Contexto de la Evidencia Digital en Colombia: Buenas prácticas y aplicación de metodologías

Emanuel Ortiz Ruiz

Redciber y ASIIF (Colombia)

1. Contexto del Cibercrimen

Los hechos por medio del tiempo han sido evidentemente complejos en materia de Ciberseguridad; algunos de ellos los señala (Ortiz Ruiz, 2019) en los orígenes del Cibercrimen, sin embargo es importante elevar estas connotaciones y divisiones a través de los avances tecnológicos de la humanidad; si bien es cierto el Cibercrimen hace parte de un título grande y contextualizado en todo, estas afectaciones a la ciberseguridad y Seguridad Digital tuvieron nacimiento mucho más antes de lo que imaginamos, por ende la importancia siempre de los sectores de la Economía en comprender la importancia de la estrecha relación que hay en la ciberdelincuencia y el aseguramiento de la evidencia Digital.

Una de las características esenciales de estos equipos interdisciplinarios en Ciberseguridad, deben enfocarse en las acciones de "Core Bussiness" y de la idea del negocio, aspectos esenciales como su orientación en materia teórica y práctica, pueden desarrollar aún más su eficiencia o efectividad en el momento de permitir afianzar su infraestructura, el enfoque del recurso técnico, humano y especializado que este le merece. A partir de esto, también es importante mencionar sus capacidades de enrolamiento estratégico con el conocimiento de su adversario, razón que involucra mucho más la sinergia de la parte técnica, con la jurídica, legal y tecnológica.

2. **La Evidencia Digital como enfoque principal para la pericia forense:**

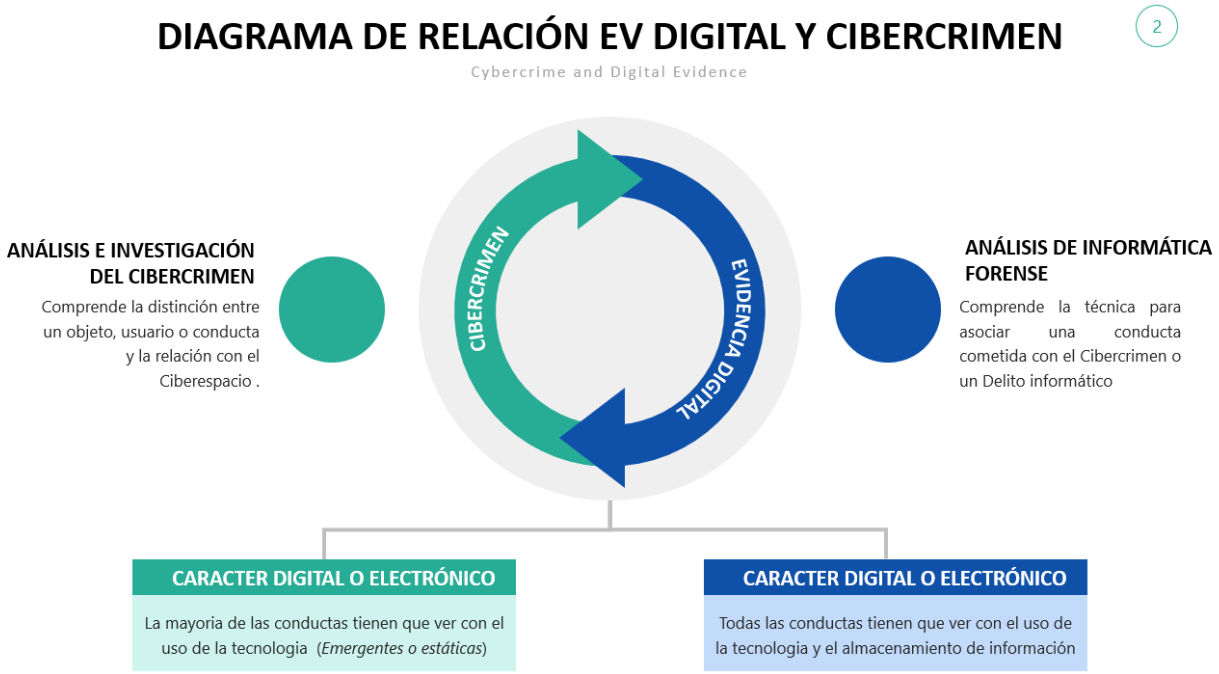
Como se mencionó anteriormente, diferentes escenarios se han venido construyendo en el mundo en esta asignatura, y para este caso en puntual, Colombia mediante la adopción del Convenio de

Budapest, de tal manera que la normatividad colombiana no fue ajena a la Ley que se sancionó el 05 de enero de 2009, sin embargo, esto se debió al incremento de conductas o delitos informáticos cometidos en el país; por ende cabe anotar que, en ese orden de ideas por medio de las normativas internacionales y la voluntad legislativa para perseguir las conductas que afectan el ciberespacio, es entendido, como ese escenario intangible, modificable y variable que está relacionado directamente con las tecnologías y su incidencia en el mundo común hiperconectado.

El cibercrimen y su estadística en el 2008 supera los indicadores de económicos a nivel regional, y frente la comisión de estas conductas tuvieron relación con los siguientes resultados se obtuvieron mediante fuentes relacionadas con la Policía Nacional de Colombia. 28.827casos durante el 2019 (ccit.org, s.f.).

De la misma manera es importante definir el cibercrimen puede tratarse de distintas opciones que faciliten que las circunstancias que induzcan a que se cometa una conducta de afectación a los tres pilares de la seguridad en la información. De tal modo que en Colombia con base a esos resultados y la aproximación teórico-práctica de la ciberdelincuencia, se ha venido construyendo unas metodologías que faciliten la interacción de los escenarios de los ciberdelitos con la evidencia digital.

Una de estas relaciones entre la evidencia digital y el cibercrimen ha permitido que la comunidad de investigadores y peritos en informática forense en Colombia, adopten diferentes procedimientos y metodologías a saber:



Grafica No. 1: Tomado del articulo Aproximación del Cibercrimen en Colombia (primera parte), adaptado a la adopción de mejores prácticas para realizar el tratamiento y aseguramiento de la evidencia digital. https://www.researchgate.net/publication/341541797_APROXIMACION_METODOLOGICA_DEL_CIBERCRIMEN_EN_COLOMBIA_PRIMERA_PARTE

En lo que representa la anterior imagen conceptual, la relación que posee el Cibercrimen como conducta autónoma de las conductas asociadas con el ciberespacio y la evidencia digital, permite que sus ejes de acción la involucren directamente las distintas metodologías para poder abordar ciencias auxiliares de la justicia; y para ello, es importante comprender su relevancia, y por medio de esta, establecer esas circunstancias de tiempo, modo y lugar para determinar si posee determinadas características para poder evaluar las acciones cometidas por el Ciberdelincuente. Es preciso indicar que los argumentos que se detallan mediante e artículo, (Ortiz, Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense", 2019), en lo que respecta con la importancia de definir aspectos sobre el origen de la IEA (Información Electrónica Almacenada) referenciado en los documentos de las principales guías para el análisis de los datos contenidos en un sistema informático.

Grafica No. 2: Tomada de la Metodología para el tratamiento hexagonal de la Evidencia Digital, estudio realizado por Emanuel Ortiz para ilustrar el enfoque de las áreas del Cibercrimen y las nuevas tecnologías. https://www.researchgate.net/publication/329923195_Tratamiento_hexagonal_de_la_Evidencia_Digital_para_entornos_digitales_o_digitalizados.

Algunas de estas buenas practicas han quedado señaladas en diferentes publicaciones, las cuales han servido para que auxiliares de la justicia, auditores forenses, investigadores criminales, peritos forenses y organizaciones público-privadas en Colombia, puedan valorar el significado de la prueba digital electrónica y llevarlo a un estrado judicial para que posteriormente sea valorado por un juez de la república.

Finalmente estas diferentes metodologías están orientadas a facilitar el trabajo diario de especialistas en informática forense, el cual cada uno de estos aspectos cobra un gran valor para poder emitir un concepto, un análisis o dictamen pericial forense. Las buenas prácticas internacionales del aseguramiento de la evidencia Digital complementan cada uno de los aspectos de *integridad y no repudio* de los diferentes escenarios de la investigación del cibercrimen y fortalecen los demás aspectos técnicos relacionados.

BIBLIOGRAFIA

ccit.org. (s.f.). *www.ccit.org.co › wp-content › uploads › informe-tendencias-cibercrimen*. Obtenido de www.ccit.org.co › wp-content › uploads › informe-tendencias-cibercrimen.

Moore, R. (2011). *Cybercrime: Investigating High-Technology Computer Crime* (2 ed., Vol. 2). New York: Anderson Publishing. Recuperado el Enero de 2020, de https://www.utica.edu

Ortiz Ruiz, E. E. (02 de Abril de 2019). Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso. *Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso*. Bogotá: ResearchGate.

Ortiz, E. (Abril de 2019). Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense". *Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense"* . Bogotá.

Rohmeyer , p., & Bayuk , J. (2019). *Financial Cybersecurity Risk Manangement.* Hoboken NJ, USA: Springer. Recuperado el 17 de Marzo de 2020

WAll, D. (2007). *The Transformation of Crime in the Information Age.* Cambridge, Inglaterra: Polity Press.