Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

Tipode artículo: Artículo original
Temática: Aplicaciones informáticas
Recibido: 17/05/16 | Aceptado: 16/06/16

Componente para monitorizar usuarios

Component for monitoring users

Elibetsy Herrera Chong[1*], Yosbel Fonseca Mendoza [1], Graciela Gutiérrez Rodríguez[1], Lisaidi Coca Conesa[1]
[1] Facultad 6, Universidad de las Ciencias Informáticas, La Habana, Cuba, {elibetsy, yfons, llcoca}@uci.cu
[*] Autor para correspondencia: elibetsy@uci.cu

Resumen

El Centro de Tecnologías de Gestión de Datos en la Universidad de las Ciencias Informáticas cuenta actualmente con diferentes proyectos implementados con el framework de desarrollo Symfony2. Una de las prioridades que se tienen en cuenta durante el desarrollo de estos proyectos es la seguridad, mediante los diferentes componentes: autenticación, autorización y auditoría. La presente investigación se enmarca en la concepción e implementación de un módulo de monitorización para aplicaciones desarrolladas con Symfony2, enfocándose en el componente más débil: la auditoría. El mismo brinda el control de monitorizar, a los administradores, las acciones realizadas por todos los usuarios, en cualquier sistema implementado con este framework. Además, posibilita visualizar las trazas realizadas mediante: gráficas de barras y de series, con el objetivo de contribuir a la toma de decisiones. El módulo se integra al Sistema Integral para la Gestión de Datos (SIGDAT) y puede ser utilizado por otros sistemas.

Palabras clave: auditoría; framework de desarrollo; seguridad

Abstract

The Center for Data Management Technologies at the University of Informatics Sciences currently has several projects implemented with the Symfony2 framework development. One of the priorities to be taken into account during the development of these projects is the assurance of security by the different components: authentication, authorization and audit. This research frames the design and implementation of a monitoring module developed with Symfony2 applications, focusing on the weakest component: the audit. The same control provides monitoring,

administrators, the actions taken by all users on any system implemented with this framework. Also possible to display the traces made by bar graphs and series, with the aim of contributing to the decision-making. The module integrates the Integrated System for Data Management (SIGDAT) and may be used by other applications.

Keywords: *audit; framework development; security*

Introducción

La informática está inmersa en la gestión integral de cada organización, teniendo asegurado un papel protagónico en el futuro de la humanidad, definida como una de las materias más importantes en la actualidad, pues por medio de esta se vive en una sociedad comandada por las nuevas tecnologías. Es muy difícil pensar en cambios, transformaciones e innovaciones y dejar atrás la informática, esto se debe al avance tecnológico en la transmisión de datos y a las nuevas facilidades de comunicación, ambos impensables sin la evolución de las computadoras y dispositivos.

Las Tecnologías de la Información y las Comunicaciones (TIC) se presentan cada vez más como una necesidad en el contexto de la sociedad, donde los rápidos cambios, el aumento de los conocimientos y las demandas de una educación de alto nivel constantemente actualizada, se convierten en una exigencia permanente. En el 2002 el Comandante en Jefe Fidel Castro Ruz crea la Universidad de las Ciencias Informáticas (UCI) para producir aplicaciones y servicios informáticos, a partir de la vinculación estudio-trabajo como modelo de formación y servir de soporte a la industria cubana del software.

La UCI está dirigida a la creación del Ingeniero en Ciencias Informáticas, con conocimientos, habilidades y valores sólidos, sustentados en una concepción científica y dialéctico-materialista del mundo, que estén comprometidos con su Patria para así poder llevar a cabo, importantes tareas dentro y fuera de las fronteras del país. Uno de los centros de la Universidad inmerso en el proceso de desarrollo de software es el Centro de Tecnologías de Gestión de Datos (DATEC). Este centro tiene como objetivo proveer soluciones integrales, productos y servicios relacionados con las tecnologías de gestión de datos, dentro del mismo se encuentra el departamento de Integración de Soluciones donde su misión fundamental es: desarrollar soluciones que permitan la captura, análisis, procesamiento y representación de la información.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

Gran parte de los proyectos desarrollados por este departamento, utilizan como framework de desarrollo Symfony2, garantizando que la seguridad del mismo sea eficiente pues incluye numerosas estrategias y utilidades para hacer frente a diversos ataques. Su arquitectura está compuesta por tres componentes esenciales en términos de seguridad: autenticación, autorización y auditoría. Aunque este último es demasiado genérico, ya que carece de componentes que permitan realizar la monitorización de las acciones realizadas por los usuarios, dejando la solución a esta necesidad en manos de los desarrolladores de cada equipo de trabajo.

Los proyectos desarrollados en este framework garantizan la autenticación y la autorización eliminando cada vez más los posibles riesgos de pérdida o robo de información. Aunque estos dos componentes están destinados a conseguir un sistema de información seguro y confiable, no completa la seguridad, ya que los administradores no poseen los elementos necesarios para monitorizar todas las acciones realizadas por los usuarios. Por lo tanto, no se pueden establecer estadísticas de lo que sucede realmente en el sistema, ni enfatizar en los recursos más explotados por los clientes, contribuyendo así, a la falta de conocimiento de cuáles zonas son las más cotizadas y a su vez más vulnerables para su futuro mantenimiento.

Por tal motivo en las soluciones desarrolladas por el departamento Integración de Soluciones de DATEC crece la necesidad de auditar las acciones de los usuarios de algunos productos e incrementar, así, la calidad y la seguridad de los mismos.

Luego de analizar la situación problemática planteada anteriormente, se identifica como problema de la investigación: ¿Cómo monitorizar las acciones de los usuarios en aplicaciones desarrolladas con Symfony2 para contribuir al fortalecimiento de la seguridad ofrecida por este framework?

En correspondencia con el problema planteado el objetivo general de esta investigación consiste en desarrollar un módulo de monitorización de usuarios para aplicaciones desarrolladas con Symfony2 que permita auditar las acciones de los usuarios.

Materiales y métodos o Metodología computacional

Seguridad en aplicaciones web

La seguridad en los sistemas informáticos se ha convertido en uno de los eslabones fundamentales de cualquier sistema, debido al aumento de los delitos informáticos, por tanto, existen cuatro pautas que son imprescindibles para la implementación de la seguridad de cualquier sistema:

- Prevención: En esta etapa se toman las acciones necesarias para prevenir una posible intrusión.
- Detección: En caso de que se produzca una intrusión en el sistema, es recomendable detectar el momento en que se produce y tomar las medidas necesarias para que no pueda ocasionar más daño.
- Restauración: Una vez que el sistema ha sido atacado será necesario restaurarlo con las copias de seguridad realizadas anteriormente.
- Análisis forense: Este último se asegura de investigar las acciones del atacante para que así no ocurran posibles ataques futuros (Losada Regos 2015).

A criterio de los autores se puede definir la seguridad, como los mecanismos de prevención, detección, restauración y análisis que se llevan a cabo para garantizar la protección de sistemas informáticos. Es importante destacar que la seguridad de la información, en todo sistema, depende en gran medida de la seguridad informática, pues es aquí donde se deben definir claramente los objetivos a partir de los cuales desarrollar las políticas y procedimientos, que definan el marco en el cual situar las medidas a implantar. Recalcar que, la seguridad absoluta no existe, debido a que es un proceso lento y continuo, que exige aprender sobre las propias experiencias.

Elementos de seguridad

El surgimiento de aplicaciones informáticas seguras lleva consigo el proceso de administrar el acceso y el uso de sus recursos. En otras palabras, conocer con precisión la identidad de cada persona en la organización, los servicios a los que puede acceder y delimitar la información que cada individuo puede ver o manipular, son procesos fundamentales en cualquier sistema. Con el objetivo de obtener un producto de software que contribuya a la automatización de los procesos es de vital importancia el uso de la autenticación, autorización y la auditoría.

Autenticación:

Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso (Burrows 2012).

La demanda por soluciones de autenticación ha provenido que cada empresa necesite incrementar el nivel de seguridad lo más alto posible debido al aumento de la piratería informática. A medida que nuevas arquitecturas de autenticación están siendo desarrolladas, la privacidad de los individuos está siendo protegida a un ritmo impresionante.

Autorización:

La autorización es la acción o especie de permiso que consiste en otorgar el consentimiento para realizar las acciones necesarias según los permisos otorgados. Este proceso determina luego de la autenticación, a qué recursos de un sistema tiene acceso una entidad o persona (Fincowsky and Franklin 2007). En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea otorgando o denegando el acceso de lectura, modificación, creación o borrado de los datos.

Auditoría

La auditoría no es más que la inspección interna o externa, de una institución o programa, que se utiliza con el objetivo de comprobar y evaluar el comportamiento del trabajo realizado. Es un término que se incorpora del mundo empresarial y judicial (Wolter and Schaad 2007).

La adecuada planeación de una institución propicia el espacio para sus evaluaciones, que permite dimensionar sus principales características, dando la oportunidad de organización a través de una auditoría contable para garantizar su buen desempeño. La auditoría proporciona a su vez un mejor control en su implementación sistemática, rentabilidad, eficiencia y seguridad en el procesamiento de la información, posibilitando un excelente manejo para la toma de decisiones.

En un mundo tecnológico como el actual, los sistemas de seguridad evolucionan con rapidez y ofrecen más funciones y un mayor nivel de integración. En realidad, los diferentes subsistemas de seguridad funcionan mejor si se comportan como un único sistema capaz de responder a todos los riesgos específicos de una instalación.

Aplicaciones del Centro de Tecnologías de Gestión de Datos

Como centro de desarrollo de software, DATEC, tiene entre sus principales objetivos desarrollar sistemas informáticos que contribuyan al proceso de informatización del país, así como aportar el máximo a la economía. Muchos de los sistemas son implementados utilizando el joven framework de desarrollo Symfony2, entre ellos: Sistema Integral para la Gestión de Datos (SIGDAT) y Generador Dinámico de Reportes (GDR 2.0).

Una de las funcionalidades requeridas por varios clientes ha sido la de poder realizar un estudio sobre las acciones de los usuarios en el sistema; hasta el momento la monitorización no se ha convertido en una solución reutilizable, pues la forma en la que el framework realiza este proceso es difícil de personalizar, lo que ha provocado el desarrollo de soluciones a la medida en cada uno de los casos.

Herramientas y tecnologías

El ciclo de vida del componente estuvo definido por la metodología de desarrollo OpenUP. Pues esta se utiliza generalmente para proyectos pequeños, generando de esta forma sólo lo necesario para el desarrollo del software sin dejar de ser completo y extensible (Diedrich 2011).

El sistema fue desarrollado en el IDE NetBeans 7.2 pues permite la integración de los diferentes módulos que pueden ser activados para permitir la creación de programas en lenguajes como Java, PHP, C++, Python, Ruby, entre otros. (Corporation 2015). Además, es apoyado por una gran comunidad de desarrolladores y ofrece una amplia documentación y recursos de capacitación. También se tuvo en cuenta que esta es una de las herramientas usadas por la Universidad y DATEC para el desarrollo de sus productos.

Para el diseño de la interfaz fue empleado la biblioteca JavaScript de alto rendimiento Ext JS v4.1.1 por las mejoras en velocidad, facilidad de uso y estabilidad respecto a la versión anterior. Además, contiene una nueva librería para crear gráficas sin usar Flash a través de los estándares HTML5, elemento importante para las gráficas de barras y de series que se realizaron durante la implementación (Sencha 2012).

Como framework de desarrollo se utilizó Symfony2 por ser un completo framework diseñado para optimizar el desarrollo de las aplicaciones web (Potencier 2009).

Arquitectura de Symfony:

Symfony es un framework de PHP basado en la arquitectura MVC (Modelo – Vista – Controlador). El Modelo – Vista – Controlador es un patrón o modelo de abstracción de desarrollo de software que separa los datos de una aplicación, la interfaz de usuario y la lógica de negocio en tres componentes distintos. MVC desacopla el concepto de interfaz de usuario y lógica de negocio incrementando la flexibilidad del software.

- Modelo: son los objetos de la aplicación, también conocida como lógica de negocio, o lógica de aplicación.
- Vista: especifica la visualización de los datos, algunas veces conocida como lógica de presentación.
- Controlador: es el coordinador entre estos dos últimos, es decir, define la forma en que la interfaz de usuario reacciona ante la entrada de usuario.

La seguridad en Symfony2 es un proceso de dos etapas, cuyo objetivo es evitar que un usuario acceda a un recurso al cual no debería tener acceso. En el primer paso del proceso, el sistema de seguridad identifica quién es el usuario obligándolo a presentar algún tipo de identificación, a este procedimiento se le denomina autenticación.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

Una vez que el sistema identifica el usuario, el siguiente paso es determinar si debería tener acceso a un determinado recurso. Esta parte del proceso se llama autorización, y significa que el sistema está comprobando para ver si se tienen los suficientes privilegios para realizar una determinada acción.

Durante las dos etapas anteriores se encuentra involucrado el proceso de auditoría, pues Symfony2 guarda mucha información de sus propios eventos en archivos de tipo log, creando un archivo por cada aplicación y cada entorno. Dentro de estos dos archivos se guarda cada evento realizado, donde cada línea incluye la fecha y hora, el tipo de evento, el objeto que ha sido procesado y otros detalles relevantes que dependen de cada tipo de evento u objeto procesado.

Luego de analizar la seguridad en el framework Symfony2 se desarrolló una aplicación que permite:

- Configurar la monitorización: Se seleccionan las entidades a monitorizar en cualquier aplicación desarrollada con Symfony2 mediante la anotación @Traza.
- Registrar datos de las trazas: Se registra en el sistema cada acción realizada por cualquier usuario, siempre y cuando el administrador decida si es monitorizada o no.
- Listar datos de las trazas: El sistema muestra todos los datos de las trazas.
- Filtrar datos de las trazas: El sistema brinda la posibilidad de seleccionar según el tipo de filtro de búsqueda que desee; como por ejemplo: usuarios, fecha (desde-hasta), ip y por las acciones realizadas.
- Graficar datos asociados a las trazas: Se muestran diferentes gráficos con los datos de las trazas. Se selecciona el criterio por el cual se desea graficar, que pueden ser:

1. Tipos de trazas (gráfico de barras).
2. Trazas por ip (gráfico de barras).
3. Acciones por hora (gráfico de series).

- Realizar salvas de las trazas: El sistema debe guardar en un fichero las trazas que se encuentran almacenadas en la base de datos.

Con el propósito de comprender con facilidad la estructura general del sistema y el comportamiento del servicio que estos componentes proporcionan se muestra en la figura 1 el diagrama de componentes.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

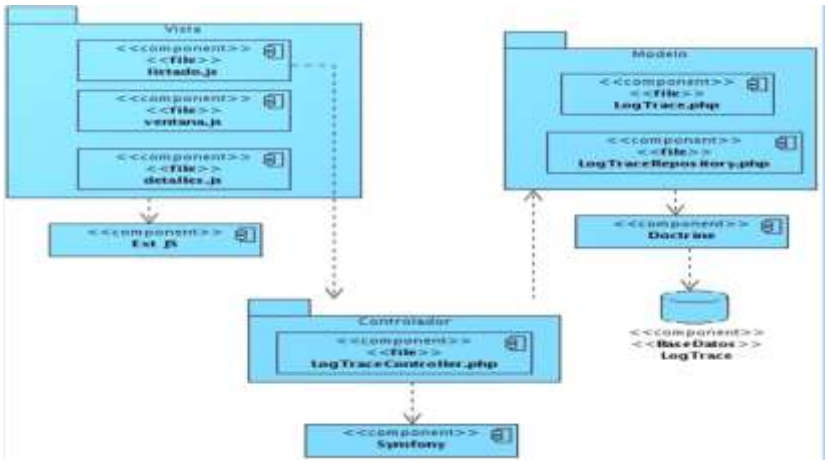

Figura 1. Diagrama de componentes.

Este diagrama está compuesto por tres paquetes de implementación básica:

1. El Paquete de Clases Vista, que agrupa los componentes que permiten la interacción directa con el usuario final del módulo, mostrando y recogiendo información.
2. El Paquete de Clases Controlado, que contendrá la clase que manipula los eventos del usuario y realiza peticiones al subsistema modelo para mostrarlas en las vistas.
3. El Paquete de Clases Modelo, que agrupa las clases que interactúan con la base de datos y velan por el cumplimiento de las reglas de negocio.

Para entender la comunicación entre el cliente y los objetos de la aplicación se define en la figura 2 el diagrama de secuencias. Un diagrama de interacción (secuencia o colaboración), representa la forma en que un cliente (actor) y otros objetos (clases) se comunican entre sí, en respuesta a un determinado suceso. En la aplicación se encuentra definido al Administrador como único actor, el cual se beneficiará de las funcionalidades.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

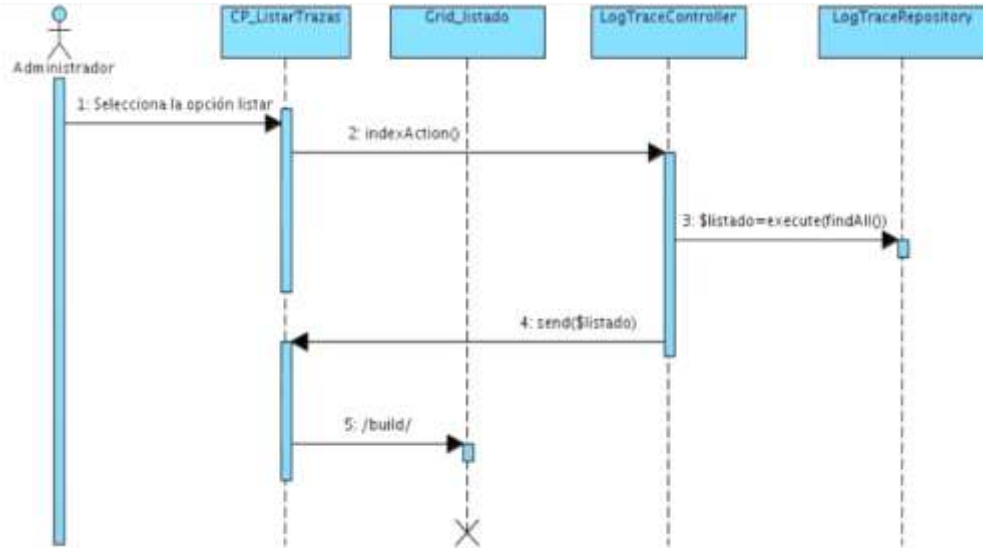

Figura 2. Diagrama de secuencias.

En este el administrador selecciona la opción Listar Trazas en la página cliente "Listar Trazas", mediante una petición AJAX al controlador "LogTraceController", este interactúa con el "LogTraceRepository" ejecutando la acción findAll(). El controlador devuelve una respuesta en formato JSON con todos los datos suministrados por el repositorio. La CP_ListarTrazas recoge estos datos y construye el "Grid_ListarTrazas"a partir de la respuesta del controlador.

Resultados y discusión

Una vez desplegado el módulo los usuarios podrán conectarse desde estaciones de trabajo por medio de un navegador web haciendo uso del protocolo de comunicación HTTP o HTTPS, pues el módulo es capaz de adecuarse al entorno donde está desplegado el proyecto original. En el servidor se encuentra la aplicación desarrollada en PHP que atenderá las peticiones realizadas por cada uno de los usuarios y que a su vez utiliza una base de datos para satisfacer esas demandas. El servidor de base de datos puede estar desplegado en la misma PC que el servidor web o potencialmente en otra PC. La comunicación entre la aplicación desarrollada y el servidor de base datos se realiza mediante el protocolo TCP/IP. (Figura 3)

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

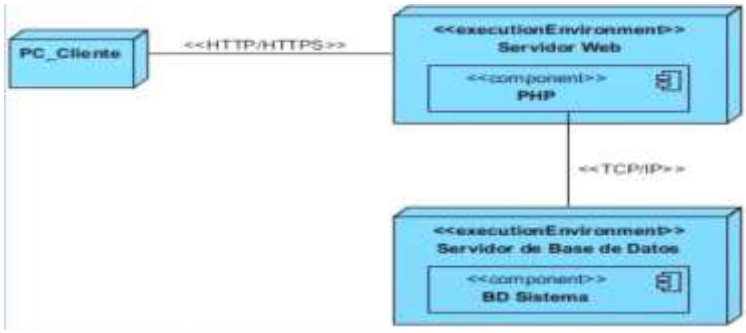

Figura 3. Diagrama de despliegue.

La figura 4 muestra una interfaz gráfica con un listado de trazas. El administrador puede realizar un filtro para la búsqueda, según los siguientes criterios: usuarios, fecha (desde – hasta), ip y acción realizada. Además, si desea examinar los datos, selecciona la opción "Detalles", la cual mostrará los últimos datos que estaban en la base de datos y los datos vigentes ingresados en el caso particularmente del "Update".

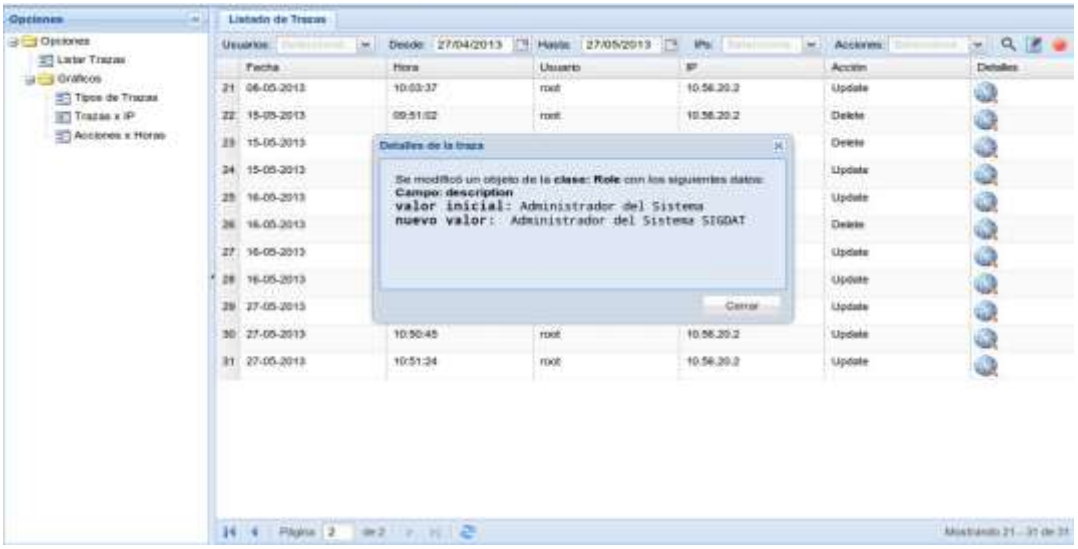

Figura 4. Interfaz: Listado de las trazas.

La gráfica contenida en la figura 5 muestra el resultado de graficar según tipo de trazas, en la que se puede especifiar un usuario específico, o mostrar todos los usuarios.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 6, Mes junio, 2016
ISSN: 2306-2495| RNPS: 2343
Pág. 17-29
http://publicaciones.uci.cu

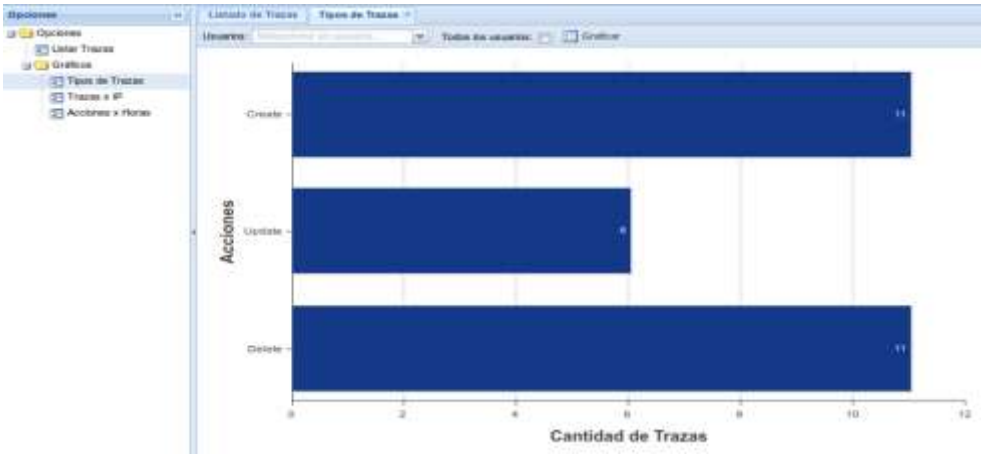

Figura 5. Interfaz: Tipos de Trazas

Con la implementación del módulo de monitorización para las aplicaciones desarrolladas con Symfony2 los administradores contarán con los elementos necesarios para monitorizar todas las acciones realizadas por los usuarios de la aplicación a la que se integre el módulo. Se podrán establecer estadísticas de lo que sucede en el sistema, enfatizando en los recursos más explotados por los clientes, contribuyendo así, a conocer cuáles zonas son las más cotizadas y a su vez más vulnerables para su futuro mantenimiento. El módulo contribuye como aporte práctico y de utilidad en aplicaciones como SIGDAT del Centro DATEC y a otras a las cuales se integre el mismo.

Conclusiones

En este trabajo se evidencia cómo el monitoreo de trazas es empleado para implementar la auditoría como mecanismo de seguridad. Este es un significativo resultado dado la importancia del control de acciones de los consumidores de los sistemas informáticos. Además, la utilización del componente de monitorización es muy ventajosa para aquellas entidades que requieran de un mayor control en sus empresas, al disponer de una herramienta que le muestre estadísticas e información contundente acerca de los logs de operaciones de sus usuarios; permitiéndole a la entidad detectar fortalezas, amenazas y mejorar en sus procesos.

Referencias

BURROWS, M. A. A logic of authentication. In Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. The Royal Society, 2012, 426(No. 1871), 233-271.

CÁCERES TELLO, J. DIAGRAMAS DE SECUENCIA. In U.D. ALCALÁ. http://www2.uah.es/jcaceres/capsulas/DiagramaSecuencia.pdf: Universidad de Alcalá, 2015, vol. 2013.

CORPORATION, O. Netbeans.org.In NETBEANS.ORG. Netbeans.org.https://netbeans.org/: https://netbeans.org/, 2015, vol. 2016.

DIEDRICH, L. G. Integração da metodologia ágil OpenUp nos processos de engenharia de software. Ministério da Educação Universidade Tecnológica Federal do ParanáDiretoria de Pesquisa e Pós-Graduação Especialização em Engenharia de Software, 2011.

FINCOWSKY, F. AND E. B. B. FRANKLIN Auditoría Administrativa: gestión estratégica del cambio. edited by A. UNIVERSIDAD CATÓLICA DE CÓRDOBA. Edition ed. Naucalpan de Juárez: Pearson Educación.: Pearson Educación, 2007. 839 p. ISBN 9702607841.

FREDERICK, S. AND C. N. RAMSAY Learning Ext JS: Build Dynamic, Desktop-style User Interfaces for Your Data-driven Web Applications. Edition ed. http://s3.amazonaws.com/academia.edu.documents/30355628/packtpub.learning.ext.js.nov.2008.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1464461902&Signature=uFCuP92IIFQZJWiZuEQ5VRISADE%3D&response-content-disposition=inline%3B%20filename%3DLearning_Ext_JS.pdf: Packt Publishing Ltd, 2008. ISBN 1847195156.

LOSADA REGOS, D. Seguridad en aplicaciones Web. Universitat Oberta de Catalunya, 2015.

MOHEDANO, J., J. M. SAIZ AND P. S. ROMÁN Iniciación a JavaScript. Edition ed.: Ministerio de Educación, 2012. ISBN 8436954335.

POTENCIER, F. The symfony Reference Guide. In.: Sensiolabs, 2009.

PRESSMAN, R. S. AND J. M. TROYA Ingeniería del software. Edition ed.: McGraw Hill, 1988. ISBN 007050783X.

QUINTERO, J. B., R. A. DE PÁEZ, J. C. MARÍN AND A. B. LÓPEZ Un estudio comparativo de herramientas para el modelado con UML. Revista Universidad EAFIT, 2012, 41(137), 60-76.

RĂDESCU, R., A. DAVIDESCU AND V. PUPEZESCU.Security And Confidentiality In The Easy Learning On-line Platform". In Proceedings of the 5th International Conference on Virtual Learning (ICVL-2010). 2010, p. 449-452.

REDDY, B. R. Simplifying addition of web servers when authentication server requires registration. In.: Google Patents, 2013.

SENCHA. Ext JS 4.1.1 Sencha Docs. In S. DOCS. Sencha Docs. http://docs.sencha.com/extjs/4.1.1/: Sencha, 2012, vol. 2012.

TSAUR, W.-J., J.-H. LI AND W.-B. LEE An efficient and secure multi-server authentication scheme with key agreement. Journal of Systems and Software, 2012, 85(4), 876-882.

WOLTER, C. AND A. SCHAAD. Modeling of task-based authorization constraints in BPMN. In Business process management. Springer, 2007, p. 64-79.