Diseño de un Sistema de Detección de Evidencias Digitales Frente a Delitos Financieros en el Sector Empresarial

Wilmer Andrés Arocha Rico[1]

RESUMEN

El desarrollo del proyecto es oportuno, ya que propone una alternativa de eliminar la problemática que padecen reiteradamente las grandes, medianas y pequeñas organizaciones, siendo las principales víctimas del delito o fraude mediante ataques informáticos que conllevan a causar daños teniendo como objetivo secuestrar o eliminar la información de estas, es por esto que 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 así la información esté segura. El propósito de este proyecto es poder brindar al usuario u organización una opción de soporte seguro de gran utilidad, y que le beneficie para que pueda alcanzar un rendimiento óptimo en cuanto a su funcionamiento sin ninguna interrupción.

PALABRAS CLAVE

Activo, confidencialidad, informática forense, metodología, software.

INTRODUCCIÓN

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

Por otra parte, esto estimula a los ciberdelincuentes a que indaguen sobre información de manera ilegal violando la seguridad, ocasionando la exclusión, daño o modificación, provocados en algunas situaciones por las mismas compañías, por hackers o grupos de ciberdelincuentes que buscan lograr su objetivo el cual es 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 en el año 2015 el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40% con respecto al 2014. Esto contrajo unas pérdidas económicas altísimas, que según el Banco Mundial (2014), las cifras llegaron cerca de unos US$500 millones aproximadamente. **(Manrique Horta. 2016. Diariamente en Colombia hay 10 millones de ataques informáticos. Diario del Huila).**

Teniendo como base lo anterior, es de suma importancia proponer una metodología eficaz y confiable, donde brinde a los profesionales del área la facilidad de acceder a los recursos, maneras, tareas y demás habilidades metodológicas ordenadas para un oportuno peritaje informático, logrando una indagación qué durante el análisis forense permita saber ¿qué?, ¿cómo?, ¿quién?, ¿de

[1] warocha@estudiantes.areandina.edu.co

dónde? y ¿cuándo? 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 que mitiguen estos ataques informáticos, un ejemplo de ello sería **Fraud** que es 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, ofreciendo a las organizaciones una tecnología inteligente, un valor cuyo costo no sea muy alto y una que tenga una mayor efectividad, además de reducir el trabajo asociado a la investigación de alertas.

Teniendo en cuenta todo lo mencionado anteriormente las organizaciones se sienten más seguras a la hora de utilizar estas aplicaciones, dando toda su confianza de que estas les darán un plus de ventaja en cuanto a la prevención de ataques informáticos realizados por los ciberdelincuentes.

OBJETIVO GENERAL

- Identificar la metodología de desarrollo útil para la creación de una aplicación orientada a la detección de evidencias digitales frente a delitos financieros.

OBJETIVOS ESPECÍFICOS

- Realizar una recopilación de los casos más relevantes de empresas desarrolladoras de software enfocados 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 dando solución a los problemas mediante una planificación adaptativa y una toma de decisiones que conllevan a avanzar de manera que se cumpla con lo propuesto.

OBJETIVO

- Hacer 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 siguientes objetivos que nos permitirán desarrollar y cumplir las metas trazadas del proyecto:

- Realizar una recopilación de los casos más relevantes de empresas desarrolladoras de software enfocados 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:

- El acceso se dará a los usuarios autorizados.
- El software se podrá instalar en cualquier sistema operativo, ejemplo: Windows, Linux, OSX, etc.
- La aplicación podrá detectar evidencias encontradas en los dispositivos en donde 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 el cual les permitirá a los usuarios intercambiar mensajes o información de forma segura.
- Debe especificarse un plan de recuperación en caso tal se presente un desastre y el cual se vea afectado el software y no interrumpa su funcionamiento.
- La aplicación deberá dar 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, 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 a otros proyectos de desarrollo de software, casas desarrolladoras de software y a 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, sea en los objetivos, proceso, etc.

5. Cierre:

Etapa final del proyecto, en esta se culmina todo el proceso de desarrollo, lo cual durante todo el proceso final se tendrán en cuenta comentarios alternos de mejora por ambas partes (Clientes-Equipo de trabajo) lo cual servirán de ayuda para corregir errores del desarrollo del proyecto.

DIAGRAMA

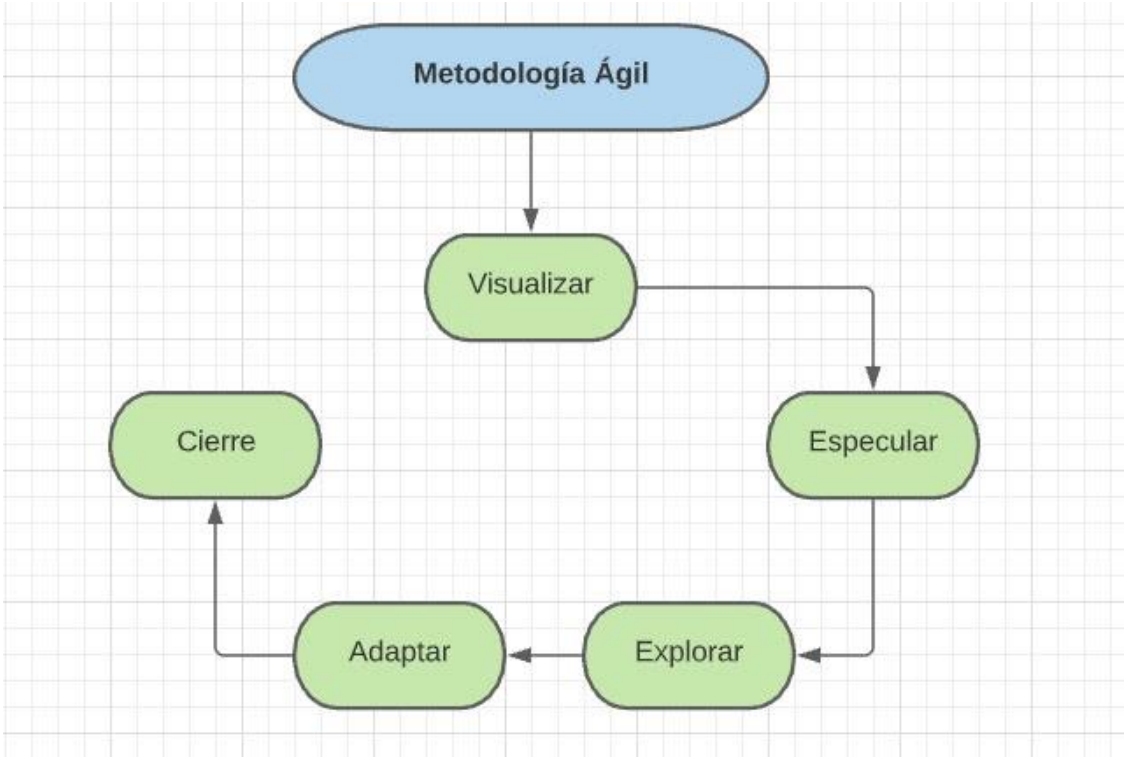

Figura 1. Nombre: Diagrama de la metodología. Fuente: Propia.

RESULTADOS

En la actualidad, el mercado global de desarrollo de software ha crecido relativamente hasta cierto punto de que la seguridad es el componente que más veeduría tiene, ya que por medio de esto se caracteriza su total confiabilidad por los usuarios. 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 otro lado, cuyo objetivo era identificar las falencias que las empresas venían presentando, ya que no tenían conocimiento acerca de las buenas prácticas de seguridad, dicha investigación llevó así a formular una serie de sugerencias para integrar buenas prácticas de desarrollo de software seguro, en base a la demanda del mercado chileno **(Vianca Rosa Vega Zepeda, 2016)**.

De este modo, y con el avance de las tecnologías a día de hoy, **(González, Romero, & Ortiz, 2018)** aseguran que la manipulación de datos es una de las principales víctimas de fraude por los ciberdelincuentes, aunque estos mismos avances a su vez han permitido que se tomen medidas de prevención rápidas en tiempo real para reaccionar y/o pronosticar antes de que el fraude sea consumado, para esto ellos citan unas plataformas financieras el cual permite realizar un análisis de datos automático para resolver las necesidades de detección de fraude, lo que conlleva a proponer diferentes metodologías de desarrollo para el diseño de una aplicación para 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 a través de redes neuronales en donde obtuvo como resultado una serie de limitaciones de solución a contratiempos financieros de diferente tipo, entre ellos asignaciones de créditos y riesgos en préstamos hipotecarios. Con esto logró hacer un sondeo frente a otras clases de riesgos como de seguros y mercadotecnia, inversiones, vigilancia, planeación, resaltando el cubrimiento y detención que permiten los sistemas inteligentes para lograr la mitigación de ser vulnerable por estos riesgos.

Por otro lado, en un estudio realizado por **(Kumar & Iqbal, 2017)**, sobre las técnicas de fraudes de MasterCard le permitió lograr 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 localizando patrones legales y criminales de transacciones que manejan el desequilibrio. En base a esta problemática, en un artículo publicado por la página www.enter.com presentan un sistema de detección de fraudes MasterCard para asistir a los bancos a enfrentar el fraude, que permitirá a estas entidades mediante esta herramienta contar con emisores de alertas avanzados para sus tarjetas y cuentas, la cual son 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, 2017)**

De acuerdo con lo mencionado anteriormente, un estudio realizado por (Nur-E-Arefin, 2010) sobre las técnicas de detección de fraude en tiempo real para para la detección de fraudes bancarios, financieros, electrónicos u otros, por medio de la utilización de algoritmos de clasificación de minería de datos donde la denominó aplicación de inteligencia computacional para identificar fraudes con tarjetas de crédito, permitiendo 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)** hace público un artículo donde se realizó una presentación 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 de esto 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 & Al Dulaimi, 2008)**.

Teniendo en cuenta lo anterior, un estudio realizado a sistemas de detección supervisado y no supervisado afirma que, cuyo objetivo primordial de un sistema de detección de intrusos (IDS), es supervisar la actividad en un servidor o en una red, donde se puedan recolectar pistas y alertas de posibles ataques o intentos de violación a la seguridad. En otras palabras, un (IDS) podrá identificar actividades maliciosas donde cuya respuesta sea de generar alarmas y utilizar ciertos mecanismos de detección de fraude, el cual estos se basan por medio de 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, realizando un análisis profundo de la temática, hoy en día las grandes o pequeñas organizaciones tienen que estar al nivel tecnológico que hoy ofrece el mercado a nivel mundial, es por eso que 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".

En base a esto, **(Basharat, Fatima, Nisa, Hashim, & Khanum, 2013)** presenta un estudio vinvulado a las buenas prácticas sobre los requerimientos de software en su artículo denominado *Requirements engineering practices in small and medium software companies: An empirical study*. Donde ellos comentan que su estudio cuyo objetivo se concentra en dichas prácticas y en definir qué medidas se están supervisando dentro de la industria de software de la pequeña y mediana empresa (MiPymes). Dicho estudio fue elaborado en base a una consulta a 15 empresas desarrolladoras de software donde se buscaba reconocer los inconvenientes presentados para así optar por buenas prácticas de requisitos de software y darle solución posible al respecto.

Abarcando más con el tema de los requisitos de software, **(Burnay, Jureta, & Faulkner, 2014)** aportaron con una investigación de manera práctica e hipotética a la obtención de los requisitos y ellos afirman que a la hora de hacer entrevistas los ingenieros e interesados presentan contrariedad, ya que estos desde sus perspectivas tienen requisitos, antecedentes y experiencias de los sistemas diferentes como también expectativas al nuevo sistema. Es por esto que buscan la manera de que los interesados puedan desarrollar propuestas que incluyan de manera 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 dirigen 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 de modo que puedan recopilar información de cada uno, en los resultados arrojados se

encontró que las empresas se clasifican así, 10 grandes (20 %), 25 de mediano tamaño (50 %) y 15 pequeñas (15 %), donde las grandes empresas generan menos permisos que las medianas y pequeñas para conocer su proceso, mientras que las medianas facilitaron 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 para 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 sólo 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, L. N. M., & López, W. M. L. (2015).

Por otro lado, al analizar la problemática que presentan al momento de utilizar una metodología de desarrollo de software, las empresas desarrolladoras recurren a metodologías acomodadas de acuerdo al requerimiento del cliente, analista o diseñador. Otra problemática que hallaron en el análisis, fue que la mayoría no sigue la fase de la metodología escogida y la adaptación "cambios" según los requisitos de quien las practica. Dado esto, para los encuestados una vez que culminan los proyectos no obtienen los resultados esperados, se presentan fallas en el software lo 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 donde se establecieron similitudes entre los 2 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 genera de manera exhaustiva el estrés como el de una metodología ágil, ya que no requiere una documentación tan amplia ni reuniones diarias en donde no se logran concretar las ideas, sino por el contrario algunos programadores presentan roces o discrepancias de acuerdo a los conceptos que cada uno tiene sobre los temas propuestos.

Por otro lado, Muñoz et al. (2016) sostuvieron:

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, se pudo encontrar un caso en el que junto a la a Escuela Superior Politécnica del Litoral y a través del proyecto VLIR-ESPOL, se inició un estudio de tipo exploratorio en 77 empresas desarrolladoras de software ubicadas en las ciudades de Quito y Guayaquil mejorando de esta manera el estado actual de conocimiento sobre el uso de métricas en las empresas. Con la información adquirida se desarrolló el proceso de medición de software dirigido a objetivos definiéndose objetivos de medición, identificándose necesidades de información y construyéndose indicadores que visualizan el estado del proceso de desarrollo del software a medida que este se va desarrollando.

Por otro lado, dentro de esto se evidencia que una de las principales dificultades en ecuador, es que las universidades no poseían capacidad de ofrecer personal especializado para 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, directores de proyectos poseían 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 siguientes:

- 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. Sólo 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 mismas y lo conforman las empresas comerciales, de servicios, financieras, industriales y gubernamentales. Sólo el 36,4% penetra en el mercado internacional.
- En el medio si 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 sólo el 24,6% son internacionalmente reconocidos. La mayoría utiliza procedimientos internos para asegurar la calidad en el software.

Finalmente se hizo una aplicación piloto del plan de métricas en 3 empresas de software que permitió identificar aspectos favorables y desfavorables que deben ser tomados en cuenta para evitar errores en la aplicación de este instrumento y mejorar la precisión de los resultados obtenidos. **Gonzalez Carrion, R. V., Hernandez Rendon, H. X., & Villavicencio Cabezas, M. K. (2009)**

En Ecuador, Quelal, Villavicencio, y Mendoza (2018) mencionaron:

Un estudio sobre el uso, utilidad y causas de dejar de usar ágiles metodologías en rganizaciones 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)

Nuevo, Piattini y Pino (2011) sostuvieron:

En otras palabras, las metodologías más difundidas para el desarrollo de software está el Proceso Unificado Racional (RUP). Aún 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

- Mediante las investigaciones realizadas a los diferentes trabajos de proyectos de investigación se logró evidenciar en los resultados y análisis que las empresas o casas desarrolladoras de software tienen participación directa en estos casos. Podemos decir que, para desarrollar un software se requiere de 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 objetivos trazados.
- Por otro lado, en el diseño de software se deben de tener en cuenta ciertas etapas fundamentales que conllevan a implementar un buen desarrollo de software, éstas son la del análisis de requerimientos y diseño, las cuales son las que más tiempo toman del proyecto.
- La documentación encontrada mediante los análisis de estudio ayudó en parte a que todo el desarrollo fuese más fácil, ya que aportaban ideas de desarrollo, procesos, directrices, entre otros. 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 a día de hoy, es recomendable no contar con un modelo de desarrollo específico, donde éste permita orientarlo y adecuarlo a los requerimientos o necesidades del cliente que 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 donde 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 y a mis padres por el constante apoyo, también a la Fundación Universitaria del Área Andina y al Ingeniero y Profesor Camilo Augusto Cardona Patiño por su gran 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, Jose Luis; Mazon Naranjo, Jorge Humberto (2007). Elaboración y análisis de métricas para el proceso de desarrollo de software para empresas desarrolladoras de software del Ecuador. Trabajo final para la obtención del título: Ingeniero en Computación Especialización Sistemas Tecnológicos. Espol.Fiec, Guayaquil. 180p. https://www.dspace.espol.edu.ec/handle/123456789/44258

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

Chavarría, A. E., Oré, S. B., & 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. 1-7. http://200.122.211.70/ojs/index.php/Revistasinergia/article/view/83

Coque-Villegas, S., Jurado-Vite, V., Avendaño-Sudario, A., & Pizarro, G. (2018). Análisis de experiencias de mejora de procesos de desarrollo de software en PYMEs.//Analysis of experiences of improvement of software development processes in SMEs. Ciencia Unemi, 10(25), 13-24. http://cienciaunemi.unemi.edu.ec/ojs/index.php/cienciaunemi/article/view/616

Di Iorio, Ana Haydée, y otros. (2017): 520 «El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense.» REDI - Universidad FASTA, Recuperado de http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1593

Gonzalez Carrion, R. V., Hernandez Rendon, H. X., & 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

Gonzalez, E., Romero, G., & Ortiz, A. (12 de junio de 2018). Detección de Fraude en Tarjetas de Crédito. Obtenido de Universidad santo tomas: https://repository.usta.edu.co/bitstream/handle/11634/12529/2018edwingonzalez.pdf?sequence=1&isAllowed=y

Grijalva Lima, Juan Sebastian, Loarte Cajamarca, Byron. (2017): 20 «Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador.» Repositorio Digital, Recuperado de http://repositorio.uisek.edu.ec/handle/123456789/2952

Guitérrez-Portela, F., Moreno-Hernández, J., Echeverry, B., & Jaramillo, A. (2019). USO DE LOS SISTEMAS INTELIGENTES PARA LA DETECCIÓN DE FRAUDES FINANCIEROS.

Revista Sinergia, 1(6), 6-30. Recuperado a partir de 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 (1 ed., Vol. 1, pp. 155-191). Colombia- Medellín: 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)

Marin, J., Nieto, Y., Huertas, F., & Montenegro, C. (2019). Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, (E17), 244-257. https://search.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393

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

Naranjo Alice, Villacis Ruiz, Viviana Marcela. Auditoría Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial. 22 de 06 de 2018. 12 de 05 de 2020 <https://www.dspace.espol.edu.ec/retrieve/128067/D-CD71164.pdf>.

Predisoft. (14 de Octubre de 2018). Detección del fraude. Obtenido de 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. http://repository.libertadores.edu.co/handle/11371/1163

Velandia, L. N. M., & 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, Jesús Hernán. (2016) Una nueva experiencia en seguridad hacking ético, situación actual de Colombia ante la seguridad informática. Universidad Militar Nueva Granada. Recuperado de 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., & 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