Revista Cubana de Ciencias Informáticas
Vol. 10, No. 2, abril-junio, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 42- 56

Tipo de artículo: Artículo original
Temática: Seguridad Informática
Recibido: 11/12/2015| Aceptado: 23/03/2016

# Procedimiento para la seguridad del proceso de despliegue de aplicaciones web

# *Procedure for the security of the deployment process of web applications*

**Adrian Hernández Yeja [1*], Joelsy Porven Rubier [1]**

[1] Universidad de las Ciencias Informáticas. Carretera de San Antonio de los Baños, Km 2 ½. La Habana. {ayeja, jporven}@uci.cu.

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

**Resumen**

El auge que ha adquirido la utilización de las aplicaciones web ha propiciado el surgimiento de riesgos de seguridad que atentan contra la disponibilidad, integridad y confidencialidad de la información. Por ello, se requiere la adopción de mecanismos para el enfrentamiento a los problemas de seguridad que se presentan diariamente en las aplicaciones web. Una de las alternativas que se recomiendan incluye la adopción de la seguridad a lo largo de todo el ciclo de desarrollo de software. En este sentido, la etapa de despliegue no está exenta de dificultades y desafíos que afrontar desde el punto de vista de seguridad, por lo que una configuración cuidadosa y la personalización del entorno pueden mejorar en gran medida el estado de seguridad de la aplicación. En este trabajo se realiza un estudio sobre la utilización de buenas prácticas establecidas y estándares en torno a la seguridad del despliegue de aplicaciones web, con un enfoque vinculado a la automatización y prácticas tradicionales del desarrollo de software. El procedimiento se ha aplicado en el Nodo Central de la Universidad de las Ciencias Informáticas y su utilización ha permitido la reducción del tiempo de realización de las operaciones y la cantidad de errores humanos cometidos desde la perspectiva de la seguridad informática. Los resultados obtenidos permiten establecer una referencia para la posible aplicación del procedimiento en otros entornos. Las herramientas utilizadas pueden ajustarse a las necesidades y políticas de la organización para su aplicación.

**Palabras clave:** despliegue, seguridad, aplicaciones web

***Abstract***

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 2, abril-junio, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 42- 56

*The momentum built using web applications has led to the emergence of security risks that threaten the availability, integrity and confidentiality of information. Therefore, the adoption of mechanisms for confronting the security issues that arise daily in web applications is required. One of the alternatives that are recommended includes the adoption of security throughout the software development lifecycle. In this sense, the stage of deployment does not have difficulties without difficulties and challenges faced from the point of view of safety, so careful configuration and customization environment which can greatly improve the security status of the application. This paper presents a study on the use of some of best practices and standards established regarding the security of the deployment of web applications with automation linked to traditional practices and software development approach where it is performed. The proposal has been implemented in the Central Node of the University of Information Science and its use has allowed us reducing the time of completion of the operations and the amount of human error from the perspective of computer security. The results allow to establish a reference to the possible application of the proposal in other environments. The tools used can be adjusted to the needs and policies of the organization for implementation.*

***Keywords:*** *deployment, security, web applications*

## Introducción

La evolución constante de la tecnología ha permitido mejorar la forma en que el hombre interactúa con la naturaleza. Una de las ciencias que más ha avanzado en los últimos años es la Informática, la cual ha influido en el desarrollo de la red de redes, Internet, para lograr un mundo interconectado, donde la comunicación y acceso a los recursos es mucho más fácil. Las aplicaciones web han facilitado dicho proceso, mediante su facilidad de uso y presencia en redes sociales, buscadores, sitios de comercio, información interactiva, las cuales han sido ampliamente adoptadas dentro de las organizaciones para soportar las funciones claves del negocio (Stuttard, 2008).

Sin embargo, el incremento del uso de las aplicaciones web ha propiciado el surgimiento de riesgos de seguridad que atentan contra la disponibilidad, integridad y confidencialidad de la información, normalmente con un objetivo lucrativo; esto se debe a que los sistemas informáticos modernos son susceptibles a problemas de seguridad, por la conectividad, extensibilidad y complejidad de los mismos.

Un ejemplo de la situación preocupante que representan las amenazas lo demuestra el reporte del impacto de las aplicaciones web en las brechas de información (Verizon, 2015), de la compañía Verizon en el año 2015, con la representación de 61 países, al menos 80000 incidentes de seguridad y el aporte de 70 organizaciones en todo el mundo. Según el informe, el 4,1% de los incidentes de seguridad fueron causados por ataques a aplicaciones web y el

9,4% de las brechas de información también a este tipo de aplicaciones; la ganancia financiera fue la causa fundamental de los ataques y el crimen organizado el actor principal de los incidentes.

Por ello, que se hace necesaria la adopción de mecanismos para el enfrentamiento a los problemas de seguridad en aplicaciones web, las cuales se presentan diariamente en el mundo tecnológico. Desde esta perspectiva, la etapa de despliegue del software constituye un momento crucial, debido, en esencia, a que se ejecutan actividades que permiten la disponibilidad de la aplicación para su utilización por los usuarios. Estas actividades incluyen la entrega, montaje y gestión en un sitio de los recursos necesarios para utilizar una versión de un sistema de software (Carzaniga, 1997).

Según el especialista de seguridad Gary McGraw (McGraw, 2006), la etapa de despliegue no está exenta de dificultades y desafíos que afrontar desde el punto de vista de seguridad, por lo que una configuración cuidadosa y la personalización del entorno pueden mejorar en gran medida el estado de seguridad de la aplicación. El diseño inteligente de un entorno de despliegue adaptado a una aplicación requiere seguir un proceso que se inicie en el nivel de los componentes de red, pasa a través del sistema operativo, y termina con configuraciones propias de seguridad y configuración del software (Paul, 2009).

En este trabajo se presenta un enfoque vinculado a la automatización, la utilización de estándares y buenas prácticas internacionales, así como tendencias novedosas en torno a la seguridad en el despliegue de aplicaciones web.

## Materiales y métodos

El despliegue de software se refiere a todas las actividades que permiten a un sistema informático que esté disponible para los usuarios. Este proceso, por razones de seguridad, debe ser estrictamente controlado por la organización con la aplicación de procedimientos y controles que permitan el cumplimiento de las políticas establecidas. En las siguientes secciones se establecen elementos importantes en torno al despliegue seguro de aplicaciones web.

### Actividades de seguridad recomendadas para el despliegue de aplicaciones web

La seguridad de la información se encarga de proteger la confidencialidad, integridad y disponibilidad de los activos de información, ya sea en el almacenamiento, procesamiento o transmisión. Se alcanza con la aplicación de políticas, educación, entrenamiento, conciencia y tecnología (Whithman, 2011). Otra definición establece la protección de los sistemas frente al acceso, uso, divulgación, alteración, modificación o destrucción de la información (Jason, 2014). En este sentido, para ser más efectivo, la seguridad de la información debe integrarse en todo el Ciclo de Desarrollo del

Software (SDLC por sus siglas en inglés) (Kissel, 2008), por lo que el software debe ser diseñado, desarrollado y desplegado con una mentalidad segura y la aplicación de estrategias que minimicen la probabilidad de la exposición e impacto a las amenazas.

En el caso de la etapa de despliegue de software, la misma constituye el momento en que el código se ha completado y la aplicación está lista para pruebas rigurosas y de validación que confirmen que no hay vulnerabilidades conocidas de seguridad; además, se configura de forma tal que no sea objeto de ningún comprometimiento de la información. Se deben planificar cuidadosamente las actividades necesarias desde la perspectiva de seguridad en torno al despliegue del software.

En la constante evolución de la seguridad, se han establecido marcos de trabajo que definen modelos de madurez que describen comportamientos, prácticas y procesos que deben ser llevados a cabo por las organizaciones para obtener resultados sustentables en términos de seguridad. Se destacan, desde esta perspectiva *Building Security In Maturity Model* (BSSIM) (McGraw, 2013) y OWASP's *Software Assurance Maturity Model* (OpenSAMM) (Chandra, 2008). Los mismos se definen como marcos de trabajo de referencia en la seguridad informática disponibles libremente.

## Controles de seguridad necesarios durante el despliegue de aplicaciones web

Los controles de seguridad son salvaguardias/contramedidas prescritas para los sistemas de información u organizaciones que están diseñados para: (i) proteger la confidencialidad, integridad y disponibilidad de la información que se procesa, se almacena y se transmite por esas organizaciones/sistemas; y (ii) satisfacer un conjunto de requerimientos de seguridad definidos (NIST, 2015).

Se requiere para la planeación de controles de seguridad apropiados en el despliegue de aplicaciones web, el entendimiento de las amenazas asociadas al entorno en que será desplegado el servidor. Una selección cuidadosa, ajustada a las necesidades de la organización y regida por estándares y regulaciones internacionales, permitirá de una forma efectiva mitigar las amenazas a las que están expuestas este tipo de aplicaciones que son frecuentemente objetivo de ataque por personas malintencionadas que buscan hacer un uso indebido de los datos y servicios que se ofrecen.

En este sentido, se han definido numerosas normativas y buenas prácticas en torno a la utilización de controles de seguridad, las cuales deben tenerse presente para soportar acciones de evaluación y mejora del estado de seguridad de las organizaciones. Algunas de las más destacadas son:

- Controles de seguridad recomendados para Sistemas de Información Federal: propone una línea base mínima de gestión, operación y controles técnicos de los sistemas de información. También se conoce como la publicación especial 800-53, la cual forma parte de la serie 800 de NIST.
- Los controles de seguridad críticos para una defensa cibernética efectiva (*Critical Security Controls for Effective Cyber Defense*): constituyen una línea base de las medidas y controles de seguridad de la información de alta prioridad que se puede aplicar en toda la organización con el fin de mejorar la defensa cibernética. Se proponen 20 controles que se consideran críticos para la seguridad de la información (Council on Cyber Security, 2015).
- ISO/IEC 27002: el mismo es una referencia para la selección de controles de seguridad enfocados a riesgos en la confidencialidad, integridad y disponibilidad de la información; no representa una especificación formal como la ISO/IEC 27001. En su edición del año 2013 (27002:2013) se especifican 14 dominios, 35 objetivos de control y 114 controles de seguridad (ISO/IEC, 2013).

A continuación, se presenta una selección de controles de seguridad que deben ser considerados durante el despliegue de aplicaciones web, basados en las normativas descritas con anterioridad y que forman parte del procedimiento que se presentará:

- Inventario de software autorizado y no autorizado: se debe comprobar el software autorizado y no autorizado en el servidor en busca de posibles brechas de seguridad que puedan atentar contra el mismo.
- Aplicación de configuraciones seguras de software en los servidores: las aplicaciones web y el sistema operativo durante el despliegue tienen configuraciones por defecto que no son recomendadas desde el punto de vista de seguridad. Se requiere la construcción de plantillas con configuraciones seguras durante cada instalación y la utilización de buenas prácticas en torno a la seguridad de los sistemas instalados.
- Limitación y control de puertos de red, protocolos y servicios: los servidores deben ser instalados solo con los servicios necesarios, debe asegurarse y validarse que los mismos cumplen con los requisitos de la organización.
- Uso controlado de privilegios administrativos: los privilegios administrativos se deben minimizar y solo ser asignados cuando se requiera. Una configuración incorrecta de los mismos representa un método primario de enfoque para los atacantes.
- Administración de la configuración: las aplicaciones web proveen muchos servicios y tienen numerosas configuraciones. Si en el entorno de despliegue no se gestionan correctamente las configuraciones, puede provocar problemas de seguridad como permisos incorrectos en directorios, servicios habilitados innecesariamente, configuraciones incorrectas, etc. Se requiere un mecanismo de administración de las configuraciones.

- Copias de seguridad de la información: se debe establecer una política de respaldo de los datos, con la definición del nivel de retención e información a resguardar.
- Sincronización de hora: el reloj de los servidores debe estar sincronizado a un servidor de tiempo correctamente configurado, con el objetivo de asegurar actividades como la exactitud en las auditorías de las trazas, que puede ser requerido en investigaciones o evidencia legal.
- Restricciones en la instalación de software: se debe definir y hacer cumplir políticas de los tipos de software que deben ser instalados en los servidores. La instalación no controlada de software puede introducir vulnerabilidades que pueden provocar fugas de información, pérdida de integridad u otros incidentes de seguridad.
- Protección contra la denegación de servicio: Se deben establecer límites y proveer a los sistemas de redundancia para protegerlos contra posibles ataques de denegación de servicio.
- Defensa contra programas malignos: se requiere la prevención, detección y recuperación ante la acción de programas malignos.
- Seguridad en las aplicaciones: la seguridad del software debe estar presente a lo largo del Ciclo de Desarrollo de Software; en el caso del despliegue se debe disponer de cortafuegos de aplicaciones para la inspección del tráfico y las pruebas continuas de seguridad a la aplicación.
- Valoración continua de vulnerabilidades y remediación: se debe establecer un programa para la identificación, clasificación, remediación y mitigación de vulnerabilidades. Se debe seguir un plan de escaneo que permita proactivamente descubrir fallas de seguridad. De esta forma, se minimizan las oportunidades de los atacantes del comprometimiento de los sistemas.
- Monitorización continua de los controles de seguridad implementados: la organización debe desarrollar e implementar una estrategia de monitorización continua para determinar si los controles planeados, requeridos e implementados son efectivos en el tiempo.

## Automatización del proceso de despliegue seguro de aplicaciones web

El despliegue de software suele ser un proceso intensivo, en algunos casos, repetitivo y con elevadas probabilidades de cometer errores, debido a que en la mayoría de los casos se realiza de forma manual por los operadores de sistemas y el número acciones a desarrollar es elevado. Si no se ejecutan todos los elementos involucrados en el despliegue de forma precisa, la aplicación no funcionará de forma satisfactoria.

La automatización, en su definición, establece la operación controlada automáticamente de un aparato, proceso o sistema mediante dispositivos mecánicos o electrónicos que toman el lugar del trabajo humano (Merriam-Webster,

2015). Desde el punto de vista del despliegue de aplicaciones, algunas razones por las que la automatización es importante incluyen (Humble, 2010):

- Se evitan errores producto de las operaciones sobre los sistemas. Estos errores podrían ser difíciles de localizar.
- Se produce un ahorro de tiempo consumido.
- Un proceso de despliegue manual debe estar documentado. El mantenimiento de la documentación es complejo y consume tiempo cuando se involucran varias personas. Un proceso automatizado funciona como la documentación, siempre deberá estar al día o de lo contrario no funcionará el despliegue.
- Un despliegue manual depende en la mayoría de los casos de personal experto para ejecutar las acciones. En la automatización se encuentra todo el proceso de forma explícita.
- Se libera de carga excesiva de trabajo a los operadores de los sistemas.
- La única forma de probar un proceso manual es ejecutándolo de esta misma forma, lo cual representa un proceso costoso. La automatización permite que el proceso se torne sencillo.
- Un proceso automatizado se puede auditar completamente.

## Gestión de la configuración

La gestión de la configuración es un pilar fundamental de la automatización. Ha sido tradicionalmente usado como una de las mejores prácticas de gestión de las Tecnologías de la Información. El mismo proporciona herramientas que permiten gestionar de forma centralizada los paquetes, archivos de configuración, estado del proceso, reglas de los cortafuegos y otros ajustes que equipan a los servidores para realizar el trabajo asignado. Sin un sistema de gestión de la configuración de forma automatizada, se realizarían todas estas tareas de forma manual o con scripts programados manualmente, lo cual consume tiempo y puede provocar errores humanos (Puppet Labs, 2015).

Debido a que la configuración de un sistema de información y sus componentes tiene un impacto directo en la postura de seguridad del sistema, se requiere de un enfoque disciplinado para proporcionar la seguridad adecuada. Los cambios en la configuración de un sistema de información a menudo son necesarios para estar al día con el cambio de funciones de negocio y servicios, así como las necesidades de seguridad de la información. Estos cambios pueden afectar negativamente la postura de seguridad que se concibió desde la instalación del sistema.

Por tanto, para que la gestión de la configuración se considere efectiva, se requiere el establecimiento y mantenimiento de la seguridad de la información y los sistemas. El proceso de gestión de la configuración centrado en la seguridad es fundamental para mantener un estado seguro bajo las operaciones normales, las operaciones de recuperación de contingencia y la reconstitución de las operaciones normales (Johnson, 2011).

## Infraestructura como código

Una de las mejores prácticas de desarrollo de software lo constituye la Integración Continua, la cual permite la reducción de riesgos y tareas repetitivas, ejecución de pruebas, generación de software listo para desplegar e incremento de la calidad; todas las tareas se ejecutan de forma automática. Esta técnica permite el monitoreo de sistemas de control de versiones, debido a que cuando un cambio se detecta, se notifica de inmediato a los involucrados de las posibles fallas detectadas (Fowler, 2006).

En los últimos años, ha existido la tendencia de aplicar prácticas del desarrollo de software como la Integración Continua a elementos de infraestructura, el cual comprende, en este contexto, el soporte a servicios o elementos como el sistema operativo, servidores, etc. Algunos conceptos como la virtualización, la nube y los contenedores, han convertido la Infraestructura en software y dato, lo que ha permitido tratarla como un sistema de software (Hüttermann, 2012).

Es por ello que, al enfoque del uso de las tecnologías de la era de la nube para construir y gestionar la infraestructura de forma dinámica, se le ha denominado Infraestructura como Código. La misma trata las herramientas y servicios que administran la infraestructura como software y adapta prácticas tradicionales de la ingeniería de software para su uso (Morris, 2015).

La posibilidad de combinar la Gestión de la Configuración con los principios y prácticas de la Infraestructura como Código en el despliegue de aplicaciones web, permitirá garantizar la calidad y ejecución efectiva del despliegue, además de garantizar técnicamente el cumplimiento de las actividades y controles de seguridad necesarios en esta etapa.

## La automatización de la seguridad del despliegue de aplicaciones web

Los aspectos de seguridad que deben tenerse en cuenta durante el despliegue de aplicaciones web, obtienen beneficios destacados con la aplicación de la automatización.

Los controles de seguridad presentados en la sección 2.2 deben observarse también desde la perspectiva de la automatización. En (Montesino, 2013) se realiza un estudio crítico de los controles de seguridad que pueden ser automatizados basado en estándares de seguridad definidos. Se obtienen diez macro-controles, los cuales están en concordancia con la selección de la automatización de controles de seguridad de este trabajo.

Algunas actividades que se desarrollan durante el despliegue como son las pruebas de seguridad, adquieren una utilidad especial con el uso de la automatización. La combinación de técnicas de integración continua y herramientas

de seguridad informática permiten añadir calidad al control de las vulnerabilidades, debido a que las mismas pueden tratarse inmediatamente y los tiempos de corrección se disminuyen.

Un ejemplo de lo expresado anteriormente lo representa la utilización del protocolo SCAP (*Security Content Automation Protocol*) (Waltermine, 2009) para la realización de auditorías y validación automatizadas basadas en líneas base de seguridad predeterminada.

De forma similar, el empleo de la gestión de la configuración, como técnica que puede llevarse a cabo de forma automatizada, permite crear durante el despliegue un punto de partida que será utilizado durante todo el ciclo de vida de producción del servidor para la ejecución de tareas de seguridad.

## Resultados y discusión

El procedimiento que se presenta está fundamentado en la utilización de estándares de seguridad y prácticas como la Infraestructura como Código, con un nivel alto de automatización del proceso y flexibilidad. Su enfoque cíclico está orientado a preparar un entorno de despliegue y establecer mecanismos de mantenimiento y control a lo largo del tiempo de producción de la aplicación. En la figura 1 se presenta el flujo de actividades del procedimiento de despliegue seguro de aplicaciones web.

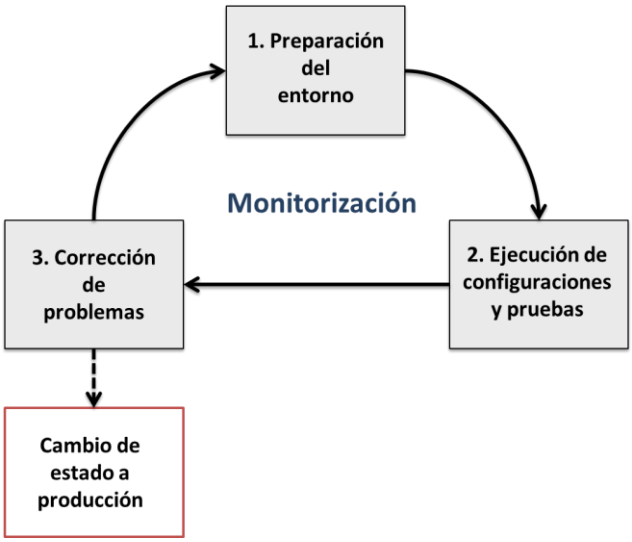



Figura 1. Flujo de ejecución del procedimiento de despliegue seguro de aplicaciones web

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 2, abril-junio, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 42- 56

### Preparación del entorno

Como ocurre con muchas actividades de seguridad, una planificación correcta puede impactar directamente en el éxito o fracaso de un proyecto. En este caso, las actividades de preparación del entorno incluyen los ajustes necesarios de las herramientas a los requisitos que exige la aplicación como el sistema operativo, servidor web, lenguaje de programación. Desde la perspectiva de seguridad, se requiere la configuración del software de seguridad para la disminución de los falsos positivos y garantizar que el nivel de detección de vulnerabilidades sea adecuado. También se deben ajustar y concebir las configuraciones que deben ser aplicadas desde el software de gestión de la configuración desde el punto de vista del entorno de pruebas y producción.

### Ejecución de configuraciones y pruebas

En esta etapa, todos los componentes se encuentran listos para la creación de un servidor de prueba al cual se le aplicarán configuraciones, actualizaciones de software y comprobaciones de seguridad recomendadas de acuerdo a estándares establecidos. Este proceso debe realizarse de forma automatizada.

### Corrección de problemas

Esta fase se caracteriza por la participación de todos los implicados en aras de resolver los posibles problemas que han sido detectados. El procedimiento que se presenta facilita el trabajo del personal de seguridad para la detección y corrección de problemas del entorno de la aplicación web antes de cambiar al estado de producción. Esto se garantiza por las bondades del servidor de integración continua, mediante módulos de reportes de estado de las acciones que se ejecutan.

### Cambio de estado de la aplicación a producción

Las fases descritas anteriormente pueden ejecutarse cíclicamente hasta obtener un estado deseado de seguridad de la aplicación y su entorno. En este caso, si se ha llegado a un acuerdo entre los desarrolladores y operadores de sistemas, la aplicación puede pasar a brindar el servicio para el que fue concebido en producción. En esta fase se pueden activar o modificar controles de seguridad que no fueron aplicados durante la etapa de pruebas como la apertura de puertos, ajustes al firewall de aplicaciones, activación del software para las copias de seguridad, etc. De igual forma, se deben eliminar datos innecesarios que se crearon de forma temporal como usuarios de prueba, direcciones IP, etc.

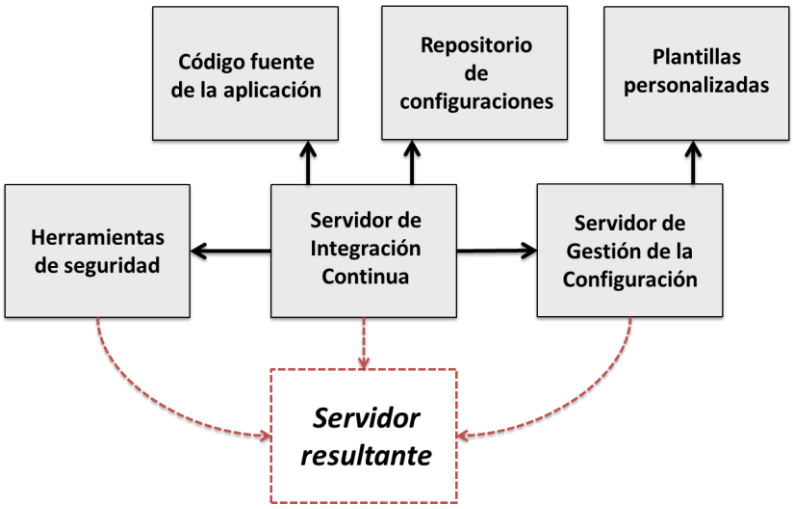
El entorno que se estableció durante el despliegue puede seguir operativo para la gestión de la configuración y detección de problemas de seguridad del servidor en el futuro.

En la figura 2 se muestra la interacción de los componentes del procedimiento de despliegue seguro de aplicaciones web. El servidor de integración continua controla todos los componentes de la arquitectura de despliegue. Se encarga

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 2, abril-junio, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 42- 56

de obtener el código fuente de la aplicación de un origen de datos que puede ser un repositorio o un servidor de FTP para ser desplegado en el servidor resultante. De igual forma, obtiene de forma actualizada las configuraciones recomendadas que serán utilizadas por las herramientas de seguridad y el servidor de gestión de la configuración. Por otro lado, se encarga de emitir reportes de los resultados de las herramientas, así como permitir la ejecución de tareas de gestión de la configuración.

El servidor de gestión de la configuración controla las configuraciones que deben ser asignadas al nuevo servidor; utiliza plantillas personalizadas que poseen configuraciones y optimizaciones basadas en estándares y buenas prácticas establecidas.




**¡Error!**

Figura 2. Arquitectura de despliegue seguro de aplicaciones web

## Aplicación del procedimiento propuesto

El procedimiento que se presentó en este trabajo ha sido aplicado en el centro de datos de la Universidad de las Ciencias Informáticas para el despliegue de aplicaciones web. La aplicación práctica del mismo se presenta en la figura 3.

Como se puede apreciar, se utilizan herramientas que están acorde con el procedimiento de arquitectura presentado. El servidor de integración continua que se utiliza es Jenkins[1], el cual brinda flexibilidad mediante la utilización de plugins para el acople de componentes y la visualización de resultados. Como servidor de gestión de la configuración

[1] https://jenkins-ci.org/

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 2, abril-junio, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 42- 56

se utiliza SaltStack[2], para controlar las configuraciones y el ciclo de vida de las máquinas virtuales en conjunto con Vagrant[3]. Algunas de las herramientas utilizadas para el análisis de seguridad son Zaproxy[4], Openscap[5], Nikto[6], Threadfix[7] y Findbugs[8]. El origen de las configuraciones y el código fuente se obtiene de un servidor de control de versiones Git[9]. Al servidor resultante se le instalan herramientas que permiten el aseguramiento de controles de seguridad como la monitorización (Nagios[10]) y las salvas de respaldo (Bacula[11]).

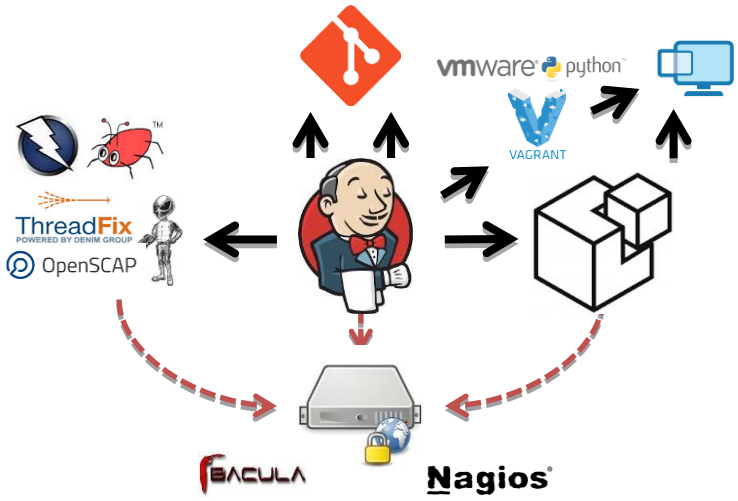



Figura 3. Aplicación práctica de la arquitectura de despliegue seguro de aplicaciones web.

## Conclusiones

En este trabajo se presenta un procedimiento para el despliegue seguro de aplicaciones web basado en buenas prácticas, estándares y elementos tradicionales del desarrollo de software.

[2] http://saltstack.com/
[3] https://www.vagrantup.com/
[4] https://www.owasp.org/
[5] http://www.open-scap.org/page/Main_Page/
[6] https://cirt.net/Nikto2/
[7] http://www.threadfix.org/
[8] http://findbugs.sourceforge.net/
[9] https://git-scm.com/
[10] https://www.nagios.org/
[11] http://www.baculasystems.com/

Las actividades y controles de seguridad presentados se derivan de prácticas probadas de prestigio a nivel internacional. El procedimiento presentado está alineado a estas directrices, con un enfoque hacia la automatización.
Los resultados obtenidos permiten establecer una referencia para la posible aplicación del procedimiento en otros entornos. Las herramientas utilizadas pueden ajustarse a las necesidades y políticas de la organización para su aplicación.

La utilización práctica de este procedimiento ha permitido mejorar los procesos de despliegue de aplicaciones web en el Nodo Central de la Universidad de las Ciencias Informáticas. La automatización del proceso ha facilitado la reducción del tiempo de realización de las operaciones y la cantidad de errores humanos cometidos. Además, la utilización de prácticas tradicionales del desarrollo de software, vinculado con tendencias modernas que se aplican en la infraestructura, ha flexibilizado la utilización de estándares y buenas prácticas de seguridad necesarias en la organización.

Este trabajo se ha desarrollado basado en prácticas de seguridad que se recomiendan durante el despliegue de software. Sin embargo, se debe tener en cuenta que la seguridad es un proceso y debe concebirse desde las fases iniciales del ciclo de desarrollo de software y continuar luego del despliegue, con lo cual se reduce el costo de solucionar problemas de seguridad.

La vinculación de los elementos presentados en este trabajo con otras prácticas seguras del desarrollo de software como la gestión de riesgos, casos de abuso, etc., contribuirá a la obtención de un software más robusto y seguro.

## Referencias

CARZANIGA, A. A Characterization of the Software Deployment Process and a Survey of related Technologies. [En línea]. 1997. [Consultado el: 10 de septiembre de 2015] 2-5 p. Disponible en: http://www.inf.usi.ch/carzaniga/papers/deployment-tr-97-84.pdf.

CHANDRA, P.: Software Assurance Maturity Model. A guide to building security into software development v1.0. [En línea], OWASP Project, 2008. [Consultado el: 9 de noviembre de 2015], 1-96 p. Disponible en: http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf

COUNCIL ON CYBER SECURITY. The Critical Security Controls for Effective Cyber Defense, version 5.1. [En línea]. Council on Cyber Security, 2015. [Consultado el: 15 de noviembre de 2015], 1-106 p. Disponible en:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf

FOWLER, M.; FOEMMEL M. Continuous integration. [En línea]. 2006. [Consultado el: 10 de septiembre de 2015]. Disponible en: http://www.martinfowler.com/articles/continuousIntegration.html

HUMBLE, J.; FARLEY, D. The Problem of Delivering Software. En: Addison Wesley. Continuous delivery, 2010 p. 6.

HÜTTERMANN, M. Infraestructure as code. En: Apress. DevOps for developers, 2012, 135-136 p.

ISO/IEC. ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2013.

JASON, A. What is information security? En: Syngress. The basics of information security: understanding the fundamentals of InfoSec in theory and practice, 2014, p. 1.

JOHNSON, A.; DEMPSEY, K., et al. Guide for Security-Focused Configuration Management of Information Systems. [En línea]. NIST special publication 800-128, 2011. [Consultado el: 15 de noviembre de 2015], 1-88 p. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

KISSEL, R.; STINE, K. Security considerations in the system development life cycle. [En línea]. NIST special publication 800-64 revision 2, 2008, [Consultado el: 11 de noviembre de 2015], 1-34 p. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

MCGRAW, G. Software security meets security operations. En: Addison-Wesley Professional. Software security: building security in, 2006, p. 228.

MCGRAW, G.; MIGUES, S.; et al: The Building Security in Maturity Model. [En línea]. BSIMM5, 2013. [Consultado el: 9 de noviembre de 2015], 1-74 p. Disponible en: https://www.bsimm.com/download/

MERRIAM-WEBSTER. Automation definition, Merriam-Webster, 2015.

MONTESINO, R.; BALUJA, W.; et al. Gestión automatizada e integrada de controles de seguridad informática. Revista de Ingeniería Electrónica, Automática y Comunicaciones, 2013, 34: 40-58.

MORRIS, K. Challenges and Principles. En: O'Reilly. Infraestructure as Code, 2015, 1-5 p.

NIST. Security and Privacy Controls for Federal Information Systems and Organizations, revision 4. [En línea]. NIST special publication 800-53, 2015, 1-462 p. [Consultado el: 15 de noviembre de 2015]. Disponible en: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

PAUL, M. The Ten Best Practices for Secure Software Development. [En línea]. International Information Systems Security Certification Consortium. 2009. [Consultado el: 13 de septiembre de 2015] 1-8 p. Disponible en: https://www.isc2.org/uploadedfiles/%28isc%292_public_content/ certification_programs/csslp/isc2_wpiv.pdf.

PUPPET LABS. Automated configuration management definition, Puppet labs, 2015.

STUTTARD, D.; PINTO, M. Common Web Application Functions. En: John Wiley & Sons, Second Edition. The web application hacker's handbook: finding and exploiting security flaws, 2008, p. 4.

VERIZON. The 2015 Data Breach Investigations Report (DBIR). [En línea]. 2015. [Consultado el: 13 de septiembre de 2015] 41-43 p. Disponible en: http://www.verizonenterprise.com/DBIR/2015

WALTERMINE, D., QUINN, S.; et al.: The Technical Specification for the Security Content Automation Protocol (SCAP). [En línea]. NIST special publication 800-126, 2009. [Consultado el: 5 de diciembre de 2015], 1-58 p. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf

WHITHMAN, M.; MATTORD, H. What is security? En: Cengage Learning. Principles of information security, 2011, p. 8.