Facultad de Contaduría Pública
Accountancy Professional Pronouncement Observatory –APPO

Documentos de las conclusiones

TÍTULO DEL EVENTO:

II Evento Internacional.
AUDITORÍA e INFORMÁTICA FORENSES: Retos y Tendencias.

OBJETIVOS

Conocer las tendencias, enfoques y nuevas técnicas que a nivel mundial se están dando en la informática forense, los retos y tendencias, construyendo vínculos o redes de conocimientos, a partir de las experiencias y los estudios de expertos, en la administración y gestión del riesgo, cumplimiento de protocolos de auditoria e informática forenses, manejo de grandes volúmenes de información, entre otros

CONFERENCISTAS y EJES TEMÁTICOS

Expertos consultores y auditores con experiencia tanto en el sector privado como el público y la academia, con diferentes experiencias en la gestión de proyectos en procura de la seguridad informática de las organizaciones y su información sensible.

A continuación la relación de conferencistas, sus perfiles y el eje temático de su presentación:

	Expositores y Moderador	Perfil académico	Título o temática de la Conferencia
1	Albert J. Marcella Jr.	Ph.D., CISA, CISM. President, Business Automation Consultants, LLC.	Fundamental Cyber Forensics. Junk Science Attack and the Investigator Rules of Evidence; Importance and Application to Forensic Investigations Establishing a Credible Chain of Custody. Investigation Methodology; The Good, the Bad, and the Dangerous. Potential Exposures; Minimizing Your Risk and Exposure Presenting the Evidence Report; Successfully.
2	Freddy Bautista García	Jefe del Centro Cibernético Policía, Experto en investigación Cibercriminal y	Necesidades del Estado y las entidades públicas frente a las

		Fraude Policía Nacional-Dirección de Investigación Criminal e INTERPOL, Presidente del Grupo de Jefes de unidades de Cibercrimen para las Américas.	tendencias en la auditoria de informática forense para apoyar la justicia.
3	Luis Edmundo Suárez Soto	Abogado Especialista en Economía y Derecho Administrativo. Líder de iniciativas estratégicas en Big Data y Analítica	Uso estratégico de la Big Data y la inteligencia en investigaciones forenses.
4	Arturo del Castillo (Mexicano)	Consultor y Asesor Empresarial.	Experiencias en Latinoamérica en la Auditoria de Informática Forense y los delitos de cuello blanco en el campo empresarial.
5	Jeimy J. Cano Martínez	PhD. CFE. Profesor Distinguido y miembro fundador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes.	Ecosistema Digital Criminal (EcoDC). Nueva frontera de la investigación criminal.

RESUMEN

La sociedad en general enfrenta modalidades cada vez más sofisticadas de criminalidad cibernética, con un enfoque globalizado. Los criminales digitales, cada vez más, aumentan su presencia en la sociedad con el máximo anonimato y el mínimo de rastros disponibles.

Se tienen identificadas varias tendencias de criminalidad en los ambientes informáticos, entre las cuales se mencionan las siguientes:

- Existen estructuras complejas de información y de redes criminales las cuales son exploradas a través de la minería de datos.
- Intensificación del uso de la criptomoneda (medio virtual de pago) como mecanismo para evadir controles y dejar el mínimo de rastro o eliminarlo de ser posible. En el nuevo diseño de la sociedad, la criptomoneda es una nueva representación de los hábitos de dicha sociedad.
- De condiciones estáticas y conocidas, han pasado a escenarios dinámicos e inciertos.

- El crimen financiero es de los que más han crecido en tiempos recientes.
- En sus inicios el crimen cibernético tenía una alta calidad técnica, la capacitación era realizada por cuenta propia; luego pasa a una etapa con calidad técnica baja, que buscaba el dinero rápido a través de replicar lo que ya estaba hecho; después, llega una generación (Millennians) que piensa diferente y roba diferente, han creado milicias cibernéticas a través de la vida virtual sin pensar en las consecuencias; en la actualidad se vislumbra la llegada de la generación de los Drones, a través del desarrollo de inteligencia artificial y la creación de robots cibernéticos y drones.

- Cada vez toma más fuerza navegar en la internet profunda o *DarkNet*; estos sitios son un "Caldo de cultivo" para los criminales debido al anonimato y la impunidad que los rodea.

- El crimen cibernético ha modificado sus estructuras operativas, pasando de una organización jerarquizada totalmente vertical a otra que actúa mediante redes que representan un sistema social, computacional o biológico.

- *Randsomware*, que radica en secuestrar los datos de la víctima a través del cifrado complejo de la información y pedir un rescate en bitcoins para liberarla.

- Mayor proliferación de focos de infección como descargas de aplicaciones, phishing, correos, entre otros.

- Otras actividades criminales en el medio virtual comprende ataque a los bienes inmuebles a través del internet de las cosas, o el cada vez más conocido uso y cambio de las *bitcoins*.

Estas nuevas tendencias del crimen cibernético e informático, demandan nuevos retos para la sociedad y los diferentes agentes que pueden aportar en la solución del problema. Entre otros retos se mencionan los siguientes:

- Cambiar el enfoque de las investigaciones, conformando equipos interdisciplinarios, que actúen organizados y con una mirada global del tema, audaces para cambiar o adaptarse a los cambios. Es decir, de condiciones estáticas y conocidas deben pasar a escenarios dinámicos e inciertos.

- En cuanto a la academia, es necesario que esta se involucre más en los proyectos de investigación sobre fraudes y crimen cibernético; debe asociarse con las industrias y el sector empresarial, pero también tiene la oportunidad para presentar y ejecutar ofertas de valor con una mirada holística de la problemática.

- Formar investigadores con un perfil transdisciplinar, con pensamiento complejo y sistemático, capaces de analizar y entender a las relaciones más que a los elementos, especializados, personas con la capacidad de tener un pensamiento disruptivo, como elemento de supervivencia.

- El Banco Central de los diferentes países, tendrán que poner en la balanza los más y los menos de la criptomoneda, conocer y entender su presente para determinar su impacto en el futuro, puesto que al ser uno de los mecanismos de pago preferido por los cibercriminales, al mismo tiempo sus condiciones de seguridad para las transacciones, resulta ser un elemento interesante para el sector financiero.

- Para el Estado y los países en general, se hacen necesarios nuevos desarrollos normativos, no solo endureciendo las penas existentes sino estableciendo nuevos criterios para tipificar las nuevas conductas delictivas de los cibercriminales.

- Fomentar la ética empresarial.

- La información debe ser analizada a través de plataformas para la toma de decisiones.

- Teniendo en cuenta que la información es considerada “el oro de las organizaciones”, hay un desafío para los investigadores forenses del cibercrimen de ampliar su horizonte y conceptos. En general, se debe ampliar el panorama y mejorar la visión hacia el crimen financiero.

- Se ha creado una economía digital criminal a partir de la creación de la oferta y demanda de crímenes en el ciberespacio. Esta situación plantea el reto de contar con suficientes y adecuados recursos, para enfrentar de manera estructurada las nuevas estructuras de los cibercriminales.

Facultad de Contaduría Pública
Accountancy Professional Pronouncement Observatory –APPO

Documentos de las conclusiones

COMENTARIOS GENERALES

Tema: **Delitos cibernéticos.**
De la data a la Evidencia Digital

El doctor Albert Marcella Jr., plantea que se necesita de un equipo multidisciplinario para realizar el análisis forense de la evidencia de los casos en donde se incluya, pero no se limite, a la auditoría de tecnología, la psicología para conocer el perfil del perpetrador, habilidades de entrevista, laboratorios especializados, uso de software especializado y certificado, entre otros.

Para él, en la actualidad los criminales tienen mayores habilidades y buscan utilizar la tecnología a su favor; para ellos la investigación resulta ser un proceso complejo que incluye prueba y error hasta lograr el objetivo que es aprovechas las vulnerabilidades de los sistemas; es por ello que los examinadores forenses deben ser personal entrenado para extraer evidencia y hacer visible lo que no es claro para la concurrencia en un juicio, la información puede pasar de una partícula simple denominada bite a ideas complejas como interpretar un concepto a través de la asignación de un código único a una combinación de caracteres. Una combinación de caracteres es un bite.

Buscar la evidencia a partir de la data, traducir de letras a código decimal y posteriormente a código binario; obtenida la información viene el tema del manejo de esa evidencia, bajo los más altos estándares de confidencialidad.

Los ciber criminales pueden recuperar información personal de los individuos a través de las redes sociales, lo que les permite ampliar el conocimiento de sus potenciales víctimas y elaborar un perfil psicológico de estos, sus rutinas en la red, gustos y preferencias.

Para el manejo de la evidencia, se debe tener en cuenta lo siguiente:

- Cadena de custodia: para prevenir que la información se corrompa y que termine siendo inservible en un juicio.
- Asegurar que se utilicen las herramientas certificadas para dar mayor validez en un juicio.

- Se deben usar dos herramientas como mínimo para obtener el mismo resultado y validar la veracidad de la información.
- Se debe preguntar ¿Cómo tomo la información y elaboro un informe no técnico?
- Se debe evitar la transferencia cruzada.
- Responder las 4 preguntas de la evidencia (Quién, Cómo, Cuándo, Dónde)
- Adquisición, nunca se debe alterar la evidencia, esta se debe mantener en su estado, realizar las copias forenses requeridas para preservar la calidad de la misma a través de una copia bit a bit. La evidencia nunca se debe trabajar sobre la original para asegurar el caso; sin embargo, "una sola pieza de información no es suficiente".
- Investigación y preparación de la información.

Tema: **Tendencias Globales del Cyber Crimen/ Crimen Organizado/ Modelo "*Crime as Service*"/ "Bussines Email Compromise"**

El doctor Freddy Bautista García plantea que las modalidades de crimen cibernético cada vez son más sofisticados y difíciles de detectar antes de que comiencen a afectar a los ciudadanos o a las instituciones. Los cyber criminales siempre se están reinventado.

El ciudadano debe ser más conocedor de los riesgos a que está expuesto al facilitar su información básica para ciertas operaciones en sitios no confiables o de alta vulnerabilidad.

Las tendencias globales del cybercrimen hoy día presentan modalidades como: secuestro de la información de los correos, cobros extorsivos por medios como las *BITCOINS* y otras criptomonedas que son tan seguras y de difícil rastreo. También ha tomado fuerza recién, la modalidad conocida como *Ransomware* para el secuestro de la información de los móviles, y los ataques sofisticados de *Malware*.

De forma más detallada, el *Randsomware* radica en secuestrar los datos de la víctima a través del cifrado complejo de la información, para luego pedir un rescate en bitcoins para liberarla. Esta modalidad afecta empresas y personas indiscriminadamente y maneja las emociones de las personas atacadas.

Documentos de las conclusiones

Cada vez son más comunes los mercados ilegales que ofrecen servicios para el crimen, algunos utilizando *DarkNet* (Internet Profunda), tema este para el cual no existe consenso en la regulación, es desarrollada en total anonimato, facilita y por lo general está asociada a transacciones fraudulentas, .

Una nueva modalidad se trata del ***B.E.C. – "Business Email Compromise",*** que consiste en comprometer al o los correos de la entidad y en el cual, por lo general, está involucrado un empleado desleal. Para atacar esta modalidad criminal es importante tomar conciencia sobre temas como son: utilizar el correo corporativo por parte de los funcionarios, proteger la información de la compañía en redes sociales, sospechar de peticiones de cambio de cuenta a última hora para hacer pagos, establecer un dominio Web de la empresa protegido de accesos particulares, entre otros.

La nueva visión del cyber crimen es analizada por los expertos con la metodología de la tricotomía del crimen que consiste en relacionar, mediante la teoría del triángulo del riesgo, los siguientes tres elementos: investigación, prevención y foco de los esfuerzos legales; como variables de estos tres elementos, se consideran el volumen de ataques, el volumen de víctimas y el ingreso por cada ataque.

Las estructuras cyber criminales también se han transformando en la medida de las condiciones. Hoy operan a través de organizaciones graduadas por niveles como son el básico, el operativo, asesor o estratégico, y los jefes. Estas estructuras tienen como objetivo obtener beneficios y/o poder, utilizan alguna forma de disciplina o control interno, por lo general implican blanqueo de dinero, operan con una cobertura internacional, y mantienen estructuras similares a las comerciales o de negocios

Aun cuando a nivel global los países han logrado algunos avances para impulsar la normatividad para atacar y controlar la cyber criminalidad, faltan muchos desarrollos; por otra parte, en las empresas falta más fuerza en el tema de segregación de funciones para que los implementadores de los sistemas de seguridad informática no sean los mismos que posteriormente las auditan, por ejemplo.

Documentos de las conclusiones

Los atacantes analizan factores como la identificación del objetivo y el compromiso de los empleados para realizar ingeniería social en donde se define el tipo de ataque a la medida que termine en un pago a los defraudadores.

Los criminales tienen una capacidad para reinventarse, siempre habrá una nueva forma de atacar y viven explotando y atacando vulnerabilidades.

A través del ENISA y el CSIRT, se ha creado la obligación para adoptar estrategias de ciberseguridad, la normativa europea es la más adelantada en este tema y se ha creado con el fin de que existan grupos de cooperaron para el intercambio de información y apoyo estratégico, adicionalmente para establecer requisitos de los operadores de servicio esenciales y los proveedores de servicio digitales

Las empresas deben adoptar medidas para garantizar la seguridad de su infraestructura.

Finalmente, la capacitación y colaboración entre los diferentes sectores, es esencial para luchar contra los atacantes.

Tema: **Big Data y la Auditoría Informática Forense.**
Retos desde la perspectiva de la Inteligencia Financiera y su impacto en la investigación criminal y judicialización

El doctor Luis Edmundo Suárez Soto sostiene que la sociedad se enfrenta a lo que se ha denominado la Tercera Revolución Industrial, que comprende una matriz de dos variables importantes: el internet y las energías renovables.

La data en internet, por ejemplo, viene con un crecimiento exponencial, la pregunta es ¿Qué estamos haciendo para proteger su integridad? Este crecimiento exponencial de los datos se debe principalmente a los avances cada vez más vertiginosos de mundo digital, es así como en el año 2013 se tenían 4.4 zettabytes que, según cálculos del *Digital Universe Research Project*, se estima que lleguen a 44 zettabytes para el año 2020. Hay tantos byts (unos y ceros), como estrellas en el universo.

Documentos de las conclusiones

El crecimiento exponencial de los datos ha dado lugar a mayores vulnerabilidades, el universo digital es inmensurable, lo cual es muy importante además porque los datos son información que se convierte en conocimiento.

Para responder a la pregunta: ¿Quién está cometiendo los delitos cibernéticos?, se ha iniciado con la identificación y entendimiento de la cadena de valor del conocimiento (datos, información y conocimiento), estableciendo la dimensión del negocio criminal en Colombia y en el mundo. Se estima que para el año 2012, los ingresos criminales fueron de US $2.6 trillones que equivalen al 3.6% del PIB global, presentándose operaciones de lavado de activos por US $1.9 trillones equivalentes al 2.7% del PIB global y es mayor al PIB de Brasil, España e Italia. Las autoridades solo han logrado incautar el equivalente al 0.2% del ingreso total.

En el caso de Colombia, por ejemplo, las operaciones de lavado de activos lograron sumas equivalentes al 3 % del PIB nacional, algo así como $20 billones de pesos.

La UIAF (Unidad de Información y Análisis Financiero) estableció un plan de trabajo a través de la utilización del Big Data para aumentar las posibilidades de obtener información, se aumentaron en un 600% los deportantes, se utilizaron videos y textos; adicional a la información financiera se realizó inteligencia financiera y económica para mejorar el conocimiento de las redes criminales y aumentar la capacidad de detección, lo cual desembocó en un proceso cíclico de investigación.

Ante la pregunta: ¿Cuál es el reto de la academia para en la formación de especialistas en auditoria forenses? Es importante advertirles que existe una nueva amenaza conocida como Convergencia Criminal, cuyos principales elementos son: acciones terroristas, crimen y corrupción. La siguiente pregunta obligada es ¿Cómo definir una estrategia para neutralizar esta amenaza? Para ello es importante contar con capital humano, actuar por distintos frentes (Estratégico, Táctico y Operativo) y desarrollar diferentes actividades como son: manejo de redes completas, implementación del flujo de trabajo para los organismos del estado, implementación de nuevas tecnologías (hardware, software y metodologías).

Otra novedad que presenta el crimen son sus estructuras operativas. Antes operaban a través de un líder que contaba con un equipo a sus disposición, la nueva tendencia es actuar mediante las redes que representen un sistema social, computacional o biológico. Esto hace que la formación y el desafío con el

conocimiento, sean los elementos con los que se tenga que enfrentar las nuevas modalidades de crimen cibernético.

Tema: **¿Por qué el cibercrimen se ha incrementado?**
Un viaje con Julio Verne

El doctor Arturo Del Castillo presenta un análisis de la evolución del cyber crimen, identificando 4 épocas así: Romántica (1990´s), Generación X (2000 a 2010), Generación Millennials (2010 a 2020), y la época de Drones (2020 - ¿?). Cada una de estas épocas se identifica con unas características, unas motivaciones y algunos hechos a destacar. Así por ejemplo, la época de los Millennials se caracteriza por presentar milicias cibernéticas con múltiples objetivos, personas solitarias con síndrome “social net”, mientras que entre sus motivaciones incluyen la obtención de dinero a cualquier forma, extorsión y cyber terror, mientras que entre los asuntos a destacar se mencionan el targets individuales y amenazas permanentes.

En un análisis de cómo evoluciona el comportamiento del ciber delincuente, se encontró que todo puede comenzar como un ciber espionaje y terminar como un ciber ataque. Como parte del mismo análisis se encontró que el 43% de los ciber ataques en el 2015 fueron realizados por Millennials, pasando otras modalidades como son el ciber crimen, cyber armas y cyber terrorismo. El nuevo estilo en la era digital incluye mega ciudades y *Cyber connections*. Los nuevos cibercriminales manejan una ética y unos valores muy diferentes a los de la gente de bien, para ellos parecen no haber consciencia del verdadero impacto negativo de lo realizado.

Se debe ampliar el panorama y mejorar la visión hacia el crimen financiero, puesto que los ataques son un asunto generalizado. Algunas veces el ciber atacante comienza como un acto aislado, algunos de ellos realizan su primer ataque antes de los 20 años.

La regulación nacional e internacional tiene un rezago en cuanto a la forma de judicializar y encontrar culpables de los crímenes que suceden en la red.

Todo esto demanda una nueva postura de las Juntas Directivas frente a los riesgos informáticos en un ambiente de Eco Sistema Digital Criminal, especialmente fomentando la ética empresarial, teniendo en cuenta además que gran parte de estos crímenes se llevan a cabo con la complicidad de personal interno de la empresa.

Tema: **Ecosistema Digital Criminal (EcoDC).**
Nueva Frontera de la Investigación Criminal

Para el doctor Jeimy Cano existe una asimetría de la criminalidad digital que va desde las que tienen mayor influencia tecnológica hasta los que tienen una mayor influencia organizacional; en ambos casos existen unos elementos o actores comunes como son la tecnología, las personas y los procesos, a través de usabilidad, accesos e identidad, para lograr espionaje, fuga de información y violación a los derechos de propiedad.

Casi siempre los fraudes ponen de manifiesto las debilidades de control interno que padecen las organizaciones, siendo una de esas debilidades las vulnerabilidades conocidas y desconocidas de las plataformas, programas o prácticas de las personas y empresas.

La actuación criminal digital generalmente aprovecha las herramientas libres y sin costos disponibles en la web; dicha actuación tiene objetivos asociados a cierta motivación de tipo personal, político, social y/o económico.

Le delincuencia digital actúa bajo ciertas premisas como son la máxima efectividad, con el mínimo de esfuerzo, uso de plataformas digitales públicas y gratuitas, asistidas por comunidades especializadas, uso de criptomonedas como medio de pago, máximo anonimato, con el mínimo de evidencia posible, y máxima ambigüedad jurídica, con el mínimo de conocimiento tecnológico disponible.

En el análisis de la evolución de la criminalidad digital, uno de los elementos a tener en cuenta es el de economía digital criminal; esta se mueve desde el tráfico de datos personales hasta los mercenarios digitales, pasando por venta de propiedad

intelectual, armas informáticas, fraude como servicio, robo de credenciales, comercialización de vulnerabilidades y propiedad intelectual.

Cada vez se tiene un mundo más digitalizado para la adquisición de bienes y servicios, a través de herramientas como redes sociales, computación móvil, internet de las cosas, entre otras.

Estos hechos han generado un entorno que el conferencista ha denominado Ecosistemas digitales criminales –EcoDC, definido como el "conjunto de relaciones entre participantes locales y globales, que crean una red flexible de capacidades, criminales para concretar nuevas posibilidades de acción ágiles, livianas, sencillas y efectivas, que alteren y confundan la realidad de los afectados (….)"

Frente a un escenario de Ecosistema Digital criminal, se plantea también un reto de cambios en el sistema de investigación criminal digital a través de lograr evidencia dinámica y no estática, orientado a plataformas digitales y no solo a dispositivos específicos, teniendo como objetivos a comunidades distribuidas en reemplazo de una persona o grupo, basada en analítica de datos y patrones de reconocimiento en vez de basarse en procedimientos conocidos y probados.

Existen nuevas exigencias para las empresas y naciones, que van desde defensa en profundidad hasta capacidad adaptativa, pasando por disciplina operativa. Estas nuevas situaciones demandan cambios en las posturas de las juntas directivas, para que sean más confiables, vigilantes y resilentes.