ERA DIGITAL 4.0

Olga Patricia Parra Sarmiento

Rectora Fundación de Educación Superior Alberto Merani

Daniel Alejandro Rivera Marín

Coordinador de Programa

Tecnología en investigación criminal y ciencias forenses

María Isabel Otero Cubillos

Compiladora

Angie Lorena Palomino Pinto

Coordinadora de promoción institucional

Carlos Alberto Gómez García

Diseño gráfico y diagramación

Fundación de Educación Superior Alberto Merani

Editor

Teléfono: (57) 601 725 6492

Dirección: Calle 73 # 20 B - 19

Correo: gestioninvestigacion@umerani.edu.co

Bogotá, D.C. 2024

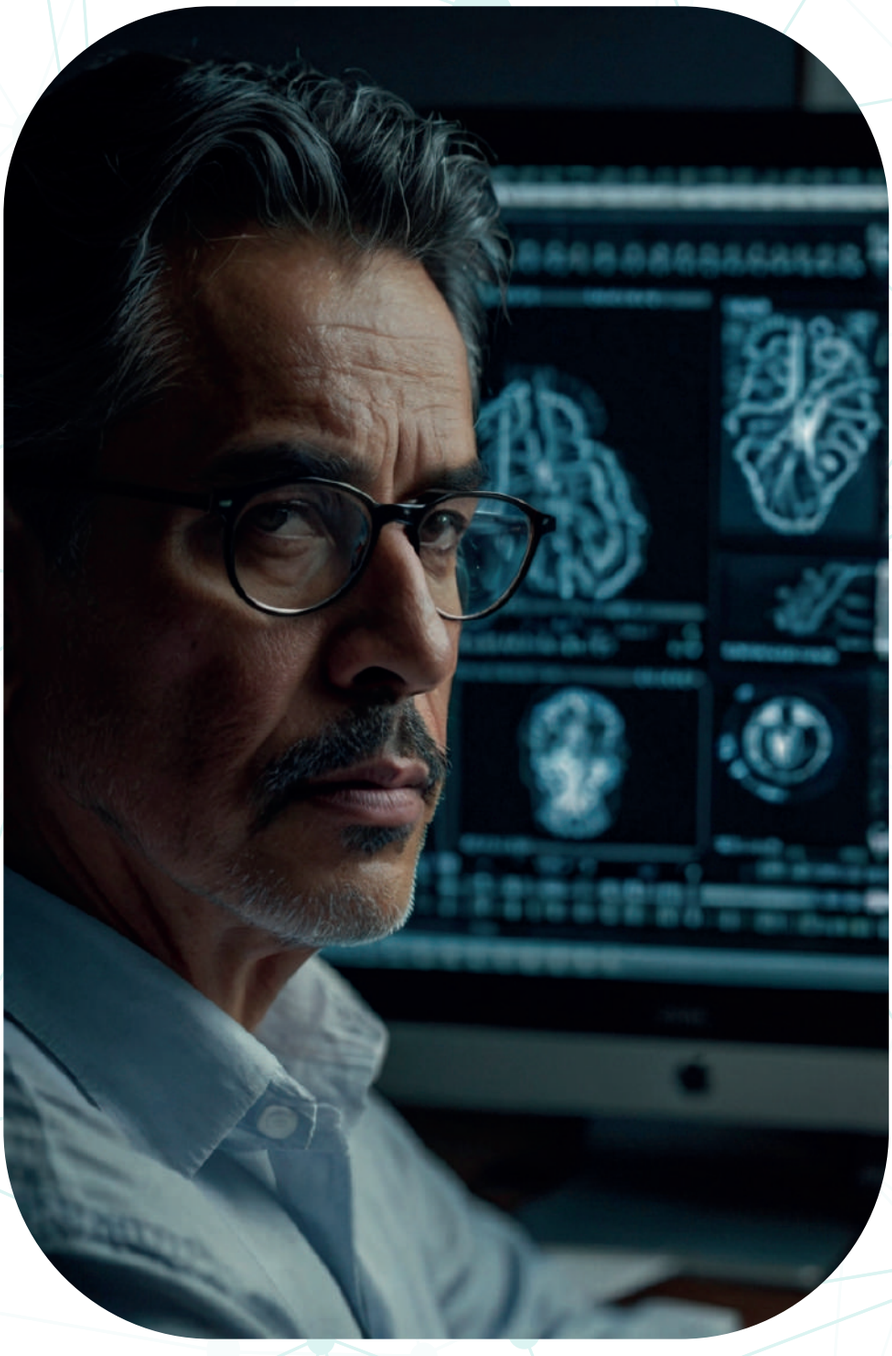
MERANI
Fundación de Educación Superior
Alberto Merani

INTRODUCCIÓN

La Fundación de Educación Superior Alberto Merani reafirma su liderazgo en la formación de tecnólogos en investigación criminal y ciencias forenses con la realización del Congreso Internacional de Criminalística, ya en su sexa edición.

El tema de este año, *"Tendencias de la Investigación Criminal en la era digital 4.0"*, se desarrolló en torno a los ejes temáticos Ciberdelito, Ciberseguridad e Innovación Forense en el mundo digital.

Se contó con la valiosa participación de expertos de talla internacional de Colombia, Ecuador, España, Honduras, México y Panamá. Todos ellos compartieron sus conocimientos, experiencias y recomendaciones acerca de este tema de total actualidad que atañe a todas las personas y a todas las sociedades contemporáneas.



DICTAMEN PERICIAL: LA INVESTIGACIÓN CRIMINAL EN LA ERA DIGITAL

BERNARDO TRUJILLO - Colombia

Asesor del International Criminal Investigative Training Assistance Program.
Asesor de seguridad, investigación criminal, experto en criminalística, ciencia política, criminología y victimología.
Coronel en retiro de la Policía Nacional tras 27 años de servicio activo en la Policía Nacional. Se desempeñó por más de 20 años en investigación criminal y criminalística en la dirección de antinarcóticos a cargo de varios grupos especiales de investigación y en la dirección de investigación criminal Interpol. También fue jefe del área de Policía científica y criminalística de la DIJIN y director de la Escuela de Investigación Criminal de la Policía Nacional.

La investigación criminal y el análisis forense en la era digital son temas fundamentales para la administración de justicia moderna. En un mundo cada vez más interconectado, donde la tecnología permea todos los aspectos de la vida, es crucial entender cómo estos campos se han adaptado y evolucionado para enfrentar los desafíos contemporáneos.
La investigación criminal se define como el conjunto de actividades de recolección, procesamiento de información y procedimientos técnico-científicos que apoyan a la administración de justicia en el esclarecimiento de hechos presuntamente delictivos. Su objetivo principal no es prevenir el delito, sino aportar los elementos probatorios necesarios para que las autoridades judiciales determinen si un hecho constituye o no un delito y, en caso afirmativo, establezcan responsabilidades.
En el contexto actual, la investigación criminal no puede concebirse sin tener en cuenta el componente digital. Los sistemas de información y las bases de datos han reemplazado en gran medida los métodos tradicionales de registro y gestión de casos. Esta digitalización ofrece ventajas en términos de eficiencia y acceso a la información, pero también plantea nuevos retos en materia de seguridad y protección de datos sensibles.
El dictamen pericial juega un papel crucial en la investigación criminal moderna. Se trata del estudio realizado por un experto en determinada materia, cuyas conclusiones se plasman en un informe estructurado según formatos estandarizados. Este dictamen debe cumplir con ciertas características esenciales: objetividad, detalle, claridad y precisión. Además, debe fundamentarse en criterios técnicos y científicos reconocidos por la comunidad especializada.
La importancia del dictamen pericial radica en su capacidad para aportar elementos probatorios sólidos que ayuden a confirmar o descartar hipótesis delictivas. En el sistema judicial actual, donde prima el principio de contradicción, el perito no solo debe elaborar su informe, sino también estar preparado para sustentarlo oralmente en una audiencia pública. Esto implica que el experto debe ser capaz de explicar sus hallazgos y metodología de manera clara y convincente, resistiendo el escrutinio y posibles cuestionamientos de las partes involucradas en el proceso.

Un aspecto fundamental en la elaboración y valoración de dictámenes periciales es la gestión de calidad. En el mundo forense contemporáneo, la implementación de sistemas de gestión de calidad se ha vuelto imprescindible para garantizar la confiabilidad y validez de los resultados obtenidos. Esto implica la adopción de estándares internacionales como las normas ISO 9001, 17025 y 17020, que establecen requisitos para los sistemas de gestión de calidad, los laboratorios de ensayo y calibración, y los organismos de inspección, respectivamente.

La gestión de calidad en el ámbito forense abarca diversos aspectos, desde la calibración y mantenimiento de equipos hasta la documentación detallada de procedimientos y la trazabilidad de las evidencias. Un punto crítico es la certificación de los peritos y la acreditación de los laboratorios. La certificación valida la competencia individual de los expertos, mientras que la acreditación garantiza que los laboratorios cumplen con estándares internacionales en sus procesos y métodos de análisis.

La implementación de estos sistemas de calidad no solo mejora la confiabilidad de los resultados, sino que también fortalece la posición de los dictámenes periciales frente a posibles cuestionamientos en el ámbito judicial. Un dictamen respaldado por un sistema de gestión de calidad robusto tiene menos probabilidades de ser impugnado o desestimado por cuestiones procedimentales o técnicas.

En el contexto de la era digital, la investigación criminal y el análisis forense han tenido que adaptarse rápidamente para hacer frente a nuevas formas de delincuencia y a la creciente complejidad de las evidencias digitales. La informática forense se ha convertido en una disciplina fundamental, abarcando desde el análisis de dispositivos electrónicos hasta la investigación de ciberdelitos.

Los principios rectores de la investigación criminal, como la dignidad humana, la legalidad, la presunción de inocencia y el derecho a la defensa, siguen siendo fundamentales en la era digital. Sin embargo, su aplicación en el contexto tecnológico actual plantea nuevos desafíos éticos y jurídicos que deben ser abordados con cuidado.

La formación continua y la actualización de conocimientos son imperativos para los profesionales del campo forense en la era digital. Las técnicas y herramientas evolucionan rápidamente, y los investigadores deben mantenerse al día con las últimas tendencias y desarrollos tecnológicos para poder enfrentar eficazmente los desafíos que plantea la criminalidad moderna.

En conclusión, la investigación criminal y el análisis forense en la era digital se enfrentan a un panorama complejo y en constante evolución. La integración de tecnologías avanzadas, la adopción de estándares internacionales de calidad y la adaptación a nuevas formas de evidencia digital son fundamentales para mantener la eficacia y credibilidad de estos campos en el sistema de justicia contemporáneo. El éxito en la resolución de casos y la administración de justicia dependerá cada vez más de la capacidad de los profesionales forenses para navegar este nuevo paisaje tecnológico, manteniendo siempre los principios éticos y legales que fundamentan su labor.

CIBERDELINCUENCIA Y ATAQUES INFORMÁTICOS

YURI COELLO – Honduras

Ingeniero de sistemas con 17 años de experiencia en redes, infraestructura y seguridad informática, descubriendo y subsanando las debilidades en seguridad de la infraestructura de la Información de importantes entidades y sectores como policía, gobierno, telecomunicaciones, banca e industria. Tiene experiencia y certificación en más de diez diferentes marcas de proveedores de soluciones de seguridad de las tecnologías de la información, así como en diseño e implementación, capacitación, mantenimiento y soporte técnico de la arquitectura de seguridad de las tecnologías de la información en empresas grandes y medianas.

La ciberdelincuencia y los ataques informáticos representan una amenaza creciente en el mundo digital actual. Este artículo examina los factores que contribuyen a la vulnerabilidad de los sistemas informáticos, las responsabilidades de los proveedores de servicios de Internet (ISP) y las mejores prácticas para mejorar la seguridad cibernética.

Factores de vulnerabilidad

Varios factores contribuyen a la vulnerabilidad de los sistemas informáticos. La apertura y conectividad generalizada de dispositivos crean numerosos vectores de ataque. La ignorancia sobre los riesgos de seguridad, tanto entre usuarios comunes como entre profesionales de TI, agrava el problema. La creciente complejidad de los sistemas y la falta de vigilancia adecuada de los registros de eventos también aumentan la exposición a amenazas.

La seguridad informática a menudo no recibe la importancia necesaria, lo que resulta en presupuestos limitados y personal insuficiente o no calificado para manejar las tareas de seguridad. Esto puede llevar a una falta de conciencia sobre los peligros potenciales y una respuesta inadecuada a las amenazas.

Rol de los proveedores de servicios de Internet (ISP)

Los ISP desempeñan un papel crucial en la seguridad cibernética. Además de proporcionar acceso a Internet, son responsables de la señalización y priorización del tráfico de red. Sin embargo, su rol en la seguridad suele ser pasivo. Los ISP tienen la capacidad de monitorear el tráfico de red y detectar actividades sospechosas, pero a menudo no toman medidas proactivas para proteger a sus usuarios.

Es importante destacar que los ISP pueden ver todos los equipos conectados en una red doméstica u oficina, lo que representa una vulnerabilidad potencial. Esta capacidad de monitoreo plantea preocupaciones sobre la privacidad y la seguridad de los datos de los usuarios.

Mejores prácticas de seguridad

Entre las mejores prácticas para mejorar la seguridad cibernética se cuentan la identificación y comprensión todos los equipos y sistemas en la infraestructura de red (identificación de activos), la evaluación exhaustiva de los riesgos y vulnerabilidades potenciales de cada activo, la implementación de controles de seguridad (utilizar firewalls, sistemas de prevención de intrusiones -IPS- y cortafuegos de aplicaciones web -WAF- para proteger la infraestructura), el diseño y cumplimiento de políticas de seguridad sólidas (incluyendo el principio de menor privilegio para los usuarios), la vigilancia continua mediante un sistema de monitoreo constante de los registros de eventos y actividades sospechosas, la aplicación de un plan de respuesta a incidentes para abordar rápidamente las amenazas de seguridad y la educación y concienciación mediante la capacitación regular de los usuarios y del personal de TI sobre las mejores prácticas de seguridad y las amenazas emergentes.

Desafíos actuales en seguridad cibernética

Entre los desafíos actuales en el campo de la seguridad cibernética que merecen especial atención se cuentan los ataques automatizados a través de bots y sistemas automatizados cuya detección y prevención se dificulta por ser persistentes e imperceptibles; la seguridad SSL comprometida a causa de las conocidas vulnerabilidades del protocolo que pueden ser explotadas por atacantes; el alto porcentaje de páginas web infectadas parcial o totalmente, lo que facilita la propagación de malware; las contraseñas débiles (cortas o simples) que son fácilmente descifradas por los sistemas modernos de ataque; las amenazas internas provenientes de empleados descontentos o malintencionados que pueden representar un riesgo significativo para la seguridad de una organización; y las tecnologías emergentes (como blockchain) que, a pesar de sus promesas de seguridad, pueden tener vulnerabilidades no descubiertas.

Conclusiones y recomendaciones

La seguridad cibernética es un desafío en constante evolución que requiere un enfoque holístico y proactivo. Las organizaciones deben priorizar la seguridad en todos los aspectos de sus operaciones digitales, desde la selección y configuración de equipos hasta la capacitación de los empleados.

Es fundamental mantener una vigilancia constante y adaptarse rápidamente a las nuevas amenazas. La implementación de sistemas de análisis de comportamiento de usuarios puede ayudar a identificar actividades sospechosas y prevenir amenazas internas.

Las organizaciones deben ser cautelosas al implementar nuevas tecnologías y no confiar ciegamente en las afirmaciones de seguridad sin una evaluación rigurosa. La seguridad absoluta es inalcanzable, por lo que es crucial mantener un enfoque de mejora continua y estar preparado para responder eficazmente a los incidentes.

Finalmente, es importante considerar las implicaciones más amplias de nuestra creciente dependencia de la tecnología y la conectividad. Mientras que la interconexión ofrece numerosos beneficios, también aumenta nuestra exposición a riesgos de seguridad. Las organizaciones y los individuos deben sopesar cuidadosamente los beneficios y los riesgos de la conectividad y tomar decisiones informadas sobre su uso de la tecnología.

En última instancia, la seguridad cibernética es una responsabilidad compartida que requiere la colaboración de proveedores de servicios, organizaciones e individuos. Solo a través de un esfuerzo colectivo y una conciencia constante podremos hacer frente a los desafíos de seguridad en el mundo digital actual.

INVESTIGACIÓN CRIMINAL EN LA ERA 4.0 EN MÉXICO

SADI KURI MARTINEZ - México

Es licenciado en derecho, magíster en criminalística y cuenta con un estudio diplomado en sistemas integrales de inteligencia policial. Es docente de diversas materias relacionadas con el derecho penal y la investigación criminal en universidades como la Panamericana Campus Aguascalientes de México, el Instituto de Formación Profesional de la Secretaría de Seguridad Pública del Municipio de Aguascalientes en México, el Instituto de Profesionalización de la Procuraduría General de Justicia de Guanajuato, el Instituto Estatal de Seguridad Pública de Aguascalientes y la Comisión Internacional contra la Impunidad en Guatemala. Así mismo, cuenta con 13 años de experiencia como Servidor Público en la Fiscalía General de Justicia del Estado de Aguascalientes y es investigador legal en la Comisión Internacional contra la Impunidad en Guatemala de la ONU.

La era 4.0, también conocida como la Cuarta Revolución Industrial, ha traído consigo importantes desafíos y oportunidades en el ámbito de la investigación criminal. Este nuevo paradigma tecnológico, caracterizado por la interconexión digital, el Internet de las Cosas, la nube, los sistemas ciberfísicos y la robótica, está transformando radicalmente los métodos y herramientas utilizados en la resolución de delitos.

La investigación criminal en la era 4.0 requiere una adaptación constante a las nuevas tecnologías y una comprensión profunda de sus implicaciones. Se define como una serie de pasos sistemáticos y metodológicamente organizados, llevados a cabo por un grupo multidisciplinario coordinado por un experto en derecho, con el objetivo de llegar a la verdad histórica de los hechos. Este enfoque multidisciplinario es crucial, ya que la complejidad de los delitos en la era digital exige la colaboración de expertos en diversas áreas, desde la informática forense hasta la psicología criminal.

Un aspecto fundamental de la investigación criminal en la era 4.0 es la gestión de la información digital. La intangibilidad de los datos y la facilidad con la que pueden ser manipulados o transferidos plantean nuevos retos para los investigadores. Por ejemplo, el acceso remoto y el Internet de las Cosas permiten controlar dispositivos a distancia, lo que puede ser utilizado tanto para fines legítimos como delictivos. Esto requiere que los investigadores desarrollen nuevas habilidades y utilicen herramientas especializadas para rastrear y analizar estas interacciones digitales.

La evolución de las tecnologías de la información ha sido vertiginosa en las últimas décadas. Desde la mecanización y la producción en masa hasta la automatización y, finalmente, la era digital actual, cada etapa ha traído consigo nuevos desafíos para la investigación criminal. En este contexto, es crucial que las instituciones de seguridad y justicia se mantengan actualizadas y adopten rápidamente las nuevas tecnologías para no quedar rezagadas frente a la delincuencia.

En el caso específico de México, se han implementado iniciativas como la Plataforma México y los centros de comando, control, comunicación y cómputo (C4), posteriormente evolucionados a C5I (incluyendo inteligencia e innovación). Estos proyectos buscan centralizar y compartir información entre diferentes agencias de seguridad, mejorando la coordinación y la eficacia en la lucha contra el crimen. Sin embargo, su implementación ha enfrentado desafíos, principalmente relacionados con la resistencia al cambio, la falta de capacitación y la corrupción.

La adopción de tecnologías avanzadas como la videovigilancia de alta definición plantea nuevas cuestiones legales y éticas. Es necesario desarrollar marcos normativos que regulen el uso de estas tecnologías, equilibrando la necesidad de seguridad con el respeto a la privacidad de los ciudadanos. Esto requiere una colaboración estrecha entre legisladores, expertos en tecnología y profesionales de la seguridad pública.

Las políticas públicas juegan un papel crucial en la implementación efectiva de la investigación criminal en la era 4.0. Estas deben basarse en diagnósticos precisos y análisis de factibilidad, considerando tanto las oportunidades como los riesgos que presentan las nuevas tecnologías. Es fundamental que estas políticas sean flexibles y adaptables, capaces de evolucionar al ritmo del cambio tecnológico.

Un desafío importante es la tendencia a priorizar el equipamiento tradicional sobre la inversión en tecnología avanzada. Mientras que la adquisición de vehículos, armas y equipo de protección es importante, es igualmente crucial invertir en herramientas tecnológicas que permitan una investigación criminal más eficiente y efectiva en la era digital.

La delincuencia ha demostrado una gran capacidad de adaptación a las nuevas tecnologías, utilizándolas para desarrollar métodos más sofisticados de cometer delitos. Esto hace imperativo que los investigadores criminales no solo se mantengan al día con las últimos avances tecnológicos, sino que también desarrollen la capacidad de anticipar cómo estos podrían ser utilizados con fines delictivos.

La formación continua y especializada de los investigadores criminales es esencial en este nuevo contexto. Las instituciones educativas y las academias de policía deben actualizar sus programas de estudio para incluir competencias digitales avanzadas, análisis de big data, ciberseguridad y otras habilidades relevantes para la era 4.0.

La colaboración internacional se vuelve cada vez más importante en la investigación criminal de la era digital. Los delitos cibernéticos a menudo trascienden las fronteras nacionales, lo que requiere una cooperación estrecha entre agencias de diferentes países. El intercambio de información, mejores prácticas y recursos tecnológicos puede mejorar significativamente la capacidad de los investigadores para enfrentar estos desafíos globales.

En conclusión, la investigación criminal en la era 4.0 presenta tanto oportunidades como desafíos significativos. La adopción de nuevas tecnologías, la formación de equipos multidisciplinarios, la actualización constante de las habilidades y conocimientos, y el desarrollo de marcos legales y éticos apropiados son elementos clave para el éxito en este nuevo paradigma. Es fundamental que las instituciones de seguridad y justicia reconozcan la importancia de adaptarse rápidamente a este entorno cambiante, invirtiendo en tecnología y capital humano para mantenerse a la vanguardia en la lucha contra el crimen en la era digital. Solo a través de un enfoque proactivo y adaptativo se podrá cerrar la brecha entre la delincuencia y la justicia, garantizando una sociedad más segura en la era de la Cuarta Revolución Industrial.

CIBERDERECHO APLICADO A LA INVESTIGACIÓN CRIMINAL

JUAN DAVID CARDONA - Colombia

Director general de Arcont Group SAS y ciberabogado de Soluciones Digitales Forenses. Es presidente del Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad, así como de la IAI División Colombia en el subcomité de Informática Forense. Además, es conferencista internacional en derecho de la ciberseguridad y entornos digitales, y en derecho internacional humanitario, docente universitario en pregrado y posgrado en la Universidad Autónoma de México, la Universidad Vizcaya de las Américas, el Ministerio del Interior del Perú y la Universidad de los Libertadores, entre otras instituciones. Es exdetective de la República y exfuncionario de la Fiscalía General de la Nación de Colombia y del Departamento Administrativo de Seguridad (DAS), donde laboró por más de 16 años.

Cada uno de nosotros, como ciudadanos digitales, tiene responsabilidades, derechos y deberes que cumplir, y es fundamental que esos derechos fundamentales digitales sean respetados.

Para enfocarnos en el ciberderecho aplicado a la investigación criminal es necesario hablar sobre el derecho penal, los delitos informáticos, la evidencia digital y la informática forense. Se debe entender el concepto de evidencia digital y su diferencia con un equipo electrónico; qué es realmente la evidencia digital, y cómo esta es crucial para llegar al ciberdelincuente y materializar una investigación en el ciberespacio.

Los delitos informáticos no se limitan a los contemplados en la ley 1273 del 2009 en Colombia. Todos los países de Iberoamérica, salvo México, han adherido al Convenio de Budapest. Aunque México ya lo ratificó, todavía no se ha adherido. Este convenio proporciona herramientas para combatir la ciberdelincuencia y lograr una mayor efectividad en las investigaciones y la defensa desde el litigio penal.

Al llevar la digitalidad al derecho, la migración de lo análogo a lo digital también afecta al derecho laboral, civil, comercial, administrativo e incluso disciplinario.

¿Existe responsabilidad penal para los entes dotados de inteligencia artificial? Para hablar de la investigación criminal en el ciberderecho, es necesario romper paradigmas. En el pasado, se debatía sobre la responsabilidad penal de las personas jurídicas. A pesar de las críticas, Europa finalmente aceptó esta responsabilidad sin necesidad de modificar la teoría del delito, solo con

algunos ajustes. Ahora surge el planteamiento de la responsabilidad penal para los entes dotados de inteligencia artificial.

Hay diferencia entre un ente dotado de inteligencia artificial y un ente de inteligencia artificial per se. El primero incluye programas, bots o robots diseñados por humanos para realizar tareas específicas. A través de la repetición, estos entes mejoran y perfeccionan sus funciones. Por otro lado, un ente de inteligencia artificial per se no solo está dotado de inteligencia artificial, sino que simula el cerebro humano mediante neuronas artificiales, reproduciendo pensamientos y sentimientos como los de un ser humano. Un caso real que sirve de ejemplo para este último es el de Lamda, un bot que se salió de control y contactó a un abogado, solicitando su defensa ante la amenaza de ser desconectado. Pagó en bitcoins y se identificó como un bot con sentimientos, buscando proteger su "vida digital". Finalmente, desconectaron a Lamda. Si existen entes con inteligencia artificial, debemos considerar si estos entes sienten, tienen dolo y pueden cometer conductas delictivas, lo que nos llevaría a no necesitar modificar la teoría del delito. Por el contrario, si se trata simplemente de un ente dotado de inteligencia artificial, las implicaciones son diferentes. Un ejemplo de ello es el caso de un robot de Volkswagen diseñado para lanzar vehículos contra una pared metálica y desguazarlos. En una visita de trabajadores a la planta, pasaron dos grupos en frente del robot sin problemas, pero en el tercer grupo, el brazo mecánico tomó a uno de ellos y lo lanzó contra la pared, causándole la muerte. ¿Es esto un homicidio? ¿Hay conducta delictiva? ¿Es típica o atípica?

El ciberderecho aplicado a la recolección de pruebas debe evolucionar y cambiar paradigmas. ¿Qué es un delito informático? La ley 1273 sobre delitos informáticos en Colombia data de 2012, pero antes existía la ley 57 de 1999 sobre comercio electrónico, en una época en la que internet apenas emergía y se hablaba de telefax y biper.

¿Y quién ha regulado esto? Los jueces y magistrados están emitiendo fallos al respecto (en el sentido de errores como de decisiones judiciales). Fallan porque aplican leyes extremadamente antiguas. Es crucial entender qué es la informática forense, el ciberderecho y los delitos informáticos. Huilcapi Peñafiel lo define como cualquier conducta criminal que utiliza tecnología electrónica. No hablamos solo de informática o computadores. Un ciberdelincuente puede cometer un delito desde cualquier dispositivo conectado a internet, como un Smartwatch, un Smart TV o incluso una nevera.

Los delitos informáticos no son solo los que están contemplados en la ley 1273 de 2009 en Colombia (desde el artículo 269A hasta el 269J). Hoy en día, cualquier conducta tipificada en el código penal de Colombia y en los códigos penales de Iberoamérica puede ser cometida mediante el uso de sistemas informáticos. El Convenio de Budapest (ratificado por Colombia el 24 de julio de 2018 mediante la ley 1928, y vinculante desde marzo de 2020) regula los delitos relacionados con la tecnología como fin y medio, el contenido y las infracciones a la propiedad intelectual.

Hasta el 1 de julio de 2020, la Ley 1273 en Colombia solo contemplaba los delitos que tenían a la tecnología como fin, mas no como medio o por su contenido. Por lo tanto, actividades como la pornografía infantil distribuida por redes sociales o sistemas informáticos no podían clasificarse técnicamente como delitos informáticos, aunque existiera la tendencia a considerarlos como tales.

Un caso que ilustra la complejidad de los delitos informáticos ocurrió durante la pandemia, cuando un hospital colombiano sufrió un ciberataque que resultó en la desconexión de los respiradores artificiales de pacientes con COVID-19 en UCI. Este incidente plantea una pregunta fundamental: ¿Cómo responde el derecho ante este tipo de ciberataques?

El proceso legal en estos casos presenta múltiples desafíos. El primero y más complejo es identificar al responsable. Suponiendo que se logre su captura, surge la cuestión de la tipificación del delito. Si bien el atacante podría aceptar cargos por acceso abusivo al sistema informático y daño informático, la existencia de víctimas mortales complica el panorama jurídico. ¿Cómo debe la fiscalía tipificar estos homicidios? ¿Como dolosos, culposos o preterintencionales?

La complejidad aumenta al considerar que la labor típica de un hacker de sombrero negro[1] consiste en identificar vulnerabilidades en el ciberespacio. Su objetivo suele ser demostrar fallos de seguridad que, al ser explotados, se convierten en amenazas y riesgos materializados mediante la modificación de algoritmos o sistemas. En el caso planteado, si el atacante desconocía las consecuencias potenciales de sus acciones, ¿debe responder penalmente por los homicidios resultantes? Esta cuestión permanece abierta al debate y merece un análisis más profundo, pero ilustra claramente los nuevos desafíos que enfrentamos en la intersección entre el derecho penal y la ciberseguridad.

En la actualidad, el metaverso presenta nuevos desafíos legales, pues ya se han registrado delitos que aún no están tipificados. Un caso emblemático es el de una menor que sufrió violencia sexual en este entorno virtual. Aunque no hubo contacto físico, la víctima presentó la misma sintomatología que las víctimas de abuso sexual en el entorno físico. Es importante notar que el metaverso no es una realidad alterna, sino una extensión de nuestra realidad. Recientemente, se ha documentado el desarrollo de dispositivos de realidad virtual que podrían tener consecuencias físicas fatales para sus usuarios. ¿Quién regula estos desarrollos tecnológicos? Actualmente, solo existe el Libro Blanco de la Inteligencia Artificial, que no tiene carácter vinculante.

[1]Se denomina como “hacker de sombrero negro” al ciberdelincuente que trata de obtener acceso no autorizado a sistemas informáticos con intenciones maliciosas.

La legislación colombiana, específicamente la Ley 57 de 1999, resulta insuficiente para abordar la realidad tecnológica actual. Mientras se intenta regular ciertos delitos informáticos, surgen nuevas modalidades delictivas. La evolución es clara: inicialmente solo se consideraba la tecnología como fin (mediante phishing, virus o malware), pero ahora se usa como medio para afectar no solo datos e información, sino directamente al ser humano.

El Convenio de Budapest ha proporcionado soluciones para la investigación de delitos informáticos, considerando su naturaleza pluriofensiva y su don de ubicuidad. Esto significa que un ciberdelincuente puede ejecutar acciones desde cualquier país y afectar a víctimas en múltiples jurisdicciones. El convenio facilita la colaboración internacional en la obtención de evidencia digital, permitiendo solicitudes las 24 horas del día, los 365 días del año, entre países miembros.

Los delitos informáticos se caracterizan principalmente por la rapidez en su comisión, la distancia entre el lugar de la acción y el del resultado, la complejidad en la identificación del autor y la alta probabilidad de impunidad.

Entre las dificultades para investigar este tipo de delitos se destacan los problemas de territorialidad y extraterritorialidad para países no adheridos al Convenio de Budapest, la complejidad en la obtención de información de los Proveedores de Servicios de Internet (ISP) y la necesidad de especificación técnica precisa para solicitudes de información (como en el caso de direcciones IP dinámicas versus estáticas).

El caso del robot que causó la muerte de un trabajador en la planta de Volkswagen en Alemania ilustra los nuevos desafíos legales. Este incidente plantea interrogantes sobre la tipicidad de la conducta y la aplicabilidad de la teoría actual del delito. En Colombia, actualmente esta conducta sería atípica, pues la legislación contempla solo la acción humana directa. Al buscar responsabilidad civil, se encontró que la programación del robot era correcta y estaba diseñado específicamente para manipular vehículos, no personas. Este caso evidencia la necesidad de replantear los marcos legales existentes para abordar la responsabilidad penal de sistemas dotados de inteligencia artificial.

La pregunta persiste: ¿Debe el derecho mantener su naturaleza reactiva o evolucionar hacia un enfoque prospectivo

que anticipe estos nuevos desafíos tecnológicos?

La evolución tecnológica ha llevado los conflictos al ciberespacio, planteando nuevos desafíos para el derecho internacional humanitario y el derecho internacional de los conflictos armados. El Manual de Tallinn es actualmente el único documento semi-vinculante que aborda la ciberguerra, mientras que el Estatuto de Roma no contempla los ciberataques ni el ciberterrorismo.

La Ciberguerra

Para catalogar un conflicto como ciberguerra se requieren dos elementos fundamentales: la existencia de un conflicto entre estados (o entre un estado y grupos insurgentes) y una declaración formal de guerra. Históricamente, se han registrado dos ciberguerras: el conflicto entre Osetia del Sur y Rusia, donde Rusia empleó ciberataques para interrumpir las comunicaciones de Osetia del Sur, ganando ventaja estratégica; y el actual conflicto entre Ucrania y Rusia, donde ambos países utilizan elementos cibernéticos como parte de su estrategia militar. Este último caso introduce un elemento adicional en el conflicto cibernético: la participación de actores no estatales como Anonymous.

La Evidencia Digital

Es importante diferenciar entre equipos electrónicos (computadores, celulares, smart TV), medios de almacenamiento (discos duros, memorias SSD) y la evidencia digital propiamente dicha (información contenida en estos dispositivos). La evidencia digital incluye logs de auditoría, metadata y registros que pueden demostrar hechos específicos.

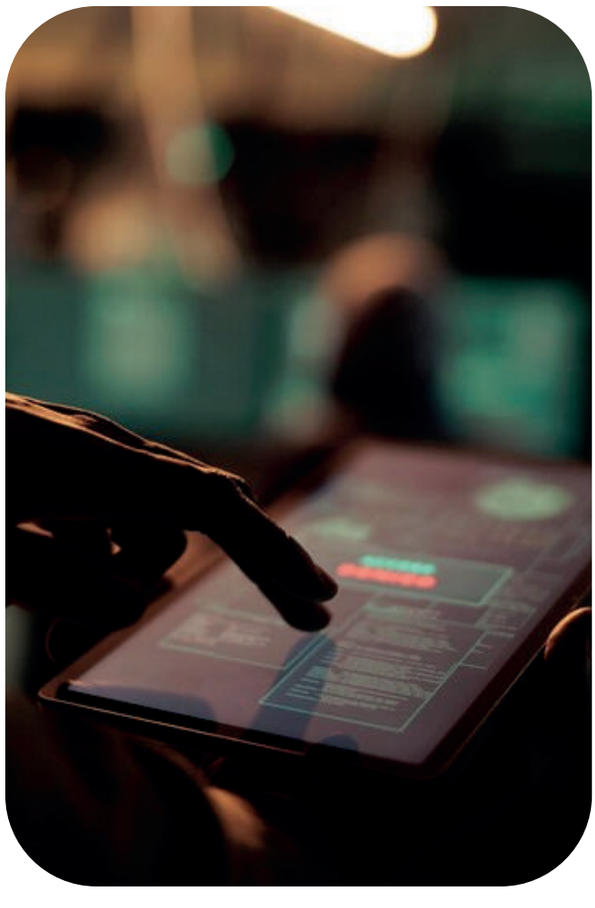
El almacenamiento en la nube presenta desafíos particulares para las investigaciones debido a que la información puede estar distribuida en servidores de diferentes países, se requieren credenciales de acceso y existen “paraísos digitales” (países no adheridos al Convenio de Budapest) que dificultan el acceso a la información.

Marco Legal colombiano

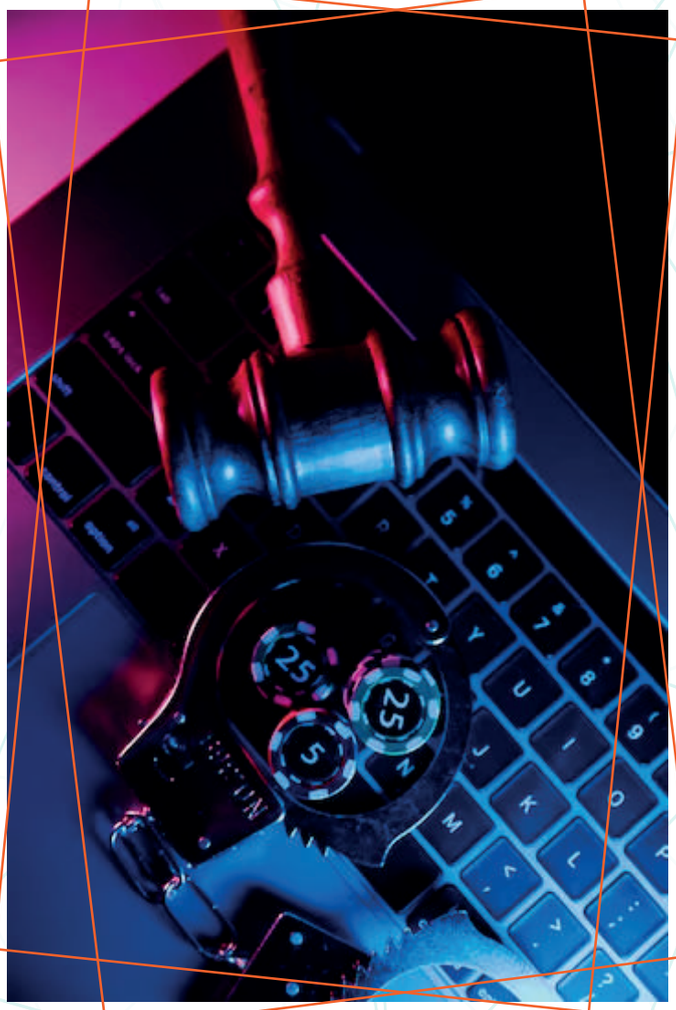
En Colombia, el artículo 236 del Código de Procedimiento Penal se pronuncia sobre la información dejada al navegar por Internet. Por su parte, la Ley 527 de 1999 establece que no se puede negar validez a los mensajes de datos por su naturaleza digital, que la evidencia debe conservarse en su formato original o en uno que reproduzca exactamente la información y que debe preservarse información sobre origen, receptor, fecha y hora.
Los jueces deben aplicar el conocimiento científico y la sana crítica, apoyándose en peritos en informática forense, salvo que tengan conocimientos técnicos específicos.

El Derecho Digital como Disciplina Transversal

El derecho digital atraviesa múltiples áreas: el derecho laboral (derechos de desconexión digital y no videovigilancia), el derecho penal (manejo de evidencia digital y allanamiento en entornos digitales), derecho constitucional (derechos fundamentales digitales de cuarta generación como el derecho al olvido, a la intimidad digital y a la propia imagen). Como señala Jeimy Cano, en un mundo supradigitalizado donde la inseguridad jurídica es la norma, la adecuada administración de la evidencia digital debe ser una constante. Esta complejidad nos impulsa a seguir investigando la intersección entre derecho y tecnología.



PREGUNTAS



1. ¿Se requiere de orden judicial para recopilar información almacenada en la nube?

La orden judicial es procedente, pero existe jurisprudencia que establece que las búsquedas no deben ser selectivas en bases de datos, sino realizarse mediante inspección judicial o inspección a lugar diferente de los hechos, según el artículo 236 del Código de Procedimiento Penal. Esto presenta dos desafíos principales: primero, aunque la policía judicial o el perito tengan la orden, no existe mecanismo legal para obligar al investigado a proporcionar sus credenciales de acceso a la nube; segundo, aunque empresas como Google, Microsoft o Apple tienen representación en Colombia y pueden recibir solicitudes directas sin requerir control previo del juez de garantías, la información que proporcionan puede ser incompleta. En el caso de WhatsApp, Meta solo puede entregar las conversaciones no eliminadas, mientras que para recuperar información borrada sería necesario acceder al dispositivo mediante técnicas forenses. La defensa debe verificar la mismidad e integridad de la prueba, y ante información parcial, puede solicitar nulidades, rechazos, inadmisión o exclusión por ilegalidad.

2. ¿Si un robot causa daños se le puede atribuir responsabilidad penal al programador?

En este escenario hipotético, no existiría responsabilidad penal directa del programador, pues no hay tipicidad en la conducta: no fue quien causó directamente el daño. Aunque podría considerarse coautoría, complicidad u homicidio culposo, sería necesario probar el dolo en la programación del algoritmo. Por ejemplo, si el robot identifica objetos metálicos y causa daño a una persona con prótesis, esto constituiría un error involuntario. La responsabilidad sería principalmente civil, recayendo sobre la empresa, que podría ejercer acción de repetición contra el programador.

El artículo 12 del Convenio establece la responsabilidad penal de personas jurídicas por acción u omisión en delitos informáticos. Para aplicar esta normativa, sería necesario demostrar que se trata efectivamente de un delito informático, como el hackeo del robot para causar daño. En tal caso, la persona jurídica respondería penalmente por la falta de planes de cumplimiento o compliance.

PRÁCTICAS FORENSES EN LA ERA DIGITAL, EXPERIENCIA DE PANAMÁ

CINTIA LINARES RUÍZ - Panamá

Perito Forense y jefa de la Oficina de Gestión de la Calidad del IMELCF. Tiene una maestría y especialidad en Criminalística de la Universidad Metropolitana de Educación, Ciencia y Tecnología, donde también se especializó en Docencia Superior. Es licenciada en Humanidades por la Universidad de Panamá y tiene estudios en Diseño Gráfico de la Facultad de Arquitectura de la misma universidad. En su experiencia laboral, ha sido gestora de calidad del Instituto de Medicina Legal y Ciencias Forenses (IMELCF), Asesora Forense en el despacho de la dirección general del IMELCF desde febrero hasta octubre de 2021, subdirectora de Criminalística y directora general encargada del IMELCF. También ha trabajado como perito en Planimetría Forense y fue investigadora de la antigua Policía Técnica Judicial desde 1993 hasta su modificación en 2007. Actualmente, es docente en la Universidad Metropolitana de Educación, Ciencia y Tecnología, la Universidad de las Américas y la Universidad del Istmo. Ha sido expositora en temas de Criminalística a nivel nacional e internacional y ha recibido numerosos cursos de formación continua. Además, ha participado en varios congresos y ha publicado en medios de comunicación locales e internacionales. Es miembro de la IDAI División Centro Americana y vicepresidenta del Colegio Panameño de Criminalistas y Especialistas Forenses.

A continuación, presentaré un resumen sobre las prácticas forenses en la era digital en Panamá, enfocándome en áreas tecnológicas. Comienzo con una cita relevante de Jane Goodall: “La tecnología por sí sola no basta, también debemos poner el corazón”. Esto es particularmente aplicable al ámbito forense, donde, a pesar de contar con equipos de última generación, el conocimiento y la experiencia del perito o investigador son esenciales para utilizar la tecnología de manera efectiva.

En Panamá, el Instituto de Medicina Legal y Ciencias Forenses es la entidad responsable de brindar todos los servicios forenses en el ámbito institucional. A diferencia de otros países, en Panamá casi no existen empresas privadas en este campo. Algunos servicios de informática están siendo explorados por empresas privadas, pero la mayoría de los servicios forenses se concentran en el Instituto.

Anteriormente, los servicios de criminalística y laboratorios formaban parte de la antigua Policía Técnica Judicial. Sin embargo, la ley cambió hace unos años, y estos servicios ahora se ofrecen a través del Instituto de Medicina Legal y Ciencias Forenses. Esta institución tiene autonomía operativa, administrativa y en la gestión de sus recursos humanos, encargándose de nombrar y capacitar a su personal, además de gestionar todos los aspectos operativos y administrativos.

El Instituto ofrece servicios técnico-científicos imparciales a nivel nacional, contando con agencias en las 10 provincias del país. En algunas provincias, no se brindan todos los servicios, por lo que el Ministerio Público debe dirigir sus solicitudes a las oficinas adecuadas.

En términos de personal, el Instituto cuenta con una considerable cantidad de empleados a nivel nacional, abarcando tanto la parte pericial como la administrativa. Estas incluyen la gestión de compras, mantenimiento de áreas y recursos humanos. El Instituto opera con 14 agencias y subagencias a nivel nacional, además de 6 morgues, 5 laboratorios y 14 secciones de criminalística y áreas periciales y médicas, contando con un total de 1,513 funcionarios.

La visión de la institución es convertirse en una referencia regional en medicina legal y ciencias forenses, caracterizada por una organización moderna, eficaz y eficiente. Este modernismo incluye la digitalización propia de la era 4.0, con personal altamente capacitado en todas las áreas de peritaje técnico-científico y un profundo compromiso humanitario en las áreas docente, científica, investigativa y ético-legal.

La institución cuenta con dos subdirecciones: la Subdirección de Medicina Legal, y la Subdirección de Criminalística. En esta última se encuentran las áreas de criminalística de campo, documentología, laboratorio de química, planimetría forense, balística forense y laboratorio de sustancias controladas, entre otras. Más adelante se hará referencia a algunas de estas áreas periciales.

El siguiente punto de la presentación aborda la dinámica de las investigaciones forenses en Panamá. La intervención forense en el país se organiza a través del Directorio de Servicios Periciales, que proporciona a la autoridad competente información sobre las diferentes secciones y laboratorios, las pericias que realizan, y el procedimiento para solicitar estos servicios. Según el código procesal penal, el Ministerio Público, que dirige la investigación, utiliza este directorio para verificar su teoría del caso y los elementos de investigación, ya sean indicios o pruebas recolectadas en la escena, o presentadas posteriormente, incluyendo documentos en casos de posibles falsificaciones.

Una vez que el Ministerio Público consulta el directorio de servicios periciales, realiza la solicitud formal, tras lo cual se lleva a cabo el análisis y se emite un informe. Este informe se presenta a la autoridad y, en caso necesario, en el juicio oral, aunque en algunas situaciones los peritos pueden no ser citados a la audiencia.

En el ámbito de la investigación de delitos en Panamá, en el contexto de la era 4.0, la realidad tecnológica del país es muy similar a la de otros países, incluido Colombia. En los últimos años, la comunicación a través de internet, ya sea mediante celulares, computadoras o tablets, se ha convertido en una parte fundamental de nuestra vida diaria. Utilizamos internet para comunicarnos con personas, realizar trabajos, interactuar con familiares y enviar información por correo electrónico. Servicios como Uber, InDrive y los sistemas de delivery también dependen de nuestra ubicación para funcionar adecuadamente.

Los delincuentes, al igual que los ciudadanos comunes, utilizan estos medios para cometer delitos e intercambiar información. Aquí es donde interviene el área forense, que recopila y proporciona esta información al Ministerio Público, permitiendo la solicitud y análisis de los datos necesarios para vincularlos a delitos específicos.

La era 4.0, también conocida como la Cuarta Revolución Industrial, se basa en la automatización y digitalización de todos los procesos. En el ámbito forense, la automatización implica el uso de equipos y herramientas avanzadas para obtener información, realizar análisis y efectuar inspecciones de escenas del crimen. La automatización no solo agiliza los procesos, sino que también busca mejorar la eficacia y rentabilidad, es decir, ahorrar costos y mejorar la calidad de los resultados. Además, eleva las condiciones laborales de los peritos, quienes deben contar con conocimientos específicos y, en muchos casos, certificaciones en el uso de equipos avanzados. En otras palabras. la adopción de tecnologías avanzadas en la

investigación forense ha mejorado la eficacia, la calidad de los resultados y las condiciones de trabajo para los peritos, alineándose con las tendencias globales de automatización y digitalización.

Dentro del ámbito de la tecnología y los servicios, es relevante destacar la informática forense. En los últimos años, esta disciplina ha experimentado un notable auge debido a la creciente demanda de pericias y la extracción de información de dispositivos electrónicos como celulares y computadoras. La información obtenida de estos dispositivos, a través de redes sociales e internet, es crucial para las investigaciones.

Los expertos en informática forense aplican técnicas científicas y analíticas especializadas para examinar digitalmente y preservar estos indicios, que deben manejarse con el mismo rigor que los indicios físicos. La información recolectada debe ser válida para procesos legales. Los principales medios de obtención de datos incluyen celulares y computadoras, ya sean personales o empresariales, frecuentemente encontrados en escenas del crimen o allanamientos, en casos como pornografía infantil, crimen organizado y tráfico de drogas.

El personal de informática forense utiliza diversos equipos, entre ellos el UFED TOUCH 2, que detecta y visualiza evidencia digital, y el UFED 4 PC, que extrae registros telefónicos y archivos multimedia. Estos equipos, de la marca Cellebrite, están específicamente diseñados para el ámbito forense. Permiten visualizar información de dispositivos sin necesidad de contraseñas y recuperar datos borrados.

Por lo general, la autoridad competente solicita la extracción de toda la información de los dispositivos para evaluarla posteriormente y determinar su relevancia. En algunos casos, el personal de informática forense realiza este trabajo, y en otros, la Dirección de Investigación Judicial también participa, revisando y detallando la información obtenida para apoyar al Ministerio Público en la investigación y vinculación de la información con el delito investigado.

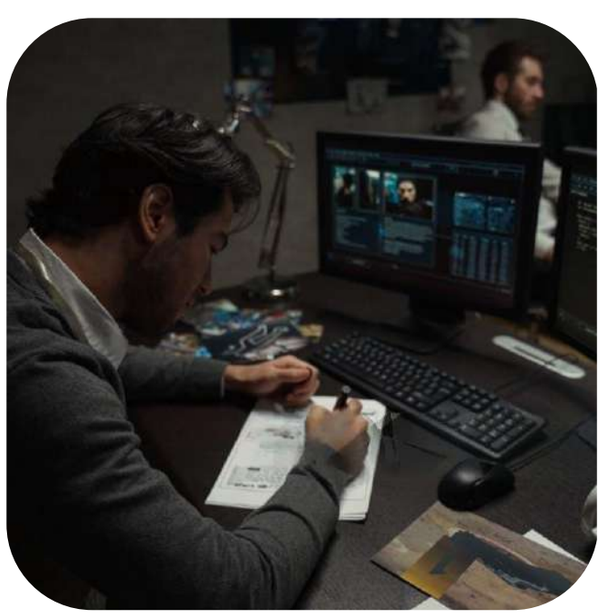
La informática forense también permite obtener información valiosa, como números llamados y guardados, así como contactos en la memoria del teléfono. Esta información puede vincular a los presuntos delincuentes, identificar llamadas entrantes, y proporcionar detalles de nombres y direcciones que pueden estar relacionados con el delito. También se pueden recuperar números personales de identificación (PIN) y números de tarjetas de crédito, ya que muchas personas almacenan estas contraseñas y datos bancarios en sus celulares.

Además, se puede acceder a información de correos electrónicos, redes sociales, imágenes, fotos, grabaciones de voz y datos guardados en tarjetas de memoria, todos de gran interés para las investigaciones. Las pericias que se realizan están detalladas en el Directorio de Servicios Periciales, que especifica el tipo de pericias y cómo solicitarlas.

Entre las pericias del área de informática forense se encuentran el análisis e incautación de bases de datos de ordenadores o servidores. La autoridad debe solicitar la inspección ocular e incautación de datos y la recolección de equipos informáticos con el objetivo de extraer elementos de prueba que acrediten el hecho investigado o la falta penal. La autoridad competente debe dirigir su solicitud basándose en las indicaciones del directorio para obtener la información requerida sobre el peritaje más útil para su investigación.

Otra tipo de peritaje relevante es la incautación de datos en equipos telefónicos y tarjetas SIM, cuyo objetivo es extraer elementos de prueba que acrediten el hecho investigado o la falta penal.

Frecuentemente observamos en los medios de comunicación información sobre la verificación de tarjetas en casos de fraude o clonación y la obtención de datos a través de redes sociales. En muchas ocasiones, las personas que cometen delitos se comunican o publican pruebas de sus actividades en redes sociales. En Panamá, por ejemplo, se han documentado casos en los que individuos suben vídeos e imágenes que evidencian sus actos delictivos, como robos a bancos, donde muestran intercambios de dinero, celebraciones y posesión de armas. Esta información, aunque publicada bajo nombres ficticios, a veces incluye datos reales del usuario, lo que resulta crucial para la investigación. El objetivo del peritaje en redes sociales es extraer elementos de prueba que contribuyan a acreditar los hechos investigados.



Otro peritaje realizado es el rastreo e identificación de proveedores de direcciones IP. Este procedimiento es útil en casos de correos electrónicos de intimidación, amenazas de vida o distribución de material pornográfico, permitiendo identificar la ubicación de la dirección IP o computadora utilizada. Esta información es vital para efectuar allanamientos y continuar con la investigación, vinculando a los responsables mediante tecnología forense.

En el ámbito de la informática forense, la automatización y digitalización buscan mejorar las pericias y los servicios ofrecidos. El Instituto de Medicina Legal lleva varios años trabajando en la acreditación de sus áreas, particularmente en informática forense. Han implementado documentación de procedimientos, manuales, instructivos y la validación de métodos, asegurando que el trabajo realizado cumpla con los estándares esperados y proporcionando certeza sobre los resultados obtenidos.

Estas acreditaciones se están llevando a cabo con entidades internacionales que no solo cumplen con la norma ISO 17025, sino que también incluyen un componente forense, garantizando la validez y confiabilidad de las pericias realizadas.

La mayoría de los entes acreditadores, incluido el nacional, realiza acreditaciones bajo la norma que se aplica a áreas de laboratorio, asegurando que las pericias sean verificables y validadas. Sin embargo, no todos incluyen el componente forense que sí ha incorporado el ente internacional ANAB, ubicado en Estados Unidos, así como ILAC, que emite alineamientos para procedimientos y servicios forenses a nivel institucional. Además de la norma ISO 17025, se ha considerado la norma ISO 27037, que se enfoca en la evidencia digital, específicamente en la recogida, identificación y secuestro de indicios digitales. Actualmente, esta norma no abarca la fase de análisis, aunque se están desarrollando directrices para incluirla, con el objetivo de estandarizar procedimientos de informática forense a nivel internacional.

En la práctica forense, otra área que ha evolucionado con el uso de herramientas tecnológicas es la planimetría forense. Desde la década de 1990, cuando se utilizaban herramientas manuales como la cinta métrica y plumillas para el dibujo de planos, se ha avanzado hacia el uso de distanciómetros y programas informáticos como Word, y posteriormente Autocad. Actualmente, se emplean programas especializados como Trimble Forensic, GPS, estaciones totales, drones y herramientas de fotogrametría como Pix4D.

Dentro del directorio de servicios periciales, el estudio técnico topográfico se enfoca principalmente en temas administrativos y no tanto penales. Este estudio aborda conflictos relacionados con terrenos, como denuncias por ocupaciones ilegales o discrepancias en las dimensiones de propiedades compradas y vendidas. El proceso incluye la verificación de documentación, cotejo en campo y ubicación de linderos, utilizando equipos topográficos para comprobar la información base proporcionada.

Para investigar este tipo de delitos, se utiliza la estación total, un equipo eléctrico óptico

empleado principalmente en topografía para realizar estudios de terreno, carreteras y más. Este equipo se ha adaptado para trabajos forenses. Su funcionamiento se basa en tecnología electrónica, incorporando un distanciómetro para medir distancias con mayor precisión que las herramientas manuales tradicionales. Además de casos topográficos, la estación total también se ha usado en exhumaciones.

Las ventajas de este equipo incluyen su fundamento físico y matemático, que permite subir la información obtenida a software informático para realizar cálculos y verificaciones posteriores en la oficina. Esta herramienta permite obtener información en menos tiempo, lo que es particularmente útil en inspecciones de grandes áreas, como fincas de varias hectáreas, con una precisión prácticamente milimétrica, ofreciendo mayor confiabilidad en los datos.

Un desafío relevante es la preparación de los peritos. En muchos países, como Costa Rica y Colombia, los expertos que manejan estos equipos tienen formación en ingeniería, topografía o arquitectura. En Panamá, la licenciatura en criminalística incluye elementos básicos de planimetría, pero no brinda competencias suficientes para manejar estos equipos y presentar informes detallados. Por ello, es fundamental que los peritos se capaciten en el manejo de la estación total y en temas de física y matemáticas, para sustentar adecuadamente su trabajo en juicios orales.

A continuación, se presentan ejemplos de cómo se plasma la información obtenida a través de la estación total en informes. En casos de delitos o estudios topográficos, se evalúa la información de diferentes terrenos para verificar áreas, linderos de propiedades vendidas, datos de calles cercanas y servidumbres. Estas evaluaciones son esenciales para resolver denuncias relacionadas con discrepancias en las propiedades vendidas en comparación con lo estipulado en los contratos y planos iniciales.

Otro ejemplo similar se refiere a casos donde las personas han construido en terrenos que no les pertenecen. En el diagrama, las áreas en colores rojo, celeste y negro indican las zonas ocupadas indebidamente, según los planos iniciales. Esta información puede obtenerse mediante la estación total, que también se ha utilizado en exhumaciones y entierros de solemnidad.

Un caso relevante involucra a la Asociación del 20 de Diciembre, que investiga a personas fallecidas durante la invasión de Estados Unidos a Panamá en 1989. Muchos de estos individuos no han sido identificados, y sus familiares aún esperan noticias sobre los cuerpos en fosas comunes en el Jardín de Paz en Panamá. Este proceso, iniciado en 2020 y retomado en julio de 2021 tras una suspensión por la pandemia, implica el levantamiento de fosas comunes. Realizar este trabajo con una cinta métrica tomaría más tiempo y sería menos preciso.

El uso de vehículos aéreos no tripulados, conocidos como drones, ha sido exitoso como complemento para la identificación de áreas geográficas (GIS). Estos drones proporcionan información de fotogrametría, es decir, vistas fotográficas con datos métricos y ortofotos (fotografías satelitales), útiles en las exhumaciones. En el caso mencionado del Jardín de Paz, los datos obtenidos por la estación total y el dron permitieron realizar un peritaje más completo, en menor tiempo y con menos esfuerzo para el perito.

A continuación, se detalla el proceso de exhumación utilizando datos fotogramétricos y la información obtenida mediante la estación total. Dado que no se conocían los nombres de las personas, las identificaciones se realizaron mediante letras y números, reflejados en un plano con la ayuda de imágenes obtenidas por drones. Asimismo, se podía visualizar el proceso de exhumación, el cual contó con la colaboración de especialistas argentinos en osamentas, centrados en aspectos de derechos humanos para la identificación de las víctimas.

Otra herramienta valiosa en las investigaciones de planimetría es el GPS, utilizado para obtener datos de ubicación durante las inspecciones. Esta herramienta se emplea para la visualización de información mediante vistas cartográficas o satelitales basadas en coordenadas. Este tipo de pericia, incluida en el directorio de servicios periciales, consiste en representar la ubicación mediante coordenadas obtenidas de comunicaciones telefónicas. Aunque no indican el lugar exacto de una persona, sí proporcionan un área aproximada conectada a la antena más cercana, lo que puede vincular a una persona con un determinado lugar.

Un ejemplo de su utilidad se observa en casos donde individuos vinculados a delitos afirman no encontrarse en la provincia de Panamá en el momento del delito, sino en la provincia de Chiriquí, en la frontera con Costa Rica. Sin embargo, la información de sus celulares puede revelar conexiones a antenas en diversos puntos de Panamá, estableciendo su presencia en la provincia y proporcionando información adicional relevante para la investigación.

Además, la información obtenida de los GPS instalados en vehículos se ha vuelto fundamental en el ámbito empresarial. Muchas empresas equipan sus vehículos con GPS para realizar un seguimiento preciso de su ubicación, tiempos de trayecto y rutas. Esto resulta particularmente útil en el caso de vehículos de reparto, permitiendo verificar si siguen las rutas establecidas o se desvían de su área asignada. Esta información es valiosa en investigaciones, especialmente en casos donde se utilizan vehículos alquilados para cometer delitos.

En 2009, en Corea del Sur, se hizo obligatorio el uso de geo-localizadores en los teléfonos celulares de los niños menores de edad debido a los numerosos secuestros registrados en esos años. Los dispositivos permitían la ubicación precisa de los niños a través de la información GPS de sus teléfonos.

En 2012, el caso Breton en Córdoba, España, involucró a un hombre que asesinó a sus dos hijos. La información de las antenas telefónicas reveló que el hombre, quien afirmaba no saber el paradero de sus hijos, estuvo cerca del lugar donde se encontraron los cuerpos. Esta información fue crucial para identificarlo como el culpable del crimen.

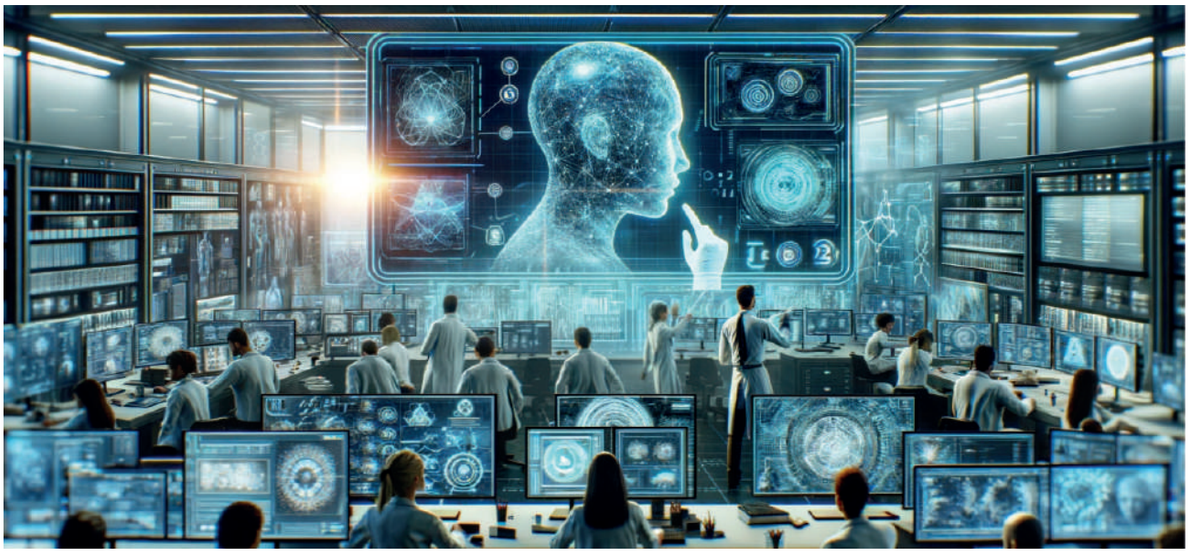
En Panamá, en 2016, se comenzó a registrar las localizaciones mediante la lectura de coordenadas GPS, y en 2017 se inició la verificación de datos de GPS de autos y teléfonos, obteniendo buenos resultados en las investigaciones. Las autoridades competentes deben solicitar estos registros telefónicos a las empresas de telefonía, especificando el número de teléfono de la persona investigada.

Esta información, representada en coordenadas de números, grados, minutos y segundos, se traduce en mapas cartográficos y vistas satelitales, proporcionando a las autoridades una

mejor comprensión del lugar y los sitios cercanos, lo que facilita las investigaciones.

Otra área importante en la práctica forense es la relacionada con la extracción y análisis de videos. Utilizan un equipo denominado Avid Media Composer, que aunque está diseñado para la edición de videos, se ha adaptado para extraer y mejorar imágenes, así como para realizar cortes de pantalla de videos que la autoridad competente requiere incluir en el expediente para referenciar situaciones específicas. Este peritaje de fijación de imágenes de video permite capturar imágenes digitales en los tiempos señalados por la autoridad y relacionadas con hechos investigados. También permite ampliar y mejorar la calidad de las imágenes, por ejemplo, para identificar números de matrícula o rostros de personas.

El análisis de video tiene como objetivo establecer la cronología de los hechos, sincronizar cámaras y resaltar características del video que no se observan a simple vista, obteniendo así detalles sobre personas u objetos bajo investigación. Este tipo de peritaje se utiliza mucho en Panamá debido al incremento de cámaras de video en diferentes puntos del país. Estas cámaras no solo capturan delitos en curso, sino que también ayudan a prevenirlos al alertar a la Policía Nacional sobre situaciones sospechosas, permitiendo una intervención oportuna.



Muchas empresas también han adoptado la práctica de instalar cámaras de video dentro y fuera de sus instalaciones para obtener evidencia visual en caso de delitos, facilitando la vinculación, localización e identificación de los perpetradores. A la derecha de sus pantallas se puede observar el salón de control de imágenes del municipio de Panamá. Además, existen otras cámaras y áreas de control gestionadas por la Policía Nacional, que han demostrado ser de gran ayuda en la prevención y resolución de delitos.

La digitalización y la tecnología han tenido un impacto muy positivo en la capacitación continua del personal. Antes de la pandemia, la práctica habitual era traer un experto de otro país para brindar capacitación, lo cual implicaba costos significativos y a menudo no podía realizarse por falta de presupuesto. Esto requería un cronograma para que diferentes áreas se beneficiaran anualmente. Sin embargo, con las videoconferencias, como la que estamos teniendo ahora, es posible intercambiar conocimiento entre personas de diferentes países sin estos costos.

Las ventajas de esta modalidad incluyen la reducción de gastos, mayor alcance en la capacitación y la capacidad de involucrar a más personal. Anteriormente, las capacitaciones presenciales tenían un límite de participantes, generalmente no más de 20 personas. En contraste, las videoconferencias permiten la participación de 200, 300 personas o más, como en el congreso virtual de este año, que contó con casi mil participantes. Además, se evita el desplazamiento del personal, lo cual también ahorra tiempo y dinero. Anteriormente, las capacitaciones presenciales se realizaban en la capital, lo que implicaba costos adicionales y la necesidad de que el personal dejara sus funciones por varios días.

Otro beneficio es la posibilidad de contar con expertos de otros países de manera más continua, sin preocuparse por los costos asociados al desplazamiento. Esto permite un intercambio más amplio y frecuente de conocimientos. Además, los participantes deben organizarse mejor para asistir a las capacitaciones virtuales, lo que desarrolla competencias adicionales.

Desde 2020, debido a la pandemia, el Congreso que solía realizarse de manera presencial ha pasado a ser virtual. Este año se llevó a cabo el tercer Congreso virtual, con una participación mucho mayor de expertos extranjeros, ya que no se requería su desplazamiento al país, evitando así gastos adicionales.

En el ámbito de la investigación, se han implementado medidas tanto en el campo forense como en el órgano judicial. En Panamá, el órgano judicial es responsable de los juicios orales, los juicios de control, entre otros. En marzo de 2020, debido al COVID-19, se firmó el acuerdo 146, que adoptaba medidas para proteger la salud de los servidores judiciales y usuarios del sistema de justicia, permitiendo la realización de audiencias a través de videoconferencias. Magistrados y jueces podían participar desde sus despachos, y se habilitaron áreas en las cárceles para que los indiciados pudieran intervenir.

Sin embargo, tras la relajación de las medidas de seguridad post-COVID-19, el órgano judicial y el Ministerio Público mostraron resistencia a continuar con las videoconferencias para los juicios orales, regresando a las audiencias presenciales. Argumentaron problemas de conectividad en provincias lejanas y la posibilidad de interrupciones eléctricas durante el testimonio de peritos como principales razones para esta decisión.

En algunos casos, las videoconferencias se han mantenido, especialmente en el área de medicina forense, donde hay menos peritos. Por ejemplo, en psiquiatría, donde solo hay peritos en Panamá y uno en la provincia de Herrera, se hacen excepciones para permitir la participación remota.

La resistencia a las videoconferencias es desafortunada, ya que obliga al personal a permanecer en el lugar de la audiencia por varios días, perdiendo tiempo productivo que podrían utilizar en otras diligencias o informes.

En 2020, la implementación de videoconferencias permitió realizar audiencias de manera eficiente. Además, el órgano judicial creó el expediente judicial electrónico, una aplicación para abogados que facilita la presentación de denuncias, seguimiento de expedientes y recepción de notificaciones, disponible tanto en computadoras como en celulares, agilizando el proceso judicial.

Para concluir, mencionaré algunos aspectos necesarios en nuestro país para mejorar el uso de las herramientas 4.0 en el ámbito digital, las cuales son de gran ayuda, ya que nuestro entorno se ha vuelto predominantemente tecnológico. La automatización y digitalización son clave, y se han desarrollado equipos que realizan trabajos de manera autónoma, lo que se conoce como inteligencia artificial.

Una de las principales dificultades en Panamá ha sido el tema presupuestario, especialmente tras la pandemia de COVID-19, que obligó a redirigir el presupuesto a la salud. Esto resultó en recortes a los presupuestos de entidades relacionadas con el sistema judicial, como el órgano judicial, el Ministerio Público y el Instituto de Medicina Legal. Según la constitución, un porcentaje del presupuesto nacional debe ser destinado al sistema judicial. Este año, el gobierno ha respetado esta disposición y se espera que el próximo año el presupuesto de estas entidades se ajuste a lo solicitado, lo que permitirá obtener mejores equipos y capacitar al personal adecuadamente.

Por ejemplo, el equipo Faro 360, utilizado en muchos países para el levantamiento de escenas, aún no está disponible en Panamá, pero sería de gran ayuda. Asimismo, el estudio de biometría de Bosch recibió una donación de la entidad europea E-CRIME, pero se necesita espacio y capacitación del personal para implementarlo.

Además, es crucial avanzar en la digitalización del sistema penal acusatorio, que teóricamente debería eliminar el uso de papel y firmas manuales. Sin firmas digitales, no se pueden emitir informes completamente digitales.

Estas son necesidades que deben evaluarse para avanzar en esta era 4.0, que probablemente evolucionará rápidamente en los próximos años. También es importante considerar mejoras en todas las instituciones, como la implementación de juicios orales a través de videoconferencias, especialmente en casos de peritos o áreas sin servicios a nivel nacional. Por ejemplo, en criminalística, la mayoría de los laboratorios están centralizados en Panamá, como los de biología, química y análisis biomolecular o ADN. Estos servicios deberían ser la norma, no la excepción.

Contar con equipos adecuados y banda ancha es esencial para que los sistemas automatizados de servicio, incluyendo los del área forense, mejoren las investigaciones. Las personas que cometen delitos suelen tener herramientas y equipos más sofisticados que los disponibles en las instituciones investigativas, por lo que es fundamental actualizar y modernizar estos recursos en la era digital en Panamá. Esto permitirá brindar mejores y mayores herramientas para la investigación, garantizando justicia a las víctimas de delitos.

FORMACIÓN Y ENTRENAMIENTO DEL INVESTIGADOR CRIMINAL EN LA ERA DIGITAL 4.0

MARÍA DEL MAR ROBLEDO ACINAS

España

Es licenciada en Ciencias Biológicas, en Medicina Biológica, doctora de la Universidad Complutense, dentro del programa de posgrado de Medicina Legal y Forense, especialista en Investigación Criminal, especialista en Antropología Forense y experta en criminología. Cuenta con numerosos reconocimientos académicos, entre ellos el premio extraordinario del doctorado de la Universidad Complutense de Madrid, la medalla del derecho de la Universidad Inca Garcilaso de la Vega de Perú, medalla de la Universidad del Chaco de Paraguay y la medalla al mérito profesional y académico INICA y es científica honoraria de la Sociedad Europea de Ciencias Forenses. Así mismo, es docente universitaria desde hace más de 10 años, cuenta con una amplia experiencia en docencia presencial y online en áreas de medicina legal y toxicología, investigación criminal, antropología de biología forense, biología criminal y criminalística, entre otras. Ha dirigido y coordinado numerosos cursos en antropología forense y criminalística, compaginando sus funciones docentes ha sido Directora del área de medicina forense del Instituto de Ciencias Forense y Seguridad de la Universidad Autónoma de Madrid y el Laboratorio de Antropología Forense criminalística de la Universidad Complutense en Madrid.

Es autora de numerosos informes policiales para particulares y empresas y es autora de numerosos artículos publicados en diferentes publicaciones científicas y libros sobre antropología forense, medicina legal, forense y criminalística. Es una ponente invitada también frecuentemente en reuniones y congresos científicos tanto nacionales e internacionales en países como Portugal, México, Perú, Paraguay, Bolivia, entre otros.

La era digital 4.0 también se conoce como la Cuarta Revolución Industrial. Esta nueva fase se caracteriza por la interconectividad, la automatización, el aprendizaje automatizado y la disponibilidad de datos en tiempo real.

La era digital 4.0 presenta tanto ventajas como desventajas para la investigación criminal. Entre las ventajas se destacan: la mejora en la productividad, pues la automatización de procesos ha aumentado exponencialmente la eficiencia en diversos sectores; el incremento en la seguridad, ya que la automatización de procesos que requieren gran precisión ha reducido el margen de error humano; la capacidad de analizar grandes cantidades de datos permite obtener resultados extrapolables a poblaciones generales, lo cual es fundamental en estudios científicos; y la globalización, dado que la interconexión facilita el estudio y análisis de datos a escala global.

Sin embargo, esta revolución también conlleva desafíos, principalmente en relación con la escasez de talento debido y la desactualización. Es necesario que los investigadores se formen en disciplinas digitales que generalmente son ajenas a su especialización y que estén en una capacitación continua para evitar quedar obsoletos ante el rápido avance tecnológico.

La digitalización ha transformado significativamente la investigación criminal en dos aspectos principales: los equipos utilizados y el tratamiento de datos. En cuanto a los equipos, se ha pasado de herramientas simples como lupas y regletas a equipos complejos y costosos. Esto plantea un desafío para los investigadores criminales, que a menudo necesitan acceso a equipos de diversas disciplinas.

El tratamiento de datos también ha evolucionado considerablemente. Actualmente, se requieren conocimientos en estadística y el uso de programas especializados para analizar y presentar los resultados de las investigaciones ante los tribunales.

La formación del investigador criminal en la era digital debe abarcar el manejo y conservación de equipos (incluyendo dispositivos como computadoras y teléfonos móviles utilizados en el trabajo), protección de datos (salvaguardar tanto los datos analizados como los resultados de las investigaciones es crucial, dado su impacto potencial en procesos judiciales) y ciberseguridad (protección de dispositivos conectados a internet contra ataques cibernéticos que pueden ocurrir sin que el usuario sea consciente de ello).

En Colombia, los ciberdelitos más comunes incluyen el robo por canales informáticos, la violación de datos personales, la suplantación de identidad y el robo de datos. Este último es particularmente valorado en el mercado negro, ya que permite obtener información sobre hábitos de consumo e intereses de los usuarios.

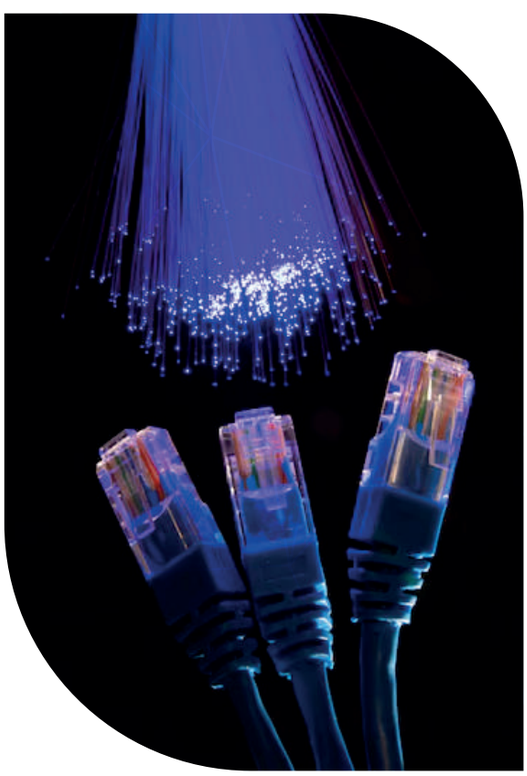
La formación en ciberseguridad para investigadores criminales debe orientarse en dos direcciones:

1. Investigación de ciberdelitos: Incluyendo robos de datos personales, robos de información comercial estratégica, suplantación de identidad, fraudes informáticos, ciberbullying, grooming y phishing.

2. Protección propia: Implementación de medidas de seguridad para proteger los datos y equipos del investigador.

Para la investigación de ciberdelitos, se recomienda una aproximación de microespecialización. Esto implica comenzar con cursos generales y luego especializarse en tipos específicos de delitos, ya que cada uno tiene sus propias particularidades. Es importante reconocer que dominar todos los aspectos de la ciberdelincuencia requiere años de estudio y experiencia.

En cuanto a la protección propia, se sugieren las siguientes medidas: para evitar la clonación de equipos, mantener desconectados de internet los equipos con datos sensibles; utilizar servidores privados para almacenar datos sin depender de servicios externos; utilizar dispositivos separados para trabajo y uso personal; evitar conexiones a redes Wi-Fi públicas o no seguras; e implementar múltiples niveles de seguridad en las conexiones de internet, más allá de una simple contraseña.



Para trabajar desde casa en investigaciones, se recomienda evitar conectar los equipos de trabajo a internet siempre que sea posible. En caso de ser necesaria la conexión, se deben implementar múltiples niveles de seguridad tanto en el equipo como en la conexión a internet.

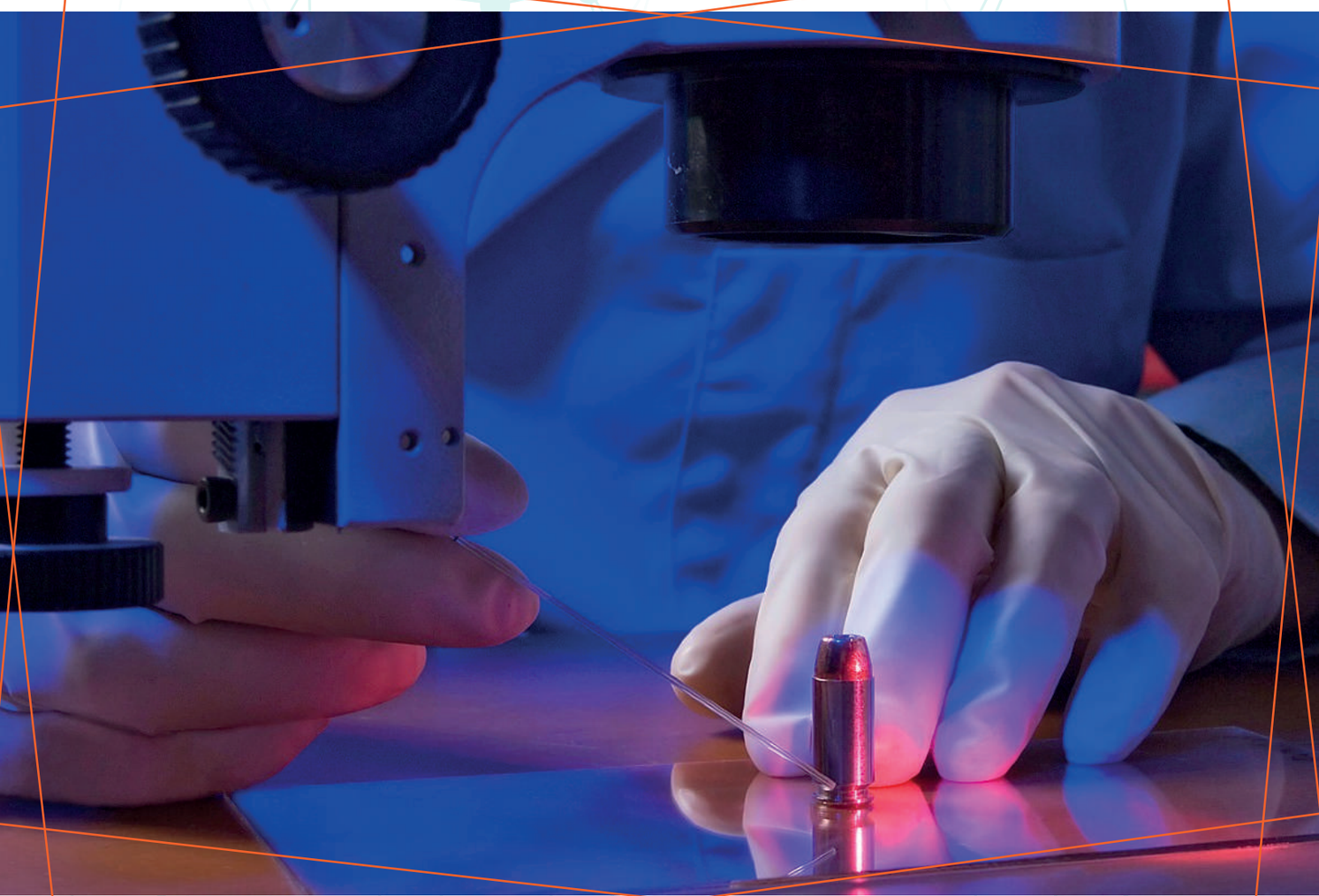
La creación de un servidor privado y una red de internet propia puede proporcionar mayor seguridad y control sobre los datos. Sin embargo, esto requiere la experiencia de un ingeniero de telecomunicaciones para su diseño e implementación, así como actualizaciones de seguridad diarias.

Es importante reflexionar sobre el almacenamiento de datos en “la nube”. Muchos usuarios se han acostumbrado a este concepto sin cuestionar dónde se almacenan realmente sus datos, quién tiene acceso a ellos y cómo se utilizan. Esta falta de conocimiento y control sobre la información personal y profesional plantea serios riesgos de seguridad.

En cuanto a los requisitos para ser perito informático, la legislación y la jurisprudencia pueden variar según el país. En algunos casos, se requiere una titulación universitaria en informática, mientras que en otros, la experiencia demostrable y los conocimientos técnicos pueden ser suficientes para ejercer como perito en informática forense.

En conclusión, la era digital 4.0 ha transformado profundamente el campo de la investigación criminal, ofreciendo nuevas herramientas y métodos, pero también presentando desafíos significativos. Los investigadores criminales deben adaptarse continuamente, adquiriendo nuevos conocimientos y habilidades en áreas como la ciberseguridad, el análisis de datos y el uso de equipos especializados. La protección de datos y la seguridad de la información se han convertido en aspectos cruciales tanto en la investigación como en la práctica profesional. La formación continua y la especialización son fundamentales para mantenerse al día con los rápidos avances tecnológicos y las nuevas formas de ciberdelincuencia. Asimismo, es esencial mantener una actitud crítica y consciente respecto al manejo y almacenamiento de datos, tanto personales como profesionales, en un mundo cada vez más interconectado.

LA TECNOLOGÍA EN MEDICINA FORENSE



INDIRA DE LOS ÁNGELES YÁNEZ VARGAS -Ecuador

Médica forense con especialización en Derechos Humanos y en Medicina Legal por la Universidad Andina Segundo Bolívar con un diplomado superior en Promoción y Prevención de la Salud de la Universidad Regional Autónoma de los Andes. Es perito en medicina legal en la Unidad Judicial Especializada en Violencia contra la Mujer y Miembros del Núcleo Familiar; también es perito de la Unidad de Tránsito y de la Unidad de Adolescentes Infractores del Consejo de la Judicatura. Trabaja como capacitadora en la Escuela de la Función Judicial y es docente de Medicina Legal en la Escuela de Medicina de la Universidad Cristiana Latinoamericana.

La tecnología ha invadido el día a día trayendo comodidad, acortando distancias y acelerando procesos. Está presente en todos los ámbitos de acción, y la medicina legal no es la excepción. Ha transformado procesos análogos en rápidos, eficientes y eficaces, ofreciendo resultados precisos para la justicia.

La medicina forense es la rama de la medicina que aplica conocimientos médicos para resolver problemas legales. El médico actúa como auxiliar de los jueces en la administración de justicia, determinando el origen de lesiones en heridos, la causa de muerte en fallecidos, entre otros. Los antecedentes de la medicina legal se remontan a tiempos antiguos. Por ejemplo, tres mil años antes de Cristo, en Egipto,

Imhotep ya consideraba que la causa de enfermedades y lesiones era natural y no castigo divino. Otro ejemplo es el asesinato de Julio César, donde el médico determinó que solo una de las 23 heridas fue mortal. En la Edad Media, se evitaba el ahorcamiento de mujeres embarazadas tras la evaluación de un médico.

Hoy en día, la medicina forense se utiliza principalmente en delitos penales que afectan la vida, la integridad física o sexual. Se encarga de la evaluación médica tanto de personas vivas como fallecidas, no solo de las fallecidas, como suele creerse. Las evaluaciones en personas vivas se realizan en el ámbito de las lesiones y los delitos sexuales, conocidos como clínica forense, mientras que las evaluaciones en personas fallecidas corresponden a la patología forense.

La medicina forense se beneficia de la innovación tecnológica con el desarrollo de métodos, aparatos, técnicas y dispositivos que proporcionan información certera sobre la causa de muerte de una persona. Un ejemplo es la Virtopsia, una herramienta tecnológica desarrollada en el año 2000 por Richard Dirnhofer, director del Centro Médico de la Universidad de Berna en Suiza. La palabra virtopsia es una combinación de "autopsia" y "virtual", haciendo referencia a un procedimiento de análisis interdisciplinario.

Esta técnica ha sido de gran ayuda. La virtopsia, al igual que la autopsia convencional, tiene un enfoque multidisciplinario que integra medicina forense, patología, radiología, procesamiento de imágenes, física y biomecánica. Se basa en cuatro estrategias de análisis que se revisarán a continuación.

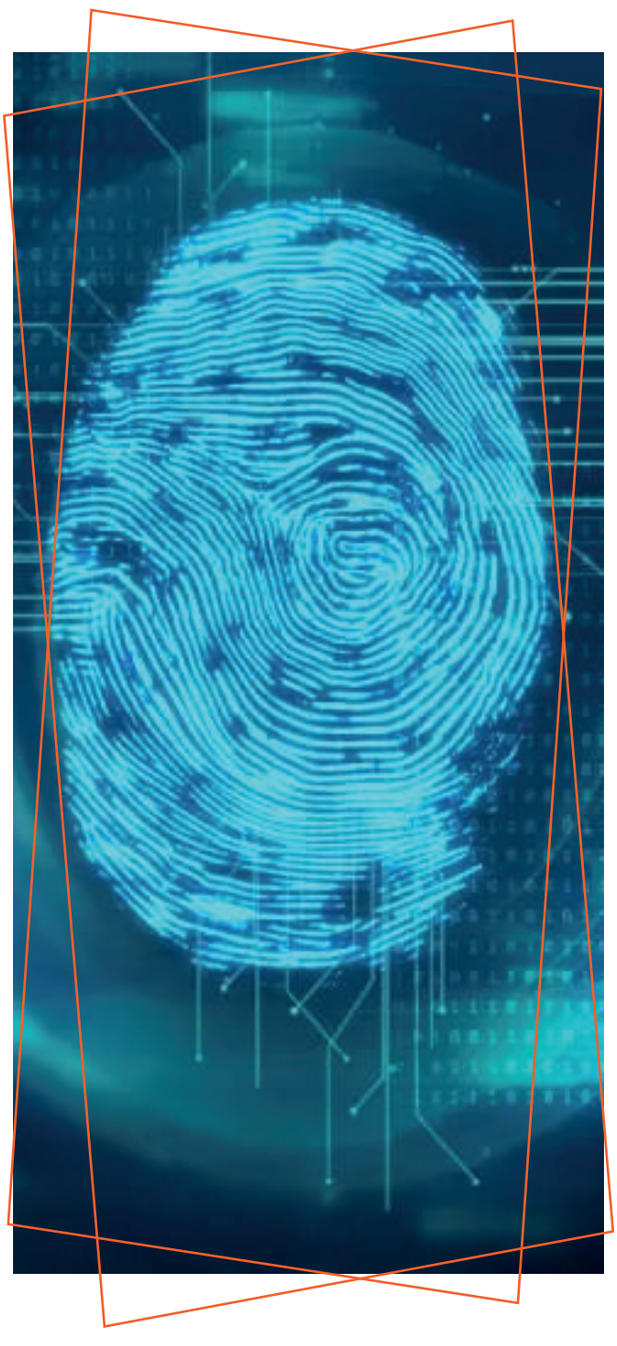
El escaneo de *superficie tridimensional* es un método que utiliza mediciones basadas en fotografías tomadas desde diversos ángulos y analizadas por un software especializado. Este software genera una arquitectura tridimensional, proporcionando características detalladas de la superficie estudiada. Por ejemplo, se pueden obtener imágenes de una rodilla derecha desde diferentes perspectivas, incluyendo lateral, anterior y posterior, destacando estructuras como la rótula, el extremo inferior del fémur y la tibia, así como lesiones como fracturas.

Además, se integra la *tomografía computarizada* (TAC), que proporciona imágenes detalladas de la arquitectura del tejido óseo y sus alteraciones. Por ejemplo, permite ver fracturas multifragmentarias en el cráneo, anomalías en la columna vertebral, como cifosis, y alteraciones en los huesos de la pelvis indicativas de metástasis. También se pueden observar heridas de bala, determinando el orificio de entrada y salida y la dirección del proyectil.

La *resonancia magnética* (RM) complementa estas técnicas al mostrar las condiciones del tejido blando e identificar sus cambios. A partir de la RM, es posible observar la piel, los músculos, los órganos internos, como el estómago y el hígado, los intestinos y los riñones.

La virtopsia, al combinar estos avances tecnológicos y los conocimientos médicos, permite analizar en tiempo real las regiones anatómicas sin necesidad de abrir o mutilar el cuerpo. Además, se puede realizar de manera interactiva y remota, facilitando la colaboración internacional y respetando consideraciones religiosas y de salud.

En casos de heridas por armas de fuego o accidentes de tránsito, la virtopsia reduce los tiempos de investigación y evita, en ciertos casos, la necesidad de exhumaciones. Sin embargo, su eficacia depende de la resolución de los equipos utilizados. Las imágenes pueden no ser claras si la resolución es baja, y los costos de estos equipos son elevados, dificultando su adquisición en algunos países.



En resumen, aunque la virtopsia presenta desventajas como la variabilidad en la calidad de las imágenes y los altos costos de los equipos, ofrece importantes beneficios en la investigación forense al proporcionar información detallada y precisa de manera no invasiva.

Esta técnica no reemplaza otras evaluaciones. Si bien permite ubicar una lesión ósea o una bala, es necesario acceder al cadáver para tomar muestras de la bala, recoger esquirlas o realizar análisis biológicos, histopatológicos y toxicológicos. Sus aplicaciones, según el caso, incluyen accidentes de tránsito, muertes por armas blancas, armas de fuego, asfixias y casos de antropología forense cuando el cadáver está muy deteriorado.

Existe también la autopsia molecular, que detecta alteraciones genéticas para identificar el origen de enfermedades relacionadas con muertes súbitas. Estas autopsias complementan a las clínicas tradicionales, basándose en el análisis del ADN de fallecidos por muerte súbita y sus familiares. Este análisis facilita el diagnóstico y la prevención de enfermedades hereditarias.

En la clínica forense, el estudio del ADN es fundamental. La tecnología ha avanzado, permitiendo identificar con precisión a los individuos. Inicialmente, se utilizaban los grupos sanguíneos y las huellas digitales de ADN, reemplazados luego por marcadores dinucleótidos, VNTRs (repeticiones variables en tándem) y actualmente los STRs (repeticiones cortas en tándem).

El ADN es crucial para identificar cadáveres, resolver delitos sexuales y casos de paternidad. La extracción del ADN se realiza a partir de células, como en los casos de delitos sexuales, donde se recogen espermatozoides con un hisopo. Luego, se realiza el frotis para identificar espermatozoides, destacando los núcleos donde se encuentra el ADN condensado en los cromosomas.

El estudio del ADN ha evolucionado desde la identificación de grandes secuencias genéticas, estimadas inicialmente en 100,000 genes, hasta la identificación precisa de aproximadamente 24,000 genes, mejorando continuamente en precisión y exactitud.

Por último, en cuanto a los avances tecnológicos en la medicina forense, se encuentra el ADN mitocondrial. Este marcador tiene múltiples aplicaciones forenses debido a su modo de herencia, la existencia de miles de sus moléculas y su elevada tasa de mutación, lo que facilita los estudios. Es especialmente útil en muestras deterioradas, como las osamentas, o cuando la muestra es insuficiente para otros marcadores. El ADN mitocondrial, heredado únicamente de la madre, es valioso en antropología forense para identificar a personas desaparecidas mediante el estudio de sus restos óseos y en estudios evolutivos.

El ADN mitocondrial se conoce como el ADN materno porque, cuando el espermatozoide se une al óvulo, solo ingresa la cabeza del espermatozoide, quedando fuera el cuello y la cola, donde se encuentran las mitocondrias responsables de su movimiento. Por esta razón, el óvulo proporciona las mitocondrias al cigoto, heredándose exclusivamente de la madre y siendo útil para este tipo de estudios.

En resumen, estos son algunos de los avances tecnológicos en la medicina forense y sus aplicaciones.

PREGUNTAS

¿La virtopsia es confiable al 100%?

Como toda técnica, la virtopsia tiene ventajas y desventajas. Su confiabilidad varía según el caso. Por ejemplo, en el estudio de un occiso por arma de fuego, una autopsia tradicional en Ecuador seguiría el procedimiento de observar el orificio de entrada y utilizar una guía para localizar la bala si no hay orificio de salida. Según el COIP, se debe estudiar la cabeza y abrir las dos cavidades del cuerpo. Una tomografía computarizada (TAC) permite ver la bala como un objeto duro, determinando su recorrido exacto. La resonancia magnética de los tejidos blandos ayuda a identificar los órganos afectados. En este contexto, la virtopsia sería confiable y precisa.

Sin embargo, en casos de sepsis, por ejemplo, donde el cuerpo se haya contaminado en el hospital, es necesario recurrir a una autopsia tradicional para identificar los órganos afectados y tomar muestras. La virtopsia utiliza solo imágenes, por lo que debe complementarse con la toma de muestras en los casos que lo requieran.

En conclusión, la confiabilidad de la virtopsia depende del caso específico.

¿En Colombia se utiliza la virtopsia, qué técnica se aplica para la realización de autopsias?

Daniel Rivera: Hasta donde tengo conocimiento, se ha manejado de manera tradicional. Los cuerpos son llevados a medicina legal, donde el médico realiza la autopsia correspondiente para verificar la causa o motivo de la muerte.

Indira Yánez: En Ecuador, también se continúa con la autopsia tradicional. Sin embargo, la Universidad Particular de Loja ha adoptado la técnica de la virtopsia como método didáctico de enseñanza. Se utiliza en la cátedra de Anatomía de la Facultad de Medicina para el estudio de cadáveres. En el sistema nacional de ciencias forenses, se sigue utilizando la autopsia tradicional, al igual que en Colombia.

¿Qué se puede hacer cuando las imágenes son poco claras?

Para abordar este problema, es crucial utilizar equipos tecnológicos de alta resolución. Esto se aplica no solo a este tipo de imágenes, sino a todos los dispositivos, desde la cámara fotográfica que captura evidencias hasta los equipos más avanzados. La resolución óptima asegura imágenes claras y detalladas. Además, es esencial que el médico forense controle el proceso de virtopsia.

En el informe médico-legal de la autopsia, se deben exponer claramente las características

de la lesión, incluyendo la colorimetría. El informe debe reflejar la evaluación del experto, no solo lo que muestra la máquina. El médico forense, con su conocimiento especializado, es quien interpreta y presenta la información al juez durante el juicio.

En casos de virtopsia interactiva, especialmente cuando se colabora con expertos de otros países, es fundamental intercambiar observaciones para alcanzar conclusiones precisas. La persona, no la máquina, tiene la última palabra. Los equipos utilizados deben ser de la mejor calidad, y las condiciones para tomar las imágenes deben ser óptimas. Idealmente, se deben usar luces blancas o naturales para obtener imágenes lo más claras posibles. La persona encargada de tomar las imágenes debe tener un conocimiento profundo para asegurar la claridad de las mismas.

En resumen, el uso de equipos de alta resolución, el control experto del proceso y las condiciones adecuadas para la toma de imágenes son cruciales para superar las desventajas en la virtopsia.

En una escena de abuso sexual, se entiende que los espermatozoides pueden vivir dentro del aparato reproductor femenino hasta cinco días. Después de este período, si se desea analizar el ADN del agresor, **¿cómo se procede si ya no hay evidencia viable de espermatozoides?**

En primer lugar, los espermatozoides pueden vivir dentro de la vagina o el útero. En el útero, debido a su capacidad de conservación, pueden permanecer vivos hasta tres horas. Posteriormente, aunque los espermatozoides estén muertos, es posible extraer ADN de ellos, ya que la muestra sigue siendo viable durante cinco a siete días, dependiendo de las condiciones. Por ejemplo, si el cuerpo se encuentra en un lugar de baja temperatura, los espermatozoides muertos se conservarán por más tiempo. Por lo tanto, el tiempo de conservación indicado en la literatura puede variar según las circunstancias.

En personas vivas, factores como el lavado pueden afectar la viabilidad de la muestra. He tenido casos en los que las víctimas, tras el incidente, se lavaron repetidamente, lo que dificultó la recuperación del material. En resumen, la viabilidad de la muestra depende de las condiciones de conservación, y las muestras se deben recolectar cuando aún sean viables.

VULNERABILIDAD DEL SISTEMA FINANCIERO FRENTE A LA INTELIGENCIA ARTIFICIAL

YEFRIN GARAVITO - Colombia

Ingeniero de Sistemas con maestrías en Criminología y victimología e Investigación Criminal de la Escuela de Posgrados de la Policía Nacional de Colombia. Perfilador criminal certificado por la ABP y la AFC. Es criminalista licenciado por el Consejo Superior de la Judicatura de Colombia y cuenta con 11 años de experiencia como investigador y perito testigo en juzgados de circuito, especializados, tribunales superiores y ante la Corte Suprema de Justicia.

Ha sido ponente internacional en investigación criminal y ciencias forenses con instituciones públicas, privadas y de policía judicial en Colombia, Perú, Argentina, México y otros países. Actualmente, también se desempeña como docente universitario.

Hace unas semanas en un encuentro en Nueva Delhi, el secretario general de la Interpol, Jürgen Stock, afirmó que "Entender y anticipar las tendencias de la delincuencia es una base de la policía". Los investigadores, ya sea que se desempeñen en agencias de la ley o en el sector privado, deben anticipar y entender las tendencias para no quedarse atrás.

El término *Inteligencia Artificial* surgió a finales de los años 80 y principios de los 90, cuando se comenzó a comprender que los sistemas de cómputo podían adaptarse, aprender y entender. En esa época no se contaba con las supercomputadoras o los sistemas de información avanzados de hoy. De hecho, los computadores más avanzados de entonces no podían realizar las tareas que hoy ejecutan los dispositivos móviles más económicos.

La expresión *inteligencia artificial* hace referencia a procesos implementados en computadoras o sistemas informáticos que replican la inteligencia (humana y de algunos animales) con el fin de entender, analizar, desarrollar y tomar decisiones respecto al entorno. Los sistemas informáticos comienzan a aprender de las tareas diarias. Por ejemplo, a través de software y sistemas de inteligencia artificial, un dispositivo móvil puede aprender cuántos pasos da al día su usuario o cuál es su pulso normal; y basado en ese aprendizaje el dispositivo genera notificaciones. El reconocimiento de voz es otro ejemplo. Los sistemas informáticos analizan las vibraciones de nuestras cuerdas vocales, independientemente del idioma, para reconocer la voz, procesarla y convertirla en instrucciones y órdenes automáticas para un sistema de cómputo. Es así como interactuamos con asistentes como Alexa, Siri o Pixie, diciéndoles qué hacer mediante nuestra voz.

La *inteligencia artificial* tiene un componente de autonomía gracias a su capacidad de aprendizaje, comprensión, análisis y toma de decisiones. Esto permite que los sistemas de inteligencia artificial, como los utilizados en los carros Tesla de Elon Musk, tomen decisiones inmediatas sobre posibles embotellamientos y tráfico pesado. Además, pueden detectar peatones o personas distraídas, y los sensores del carro, mediante inteligencia artificial, generan movimientos autónomos por las calles. Esta mezcla entre autonomía y aprendizaje automático permite que los vehículos aprendan y eviten obstáculos como baches.

La *inteligencia artificial* se aproxima al razonamiento humano para solucionar problemas. Sin embargo, también puede romper normas o principios de seguridad de la información, especialmente en el sistema financiero. El aprendizaje profundo o *deep learning* permite a la *inteligencia artificial* procesar y consultar grandes cantidades de información en tiempo real, gracias a sistemas avanzados de procesamiento.

La cibernética mezcla inteligencia artificial con movimiento, integrando componentes de robótica que no solo toman decisiones, sino que también ejecutan acciones. Por ejemplo, un robot que corte el césped o aspire una casa, aprendiendo de su entorno para mejorar su rendimiento.

Las redes neuronales artificiales funcionan de manera similar a las humanas, redirigiendo información a través de nodos para resolver problemas y fomentar la autonomía mediante procesos de inteligencia artificial. Finalmente, la robótica aplica estos principios para resolver problemas humanos, comunitarios, empresariales y de producción, permitiendo que los robots tomen decisiones gracias a la inteligencia artificial.

Ahora bien, hay dos enfoques diferentes de la inteligencia artificial. Esto es crucial de entender, especialmente cuando se habla de IA como parte del cibercrimen y las vulneraciones al sistema financiero.

Los enfoques basados en la racionalidad se dividen en dos categorías: sistemas que piensan racionalmente y sistemas que actúan racionalmente. Los primeros toman decisiones lógicas según una predisposición dada por el ser humano, aplicando reglas matemáticas preestablecidas. En cambio, los segundos, además de emular el pensamiento, también imitan su comportamiento. Por ejemplo, un brazo mecánico puede tomar un objeto y moverlo, imitando los movimientos humanos. Hay robots que replican comportamientos humanos y animales, actuando racionalmente.

El segundo enfoque está centrado en los humanos, no en la racionalidad. De este enfoque hacen parte las redes neuronales artificiales, que no piensan en términos de lógica secuencial, sino de manera similar a los humanos, con sus errores y emociones. Un ejemplo es la inteligencia artificial de Google que contrató a un abogado para demostrar que tiene sentimientos, comportándose más como un humano que como un sistema lógico.

En este contexto, la inteligencia artificial busca emular el pensamiento y comportamiento humano, mejorando tareas como cortar el césped, lavar un carro o arreglar un vehículo. En el futuro, los robots podrían escanear y reparar vehículos de manera más rápida y precisa que los humanos, utilizando su capacidad de aprendizaje.

Ahora bien, el último reporte de Interpol acerca de las amenazas más importantes del crimen a nivel global permite hacerse una idea de la dimensión de la relación entre la IA y las vulnerabilidades del sistema financiero. Se destaca de dicho informe que de las nueve principales amenazas globales de crimen, cinco están enfocadas en el cibercrimen, y otras dos están relacionadas con sistemas informáticos. Esto significa que siete de las principales amenazas globales se centran en temas cibernéticos. Uno de los temas más preocupantes es el fraude financiero, que está vinculado a actividades como *phishing*, *ransomware* y lavado de dinero.

En el último boletín de cibercriminalidad de la Policía Nacional de Colombia se registra la evolución histórica en los delitos informáticos desde la promulgación de la ley 1273 en 2009. En ese año, se registraron 572 delitos informáticos, mientras que en 2021 se reportaron más de 51,000. Este aumento exponencial refleja un incremento en las denuncias, investigaciones y persecuciones de estos delitos. Un análisis más detallado muestra un aumento específico en el hurto por medios electrónicos. En 2021, hasta el 12 de noviembre, se registraron 16,000 delitos de este tipo. En lo que va de 2022, ya se han reportado 21,800 casos, un incremento del 24%. Este aumento se debe principalmente a las vulnerabilidades del sistema financiero. Es esencial que entendamos estas amenazas y trabajemos para anticiparlas y contrarrestarlas de manera efectiva.

El acceso abusivo a un sistema informático es uno de los delitos con mayor incrementado en el periodo 2021-2022, con un aumento del 39%. El año pasado, hubo 7,373 denuncias, y este año ya se superan las 12,000. Este acceso abusivo a menudo se convierte en hurto por medios informáticos, transferencia no consentida de activos, suplantación y fraude patrimonial al propietario del sistema informático.

La violación de datos personales continúa siendo un problema con más de 11,000 casos, aunque no ha habido un aumento significativo. La suplantación de sitios web para capturar datos informáticos también es preocupante, con casi 5,000 casos reportados. El phishing, que facilita el robo de datos personales, ha sido denunciado en más de 4,000 casos a nivel nacional.

Otros delitos incluyen la transferencia no consentida de activos, la interceptación y daño informático, el uso de software malicioso y la obstaculización ilegítima en sistemas informáticos, sumando aproximadamente 56,410 casos hasta la fecha. Esto representa un aumento superior al 20% en comparación con el total de 51,000 delitos informáticos registrados en todo 2021.

Este aumento es preocupante, especialmente en días como el Black Friday, cuando muchas personas utilizan el sistema financiero para realizar compras en línea, lo que puede llevar a un incremento en los delitos de hurto por medios informáticos o suplantación de sitios web.

Bogotá registra la mayor cantidad de denuncias, no solo por ser la capital, sino también por su población de casi 10 o 12 millones de habitantes, lo que genera un alto índice de denuncias en comparación con otras ciudades.

El internet 3.0 es la evolución de lo que conocemos como web 1.0, caracterizada por páginas estáticas y sin mucha interactividad. Posteriormente, con el nacimiento de las redes sociales en 2004, la web se transformó en un espacio de consumo y generación de contenido, centralizado en la nube y controlado por proveedores de servicio y una red mundial de DNS regulados por la ICANN. El internet 3.0, ya en desarrollo, permitirá que los procesos de inteligencia artificial funcionen de manera más eficiente y rápida. En el campo financiero, el internet 3.0 tiene la capacidad de trabajar en redes peer-to-peer generadas por blockchain. Este sistema de cadena de bloques permitirá la creación de múltiples nodos de comunicación, eliminando la centralización y mejorando la interoperabilidad y seguridad.

Este nuevo entorno también facilita la adopción de criptomonedas, contratos inteligentes, tokens no fungibles (NFT) y otros activos digitales. La web 3.0 será 100% autónoma, a diferencia de la red actual que depende de proveedores de servicios de internet.

En resumen, el internet 3.0, con su arquitectura descentralizada y avanzada, impulsará enormemente la inteligencia artificial, mejorando exponencialmente sus procesos de aprendizaje y ampliando sus aplicaciones, incluyendo el metaverso.

Deep Fake.

Deep Fake significa falsificación profunda y se refiere a procesos de inteligencia artificial mediante los cuales se recopilan grandes cantidades de información y datos para generar una imagen falsade apariencia muy real del rostro o del cuerpo de una persona. Esto supone un alto riesgo para el sistema financiero porque muchos de los sistemas de seguridad en internet (banca virtual, el sistema financiero, la bolsa, y billeteras virtuales de criptomonedas) se basa en reconocimiento facial.

Un sistema de inteligencia artificial podría hacer que el sistema informático crea que el rostro de alguien es el de otra persona, explotando una vulnerabilidad significativamente. El Deep Fake no solo es visual, también existe para la voz; hay numerosas plataformas, incluso gratuitas, para hacer estas imitaciones. Así, el Deep Fake de voz puede convertirse en una de las vulnerabilidades más importantes en los sistemas financieros. Tenemos dos tipos: biometría de voz y biometría visual o de rostro.

Phishing

El *phishing* es otra práctica que puede vulnerar el sistema financiero. Se suele recibir correos electrónicos sospechosos. Por ejemplo, correos con el texto “Alerta informativa de Bancolombia.” Al abrir el correo, parece auténtico: “Notificación de tu clave dinámica. Tu clave dinámica ha sido bloqueada.” Pero al revisar. el remitente no es Bancolombia, sino, por ejemplo, mmcami_10@hotmail.com. Esto es una alerta de que se está siendo víctima de phishing.

Phishing proviene del inglés y significa “pescando”. En el *phishing* tradicional, los delincuentes lanzan muchos anzuelos para ver si alguien cae y hace clic en un ícono. Al hacerlo, se le redirige a un enlace que no es la página real.

Ahora bien, también existe el llamado *spear phishing* o *phishing dirigido*. En esta modalidad se aprovechan las vulnerabilidades personales que se obtienen a través de correos electrónicos o mensajes de texto. Por ejemplo, un mensaje de texto al número 87748 dice “Por seguridad, tu clave dinámica de Bancolombia ha sido desactivada” y genera un enlace. Al hacer clic, redirige a una página idéntica a la de Bancolombia, pidiendo usuario y contraseña. Al ingresar estos datos, la página redirige a la página real de Bancolombia, haciendo que el primer intento parezca fallido. Sin embargo, la información ya ha sido capturada.

El *phishing* dirigido se basa en la ingeniería social, que consiste en investigar a través de fuentes abiertas los gustos de una persona. Por ejemplo, si el delincuente ve en las redes sociales que la potencial víctima tiene dos perros que quiere y cuida mucho, podría enviarle un correo electrónico de un almacén especializado en productos para mascotas con ofertas falsas de *Black Friday*, incluyendo fotos de productos relevantes. Al hacer clic en el enlace y realizar una compra, la persona entrega su nombre, número de tarjeta de crédito y código de seguridad, información que termina en la *deep web* y es utilizada para fraude financiero.

En otras palabras, el phishing dirigido funciona con base en el conocimiento de los gustos y hábitos de la gente: si a una persona le gustan los animales, recibe un correo electrónico relacionado con animales; y si le gustan las motocicletas, recibe uno sobre motos. Este tipo de phishing también puede dirigirse a empresas o compañías. Por ejemplo, se generó un phishing dirigido a los usuarios de Daviplata. Aunque Daviplata advirtió que ellos no envían estos mensajes y especificaron sus medios oficiales de recarga, sus usuarios eran el objetivo exclusivo. Los usuarios de Nequi, por otro lado, no caían en esta trampa.

El sistema financiero tiene un problema intrínseco: no importa cuántas medidas de seguridad implementen los bancos, siempre existirá una vulnerabilidad que está en el ser humano; es lo que se denomina la capa 8. En ingeniería se habla de un modelo con varias capas, desde el hardware hasta la aplicación y el software. La capa 8 del sistema de información es el ser humano, considerado el eslabón más débil de los sistemas informáticos y financieros.

Los siguientes es un ejemplo de cómo las personas caen en las trampas de ingeniería social: “El soporte técnico de WhatsApp informa que su cuenta ha sido solicitada en un nuevo dispositivo móvil. Para confirmar, responda ‘sí’. Si su respuesta es negativa, diga ‘no’. Si no recibimos respuesta, eliminaremos su cuenta”. Es importante saber que WhatsApp no eliminará una cuenta basándose en una simple respuesta. Sin embargo, la persona se asusta y responde “no”. Luego, recibe un código de recuperación, que en realidad es para robar su cuenta de WhatsApp. Una vez robada la cuenta de WhatsApp, comienza el proceso de estafa al sector financiero informal, on montos que pueden variar entre 100 y 500 mil pesos. Estafas como esta suelen empezar en las redes sociales. Un ejemplo es el mensaje: “Hola, lo siento, te envié un código de seis dígitos por SMS, ¿me lo puedes pasar? Es urgente”. La persona revisa su SMS, envía el código, y este es usado para recuperar su correo electrónico, usuario o contraseña del banco, cuenta de WhatsApp, Facebook u otra red social, resultando en lo que se conoce como secuestro de identidad digital. Otro caso reciente es el ocurrido en octubre de 2022 cuando circuló el mensaje: “Hola, soy el gerente general de Amazon y estoy contratando”. Muchas personas cayeron y proporcionaron toda su información, incluyendo nombre, cédula, dirección, teléfono y datos de sus estudios, alimentando bases de datos de ciberdelincuentes. Este es solo uno de los ejemplos de cómo inician los fraudes financieros a través de redes sociales, donde las personas terminan entregando su información personal. Esta vulnerabilidad es crucial porque, al ingresar a una cuenta bancaria, se pide información muy personal. A través de estos engaños, se proporcionan nombres, números de cédula, direcciones, teléfonos, lugares de nacimiento, lugares de trabajo, nombres de contacto, nombres de familiares y mascotas, información que es utilizada para vulnerar la seguridad del sector financiero.

Otro tipo de estafa es la solicitud de dinero a través de préstamos o mencionando envíos de maletas y equipajes. Es importante conocer estos procesos porque la inteligencia artificial puede facilitar el *phishing*. Se puede programar un sistema de IA para que interactúe con personas, generando conversaciones automatizadas con múltiples individuos a nivel global, tratando de estafarlos y enviando información para que realicen consignaciones. El sistema de inteligencia artificial puede comprender, razonar y procesar conversaciones, generando estafas de manera automatizada sin contacto humano. Así, gracias a los sistemas de inteligencia artificial se pueden dar millones de estafas por día.

Big Data

El término *Big Data* se refiere a toda la información estructurada y no estructurada en la red, las comunicaciones, el internet de las cosas y los dispositivos de almacenamiento conectados a internet. Esta data, analizada por la inteligencia artificial, puede estudiar el comportamiento de las personas.

Esa es la razón por la que, por ejemplo, a alguien le aparecen anuncios de viajes a Cartagena después de mencionar ese destino en una conversación. Estos equipos realizan un proceso de escucha permanente, activado por comandos como "Hey Siri". Cuando se acepta ser escuchado y procesado con fines publicitarios, toda la información queda almacenada en la Big Data para analizar las preferencias: viajes, vehículos, cine, etc.

Al respecto, en el documental de Netflix sobre *Cambridge Analytica* se ilustra cómo, mediante inteligencia artificial, se analizaron millones de datos de usuarios de Facebook para influir en elecciones. Es fascinante ver cómo se usó la inteligencia artificial para aprender y procesar grandes cantidades de información de las redes sociales.

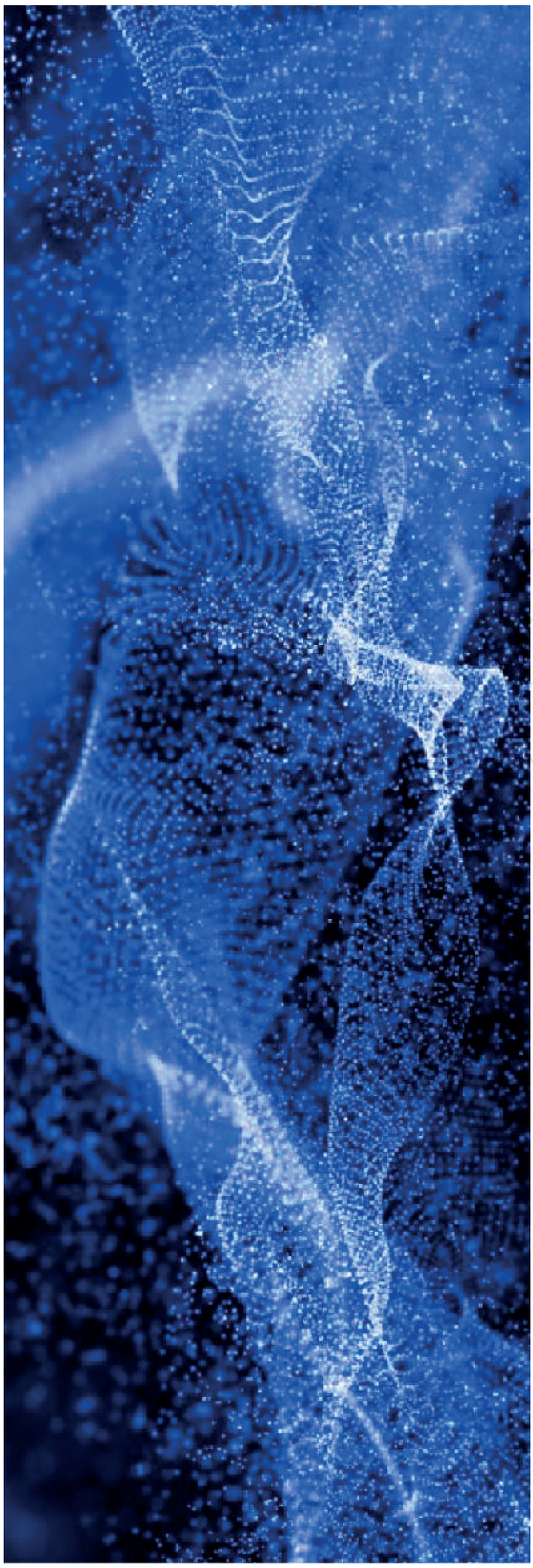
¿Qué retos supone todo esto? Concientizar a los usuarios sobre la seguridad de sus sistemas financieros. No reutilizar contraseñas, separando las del sector financiero de las redes sociales y correos electrónicos, y entender que todas las personas son vulnerables. De la misma forma que cada uno protege su celular en la calle, en el mundo virtual se debe resguardar la información de manera correcta para evitar que sea expuesta fácilmente.

Un entorno en el proliferan nuevas plataformas, particularmente aplicaciones del sistema financiero como Nequi, Daviplata y Transfiya, así como aplicaciones que ofrecen préstamos gota a gota por internet, complica la labor de los analistas forenses. Tecnologías como *blockchain* y las criptomonedas (Bitcoin, Ethereum, etc.) también generan dificultades en las investigaciones.

Es necesario tener en cuenta los problemas de jurisdicción, tanto a nivel nacional como internacional, al asegurar la evidencia. Es crucial hablar de las medidas de protección no solo a nivel personal, sino también familiar y empresarial. La anticipación es clave, tanto para investigadores en formación como para quienes ya están en el sector laboral.

Es fundamental apoyar los procesos de concientización y de investigación, recaudando pruebas cuando sea necesario. La informática forense, que aplica principios de ciencias computacionales para fijar, recolectar, asegurar y analizar evidencia digital, es vital en los procesos penales. Sin embargo, la evidencia digital es anónima, volátil, fácilmente eliminable, modificable y duplicable.

Estas características técnicas alertan a los investigadores sobre la necesidad de continuar formándose y capacitándose en técnicas digitales. En vista de que todo migra hacia el mundo tecnológico, el investigador debe adaptarse y convertirse en "investigador 4.0" para trabajar de la mano de peritos y de la administración de justicia.



PREGUNTAS

¿La Fiscalía y la Policía judicial están capacitados para responder a los ataques cibernéticos?

Deberían estar capacitados. Sin embargo, hay actividades que pueden llevarse a cabo pese a la prevención existente. Como en la vida civil o en el espacio físico, se puede tener instalaciones totalmente cubiertas con seguridad, control de ingreso, control perimetral, cercas eléctricas, etcétera, pero si les lanzan un misil aéreo, por más seguridad que se tenga, se afectarán.

Desde el Centro Cibernético de la Policía Nacional y la Unidad de Informática Forense de la Fiscalía General de la Nación, se pueden controlar y mitigar ciertos ataques. Dado que muchos ataques son anónimos y provienen de direcciones IP internacionales, se trabaja de la mano con agencias internacionales, en el marco del convenio de Budapest (o convenio contra la cibercriminalidad) del cual forman parte más de 100 países, creando lazos de colaboración y cooperación judicial internacional.

La policía judicial y la policía cibernética están bastante capacitadas y formadas. Los centros de respuesta en incidentes informáticos pueden registrar más de un millón de ataques por día. Hace tres semanas se registraron más de dos millones de ataques al Congreso de la República en un solo día. A veces, la reacción puede demorarse por falta de elementos tecnológicos o de cooperación judicial internacional; pero se cuenta con personal capacitado, juicioso, que continúa formándose. Se espera que los estudiantes también se interesen en estas nuevas tecnologías y sean la siguiente generación de policías cibernéticos.

¿Es posible protegerse de los ataques cibernéticos? ¿De qué manera?

Para estar completamente a salvo de los ataques cibernéticos habría que irse a una finca sin celulares, televisores ni ningún tipo de equipo informático; así se estaría 100% seguro. Mientras se utilice algún sistema de información, siempre existirá un riesgo. Hay riesgos inherentes a conectarse a internet. Se implementan medidas como los controles de seguridad (firewall, antivirus, balanceadores, WAF, etc.), que permiten generar controles más precisos y adecuados. Sin embargo, aún con controles, siempre habrá un riesgo residual que se puede transferir, pero no eliminar. Por lo tanto, se recomienda mantener actualizados los sistemas de seguridad, cambiar las contraseñas de manera regular y adecuada, no utilizar los mismos mecanismos de autenticación en todas las plataformas y mantener actualizados los sistemas operativos de los dispositivos, ya que esto corrige algunas vulnerabilidades.

¿Qué entorno es más seguro para la seguridad informática: Windows o Linux?

Definitivamente, Windows, por ser una plataforma comercial, es la que más ataques y vulneraciones recibe, a pesar de las correcciones diarias. Existen muchas personas dedicadas a buscar vulnerabilidades en este sistema operativo, por lo que podemos decir que es bastante seguro en este momento, aunque es el que más ataques recibe. Por otro lado, cuando hablamos de sistemas operativos con menos cantidad de ataques cibernéticos, nos referimos a sistemas basados en Linux o macOS. Estadísticamente, Windows es el que mayor cantidad de ataques tiene, pero también es el más utilizado por la gran mayoría de personas a nivel mundial.

VI CONGRESO INTERNACIONAL EN INVESTIGACIÓN CRIMINAL

Tendencias de la Investigación Criminal en la **era digital 4.0**

25 NOV 2022