E-ISSN 2619-6301 No. 14, Año 2021

DISEÑO DE UN SISTEMA DE DETECCIÓN DE EVIDENCIAS DIGITALES FRENTE A DELITOS FINANCIEROS EN EL SECTOR EMPRESARIAL

Wilmer Andrés Arocha Rico*

RESUMEN

El desarrollo del proyecto es oportuno. Propone una alternativa de eliminar la problemática que padecen reiteradamente las grandes, medianas y pequeñas organizaciones, las principales víctimas del delito o fraude mediante ataques informáticos que causan daños con el objetivo de secuestrar o eliminar la información de estas organizaciones. Por esta razón surge la idea de diseñar una aplicación basada en una metodología que permita no solo detectar las evidencias digitales frente a estos casos, sino que también ayude a mitigarlos para que la información esté segura. El propósito de este proyecto es brindar al usuario u organización una opción de soporte seguro de gran utilidad que la beneficie, a fin de que alcance un rendimiento óptimo en cuanto a su funcionamiento sin ninguna interrupción.

Palabras clave: Activo, Confidencialidad, Informática forense, Metodología, *Software*

* warocha@estudiantes.areandina.edu.co

INTRODUCCIÓN

En la actualidad es impresionante observar cómo el avance tecnológico día a día ha tenido un gran impacto en el mundo., y cómo, a su vez, se ha incrementado para las tecnologías de las actividades delictivas. Es por esto que hoy las grandes, medianas y pequeñas organizaciones administran su información con sistemas informáticos que les ayudan a optimizar sus procesos con un alto rendimiento, pues la considera su activo más importante y de mayor valor.

Por otra parte, esto estimula a los ciberdelincuentes a que indaguen sobre información de manera ilegal, de forma que violan la seguridad u ocasionan su exclusión, daño o modificación, provocados en algunas situaciones por las mismas compañías, por hackers o grupos de ciberdelincuentes que buscan lograr su objetivo: vulnerar la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos de las organizaciones. Con esto, se puede decir que Colombia es un país con alto índice de delitos informáticos cometidos y uno de los más afectados. Un dato evidente es que en el 2015 el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, lo que evidencia un aumento del 40 % con respecto al 2014. Esto supuso unas pérdidas económicas altísimas, las cuales, según el Banco Mundial (2014), llegaron a cifras de cerca de unos USD 500 millones, aproximadamente (Manrique Horta, 2016).

Teniendo como base lo anterior, es de suma importancia proponer una metodología eficaz y confiable que brinde a los profesionales del área la facilidad de acceder a los recursos, las maneras, las tareas y demás habilidades metodológicas ordenadas para un oportuno peritaje informático, logrando una indagación que durante el análisis forense permita saber qué, cómo, quién, de dónde y cuándo se cometió el delito informático. A partir de esto es importante presentar una propuesta de desarrollo de aplicación que permita identificar los fraudes financieros para que se tomen medidas de prevención al respecto y mitiguen estos ataques informáticos. Un ejemplo de lo anterior es Fraud, un *software* para la localización del fraude en todos sus niveles: fraude financiero, fraude bancario, fraude electrónico, fraudes con tarjetas de crédito y muchas clases de fraude más. Fraud ofrece a las organizaciones una tecnología inteligente, cuyo costo no sea muy alto y tenga una mayor efectividad, además de reducir el trabajo asociado a la investigación de alertas.

De acuerdo con lo anterior, las organizaciones se sienten más seguras a la hora de utilizar estas aplicaciones, de manera que están totalmente confiadas en que estas les darán un plus de ventaja en cuanto a la prevención de ataques informáticos realizados por los ciberdelincuentes.

Objetivo general

El objetivo general es identificar la metodología de desarrollo útil para la creación de una aplicación orientada a la detección de evidencias digitales frente a delitos financieros.

E-ISSN 2619-6301 No. 14, Año 2021

Objetivos específicos

Los objetivos específicos se enlistan a continuación.

- Realizar una recopilación de los casos más relevantes de empresas desarrolladoras de *software* enfocadas en la recolección de evidencias digitales frente a delitos financieros.
- Comparar la documentación recopilada para identificar las metodologías y las buenas prácticas de desarrollo empleadas por las empresas.
- Analizar las metodologías de desarrollo para aplicaciones forenses que permitan una adecuada detección de evidencias digitales frente a delitos financieros.
- Proponer una metodología de desarrollo que permita la creación de un *software* para la detección de evidencias digitales frente a delitos financieros.

Materiales y métodos

Después de las investigaciones realizadas y el análisis a varias metodologías adecuadas para el desarrollo de *software*, se decide escoger la metodología ágil, ya que es un metodología que se basa en dividir el proyecto en *sprint*, lo cual permite trabajar en conjunto y tener una mejor gestión de planificación de desarrollo de *software*. Esta metodología permite trabajar de manera adecuada y solucionar los problemas mediante una planificación adaptativa y una toma de decisiones que conllevan a avanzar de manera que se cumpla con lo propuesto.

Objetivo

El objetivo es lograr una metodología ajustada para el desarrollo de aplicaciones orientadas a la detección de evidencias digitales frente a los delitos financieros.

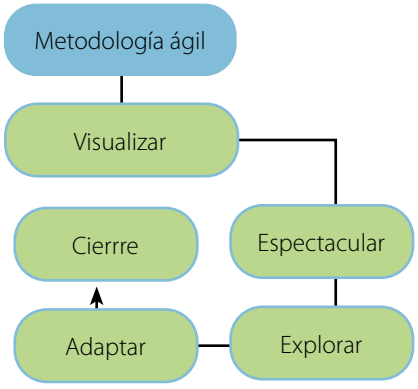
Pasos

1. *Visualizar*. Para el desarrollo del presente proyecto se plantean los objetivos que se enlistan a continuación y nos permitirán desarrollar y cumplir las metas trazadas del proyecto.
   - Realizar una recopilación de los casos más relevantes de empresas desarrolladoras de *software* enfocadas en la recolección de evidencias digitales frente a delitos financieros.
   - Comparar la documentación recopilada para identificar las metodologías y las buenas prácticas de desarrollo empleadas por las empresas.
   - Analizar las metodologías de desarrollo para aplicaciones forenses que permitan una adecuada detección de evidencias digitales frente a delitos financieros.
   - Proponer una metodología de desarrollo que permita la creación de un *software* para la detección de evidencias digitales frente a delitos financieros.
2. *Especular*. En esta fase se definirá la visión que tiene el proyecto, lo cual se convertirán en requisitos previos a tener en cuenta como prioridad para el desarrollo del proyecto, los cuales se enlistan a continuación.

- El acceso se dará a los usuarios autorizados.
- El *software* se podrá instalar en cualquier sistema operativo, por ejemplo, Windows, Linux, OSX, etc.
- La aplicación podrá detectar evidencias encontradas en los dispositivos en los que se cometió el delito y así emitir una alerta de seguridad de lo encontrado.
- El sistema deberá garantizar la mayor protección de la información sobre las casas desarrolladoras de *software* "clientes" del acceso no autorizado.
- No se necesitará una aplicación adicional para el uso del sistema, aparte del navegador web.
- La aplicación tendrá un sistema de cifrado o encriptación que les permitirá a los usuarios intercambiar mensajes o información de forma segura.
- Debe especificarse un plan de recuperación en caso de que se presente un desastre y se vea afectado el *software,* de modo que no interrumpa su funcionamiento.
- La aplicación deberá arrojar un informe detallado de los resultados de las evidencias encontradas en los dispositivos analizados.

3. *Explorar*. En esta fase tendremos en cuenta el objetivo general: la identificación de la metodología de desarrollo útil para la creación de una aplicación orientada a la detección de evidencias digitales frente a delitos financieros. Para lograr esto se propone realizar estudios previos de otros proyectos de desarrollo de *software*, casas desarrolladoras de *software* y diferentes metodologías en América, lo cual nos permitirá escoger una metodología ágil que nos facilite cumplir con los objetivos propuesto.
4. *Adaptar*. En esta fase se realiza un análisis de todo lo que se lleva trabajado por medio de las investigaciones pertinentes para el desarrollo del proyecto en cuanto a la problemática o requerimientos del cliente; por otro lado, está abierta la posibilidad a cambios que requiera el proyecto, bien sea en los objetivos o bien el proceso, etc.
5. *Cierre*. Es la etapa final del proyecto. En esta se culmina todo el proceso de desarrollo; durante todo el proceso final se tendrán en cuenta comentarios alternos de mejora por ambas partes (clientes-equipo de trabajo), lo cual servirá de ayuda para corregir errores del desarrollo del proyecto.

Figura 1. Diagrama de la metodología



Fuente: elaboración propia.

Resultados

En la actualidad, el mercado global de desarrollo de *software* ha crecido relativamente hasta el punto de que la seguridad es el componente que más veeduría tiene, ya que por medio de esto se caracteriza su total confiabilidad por parte

E-ISSN 2619-6301 No. 14, Año 2021

de los usuarios. Esto se encontró en una gran investigación de campo, la cual sirvió para recoger mediante una encuesta los datos sobre cómo las empresas chilenas concebían el desarrollo de *software* con la seguridad informática y qué herramientas, metodologías o estrategias utilizaban para verificar la seguridad de las aplicaciones realizadas. Por otra parte, el objetivo de la investigación era identificar las falencias que las empresas presentaban, ya que no tenían conocimiento acerca de las buenas prácticas de seguridad, lo que llevó llevó a formular una serie de sugerencias para integrar buenas prácticas de desarrollo de *software* seguro con base en la demanda del mercado chileno (Vega Zepeda, 2016).

De este modo, y con el avance de las tecnologías a día de hoy (González *et al.,* 2018), se asegura que la manipulación de datos es una de las principales modalidades de fraude que sufren los ciberdelincuentes, aunque estos mismos avances han permitido que se tomen medidas de prevención rápidas en tiempo real para reaccionar y/o pronosticar antes de que el fraude sea consumado. González *et al.* (2018) mencionan unas plataformas financieras que permiten realizar un análisis de datos automático para resolver las necesidades de detección de fraude, lo que conlleva a proponer diferentes metodologías de desarrollo con miras al diseño de una aplicación cuyo fin es detectar la evidencia digital de estos fraudes o delitos financieros.

En este apartado Coello (2016) realizó una investigación para su proyecto sobre sistemas de detección de fraudes financieros por medio de redes neuronales en la que obtuvo como resultado una serie de limitaciones de solución a contratiempos financieros de diferente tipo, entre estos asignaciones de créditos y riesgos en préstamos hipotecarios. Con esto logró hacer un sondeo frente a otras clases de riesgos como, por ejemplo, los de seguros y mercadotecnia, inversiones, vigilancia o planeación, resaltando el cubrimiento y la detención que permiten los sistemas inteligentes a fin de mitigar la vulnerabilidad por estos riesgos.

Por otra parte, un estudio realizado por Kumar e Iqbal (2017) sobre las técnicas de fraudes de MasterCard señala que se logró la tipificación de fraudes con tarjetas de crédito empleando enfoques de aprendizaje automático logaritmo ROC, la cual sirvió para clasificar varias técnicas utilizadas en la detección de fraudes de MasterCard y evaluar cada principio vinculado con la metodología admitida mediante la localización de patrones legales y criminales de transacciones que manejan el desequilibrio. Con base en esta problemática, en un artículo publicado en la página Enter.com se presenta un sistema de detección de fraudes MasterCard para asistir a los bancos, el cual permitirá a estas entidades contar con emisores de alertas avanzados para sus tarjetas y cuentas, los principales factores atacados por los ciberdelincuentes. Es por esto que la herramienta podrá reconocer la comercialización activa de los datos de cuentas y tarjetas, ya que estas tienen un riesgo elevado de uso fraudulento para hechos maliciosos (Ángulo, 17 de octubre de 2017).

De acuerdo con lo mencionado, el estudio realizado por Nur-E-Arefin (2010) presenta las técnicas de detección de

fraude en tiempo real para para fraudes bancarios, financieros, electrónicos u otros, por medio de la utilización de algoritmos de clasificación de minería de datos. Las denominó "aplicación de inteligencia computacional para identificar fraudes con tarjetas de crédito", ya que permiten al usuario obtener un mayor beneficio en cuanto a tecnología inteligente, menos costos y mayor efectividad en seguridad y funcionamiento.

Para concluir esta problemática, la Universidad Central (2017) publicó un artículo que trata sobre la combinación de codificadores automáticos y una máquina de vectores de soporte de clase para supervisar la detección de transacciones fraudulentas en tarjetas de crédito, cuyo objetivo es minimizar el ataque a los sistemas bancarios. Por último, dicha presentación fue nombrada como "un modelo de aprendizaje no supervisado basado en la combinación de un codificador automático" y "una máquina de vectores de soporte de una clase" (O'SVM) (Jerash y Al Dulaimi, 2008).

Teniendo en cuenta lo anterior, un estudio realizado a sistemas de detección supervisado y no supervisado afirma que el objetivo primordial de un sistema de detección de intrusos (IDS) es supervisar la actividad en un servidor o en una red, de modo que se pueda recolectar pistas y alertas de posibles ataques o intentos de violación a la seguridad. En otras palabras, un IDS podrá identificar actividades maliciosas, de forma que su respuesta sea generar alarmas y utilizar ciertos mecanismos de detección de fraude, con base en patrones de conocimiento, análisis de protocolos o código de firmas. Por último, también afirma que no son perfectos y pueden presentar fallas como cualquier sistema (Morales, 2018).

Por último, al realizar un análisis profundo de la temática se encuentra que hoy las grandes o pequeñas organizaciones tienen que estar en el nivel tecnológico que actualmente ofrece el mercado en el ámbito mundial. Por esta razón, las casas desarrolladoras de *software* son las principales opciones para renovar los procedimientos en las organizaciones en cuanto al manejo de su información privada y los datos de usuarios. Dicho lo anterior, se requiere que el *software* cumpla con los estándares y requisitos esenciales que requiera el cliente, en este caso las organizaciones. Puello *et al.* (2016) afirma: "Las empresas dedicadas a la producción de *software* deben establecer los mecanismos de control que permitan determinar que su producto cumpla con métodos, requisitos, parámetros y estándares de calidad, que garanticen que su producto esté libre de errores".

Con base en esto, Basharat *et al.* (2013) presentan un estudio vinculado a las buenas prácticas sobre los requerimientos de *software* en el artículo "Requirements Engineering Practices in Small and Medium Software Companies: An Empirical Study". La investigación se concentra en dichas prácticas y en definir qué medidas se supervisan en la industria de *software* de la pequeña y mediana empresa (mipymes). Este estudio fue elaborado con base en una consulta realizada a quince empresas desarrolladoras de *software*, y se buscaba con esta reconocer los inconvenientes presentados para así optar por buenas prácticas de requisitos de *software* y darle una solución posible.

E-ISSN 2619-6301 No. 14, Año 2021

Al abracar más el tema de los requisitos de *software*, Burnay *et al.* (2014) aportaron con su investigación, de manera práctica e hipotética, a la obtención de los requisitos. Afirman que a la hora de realizar entrevistas los ingenieros e interesados presentan contrariedad, ya que, desde sus perspectivas, tienen requisitos, antecedentes y experiencias de los sistemas diferente, así como expectativas frente al nuevo sistema. Es por esto que buscan la manera de que los interesados puedan desarrollar propuestas que incluyan de forma explícita los temas concernientes con la distinción de requisitos de *software* para así evidenciar los apartados principales y que sean discutidos entre los participantes durante el proceso de requisitos.

Discusión y análisis

En este caso, un grupo de investigadores se dirige a un número de empresas y a estudiantes de noveno y décimo semestre de ingeniería de sistemas, de forma general, con el fin de hacerles una encuesta que les permita recopilar información de cada uno. En los resultados arrojados se encontró que las empresas se clasifican así: diez grandes (20 %), veinticinco de mediano tamaño (50 %) y quince pequeñas (15 %). Las grandes empresas generan menos permisos que las medianas y pequeñas para conocer su proceso, mientras que las medianas señalaron que conocieron su proceso para el desarrollo de *software*. En cuanto a las pequeñas, son las más numerosas y a la vez tienen más dificultad de ser identificadas y acceder a sus procesos. La actividad de las empresas desarrolladoras de *software* está dirigida, principalmente, al sector de la banca (20 %), que es mucho más fuerte que los demás. Por ejemplo, al sector estatal solo le corresponde el 18 %, a la industria el 16 %, al sector financiero el 15 %, al de seguros y de salud el 8 %, y al educativo y de seguridad social el 5 %. Es comprensible que los sectores mejor cubiertos sean los de la banca y el Estado, pues en ellos se encuentra la mayoría de empresas de la capital de la República de Colombia (Velandia y López, 2015).

Por otra parte, al analizar la problemática que presentan en el momento de utilizar una metodología de desarrollo de *software*, las empresas desarrolladoras recurren a metodologías acomodadas de acuerdo con el requerimiento del cliente, el analista o el diseñador. Otra problemática que hallaron en el análisis fue que la mayoría no sigue la fase de la metodología escogida y la adaptación "a cambios" según los requisitos de quien las practica. Dado esto, según los encuestados, una vez que culminan los proyectos no obtienen los resultados esperados y se presentan fallas en el *software*, lo que conlleva a hacerles reajustes en caliente para corregirlos.

De acuerdo con los resultados de los sondeos realizados a profesionales y estudiantes de ingeniería de sistemas, se realizó un análisis a los datos reunidos en el que se establecieron similitudes entre los dos tipos de encuestas. Allí se encontró que muy poco se usa una metodología sencilla y de fácil uso para los desarrolladores de proyectos pequeños y medianos que no genere de manera exhaustiva el estrés como de una metodología ágil, ya que no requiere una documentación tan amplia ni reuniones diarias en las que no se logra concretar

las ideas, sino que, por el contrario, algunos programadores presentan roces o discrepancias de acuerdo con los conceptos que cada uno tiene sobre los temas propuestos.

Por otra parte, Muñoz *et al.* (2016) señalan lo siguiente:

> Hoy en día, las pymes están utilizando metodologías ágiles como un esfuerzo para producir *software* que cumpla con el tiempo solicitado por el mercado. Sin embargo, la falta de conocimiento sobre cómo utilizarlos adecuadamente da como resultado en su adopción empírica con un desarrollo de *software* ineficiente. En este contexto, un conjunto de herramientas de *software* que pretenden ayudar a las pymes en la implantación de una metodología ágil. (p. 123)

Durante las investigaciones fue posible encontrar un caso en el que la Escuela Superior Politécnica del Litoral, por medio del proyecto VLIR-ESPOL, inició un estudio de tipo exploratorio en 77 empresas desarrolladoras de *software* ubicadas en Quito y Guayaquil. De esta manera, se mejoró el estado actual de conocimiento sobre el uso de métricas en las empresas, y, con la información adquirida, se desarrolló el proceso de medición de *software* dirigido a objetivos. Así, se definieron objetivos de medición, de modo que se identificaron necesidades de información y se construyeron indicadores que visualizan el estado del proceso de desarrollo del *software* a medida que este se desarrolla.

Por otra parte, se evidencia que una de las principales dificultades en Ecuador es que las universidades no poseían capacidad de ofrecer personal especializado para el desarrollo de *software* altamente técnico. Las empresas que se encontraban en el proceso de obtención de certificaciones de calidad necesitaban mecanismos accesibles y muy pocos gerentes, así como directores de proyectos con la capacidad para administrar el proceso de exportación de *software*.

Teniendo en cuenta lo anterior, los resultados del estudio aplicado a 77 empresas de *software* ubicadas en Quito, Guayaquil y Cuenca por el subcomponente 8 del proyecto VLIR-ESPOL (2003) fueron los que se enlistan a continuación.

- El 51 % de las empresas son medianas o pymes, el 40,4 % son pequeñas y el 8,6 % son grandes. El 46 % de las empresas realizan consultorías, desarrollo y venta de sus aplicaciones en conjunto.
- La edad promedio de los gerentes bordea los 33 años, y la edad promedio de las empresas es 7,4 años. Solo el 19,4 % de las empresas utilizan una combinación entre experiencia, habilidades y capacidades de los desarrolladores.
- El mercado objetivo se divide según el tamaño de las empresas y lo conforman las comerciales, de servicios, financieras, industriales y gubernamentales. Solo el 36,4 % penetra en el mercado internacional.
- En el medio sí se tiene conocimiento sobre las normas de calidad en el desarrollo del *software*, pero al parecer no sobre los beneficios que podrían obtener al estar certificados.
- El 36,3 % de las empresas utilizan estándares de calidad en el desarrollo de *software*, de los cuales solo el 24,6 % son internacionalmente reconocidos. La mayoría utiliza pro-

E-ISSN 2619-6301 No. 14, Año 2021

cedimientos internos para asegurar la calidad en el *software*.

Finalmente, se hizo una aplicación piloto del plan de métricas en tres empresas de *software*. Permitió identificar aspectos favorables y desfavorables que se deben tener en cuenta para evitar errores en la aplicación de este instrumento y mejorar la precisión de los resultados obtenidos (González Carrión *et al.*, (2009).

En el contexto del Ecuador, Quelal *et al.* (2018) señalan lo siguiente: (2018):

> Un estudio sobre el uso, utilidad y causas de dejar de usar ágiles metodologías en organizaciones medianas y grandes. Los resultados muestran que un porcentaje considerable de profesionales no reciben entrenamiento formal antes de adoptar metodologías ágiles, y que un alto porcentaje de organizaciones, especialmente públicas, deciden abandonar su uso. Sin embargo, las empresas privadas de la Banca son las que siguen utilizando ágiles. Sus resultados dan a conocer que 48 % de los encuestados afirman haber utilizado alguna vez metodologías ágiles dentro de sus proyectos, siendo Scrum el más preferido por las organizaciones (68,75 %), seguido de Kanban (25 %) y XP (18,75 %). (pp.1-6)

Por su parte, Nuevo *et al.* (2011) afirman:

> En otras palabras, las metodologías más difundidas para el desarrollo de *software* está el Proceso Unificado Racional (RUP). Aun así, en las últimas décadas se han desarrollado una secuencia de metodologías llamadas "metodologías ágiles", que tienen como objetivo desarrollar *software* rápidamente, centrándose en las personas y en la entrega frecuente de *software*. De las metodologías ágiles existentes, Scrum es una de las de aplicación más amplia, debido a su capacidad para complementar otros métodos y procesos. Por esta razón, las estrategias propuestas por Scrum pueden ser adecuadas para la gestión distribuida y despliegue de las fases y disciplinas de la RUP. (p. 66)

Sugerencias

A continuación, se enlistan algunas sugerencias.

- Mediante las investigaciones realizadas sobre los diferentes trabajos de proyectos de investigación se evidenció, en los resultados y los análisis, que las empresas o casas desarrolladoras de *software* tienen participación directa en estos casos. Podemos decir que en el propósito de desarrollar un *software* se requiere una buena planificación, estructuración y un buen control sobre el proyecto, ya que si no son concisos, ordenados, claros y específicos no cumplirán con las expectativas y los objetivos trazados.
- Por otra parte, en el diseño de *software* se debe tener en cuenta ciertas etapas fundamentales que conllevan a su buen desarrollo. Estas son análisis de requerimientos y diseño, las cuales son las que toman más tiempo del proyecto.
- La documentación encontrada mediante los análisis de estudio ayudó, en parte, a que todo el desarrollo fuese más fácil, ya que aportaba ideas de desarrollo, procesos y directrices, entre otros aspectos. Esto

de una u otra forma nos permitió tener claridad sobre lo que se debía hacer y planificar de manera organizada su proceso de desarrollo.

- Con los constantes cambios en las tecnologías utilizadas hoy es recomendable no contar con un modelo de desarrollo específico, de manera que este permita orientarlo y adecuarlo a los requerimientos o necesidades del cliente y, según su interpretación, generalice y cumpla con sus expectativas.
- Los análisis realizados a los diferentes trabajos nos permitió obtener como resultados que las metodologías escogidas se basaban por estándares en los que sus autores implementaban métodos de estudio y de investigación para lograr los objetivos.

Agradecimientos

En primer lugar, darle gracias a Dios porque nos permitió llegar hasta acá, a mis padres por el constante apoyo, a la Fundación Universitaria del Área Andina y al ingeniero y profesor Camilo Augusto Cardona Patiño por su orientación durante el proceso y desarrollo del presente artículo.

REFERENCIAS

AENOR. UNE 71506. (2013). *Tecnologías de la información (TI). Metodología para el análisis forense de las evidencias electrónicas*. Recuperado de http://www.aenor.es/aenor/inicio/home/home.asp

Alvear Cervantes, J. L. y Mazón Naranjo, J. H. (2007). *Elaboración y análisis de métricas para el proceso de desarrollo de software para empresas desarrolladoras de software del Ecuador* (tesis de grado). Espol. Fiec. https://www.dspace.espol.edu.ec/handle/123456789/44258

Angulo, S. (2017, octubre 17). Herramienta de MasterCard. Enter.co. https://www.enter.co/especiales/empresas/herramienta-mastercard-identifica-fraudes/

Chavarría, A. E., Oré, S. B. y Pastor, C. (2016). Aseguramiento de la calidad en el proceso de desarrollo de *software* utilizando CMMI, TSP y PSP. *RISTI-Revista Ibérica de Sistemas y Tecnologías de Información*, 20, 62-77. https://pdfs.semanticscholar.org/230c/177c4a620147c2f9dfbf9c1e9c9c7785e207.pdf

Coello, C. C. (2016). Uso de técnicas de inteligencia artificial para aplicaciones financieras. *Revista Sinergia*, 1-7. http://200.122.211.70/ojs/index.php/Revistasinergia/article/view/83

Coque-Villegas, S., Jurado-Vite, V., Avendaño-Sudario, A. y Pizarro, G. (2018). Análisis de experiencias de mejora de procesos de desarrollo de *software* en pymes. *Ciencia Unemi*, *10*(25), 13-24. http://cienciaunemi.unemi.edu.ec/ojs/index.php/cienciaunemi/article/view/616

Di Iorio, A., Castellote, M., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. Giaccaglia, M., Cistoldi, P., Podestá, A., Iturriaga, J., Greco, F., Alberdi, J. I., Ruiz, G., Trigo, S. y Nuñez, L. (2017). *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense*. REDI; Universidad FASTA. http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1593

González Carrión, R. V., Hernández Rendon, H. X. y Villavicencio Cabezas, M. K. (2009). *Desarrollo de un código de métricas para pequeñas empresas ecuatorianas desarrolladoras de software en conjunto con el proyecto VLIR-ESPOL*. https://www.dspace.espol.edu.ec/handle/123456789/562

González, E., Romero, G. y Ortiz, A. (2018, junio 12). *Detección de fraude en tarjetas de crédito*. Universidad Santo Tomás. https://repository.usta.edu.co/bitstream/handle/11634/12529/2018edwingonzalez.pdf?sequence=1&isAllowed=y

E-ISSN 2619-6301 No. 14, Año 2021

Grijalva Lima, J. S. y Loarte Cajamarca, B. (2017). *Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador*. http://repositorio.uisek.edu.ec/handle/123456789/2952

Gutiérrez Portela, F., Moreno Hernández, J., Echeverry, B. y Jaramillo, A. (2019). Uso de los sistemas inteligentes para la detección de fraudes financieros. *Revista Sinergia*, *1*(6), 6-30. http://200.122.211.70/ojs/index.php/Revistasinergia/article/view/83

Hernández Quintero, H. A. (2018). Los delitos financieros en Colombia: antecedentes, evolución y futuro. En *Temas de derecho penal económico y patrimonial* (1a ed., vol. 1, pp. 155-191). Universidad Pontificia Bolivariana. https://pure.unibague.edu.co/es/publications/los-delitos-financieros-en-colombia-antecedentes-evoluci%C3%B3n-y-futu

Manrique Horta. (2016). Diariamente en Colombia hay 10 millones de ataques informáticos. *Diario del Huila*. Recuperado de http://diariodelhuila.com/economia/%E2%80%9Cdiariamente-en-colombia-hay-10-millones-de-ataques-informaticos%E2%80%9D-cdgint20160312211955155)

Marín, J., Nieto, Y., Huertas, F. y Montenegro, C. (2019). Modelo ontológico de los ciberdelitos: caso de estudio Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*, E17, 244-257. https://search.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393

Miranda, E. A., Bernardis, H. y Riesco, D. E. (2020). *Ingeniería de software al servicio de la informática forense y la evidencia digital*. En XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020). El Calafate, Santa Cruz. http://sedici.unlp.edu.ar/handle/10915/104037

Naranjo, A. y Villacis Ruiz, V. M. (2018). *Auditoría forense: metodología, herramientas y técnicas aplicadas en un siniestro informático de una empresa del sector comercial*. https://www.dspace.espol.edu.ec/retrieve/128067/D-CD71164.pdf

Predisoft. (2018, octubre 14). Detección del fraude. *Sistema para la prevención del fraude en múltiples canales*. http://predisoft.com/psfraud-sistema-deteccion-fraudes-bancarios-y-otros-canales/

Ramírez Aguilera, J. A. (2017). *Implicaciones de seguridad en metodologías ágiles de desarrollo de software* (trabajo de grado). Fundación Universitaria Los Libertadores. http://repository.libertadores.edu.co/handle/11371/1163

Velandia, L. N. M. y López, W. M. L. (2015). Escoger una metodología para desarrollar *software*, difícil decisión. *Revista Educación en Ingeniería*, *10*(20), 98-109. https://educacioneningenieria.org/index.php/edi/article/view/579/275

Vidal Londoño, J. H. (2016). *Una nueva experiencia en seguridad hacking ético, situación actual de Colombia ante la seguridad informática* (tesis de grado). Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/15838/vidallondo%c3%b1ojes%c3%bashern%c3%a1n2017.pdf?sequence=1&isAllowed=y

Zambrano, A., Guarda, T., Valenzuela, E. V. H. y Quiña, G. N. (2019). Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web. *Revista Ibérica de Sistemas e Tecnologias de Informação*, E17, 299-308. https://www.researchgate.net/profile/Teresa-Guarda/publication/331178479_Mitigation_techniques_for_security_vulnerabilities_in_web_applications/links/5fabe891a6fdcc331b9478b4/Mitigation-techniques-for-security-vulnerabilities-in-web-applications.pdf