Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 8, Mes agosto, 2016
ISSN: 2306-2495 | RNPS: 2343
Pág. 39-49
http://publicaciones.uci.cu

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 17/06/2016 | Aceptado: 18/08/2016

Comprobación de políticas de seguridad informática a través del Sistema Gestor de Recursos de Hardware y Software (GRHS)

Checking security policies through of System Manager of Hardware and Software Resources (GRHS)

Dania Carmenate Cantero[1*], Dagoberto Félix Pérez Montesinos[2], Yor Alex Remond Recio[1], Ramón Alexander Anglada Martínez[3]

[1] Centro Telemática, Facultad 2. Universidad de las Ciencias Informáticas, Cuba, Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, Cuba, {dcarmenate, reymond@uci.cu}, CP.: 19370.
[2] Centro de Informatización de Gestión de Entidades, Facultad 3. Universidad de las Ciencias Informáticas, Cuba, Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, Cuba, dagofp@uci.cu, CP.: 19370.
[3] Dirección de Seguridad Informática. Universidad de las Ciencias Informáticas, Cuba, Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, Cuba, raanglada@uci.cu, CP.: 19370.

[*] Autor para correspondencia: dcarmenate@uci.cu

Resumen

Los controles de seguridad informática son un punto esencial para todas aquellas empresas donde se haga uso de las Tecnologías de la Información y la Comunicación. El control automático mediante un software, sin la intervención humana, garantiza ahorro en cuanto a tiempo, recurso y personal. El presente trabajo de investigación tiene como objetivo desarrollar un módulo al sistema GRHS que permita comprobar las políticas de seguridad informática del centro Telemática de manera automatizada. Surge ante la necesidad de mantener el control de las políticas de seguridad informática del centro TLM. A partir de la realización del módulo de seguridad se obtuvo como resultado la comprobación de las políticas de seguridad en la red de computadoras del centro TLM, verificando las políticas relacionadas a: antivirus, BIOS, sistema operativo, protección de datos, contraseñas guardadas en Firefox y Thunderbird, bloqueo automático de la pantalla, carpetas compartidas, dominio de la máquina, cortafuegos, grupos de administradores y cuentas de usuarios en las máquinas.

Palabras clave: *controles; políticas de seguridad informática; red de computadoras.*

Abstract

The security controls are a key point for those companies where the use of information and communications technology is made. Automatic control by software, without human intervention, guarantees savings in terms of time, resources and personnel. This research aims to develop a module to GRHS system enabling the security policies of

telematics automated center. It arises from the need to maintain control of the security policies of TLM center. From the realization of the security module is obtained as result checking security policies on network computers TLM center, verifying the policies related to: antivirus, BIOS, operating system, data protection, and passwords stored in Firefox and Thunderbird, automatic screen lock, shared folders, control of the machine, firewall, administrator groups and user accounts on the machines.

Keywords: *controls; security policies; network computers.*

Introducción

La creciente evolución tecnológica ha hecho que las Tecnologías de la Información y la Comunicación (TIC) faciliten la vida cotidiana y profesional de las personas. Las TIC están presentes en gran parte de las actividades humanas: en el ocio, en la educación, en la comunicación, en la forma de relacionarnos con los demás y en el mundo de los negocios. Variadas empresas y organizaciones son completamente dependientes de estas tecnologías para llevar a cabo sus actividades (EMPRENDEDORES, 2010).

Esta revolución ha sido propiciada por la aparición de la tecnología digital. La tecnología digital, unida al desarrollo de ordenadores cada vez más potentes, han permitido a la humanidad progresar rápidamente en la ciencia y la técnica desplegando las armas más poderosas: el conocimiento y la información (SERVICIOS TIC, 2014).

La información en ocasiones es almacenada, procesada y transmitida en formato digital, encontrándose constantemente expuesta a múltiples amenazas: robos, duplicación, uso indebido, eliminación, entre otros; provocando la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual, generalmente implica graves consecuencias para las empresas y en muchas ocasiones daños irreparables.

Muchos de los riesgos que afectan a la información se deben a la actividad humana, pero en realidad es a la ausencia o mal uso de un control de la seguridad informática donde se encuentran estas almacenadas. El control de la seguridad informática se puede realizar de forma manual o automatizada, siendo la forma automatizada la más recomendable para instituciones y empresas donde se haga uso de las TIC, debido a que es un proceso menos complejo y más efectivo en un entorno de constantes amenazas de seguridad, y teniendo en cuenta la gran cantidad de medidas a implementar.

La gestión automatizada de un control de seguridad informática implica que la operación, monitorización y revisión tanto del software como del hardware de una estación de trabajo se realice de forma automática, mediante sistemas informáticos; sin que se produzca la intervención humana en la realización de estas acciones (MONTESINO, 2013).

En Cuba el control de la seguridad informática en todas las entidades se ha convertido en un papel importante, los avances alcanzados en los últimos años en la informatización de la sociedad con el incremento de tecnologías de la información en todos los sectores y en particular de las redes informáticas y sus servicios asociados, y el impulso orientado por la dirección del país al desarrollo acelerado de programas que multipliquen dichos logros, han requerido la adopción de medidas que garanticen un adecuado nivel de seguridad para su protección y ordenamiento (MENÉNDEZ, 2007).

Una de las instituciones educacionales presentes en el país que impulsa la gestión automatizada de las políticas de seguridad informática es la Universidad de las Ciencias Informáticas (UCI). Como centro de excelencia en la formación de profesionales competentes en la rama de la Informática y en el desarrollo de software, cuenta con una estructura especializada para la actividad productiva, dentro de la cual se encuentra el Centro de Telemática (TLM), encargado del desarrollo de sistemas y servicios informáticos en las ramas de las Telecomunicaciones y la Seguridad Informática.

El centro TLM tiene definidas políticas de seguridad informática con el objetivo de garantizar la protección de la información contenida en sus máquinas y el conocimiento generado por sus especialistas. Dichas políticas deben estar establecidas en cada una de las estaciones de trabajo del centro y son verificadas frecuentemente por el asesor de tecnología o por un grupo de personas a los cuales se asigna esta tarea. La verificación del cumplimiento de estas políticas se realiza de manera manual, computadora por computadora, lo cual implica costo en cuanto al tiempo que se emplea en comprobar el cumplimiento de las políticas en todas las máquinas del centro. Al realizar de manera manual esta comprobación, aumenta la probabilidad de cometer errores y obviar la comprobación de una determinada política que pueda ser objeto luego de una brecha de seguridad.

El centro además cuenta con un sistema informático denominado Gestor de Recursos de Hardware y Software (GRHS), sistema encargado de obtener las propiedades de las piezas y programas instalados en una red de computadoras, con el fin de contabilizar los cambios realizados y tomar acciones automáticas en caso de cambios no autorizados. El sistema a pesar de obtener la información relacionada al software de una estación de trabajo no contribuye a verificar cada una de las políticas de seguridad informática establecidas, pues no brinda información detallada de las mismas.

DESARROLLO

Las metodologías de desarrollo de software son un conjunto de procedimientos, técnicas y ayudas a la documentación para el desarrollo de productos de software (PRESSMAN, 2007). Las metodologías se pueden clasificar en ágiles y tradicionales. Las metodologías tradicionales centradas específicamente en el control del proceso, han demostrado ser efectivas y necesarias en un gran número de proyectos, sobre todo aquellos proyectos de gran tamaño (respecto a tiempo y recursos) (INNOVALPROCESS, 2014). Dentro de las metodologías tradicionales podemos encontrar a OPEN, METRICA y Proceso Unificado Relacional (RUP según sus siglas en inglés).

Para las metodologías ágiles los individuos y las interacciones entre ellos son más importantes que las herramientas y los procesos empleados en el desarrollo del software. Es más relevante crear un software que funcione, que escribir documentación exhaustiva. La colaboración con el cliente debe prevalecer sobre la negociación de contratos. La capacidad de respuesta ante un cambio es más importante que el seguimiento estricto de un plan. Algunos ejemplos de metodologías de este tipo son: SCRUM y Programación Extrema (XP según sus siglas en inglés).

Metodología de desarrollo seleccionada. XP

XP es una metodología ágil centrada en potenciar las relaciones interpersonales como clave para el éxito en el desarrollo de software, promoviendo el trabajo en equipo, preocupándose por el aprendizaje de los desarrolladores, y propiciando un buen clima de trabajo. Se basa en la retroalimentación continua entre el cliente y el equipo de desarrollo, comunicación fluida entre todos los participantes y simplicidad en las soluciones implementadas. XP se define como adecuada para proyectos con requisitos imprecisos y muy cambiantes y donde existe un alto riesgo técnico (INNOVALPROCESS, 2014).

Se selecciona la metodología XP para el desarrollo del presente trabajo debido a que el mismo se trata de un proyecto pequeño y de corto tiempo, donde no se necesita la generación de tantos artefactos y los requisitos pueden cambiar con el tiempo a medida que avanza el trabajo; el equipo de desarrollo está compuesto por dos programadores, en el cual el grado de interacción entre los miembros es alto pues existe una buena comunicación y entendimiento entre ambos; además el cliente pertenece al equipo de desarrollo, lo que posibilita un mayor intercambio de opiniones logrando un producto que satisfaga las necesidades del cliente en el menor tiempo posible y con la calidad requerida.

Herramientas y tecnologías

Los lenguajes y las herramientas empleadas en el desarrollo del módulo fueron definidos por el centro TLM. Constituyendo Python el lenguaje principal del centro. A continuación, se describen las herramientas y lenguajes utilizados.

Lenguaje de programación

Un lenguaje de programación permite crear un grupo de instrucciones que luego se convertirán en un programa. Teniendo en cuenta que el centro TLM define las tecnologías con que se desarrollarán sus productos, para el desarrollo del módulo será utilizado Python 2.7 como lenguaje del lado del servidor y HTML5, CSS3 y JavaScript como lenguajes del lado del cliente. A continuación, una breve descripción de estos lenguajes.

HTML5

El HTML5 es la última versión del Lenguaje de Marcado de Hipertexto (código en que se programan los sitios web), y cambia los paradigmas de desarrollo y diseño web que se tenían al introducir herramientas notables como etiquetas que permiten la publicación de archivos de audio y video; cambios en los llenados de formularios; y una web semántica mucho mejor aprovechada. Se utilizará el lenguaje HTML5 para el diseño de las interfaces del módulo, aprovechando las características del soporte para CSS3 y el manejo mejorado de formularios en el navegador.

CSS3

Las hojas de estilo en cascada (Cascading Style Sheets o CSS) son las que ofrecen la posibilidad de definir las reglas y estilos de representación en diferentes dispositivos, ya sean pantallas de equipos de escritorio, portátiles, móviles, impresoras u otros dispositivos capaces de mostrar contenidos web. Permiten definir de manera eficiente la representación de nuestras páginas y es uno de los conocimientos fundamentales que todo diseñador web debe manejar a la perfección para realizar su trabajo. Su uso permitirá obtener un mayor control de la presentación de la aplicación al poder tener todo el código CSS3 reunido en uno, lo que facilitará su modificación.

JavaScript

JavaScript es un lenguaje de programación que se utiliza principalmente del lado del cliente, permitiendo crear efectos atractivos y dinámicos en las páginas web. Los navegadores interpretan el código JavaScript integrado en las páginas web. Se utilizará este lenguaje para el manejo de los datos del lado del cliente.

Python 2.7

Python es un lenguaje de programación que soporta múltiples paradigmas, incluyendo programación orientada a objetos, programación imperativa y funcional. El código Python define objetos incorporados como listas enlazadas, tuplas, tablas hash y enteros de longitud arbitraria. Es el lenguaje de programación que utiliza el sistema GRHS.

Framework de desarrollo

Un framework de desarrollo es un ambiente de trabajo que contiene librerías de códigos y módulos que pueden ser reutilizados para el rápido desarrollo de aplicaciones. El centro TLM definió para el desarrollo del módulo la utilización de Django 1.4, jQuery 1.9, Twitter Bootstrap 3.0 y Backbone 1.1.

Django 1.4

Django es un framework web de código abierto escrito en Python que permite construir aplicaciones web de forma rápida y con menos código. Usa una modificación de la arquitectura Modelo-Vista-Controlador (MVC), llamada MTV (Model – Template – View), que sería Modelo-Plantilla-Vista. Está liberado bajo la licencia BSD y se centra en automatizar todo lo posible. Es el marco de trabajo que utiliza GRHS.

jQuery 1.9

jQuery es una biblioteca gratuita de Javascript, cuyo objetivo principal es simplificar las tareas de creación de páginas web responsives, acordes a lo estipulado en la web 2.0, la cual funciona en todos los navegadores actuales. Se utilizará el framework de desarrollo jQuery en su versión 1.9 ya que se utiliza para manejar todas las operaciones de las acciones del cliente en la aplicación gadmin del sistema GRHS.

Twitter Bootstrap 3.0

Bootstrap es un framework que simplifica el proceso de creación de diseños web combinando CSS y JavaScript. Es un framework potente con numerosos componentes web que ahorrará mucho esfuerzo y tiempo. En el desarrollo de la aplicación se empleará Boostrap 3.0 para la creación de las interfaces, ofreciendo una mejor integración con librerías como JQuery y proporcionando un diseño sólido basado en estándares como CSS3 y HTML5 que también serán usados en la solución.

Backbone 1.1

Backbone es un pequeño framework que permite construir aplicaciones usando Javascript, basado en el paradigma de diseño de aplicaciones Modelo Vista Controlador. Su objetivo consiste en probar y definir un conjunto de estructuras de datos junto al manejo de la interfaz por medio de vistas que son útiles cuando se construyen aplicaciones Javascript. Es utilizado en el módulo en la construcción de las tablas.

Herramienta CASE: Visual Paradigm 5.0

Visual Paradigm es una herramienta profesional que soporta el ciclo de vida completo del desarrollo de software: análisis y diseño orientados a objetos, construcción, pruebas y despliegue. Permite dibujar todos los tipos de diagramas de clases, generar código desde diagramas y generar documentación. Esta herramienta es utilizada para el

modelado de los diagramas de clases persistentes y el modelo físico de la base de datos, además para la representación de las capas del patrón arquitectónico Modelo – Vista – Plantilla.

Editor de código: Sublime Text 3

Para la implementación del software se empleará el editor de código Sublime Text. Es un editor multiplataforma y su sistema de resaltado de sintaxis soporta un gran número de lenguajes como CSS, HTML, JavaScript y Python. También tiene como características una mejor edición de HTML, incluyendo etiquetas de cierre automático y autocompletamiento de las mismas.

Sistema Gestor de Bases de Datos (SGBD)

Un SGBD es un conjunto de programas que permiten la creación de base de datos y proporciona herramientas para añadir, borrar, modificar y eliminar datos de la base de datos, además de mantener la integridad, confidencialidad y seguridad de los datos.

PostgreSQL 9.3

PostgreSQL es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente.

PostgreSQL tiene las siguientes características principales:

- Arquitectura cliente-servidor con un amplio rango de drivers y clientes.
- Diseño de alta concurrencia donde los lectores y escritores no se bloquean.
- Altamente configurable y extensible para muchos tipos de aplicación.
- Excelente escalabilidad y rendimiento con características de ajustes extensas.
- Optimizador de consultas sofisticado, adecuado para inteligencia de negocios.
- Soporta totalmente el acceso y procedimientos de base de datos en Java, Python, Perl, PHP, entre otros.
- Altamente confiable con características extensivas para durabilidad y alta disponibilidad.
- Soporta el uso de índices, reglas y vistas.
- Incluye herencia entre tablas, aunque no entre objetos, ya que no existen.

Resultados y discusión

La solución propuesta está diseñada para permitir el control de las políticas de seguridad informática en las estaciones de trabajo del centro TLM de manera automatizada. El presente sistema permitirá a los asesores de tecnologías o jefes

de centro llevar un control de todas aquellas máquinas inventariadas que cumplen o no con las políticas de seguridad establecidas por la universidad para los centros de producción, departamentos y laboratorios de docencia.

La solución está compuesta por un plugin para gclient y un módulo para la aplicación gadmin del sistema GRHS. El plugin de seguridad informática por su parte estará integrado por subplugins, los cuales serán los encargados de obtener de las máquinas donde esté instalado gclient, aquellas propiedades vinculadas a las políticas de seguridad, dígase entre estas: nombre del dominio, identificador, instalación de antivirus y firewall, uso de contraseña BIOS, grupos de administradores, carpetas compartidas, sistema operativo, entre otras propiedades; para su posterior verificación por el asesor de seguridad si la máquina cumple con el uso de las políticas. Las propiedades obtenidas de la máquina serán almacenadas en una base de datos local, además contará con un módulo visual en la interfaz de la aplicación gclient, donde se mostrarán los datos recogidos. En la figura 1 se muestra el funcionamiento del plugin.

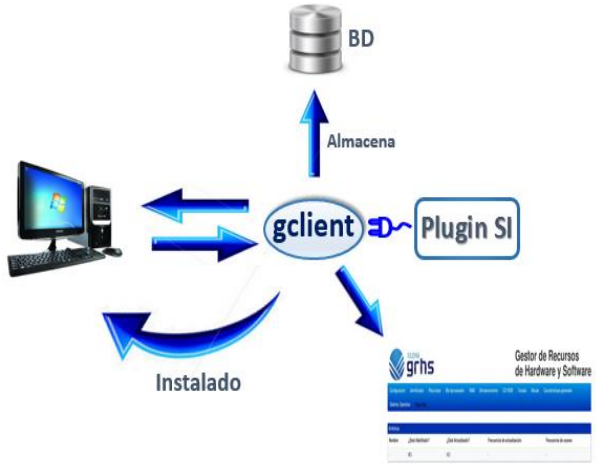

Figura 1: Funcionamiento del *plugin* de seguridad informática.

La aplicación gclient enviará la información al servidor (gserver), donde se encontrarán almacenadas en una base de datos la información enviada por los clientes de la red de computadoras con que cuenta el centro TLM. Dicha información que se encuentra en el servidor será utilizada por el módulo de seguridad informática en la aplicación gadmin, en la cual el asesor de seguridad podrá visualizar todas las estaciones de trabajo del centro con sus propiedades, además podrá realizar búsquedas por diferentes criterios y exportar esta información a formato Excel. En la siguiente figura se muestra la propuesta de solución para el módulo de seguridad informática.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 8, Mes agosto, 2016
ISSN: 2306-2495 | RNPS: 2343
Pág. 39-49
http://publicaciones.uci.cu

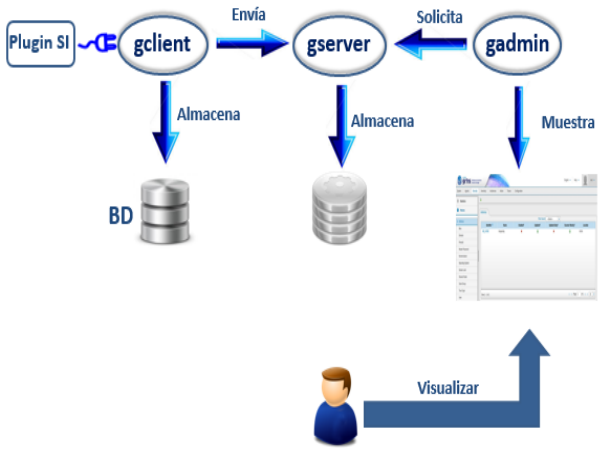

Figura 2: Solución para el módulo de seguridad informática.

Propiedades del producto

Para un correcto funcionamiento del sistema se deben tener en cuenta los siguientes requisitos no funcionales:

Usabilidad

El usuario que interactúe con el módulo de seguridad del sistema GRHS, deberá tener conocimientos básicos de informática y notará que es de fácil manejo y comprensión.

Hardware

Características del hardware del servidor para 100 clientes:

- 4 GB de RAM.
- 20 GB de disco duro.
- 2 núcleos, cada uno de 3.0 GHz.
- Características del hardware del cliente:
- 256 MB de RAM.
- 1 procesador de 2.0 GHz.
- 2 GB de espacio en el disco duro.

Software

- Características del software en el servidor:
- Sistema operativo: Ubuntu Server 12.04, Debian 7, Centos 6.x, Centos 7.
- Servidor web: Nginx 1.2, uWsgi

- Python 2.7.
- Características del software en el cliente:
- Sistema operativo: Windows 7, Windows 8, Debian 6.0, Debian 7.0, Ubuntu 11.04, Ubuntu 12.04, Ubuntu 14.04, Nova 2013.
- Python 2.7.

Interfaz

La solución propuesta poseerá una interfaz que cumpla con las pautas de diseño de Xilema Base – Web.

Conclusiones

Una vez finalizada la investigación se arribaron a las siguientes conclusiones:

1. Después de haber analizado las características de los sistemas que automatizan determinados controles de seguridad informática, se concluyó que el sistema que más facilidades brindaba para dar solución al problema planteado era el GRHS.
2. Se realizaron pruebas de aceptación y unitarias con el objetivo de comprobar la correcta implementación de cada una de las funcionalidades y así evidenciar la calidad del sistema desarrollado.
3. Con el desarrollo del plugin de seguridad para la aplicación gclient y el módulo al GRHS se logró obtener un producto que permita a los asesores controlar y monitorear el establecimiento de cada una de las políticas de seguridad en una red de computadoras.
4. Por todo lo anteriormente expuesto, se concluye que los objetivos propuestos para el presente trabajo se han cumplido satisfactoriamente, poniendo en práctica todas y cada una de las tareas propuestas para el desarrollo del módulo de seguridad informática.

Referencias

EMPRENDEDORES UNL. [En línea] Universidad Nacional del Litoral, 2010. [Citado el: 18 de Noviembre de 2014.] http://www.unl.edu.ar/emprendedores/?p=4776.

SERVICIOS TIC. [En línea] [Citado el: 18 de Noviembre de 2014.] http://www.serviciostic.com/las-tic/definicion-de-tic.html.

MONTESINO PERURENA, Raydel; BALUJA GARCIA, Walter y PORVEN RUBIER, Joelsy. Gestión automatizada e integrada de controles de seguridad informática. EAC [online]. 2013, vol.34, n.1 [citado

2016-08-18], pp. 40-58 . Disponible en: <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000100004&lng=es&nrm=iso>. ISSN 1815-5928.

MENÉNDEZ, Ramiro Váldes. Resolución 127/2007. La Habana, Cuba : s.n., 2007. ISSN 1682-7511.

PRESSMAN, Roger. Ingeniería de software. Un enfoque práctico. Ingeniería de software. s.l. : 7ma, 2007.

INNOVALPROCESS. [En línea] [Citado el: 30 de Noviembre de 2014.] http://www.innovalprocess.com/Temarios/Temario_IngenieriaSoftware.pdf.