


DOCUMENTOS  
DE TRABAJO AREANDINA  
ISSN: 2665-4644

Facultad de Ingenierías  
y Ciencias Básicas



# ANÁLISIS FORENSE: LAS CARACTERÍSTICAS QUE DEBE TENER UNA METODOLOGÍA PARA ABORDAR LA INVESTIGACIÓN DE DELITOS FINANCIEROS

CAMILO AUGUSTO CARDONA PATIÑO



Las series de documentos de trabajo de la Fundación Universitaria del Área Andina se crearon para divulgar procesos académicos e investigativos en curso, pero que no implican un resultado final. Se plantean como una línea rápida de publicación que permite reportar avances de conocimiento generados por la comunidad de la institución.

# ANÁLISIS FORENSE: LAS CARACTERÍSTICAS QUE DEBE TENER UNA METODOLOGÍA PARA ABORDAR LA INVESTIGACIÓN DE DELITOS FINANCIEROS

## Camilo Augusto Cardona Patiño

Especialista en Gerencia de Tecnología. Docente categorizado por Minciencias, adscrito a al programa de Ingeniería de Sistemas, Facultad de Ingeniería y Ciencias Básicas, Fundación Universitaria del Área Andina, sede Bogotá.

Orcid: <https://orcid.org/0000-0001-8758-6603>  
Correo electrónico: [ccardona19@areandina.edu.co](mailto:ccardona19@areandina.edu.co)

### Cómo citar este documento:

Cardona Patiño, C. A. (2021). Análisis forense: las características que debe tener una metodología para abordar la investigación de delitos financieros. *Documentos de Trabajo Areandina* (2021-2). Fundación Universitaria del Área Andina. <https://doi.org/10.33132/26654644.2024>

## Resumen

En el mundo hay una gran carencia de especialistas y profesionales a nivel de seguridad informática (Roque Hernández y Juárez Ibarra, 2018), razón por la cual, es necesario incentivar la formación, así como generar concientización tanto para especialistas, profesionales y como para los usuarios habituales de esta, especialmente; ya que, de una otra forma, todos interactuamos con la tecnología que, inherentemente, cuenta con una gran cantidad de potenciales fallas que se pueden aprovechar para vulnerar las diferentes medidas de seguridad que se puedan implementar. Este trabajo, se enfoca en explorar e identificar los posibles requerimientos para el planteamiento de una metodología que permita abordar, desde una perspectiva planificada, el proceso de investigación forense en casos relacionados con fraudes financieros, de manera que se puedan optimizar los resultados en las fases de recolección y análisis de evidencias. Para el desarrollo de la presente investigación, se recurrió a la revisión de literatura vigente sobre el enfoque y conocimiento que se tiene acerca de los ataques cibernéticos a infraestructuras de entidades financieras. A partir de esta revisión, será posible estructurar las características fundamentales que debe tener una metodología de investigación digital forense.

**Palabras clave:** ciberataques, delitos financieros, informática forense, investigación, metodología.

## Introducción

Como resultado de las medidas tomadas para afrontar la pandemia del COVID-19, en los últimos dos años, Garfin (2020) explica que se ha visto un aumento sustancial en el uso de la tecnología como mecanismo para mantener, en cierto grado, el desarrollo de las diferentes actividades humanas. Ámbitos como la educación, el entretenimiento, el comercio y las transacciones económicas han acelerado la normalización y adopción de tecnologías que reemplazan su equivalente en



el mundo de la educación humana, de esta forma, las aulas hoy están vacías, pero las salas virtuales están saturadas, la genta cada vez va menos a los bancos y mejoran su relación con las aplicaciones financieras.

Estos aspectos no pasan desapercibidos por los piratas informáticos, quienes, a su vez, han tenido un aumento sin precedentes en la cantidad de ataques, según el FBI, en su publicación *Internet Crime Report 2020*, en este año se identificó un total de 791 790 quejas sobre crímenes en internet, que con relación a las 467 361 del 2019, equivale a un aumento del 69 %, cifra alarmante, pero consistente con el aumento en el uso de las tecnologías de información y la comunicación (TIC).

Bajo este escenario, resulta claro que existe una urgente demanda de herramientas, técnicas y modelos que permitan afrontar esta realidad, entendiendo que, en principio, no es posible diseñar un sistema 100 % seguro. Se deben desarrollar propuestas que, en primer lugar, se enfoquen en reducir y mitigar cualquier posible incidente que atente contra la seguridad informática, pero, a la par, es necesario ir pensando en metodologías que apoyen la labor del investigador digital forense, profesional encargado de recuperar, salvaguardar y analizar las evidencias cuando se ha producido una violación a los mecanismos de protección de la información y la infraestructura. En el desarrollo del siguiente artículo se abordan las características que debe incluir una metodología de esta naturaleza.

## Desarrollo del texto

La seguridad informática es una de las grandes preocupaciones del mundo hoy en día. Esta afirmación se encuentra respaldada por gran cantidad de datos y estudios, desde las perspectivas técnicas y económicas, este último campo es tan relevante en la actualidad porque allí se generan y gestionan los recursos que soportan el comercio, los fondos para los

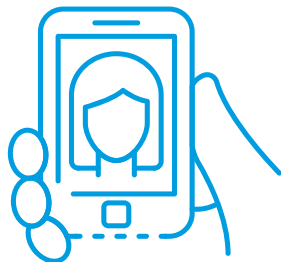


procesos de educación, la investigación y el desarrollo de nuevos productos y servicios, solo por mencionar algunos. Ahora bien, esta situación en últimas puede ser vista como una ventaja, como un punto a favor de la seguridad informática, ya que al existir una necesidad, su reconocimiento por parte de empresas, gobiernos, entidades no gubernamentales, se hace cada vez más evidente, lo que demanda la asignación cada vez mayor de recursos para su desarrollo e implementación.

Dentro de los estudios previamente mencionados, se encuentra el del Foro Económico Mundial que, en la publicación del Informe Global de Riesgos del año 2021 (World Economic Forum, 2021) evidencia los peligros, los riesgos claros y presentes a corto plazo en un futuro relativamente cercano (0 a 2 años). Es posible apreciar en este análisis el contexto en que se abordan los temas económicos, ambientales, geopolíticos, sociales y tecnológicos, consolidados a través de diferentes procesos de recolección de evidencias, que registran aspectos y preocupaciones de los principales representantes mundiales del entorno económico; además, establece, según sus apreciaciones, el potencial que tienen tales riesgos para convertirse en una amenaza crítica para el mundo. Llama la atención que entre los riesgos que se consideran de mayor impacto se encuentra uno de orden tecnológico, relativo a las fallas en ciberseguridad. El 39 % de los líderes mundiales que participaron de este estudio manifiesta un alto nivel de preocupación debido a que la infraestructura y las medidas de seguridad empresariales, de una u otra forma se ven superadas o se vuelven obsoletas, por la sofisticación de las herramientas y los métodos de ataque, cada vez más frecuentes y fáciles de orquestar, automatizar y desarrollar. Situación que, según el Foro Económico Mundial, se traduce en una serie de trastornos económicos, pérdidas financieras, tensiones geopolíticas y, en últimas, inestabilidad geopolítica.

El 39 % de los líderes mundiales que participaron de este estudio manifiesta un alto nivel de preocupación debido a que la infraestructura y las medidas de seguridad empresariales...

De acuerdo con la publicación del líder de pensamiento global en ciberseguridad y tecnología emergente, Brooks (2021), que publicó en la revista *Forbes* un artículo sobre estadísticas de ciberseguridad, durante el 2020, se rompieron los récords con respecto



Finalmente, no se pueden dejar de mencionar las falencias relativas a la condición del ser humano, como propensión a todo tipo de errores...

a ciberataques, pérdida de datos y pérdidas de activos financieros por medios digitales, ya que los delitos informáticos se han vuelto cada vez más numerosos, sofisticados y costosos que nunca, pues incluyen herramientas de inteligencia artificial y redes 5G.

Son múltiples y muy variados los riesgos para las entidades financieras, según Hasham *et al.* (2019), existen, en primer lugar, las vulnerabilidades que no son ajenas a cualquier desarrollo o infraestructura tecnológica, pero surgen otros que se derivan de los procesos de automatización y digitalización, así como el aumento en demanda y volumen de transacciones, que a su vez requieren de una mayor integración de plataformas financieras, generando de paso mayores riesgos asociados. Finalmente, no se pueden dejar de mencionar las falencias relativas a la condición del ser humano, como propensión a todo tipo de errores, malas prácticas para el uso de la tecnología y corruptibilidad.

El avance de la presente investigación recopila la información relativa a los patrones identificados en fraudes financieros realizados por medio de las tecnologías de la información y la comunicación, con los cuales se procede a identificar cuáles serán los procedimientos, controles y actividades clave para proponer una metodología que ayude a fortalecer las fases de recolección y análisis de evidencias, de forma que se logre investigar con mayor eficiencia los delitos que atenten contra infraestructuras que dan soporte a los servicios financieros.

El perfil cibernético de la mayoría de los delitos y fraudes financieros se puede modelar a través de tres momentos clave: el primero incluye el acceso ilegal a los sistemas, el segundo tiene que ver con la alteración o inserción de códigos y, finalmente, la transferencia no consentida de los activos financieros. Sin embargo, este enfoque se percibe incompleto, ya que no considera uno de los eslabones más débiles de la cadena, las personas, ya que son estas, las que en ocasiones por malas prácticas, desconocimiento o exceso de confianza, terminan



Se ha identificado que muchas veces la vulneración de los procesos comerciales surge por una falla en la gestión y control de los procesos empresariales ...

comprometiendo la confiabilidad de los sistemas de protección y datos.

En los últimos años, las empresas y los gobiernos han ido reforzando respectivamente las prácticas y la normativa legal en torno a prevenir los ciberdelitos; no obstante, es necesario abordar esta creciente problemática desde un enfoque integral, que, en primer lugar, sea efectivo para evitar la mayor cantidad posible de incidentes, pero que, además, en los casos en que el ataque tenga éxito, permita generar una completa trazabilidad sobre el hecho, facilitando el proceso de recolección de evidencias, que a su vez servirán para mejorar la seguridad informática e identificar a los responsables.

Para atender esta necesidad y apoyar la sistematización de todos los procesos comerciales y empresariales de manera global, se ha identificado que dentro de su estructura, la metodología propuesta debe abordar de manera integral las siguientes características.

### Involucrar todos los procesos empresariales

Se ha identificado que muchas veces la vulneración de los procesos comerciales surge por una falla en la gestión y control de los procesos empresariales (Plachkinova & Maurer, 2018), entiéndase como procesos comerciales, aquellos que responden a la naturaleza propia del nicho de mercado, así, por ejemplo, para una entidad financiera, este tipo de procesos incluye las transacciones, movimientos de cuenta, pagos y retiros, etc. En tanto que, los procesos empresariales son actividades que se requieren para el correcto funcionamiento de la organización, algunos ejemplos pueden ser el área contable y la gestión de recursos humanos.

Para prevenir que se puedan orquestar ataques por las líneas más frágiles de la cadena de seguridad, la metodología deber ser transversal a todos los procesos de la organización, involucrando a todos los empleados en sus distintos roles y funciones.





## Intuitivo y alineado con los procesos vigentes

Para facilitar, agilizar la implementación y reducir la resistencia al cambio, los controles y medidas deberán ser ajustados a las labores que ya se vienen desempeñando dentro del funcionamiento normal de la entidad financiera. Esta situación requiere, entonces, que exista un proceso de asimilación de las actividades, que permitan una fusión armonizada con la menor alteración posible.

## Posibilidad de manejar varios frentes de protección

Para poder atender de manera eficiente casos sospechosos, posibles riesgos, eventuales incidentes y violaciones a la seguridad de la información, la metodología debe incluir la viabilidad de generar varias líneas de protección, así como diferentes niveles de complejidad, acorde a las necesidades de cada evento, de las que serán responsables personas con diferentes cualidades y capacidades, ya sea que la respuesta requiera de monitoreo o una respuesta progresiva.

...la metodología debe incluir la viabilidad de generar varias líneas de protección, así como diferentes niveles de complejidad, acorde a las necesidades de cada evento...

## Gestión de responsabilidad

En todos los niveles de respuesta y ejecución, se deben establecer con claridad y en detalle las responsabilidades que recaen en cada uno de los actores involucrados con el funcionamiento y operación de la entidad financiera, ya sea a escala comercial o empresarial, recordando que todos los flancos deben ser abordados desde la metodología.



## Monitoreo y seguimiento

Ya sea que los controles y medidas se realicen de forma manual o automática, la metodología debe incluir herramientas que en tiempo real permitan registrar y analizar los patrones y el comportamiento de la información y que, además, operen en conjunto con cada uno de los frentes de protección desplegados.

## Debe ser sistemática

Para asegurar su correcto funcionamiento, la metodología debe proporcionar protocolos claros y ordenados, de conocimiento público al interior de la empresa, certificando que cada uno de los actores tengan un profundo conocimiento de sus roles y responsabilidades frente a la prevención y acción en casos de posibles ataques o vulneraciones informáticas.

## Proveer mecanismos para garantizar la investigación

Finalmente, para apoyar las actividades relacionadas con la investigación digital forense, la metodología debe permitir la correcta ejecución de los cuatro pilares fundamentales de la informática forense: i) identificación, ii) recolección, iii) análisis y iv) confirmación. Sin embargo, cuando el modelo se ejecuta correctamente de acuerdo con las características mencionadas con anterioridad, los registros y evidencias se irán generando en la medida que la operación se desarrolla con normalidad, en este punto, se propone, a manera de verificación, realizar ejercicios de control para comprobar que efectivamente se está generando toda la trazabilidad, con el fin de que eventualmente facilitará el rastreo de cualquier acción ejecutada por empleados, clientes, colaboradores y atacantes.

Actualmente, la colaboración es clave para frenar y mitigar los efectos del ciberdelito, especialmente los asociados con entidades financieras...

Actualmente, la colaboración es clave para frenar y mitigar los efectos del ciberdelito, especialmente los asociados con entidades financieras, pues como lo afirma Hasham *et al.* (2019), los ciberdelincuentes trabajan en cooperación para vulnerar las infraestructuras tecnológicas. En ese sentido, resulta natural que se comiencen a generar propuestas que involucren a diferentes representantes de todos los sectores (público, privado, ONG, académico, productivo), en la búsqueda de soluciones innovadoras, que, desde la prevención y el monitoreo, permita no solo disminuir los ciberataques que logran tener éxito, sino que, por medio de la trazabilidad, se logre identificar a los responsables y comprender mejor la taxonomía del ataque mismo.

## Referencias

- Brooks, C. (2021, 2 de marzo). Alarming cybersecurity stats: What you need to know for 2021. *Forbes*. <https://n9.cl/c5p0m>
- Brunová, M. (2018). Cyber security, providing evidence in cyberspace and searching for and securing digital footprints. *European Science*, 5(2), 42-46. <https://n9.cl/nduzu>
- Febriansyah, L., & Riadi, I. (2018). Analysis on predicting cyberterrorism using AHP (*Analytical Hierarchy Process*) method. *Journal of Theoretical and Applied Information Technology*, 96(22), 7563-7575. <http://www.jatit.org/volumes/Vol96No22/25Vol96No22.pdf>
- Federal Bureau of Investigation (FBI). (2021). *Internet Crime Report 2020*. Federal Bureau of Investigation. [https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

- Garfin, D. R. (2020). Technology as a coping tool during the coronavirus disease 2019 (COVID-19) pandemic: Implications and recommendations. *Stress and Health*, 36(4), 555-559. <https://doi.org/10.1002/smi.2975>
- Hasham S., Joshi, S., & Mikkelsen, D. (2019, 1 de octubre). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*. <https://n9.cl/crwuk>
- Jubany Ticó, M. (2018). Automation of processes in forensic analysis [tesis de maestría, Universitat Politècnica de Catalunya]. Repositorio Institucional. <http://hdl.handle.net/2117/125495>
- Plachkinova, M., & Maurer, C. (2018). Security breach at target. *Journal of Information Systems Education*, 29(1), 11-20. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=jise>
- Roque Hernández, R. V. y Juárez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *PAAKAT: Revista de Tecnología y Sociedad*, 8(14), 1-13. <https://www.redalyc.org/articulo.oa?id=499063347005>
- World Economic Forum. (2021). *The Global Risks Report 2021 16th edition*. World Economic Forum. [http://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2021.pdf](http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf)

