Inventario seguro en ambientes informáticos con alertas automáticas y registro de historial para activos de T.I. (I.S.A.I.)

Silvia Árias; Fabian Alejandro Gibellini: Analia Lorena Ruhl; Monica Serna; Alejandra Di Gionantonio; Nora Flores; Daniel Arch, Milagros Zea Cárdenas; Germán Parisi; Diego Barrionuevo

Universidad Tecnológica Nacional,
Facultad Regional Córdoba,
Argentina

s_autn@hotmail.com, fgibellini@bbs.frc.utn.edu.ar, analialorenaruhl@gmail.com, sernamonicam@gmail.com, ing.alejandradg@gmail.com, ingnoraflores@gmail.com, daniel.arch@pjn.gov.ar, milyzc@gmail.com, germannparisi@gmail.com, santosdiegob@gmail.com

III Workshop sobre Creatividad e Innovación en Informática (III WCII)
Aplicaciones Creativas e Innovadoras en Informática

Desarrollos informáticos creativos e innovadores

Resumen

En el Laboratorio de Ingeniería en Sistemas de Información de la Universidad Tecnológica Nacional - Facultad Regional Córdoba (U.T.N. - F.R.C.) se desarrolló un sistema de información que permite conocer el estado de sus máquinas en cualquier momento a través de un inventariado automático y monitoreo generando alertas ante cambios el hardware seleccionados (memorias, disco, procesador), de esta forma dar soporte a la toma de decisiones relacionadas a los mismos. El proyecto que se reporta se conoce como “Inventario Seguro en Ambiente Informáticos con Alertas Automáticas y Registro de historial para activos de TI” (I.S.A.I.) - Código: EIUTNCO0002226, y se encuentra homologado por la Secretaría de Ciencia y Técnica de la UTN - FRC, radicado en el Laboratorio de Ingeniería en Sistemas de Información de la U.T.N. - F.R.C., quien es a su vez es el organismo que contribuye a su financiamiento.

Palabras clave: Inventario. Alertas automáticas. Monitoreo. Historial. Multiplataforma.

Proyecto que se reporta

Este proyecto está inserto dentro de la línea de investigación para seguridad y protección de activos de T.I. afectados en los ámbitos académico, gubernamental y empresarial.

La concreción de este proyecto constituyo una posibilidad que favorece ampliamente el crecimiento de la seguridad física en las instituciones públicas del país, donde se sufren permanentemente sustracciones indetectables, por parte de los intrusos.

El mismo tiene como producto el desarrollo de

un software de código abierto, por lo que todo aquel que desee implementar el sistema podrá acceder a la aplicación y su código, como así también adaptarlo para la estructura del ambiente informático sobre el cual lo desee trabajar.

El equipo de trabajo está formado por una Directora, la Ingeniera Silvia Arias, dos Investigadores Tesistas, la Ingeniera Alejandra Di Gionantonio y el Ingeniero Daniel Arch, cuatro Investigadores de Apoyo Ingenieras Analía Lorena Ruhl, Mónica Serna, Nora Flores y el Ingeniero Fabián Gibellini, actualmente Investigador Tesista, un Técnico de Apoyo durante el primer año, Marco Rapallini, quien cambió a partir del segundo año del proyecto por el alumno Diego Barrionuevo. Se incorporó al mismo una becaria alumna Milagros Zea Cárdenas, quien se integró en el primer año del proyecto y continúa hasta la actualidad, y un becario Graduado en el tercer año del Proyecto Ingeniero Germán Parisi.

El Proyecto comenzó el 1 de enero de 2014 por un período de tres años, llegando al final de este periodo se logró una prórroga hasta el 31 de diciembre de 2017 por cambios detectados para alcanzar el objetivo inicial, más específicamente la inclusión del desarrollo del un recolector de inventarios. En esta prórroga se incorpora como integrante al Ingeniero Germán Parisi en el rol de Investigador de Apoyo.

Introducción

LabSis es el Laboratorio de Sistema de la Universidad Tecnológica Nacional, Facultad Regional Córdoba (U.T.N. - F.R.C.), es un ente dependiente del Departamento de Sistema de la mencionada facultad. En este Laboratorio se detectaron las siguientes necesidades para mejorar su servicio a la comunidad y optimizar sus procesos de mantenimiento preventivo y correctivo del hardware:

- Llevar un inventario informatizado, catalogado y actualizado de todas las computadoras, pertenecientes a la plataforma tecnológica, distribuidas en cada una de las aulas.
- Lograr una trazabilidad del estado de los activos inventariados, lo que exige un monitoreo de los mismos, para conocer cierta predictibilidad en su comportamiento a corto plazo, ya que esto repercute sustancialmente en los sistemas informáticos que se ejecutan sobre estos activos; maximizando y potenciando su rendimiento y eficiencia.
- Dar soporte a la toma de decisiones relacionadas al hardware, como por ejemplo el tiempo promedio de vida útil de cierto dispositivo lo que permitirá establecer períodos para la compra de los mismos basados en datos de la realidad.
- Permitir mejorar la distribución de los costos de inversión en esta área.

En base a estas necesidades se determinó que la creación de un sistema que realice un inventario automatizado con monitoreo incluido y genere alertas (vía web o email) cuando se presente cambios en los activos

monitoreados lograría subsanar las necesidades identificadas y planteadas.

A partir de esto, se impulsó el proyecto "Inventario Seguro en Ambiente Informáticos con Alertas Automáticas y Registro de historial para activos de TI" (I.S.A.I.), el cual fue homologado por la Secretaría de Ciencia y Tecnología bajo el código: EIUTNCO0002226.

En el presente documento se exponen las memorias del ya mencionado proyecto.

Metodología

El proceso de control empleado en el proyecto es un proceso empírico, el cual asegura que el conocimiento procede de la experiencia y de tomar decisiones basándose en lo que se conoce, lo empírico.

Existen tres pilares que sostienen cada implementación de un proceso de control empírico: la transparencia, la inspección, y la adaptación.

- Transparencia: Los aspectos significativos del proceso deben ser visibles a los responsables de los resultados.
- Inspección: El equipo debe inspeccionar con frecuencia lo que está produciendo, y cotejar con los objetivos para detectar variaciones indeseables.
- Adaptación: Si se determina que uno, o más aspectos de un proceso se desvían fuera de los límites aceptables, y que el producto resultante será inaceptable, se debe ajustar el proceso o el material que está siendo procesado. El ajuste debe hacerse tan pronto como sea posible, para minimizar aún más la desviación.

Particularmente, se aplicó una adaptación del framework SCRUM según las necesidades del equipo para aumentar la eficiencia de las personas involucradas en el proyecto a través del compromiso con el mismo y el trabajo en equipo. SCRUM tiene sus bases en los principios Ágiles, listados a continuación:

- Individuos e interacciones sobre procesos y herramientas.
- Software funcionando sobre documentación extensiva.
- Colaboración con el cliente sobre negociación contractual.
- Respuesta ante el cambio sobre seguir un plan.

Según Highsmith & Cockburn, lo que es nuevo en los procesos ágiles no son las prácticas que usan, sino que reconozcan a las personas como primeros implicados en el éxito de un proyecto, además de un intenso foco en la efectividad y la manejabilidad. Esto, genera una nueva combinación de valores y principios que definen una visión ágil del mundo.

SCRUM emplea un enfoque iterativo e incremental para optimizar la previsibilidad del riesgo y control.

Utilizar este framework consistió en:

1. Definir Equipos Scrum con funciones y roles bien definidos:

    a. Product Owner (PO): conoce el dominio de negocio.

    b. Scrum Master (SM): su principal responsabilidad es facilitar las

gestiones que se le puedan presentar al equipo. También es parte del equipo.

c. Scrum Team (ST), el resto del equipo.

2. Establecer cuatro reuniones formales para la inspección y la adaptación:

a. Planificación de Sprint

b. Scrum diaria.

c. Revisión del Sprint: Reunión con el PO para la aceptación o no del resultado del sprint.

d. Retrospectiva del Sprint: El objetivo es mejorar el equipo a través de un feedback respecto al sprint que está terminando.

Desarrollo

El sistema desarrollado está formado por dos subsistemas, un subsistema de gestión y monitoreo y un subsistema de recolección de datos de los dispositivos, este último fue desarrollado recientemente, luego de que el software elegido originalmente para esta función, el OCS - Inventory mostró inconsistencias en la recolección de datos.

Para el subsistema de recolección de datos se priorizaron y seleccionaron los componentes a ser inventariados, en base a las necesidades del Laboratorio. Los elementos seleccionados son:

- Elementos de almacenamiento: Disco duro (unidades físicas).

- Elementos de procesamiento: CPU (seleccionando entre sus características velocidad, caché, generación, fabricante).

- Memorias RAM: Memoria (slot que usa, tipo y fabricante).

Además se obtienen datos del equipo, como nombre de la máquina, arquitectura (32 o 64 bits), nombre y versión del sistema operativo.

El subsistema de recolección de datos utiliza una arquitectura cliente - servidor. El servidor fue desarrollado en python 2.7. Para el desarrollo del cliente, se tuvo en cuenta la heterogeneidad de los sistemas operativos utilizados en las aulas del LabSis, por lo que se realizaron clientes tanto para sistemas operativos Windows como para GNU/Linux, específicamente Debian. Según el sistema operativo del equipo, los clientes utilizan distintas tecnologías que permiten la obtención de datos de los componentes seleccionados. Estos datos se recolectan después de cada encendido de una máquina y son enviados al módulo servidor del recolector de inventarios, este servidor siempre tendrá almacenado el último inventario recibido de cada computadora.

El subsistema de monitoreo está desarrollado en PHP 5.5. El mismo obtiene cada cierto intervalo de tiempo, el cual es configurable, el inventario almacenado en el servidor del recolector, verifica si existió un posible cambio con respecto al último inventario registrado en este subsistema para esta máquina. Si esta verificación da positivo recién compara el inventario obtenido desde el servidor recolector con el último inventario registrado en este subsistema para esa máquina en particular. Esta comparación ya implica comparar características de cada componente, validar si hay componentes nuevos

componentes, por ejemplo, si la máquina necesitó más almacenamiento y se le agregó un disco, si un componente fue retirado, por ejemplo, se quitó una memoria RAM. A cada uno de estos casos se lo denomina cambio en la máquina. En el caso que identifique cambios en la máquina o discrepancias, almacena estos cambios en una base de dato logrando un historial de los cambios que existieron en cada máquina monitoreada, historial que es mostrado cuando se ingresa a ver una máquina en particular. Una vez almacenados estos cambios genera alertas que son enviadas a los usuarios vía email, además de mostrarlas en la aplicación web como alerta. Los usuarios finales acceden a través de un navegador web a este subsistema para poder visualizar las máquinas inventariadas, sus componentes actuales y un historial de componentes para cada máquina.

La Fig. 1. muestra la arquitectura general del sistema.

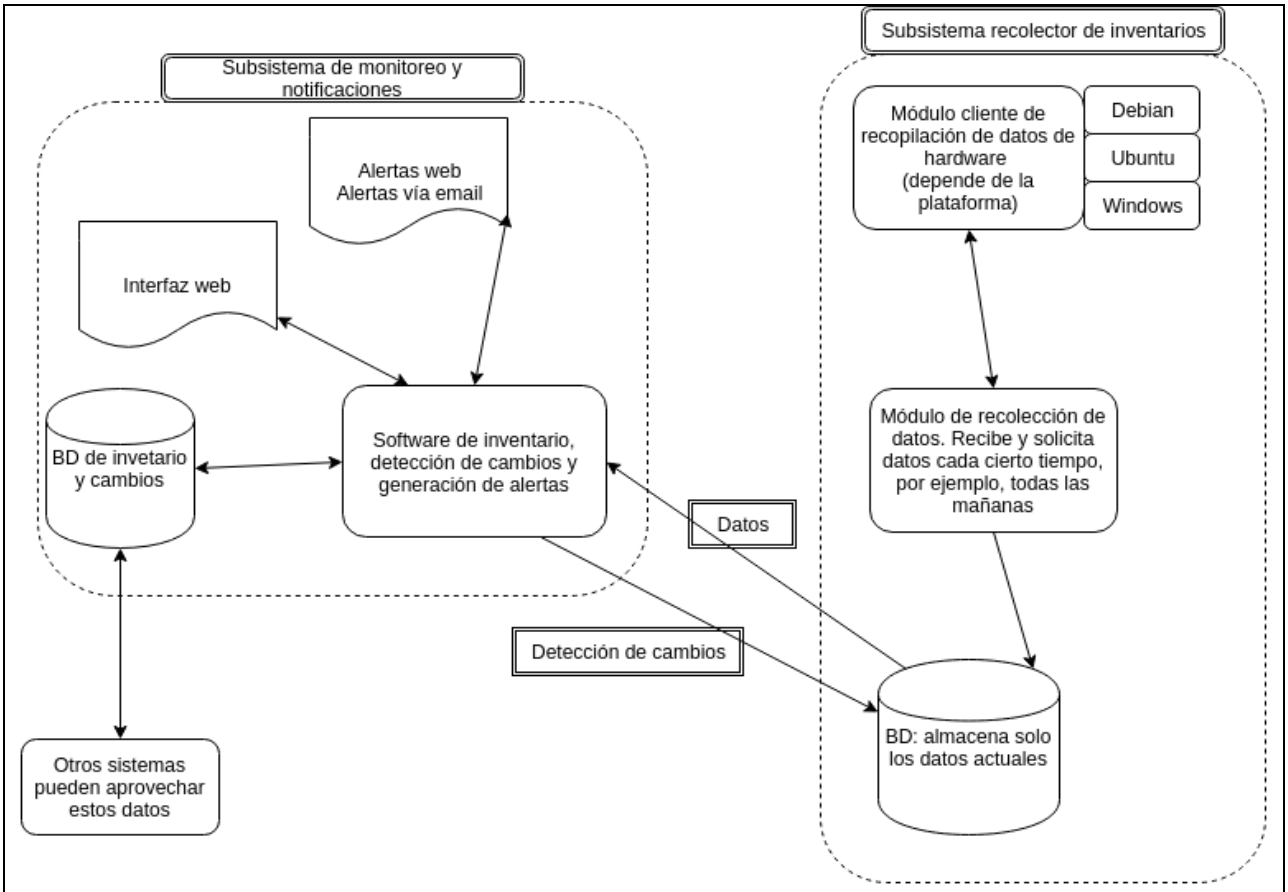

Fig. 1. Arquitectura del sistema

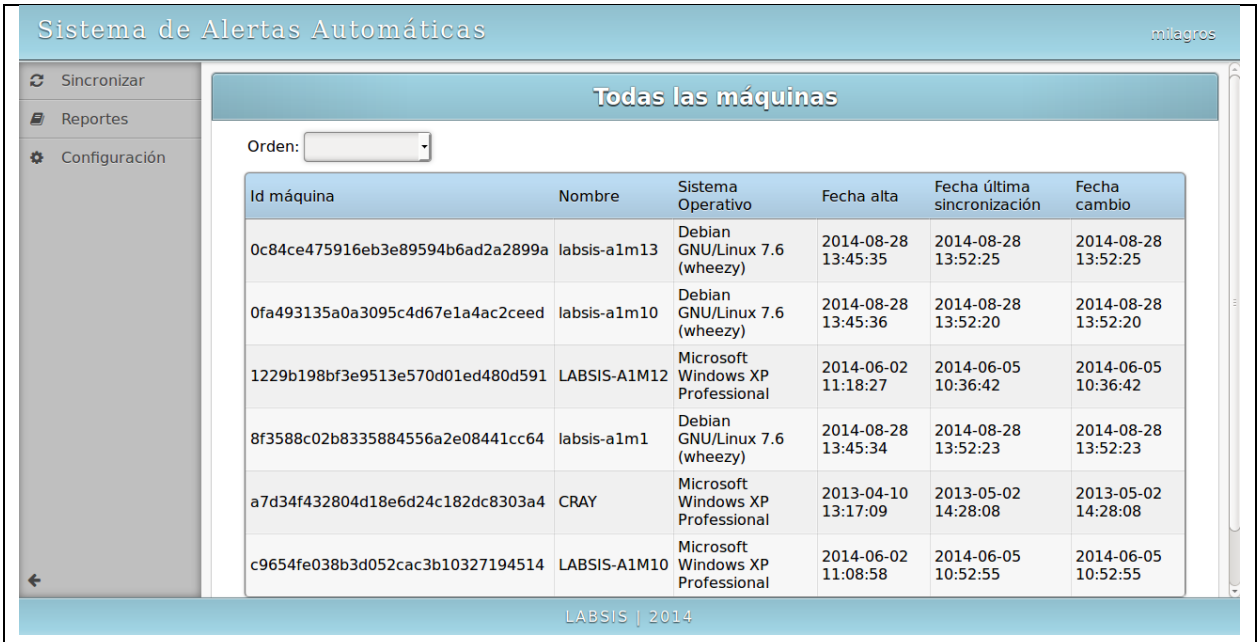

Fig. 2. Interfaz de usuario mostrando máquinas monitoreadas.

La Fig. 2 muestra una de las interfaces deusuario del subsistema de monitorio.

Justificación

El sistema hasta aquí logrado supera ampliamente los objetivos iniciales ya que inicialmente se pensaba reutilizar un componente (el OCS Inventory), lo cual tomó otro rumbo cuando se tomó la decisión de desarrollar un subsistema que reemplace esta funcionalidad. Esto fue posible gracias a que se logró en el subsistema de inventariado y monitoreo cierta abstracción para el procesamiento de los datos, de forma que el impacto en el sistema al cambiar la fuente de inventarios fue mínimo.

Si bien el desarrollo de este sistema fue pensado para cubrir las necesidades del LabSis, puede ser aplicable a cualquier institución pública o privada, con una adecuada adaptación de su código, solo en caso de ser necesaria, gracias a que el software posee una licencia libre y su código está publicado en github.com.

Además los datos que genera el Subsistema de Monitoreo y Notificación conforman una base de conocimiento a ser potencialmente explotada por otros proyectos, que aplicando técnicas y algoritmos de minería de datos pueden producir información valiosa para una institución y sus activos TI. Este último es el caso del proyecto “Generación de Modelo Descriptivo para la prevención de incidentes en equipos informáticos en el contexto del laboratorio de sistemas (Fase II)”, el cual también se lleva a cabo en la UTN - FRC.

Los datos generados por el subsistema recolector también pueden ser usados si lo único que se requiere es un sistema de inventariado.

Referencias

Bunge, M. 1998. La ciencia su Método y su

Filosofía. Editorial Siglo Veinte. Buenos Aires.

Corso, C., Maldonado, C., Gibellini, F., Ciceri, L., Martínez, G., Pereyra, F., Donnet, M. Generación de Modelo Descriptivo para la prevención de incidentes en equipos informáticos en el contexto del laboratorio de sistemas (Fase II). Departamento de Ingeniería en Sistemas Universidad Tecnológica Nacional, Facultad Regional Córdoba.

Framework Scrum. Página oficial: https://www.scrumalliance.org/why-scrum/scrum-guide. Última Visita: 18-08- 2017.

Beck, K., Beedle, M., Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., et al (2001). Principios del software ágil. Acceso a la información: http://agilemanifesto.org/. Última Visita: 27-06-2017.

Highsmith, J., Cockburn, A. (Febrero 2009). Agile Software Development: The Business of Innovation. Computer Science. Department. University of Southern California .Editor: Barry Boehm. Los Ángeles, CA 90089.

Free Software Foundation, Página Oficial, http://www.fsf.org/about/what-is-free-software. Última visita: 27-06-2017.

OCS Inventory. Página oficial. http://www.ocsinventory-ng.org/en/.

Python. Página oficial. https://www.python.org/. Última visita: 13-03-2017.