Prototipo Web para Gestión de Experiencias de Informática Forense

Carlos Orellana[1] Cecilia Lara[1] Liliana Figueroa[1]

[1] Instituto de Investigación en Informatica y Sistemas de Información, Facultad de Ciencias Exactas y Tecnologías, Universidad Nacional de Santiago del Estero
orellanacarlos3003@gmail.com; clara@unse.edu.ar; lmvfigueroa@yahoo.com.ar

Resumen. La informática forense requiere que quienes realizan el análisis forense de los distintos dispositivos, los peritos informáticos, cuenten con cierta experiencia para hacerlo. Esta experiencia puede ser almacenada y reutilizada por los demás peritos, para nutrirse y evitar errores a lo largo de la adquisición y análisis de la evidencia digital. Para ello, se plantea el desarrollo de un prototipo de aplicación web que funcione como un repositorio de las experiencias de los peritos del Ministerio Publico Fiscal de Santiago del Estero, para que estos puedan almacenar sus experiencias y también consultar evidencias de otros peritos, fomentando así el aprendizaje y el reuso de las experiencias. Este prototipo se desarrolló mediante una metodología ágil, recabando requerimientos en historias de usuario, el diseño de la base de datos, y programando en distintos frameworks para front-end y back-end. Luego este prototipo fue expuesto a los peritos informáticos parra retroalimentación, y así terminar de darle forma con las sugerencias de estos.

Palabras claves: Aplicación web, Informática forense, Experiencias

1 Introducción

Resulta relevante destacar los desafíos que genera el avance tecnológico para incorporar la utilización de la evidencia digital al sistema procesal penal, como prueba fundamental en la investigación de cualquier delito. Entonces, es necesario contar con métodos científicos que permitan recolectar, analizar y validar pruebas digitales que sean legalmente aceptables y que ayuden a resolver la investigación penal, con el fin de recolectar evidencias que cumplan los principios de admisibilidad y tengan validez en el proceso judicial [1].

En el contexto de estos laboratorios se pueden identificar diferentes problemas entre los que se puede destacar que las experiencias y las capacitaciones que se adquieren durante la realización de las pericias no se documentan para fomentar el autoaprendizaje organizacional.

Así la Gestión del Conocimiento es un conjunto de actividades y estrategias que se utilizan para crear, compartir y aplicar el conocimiento generado por el recurso humano en beneficio de la organización. Según lo plantea [2] el objetivo de esta gestión es com-

partir las experiencias positivas o negativas con el fin de utilizarlas cuando sea necesario y a la vez actualizar el conocimiento requerido para las actividades principales que se desarrollan en el contexto de una institución. De esta manera este paradigma de la gestión del conocimiento tiene que ver con la actitud de compartir conocimientos de manera generosa y desinteresada, más que proteger el conocimiento en sí.

En estos últimos años se han desarrollado repositorios [3] que permiten entre otras cosas compartir experiencias y registrar conocimientos que van surgiendo del proceso de obtención de la evidencia digital. Esto puede implementarse con una herramienta de software que sea capaz de: producir conocimiento forense reutilizable para que sirva de apoyo durante las investigaciones, organizar experiencias pasadas para fomentar el intercambio de conocimientos entre expertos forenses y registrar la información recopilada de manera que facilite la evaluación de la calidad.

Este trabajo surge en el marco de un proyecto de investigación Informática Forense: Métodos, Herramientas y Técnicas de la Universidad Nacional de Santiago del Estero y describe el desarrollo de un prototipo de software que permita la gestión de experiencias de los peritos informáticos que forman parte del laboratorio de informática forense. Esta herramienta pretende ser un recurso estratégico que permita gestionar de manera eficiente el conocimiento y la experiencia adquirida, de manera tal que promueva el trabajo eficiente de la labor de los peritos.

2 Metodología

Para el desarrollo de la aplicación, se implementó un marco de trabajo ágil, SCRUM [4], organizando el trabajo en sprint de dos semanas. Para la definición de requerimientos se empleó historias de usuario, las cuales permiten describir de forma breve una funcionalidad software tal y como la percibe el usuario. Se realizaron reuniones de revisión de sprint (sprint review) con el cuerpo de peritos, con el propósito de presentar los resultados del trabajo y discutir el progreso hacia el objetivo del prototipo. Para el diseño de la base de datos se empleó la herramienta CASE Software Ideas Modeler [5].

La arquitectura de la aplicación es de tipo cliente servidor, posibilitando a los peritos acceder al servidor web, para poder realizar búsquedas y también ofrecer la opción de gestionar sus propias experiencias.

La programación posee dos partes: el front-end, donde se optó por trabajar con HTML para estructurar la aplicación, la librería Bootstrap de CSS y Angular material para darle estilos y el framework Angular basado en TypeScript; el back-end, donde se empleó Java con la arquitectura Api-Rest, mediante la herramienta de SpringBoot, con el framework Spring.

2.1 Historias de usuario

Las principales historias de usuarios son: HU1: Registrar mis experiencias y conocimiento durante la adquisición de evidencia digital para compartirlas con aquellos compañeros que necesiten. HU2: Modificar y/o eliminar experiencias y conocimientos en caso de algún error en la carga de estas para no entorpecer la ayuda a los compañeros. HU3: Buscar las experiencias de los compañeros, a través de diferentes criterios de búsqueda para obtener los resultados deseados y ahorrar tiempo.

2.2 Diseño inicial de la base de datos

En la Fig. 1 se puede observar el diagrama entidad-relación empleado como modelo de la base de datos, en el cual se define una entidad “Experiencia” donde se consigna la descripción de la experiencia, el legajo fiscal y el perito que registra la experiencia. Se ha definido una entidad “Dispositivo”, donde se caracteriza a los dispositivos trabajados y una entidad “Herramienta” para describir a la herramienta forense empleada en una experiencia en particular. También, se contempla el registro de datos de la causa y de la solicitud de pericia con el propósito de identificar en los registros internos de la oficina el pedido de trabajo técnico recibido.

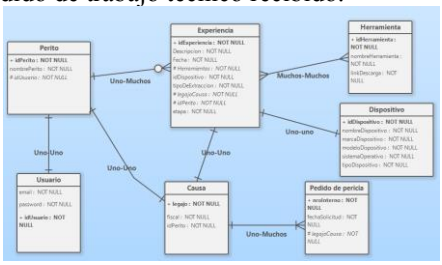

Fig. 1. DER realizado con Software Ideas Modeler

2.3 Programación

Para el desarrollo con las tecnologías antes mencionadas, se utilizaron dos entornos de desarrollo integrado (IDE). El primero corresponde a Visual Studio Code, el cual se empleó para la programación del front-end. El segundo es Netbeans, que se utilizó para la programación del back-end.

2.4 Retroalimentación y puesta a punto

En cada finalización de un sprint se realizó una reunión de revisión de sprint hasta llegar a una primera versión final del prototipo, el cual fue presentado al grupo de peritos informático. Como resultado surgieron los puntos a mejorar y/o agregar en la aplicación web, algunos de los cuales son: tener en cuenta el tipo de dispositivo para solicitar los datos que lo caractericen, actualizar el nombre de los controllers en la Api, completar la búsqueda con el uso de etiquetas previamente definidas, optimizar el modelo de datos, modificar paletas de colores, tener en cuenta aspecto de navegación, textos descriptivos en el formulario y presentar información sobre el procesador que tiene un determinado dispositivo móvil (se puede emplear como consulta de este dato el sitio web https://www.kimovil.com/es/). Siguiendo la metodología se asignó prioridades para ser tratadas en los siguientes sprint.

3 Prototipo

A continuación, a modo de ejemplo se presenta la interfaz de carga de registro de las experiencias del perito informático. En la Fig.2 El sistema presenta una interfaz con diseño “Stepper UI” que guía a los usuarios a través de un proceso o flujo de trabajo de varios pasos. Se puede observar que la carga se divide en partes: información principal

de la experiencia, información de la herramienta forense empleada para la extracción de datos, información del dispositivo a peritar e información de la causa penal en la cual se solicita la realización de la pericia informática.

Fig. 2. Interfaz de carga de experiencias de pericias informáticas

En el paso 1 “Experiencia”, Fig. 3, se observa que el formulario solicita la descripción de la experiencia que se desea registrar, la fecha en la cual se carga, ofrece la posibilidad de agregar algún archivo de tipo instructivo y solicita categorizar el tipo de experiencia (descripción de procesos, buenas prácticas o soluciones a errores o fallas)

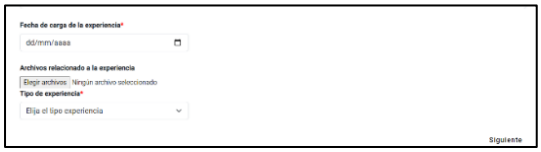

Fig. 3. Carga de datos sobre la experiencia

En el paso 2 “Herramienta”, Fig. 4, se observa que se requiere la carga de la herramienta forense empleada para la extracción de datos y el tipo de extracción (física, sistema de archivo, lógica, copia bit a bit de disco rígido)

Fig. 4. Carga de la herramienta forense empleada

En el paso3 “Dispositivo”, Fig. 5, se puede ver la solicitud de datos del dispositivo, dependiendo del tipo se requiere cargar marca, modelo, numero de serie, entre otros.

Fig. 5. Carga de datos del dispositivo peritado

En el paso 4 “Causa”, Fig. 6, se solicita la carga de el legajo fiscal que identifica a la causa judicial. Además, permite la carga del oficio de solicitud de la pericia informática

requerida en relación a la causa que se investiga. Para finalizar, se presenta la opción final de carga de la experiencia.

Fig. 6. Carga de datos de la causa judicial

4 Conclusiones y trabajos futuros

Haber diseñado el desarrollo de una propuesta que favorece a compartir y generar conocimiento en la oficina de informática forense, promoviendo de esta manera un trabajo colaborativo. Para el desarrollo de la herramienta se empleó la metodología SCRUM que permitió hacer incrementos en las funcionalidades del prototipo en un corto periodo de tiempo y facilitar la participación de los peritos en el desarrollo incremental de la herramienta.

La propuesta de realizar una aplicación para la gestión del conocimiento y experiencia para la oficina de informática forense pretende brindar a los peritos un soporte para el trabajo colaborativo y aprendizaje organizacional, así como también contribuir a mejorar en la gestión del laboratorio. Para trabajos futuros, se espera ofrecer una API que proporcione información sobre el tipo de procesador que tiene un determinado dispositivo móvil.

Referencias

1. Tejo Machado, N., Rodrigues Martinez Basile, F., Cezar Amate, F., & Ramírez López, L. J. Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. Revista Científica General José María Córdova, 19(33), 181-203 (2021).
2. RODRÍGUEZ, G., GIL, J. Y GARCÍA, E. Metodología de la investigación cualitativa. Málaga: Aljibe (1999).
3. Herrera, S. I., Figueroa, L. M., Lara, C., Viaña, G., Méndez, A., Palomo, L., & Pianazzola, L. Informática forense: métodos, herramientas y técnicas. In XXIV Workshop de Investigadores en Ciencias de la Computación. Mendoza, Argentina (2022).
4. Menzinsky, A; López, G; Palacio, J. Scrum Manager. Guía de formación. Versión 2.6 – (2016), https://www.scrummanager.com/files/sm_proyecto.pdf, último acceso 29 de julio de 2024.
5. Software Ideas Modeler, último acceso 29 de julio de 2024.