0.3 TENDENCIAS DE SEGURIDAD Y VULNERABILIDADES EN SISTEMAS BASADOS EN LA NUBE

[1] Ing. Ivette Mateo

Docente ITSVR

[2] Msc. Edison Neira Cedillo

Docente ITSVR

Recibido: Mayo 2017 Revisado: Junio 2017 Publicado Julio 2017

Resumen

El constante crecimiento de la tecnología ha llegado al punto donde muchos servicios que antes eran usados desde la propia infraestructura física de la empresa u organización, ahora pueden estar alojados físicamente en cualquier parte del mundo y accedidos haciendo uso del internet, a esto lo conocemos como “Cloud Services”. Esto conlleva a que las seguridades se incrementen y se deban tomar medidas para evitar ataques al servicio. Se analizarán datos estadísticos sobre las eventualidades suscitadas últimamente y se revisarán varias recomendaciones para prevención de las mismas.

Palabras claves: Seguridad informática Ataques informáticos Técnicas de ataques informáticos Servicios en la nube

Introducción

Durante los últimos años la tecnología ha evolucionado de tal manera que los equipos de cómputo dependen mucho del internet para interconectarse con otros equipos para intercambiar recursos. Esto da origen al concepto de NUBE o Cloud Computing, el cual (Reimche, 2013) la define como "Computación basada en el internet mediante recursos compartidos", esto con el paso de los años va evolucionando hasta llegar a usar servicios de servidores en la nube, el cual para las empresas representa ahorros tanto en costo de mantenimiento, licenciamiento e incluso ahorro de recurso humano, pues todos estos servicios son manejados por un proveedor que se encargará de todo el trabajo.

El termino computación en la nube se ha generalizado, al referirse a soluciones tecnológicas de software como servicio. Lo importante para el usuario es que el servicio funcione correctamente sin importar donde este localizado el servidor.

La demanda de estos servicios ha incrementado en los últimos dos años a nivel mundial por parte de clientes corporativos y entidades públicas.

El siguiente gráfico muestra la evolución de los ingresos por servicios de cloud computing a nivel mundial desde 2013 hasta 2015, así como previsiones para 2016 y 2019. (statista.com, 2016). La estadística incluye una distribución por área geográfica de los mismos.

EVOLUCIÓN DE LOS INGRESOS POR SERVICIOS DE CLOUD COMPUTING A NIVEL MUNDIAL

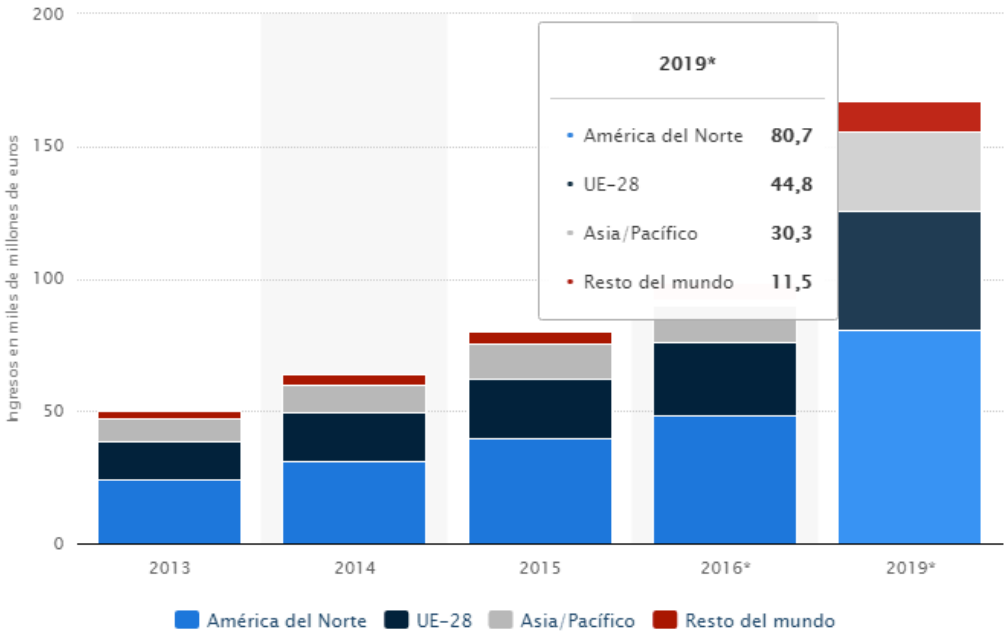

Ilustración 1: Evolución de la facturación por servicios de cloud computing a nivel mundial de 2013 a 2019, por área geográfica (en miles de millones de euros) Fuente: Statista.com

Como podemos apreciar, en la Unión Europea la facturación por prestación de servicios en la nube creció de manera continuada durante todo el periodo, de forma que en 2015 superó por primera vez la cifra de los 20.000 millones de euros.

Existen diferentes tipos de servicios de cloud server, entre ellos el IaaS (Infraestructure as a Service), definida por Gartner, como "una oferta estandarizada, altamente automatizada, donde son propiedad de los recursos informáticos, complementados por las capacidades de almacenamiento y red y celebrados por un proveedor de servicios y ofrecen a los clientes bajo demanda". (Gartner, 2017). Por lo tanto quien contrata este servicio tiene control y responsabilidad total sobre la infraestructura alojada en la nube.

Otro tipo de servicio es SaaS (Software as a Service), según definición de Gartner, es el software de propiedad, entregado y gestionado de forma remota por uno o más proveedores. (Gartner, 2017) donde es el proveedor del servicio quien se encarga de la administración total del equipo en la nube. Este trabajo tratará específicamente sobre SAS, ya que, dada las facilidades que esta ofrece a los usuarios, es el más ofertado, y, por tanto supone un reto en lo que a seguridad informática se refiere.

Los proveedores de servicio SAS, tienen como principal preocupación la seguridad no solo física sino lógica de sus equipos y servicios, por tanto se debe considerar las vulnerabilidades a los cuales los servidores se encuentran expuestos, entre ellos tenemos

DoS: Denegación de servicio.
SPAM: Envío masivo de correo
Suplantación de identidad.

Ante esta situación, la pregunta a plantearse es: ¿Cuáles son los niveles de percepción de riesgo en los sistemas informáticos basados en la nube?

Esto influye mucho en el desarrollo del negocio de servicios en la nube, especialmente en el área de servidores, pues del nivel de apreciación de la seguridad por parte de los clientes incidirá en la decisión de adquirir o no el servicio, por tanto es un problema que debe ser tratado con la exigencia del caso para el desarrollo y evolución del uso de la tecnología en la nube.

Todo esto nos lleva a la siguiente hipótesis: “El incremento de la utilización de los servicios en la nube está exigiendo maximizar los niveles de seguridad por parte de los proveedores”

Si no se ofrece seguridad en la información, difícilmente las personas decidirán confiar la información a un servicio en la nube, por tanto se deben analizar las diferentes circunstancias que debilitan la seguridad de la información en estos servicios.

La meta de este trabajo es el de llegar a determinar los métodos de seguridad para la prevención de ataques en los servidores alojados en la nube.

OBJETIVO

Analizar las herramientas de seguridad existentes para prevenir ataques en los actuales servicios en la nube.

El objetivo principal de este trabajo es el de revisar las vulnerabilidades junto con su respectiva solución de software.

Este estudio se realizó porque es necesario conocer la evolución de herramientas de software de seguridad aplicadas a servidores en la nube.

MATERIALES Y MÉTODOS

El estudio se realizó revisando cifras estadísticas de diferentes casas comerciales especializadas en seguridad, revisando la demanda en lo que a servicios en la nube respecta y la revisión de software estratégico para prevenir ataques.

Las empresas en Latinoamérica están haciendo más uso de servidores en la nube, según (TI, 2017) “Una encuesta global de IBM, llevada a cabo con más de 1.000 ejecutivos de 18 industrias, señala que casi todas las empresas encuestadas están usando la nube, pero solamente en algunas áreas de su negocio”, además, según el siguiente gráfico:

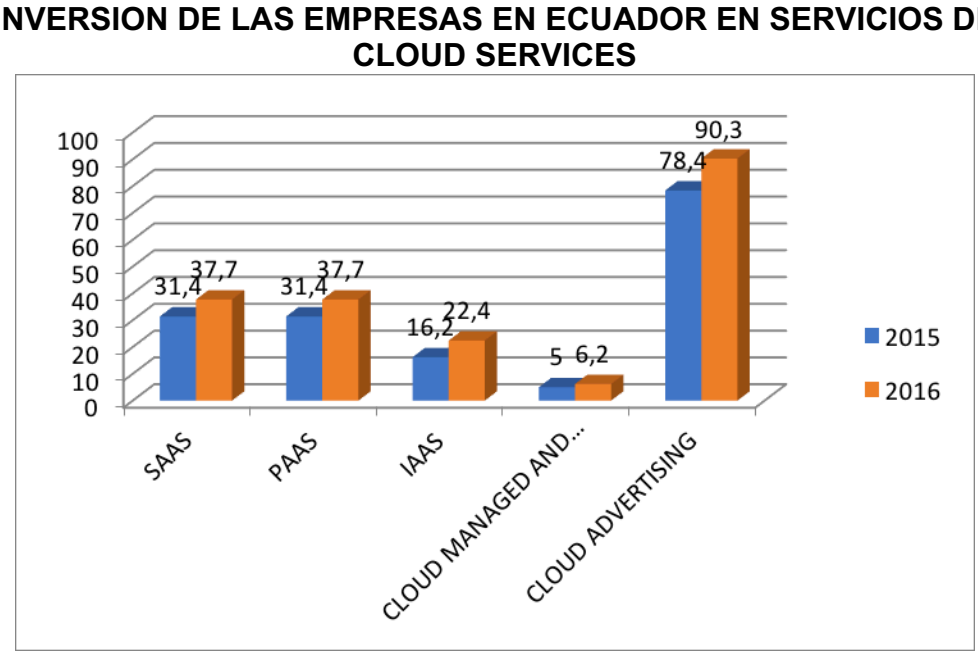

Ilustración **2**: Inversión de las empresas en ecuador en servicios de cloud services Fuente: Computer World

En esta gráfica podemos apreciar el crecimiento de inversión en los diferentes tipos de servicios en la nube que las empresas ecuatorianas contrataron entre los años 2015 y 2016, el servicio de Software como servicio (SAAS por sus siglas en inglés) donde el proveedor se encarga de dar todas las facilidades de uso a sus clientes en conjunto con el Servicio de Plataforma como Servicio (PAAS), sobre el cual el cliente se encarga de la gestión del servidor en la nube, muestran un incremento de 6.2 puntos porcentuales para el año 2016, este mismo incremento se refleja en el servicio de Infraestructura como Servicio (IAAS).

Evidenciando el crecimiento del uso de servicios en la nube, se demuestra el crecimiento de ataques a los mismos. El principal ataque a los que se exponen estos es el de Denegación de Servicio (DoS) (Brito, 2009) explica que estos "consisten en aprovechar una gestión incorrecta de los recursos de una aplicación para realizar peticiones masivas y provocar su saturación", la siguiente gráfica nos indica el incremento durante el segundo trimestre del 2016 de este tipo de ataques:

Dinámica de ataques DDOS durante el segundo trimestre del 2016

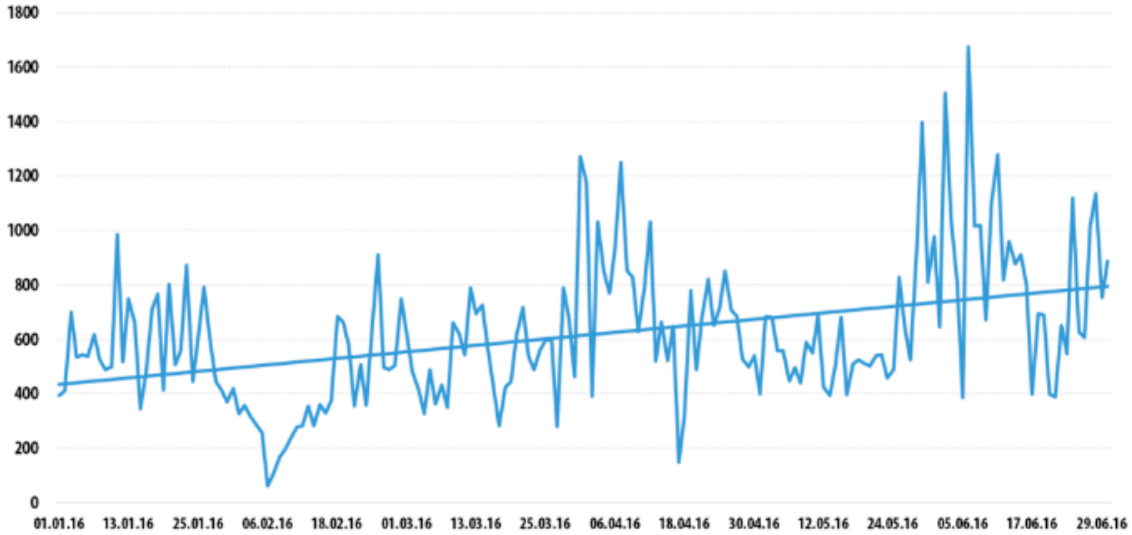

Ilustración 3: Dinámica de ataques DDOS durante el segundo trimestre del 2016 Fuente: securelist.lat

Esto es corroborado por digitalattackmap.com, sitio especializado en monitorear ataques de DoS en colaboración con Google y Arbor Networks, donde los ataques son sectorizados:

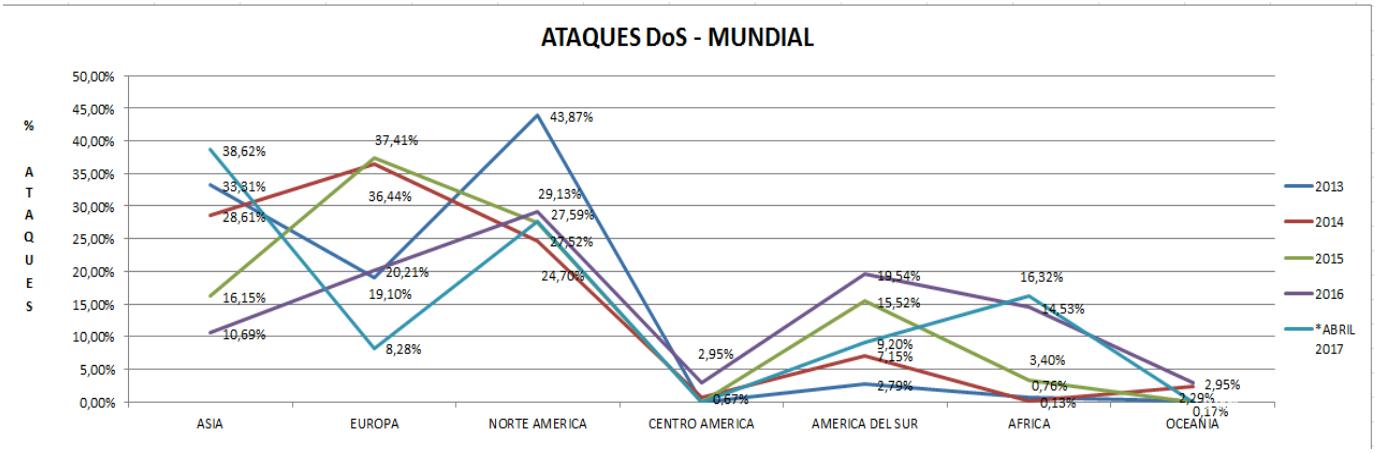

Ilustración 4: Ataques DoS – Mundial Fuente digitalattackmap.com

En lo referente a América del sur, tenemos el siguiente gráfico:

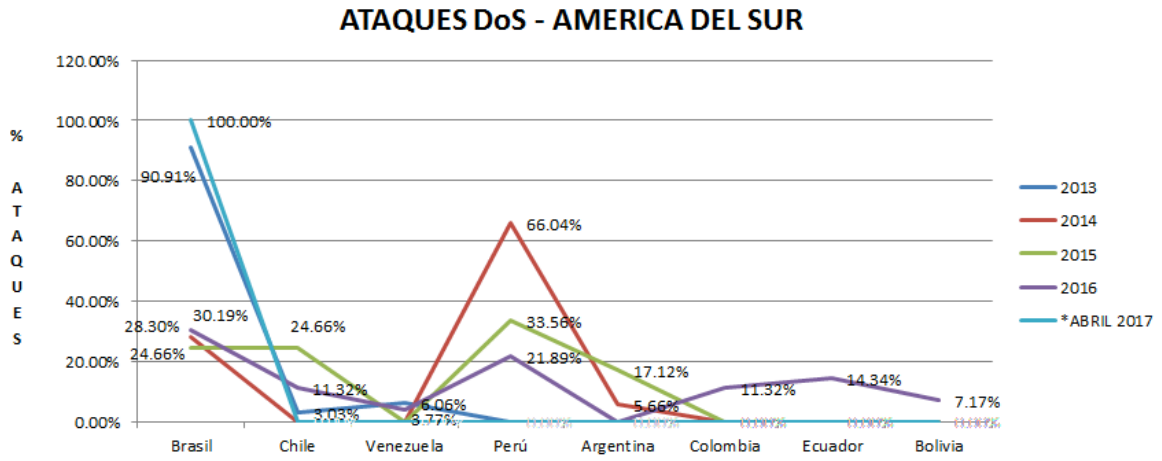

Ilustración 5: Ataques DoS – America del Sur. Fuente: digitalattackmap.com

Ecuador se encuentra en estas estadísticas con un porcentaje de ataques del 14.34% durante el año 2016, con lo que se evidencia que no se puede desapercibir las vulnerabilidades a los que se encuentran expuestos los servidores en la nube y se deben tomar las precauciones del caso.

III. Análisis y propuesta

Las cifras expuestas denotan la inseguridad a la que se encuentran expuestos los servicios y servidores en la nube, por lo que es necesaria la mejora de seguridades y protección a los mismos.

La casa desarrolladora de software de seguridad ModSecurity recomienda que las seguridades a tomar en los servidores en la nube deben incluir:

- Monitoreo de seguridad de las aplicaciones en tiempo real y control de acceso
- Registro del tráfico HTTP completo
- Supervisión de la seguridad pasiva continua
- Restricciones en aplicaciones web

Aunque no existe seguridad al 100% en el internet, es necesario sobre los procedimientos básicos de seguridad en la web, tener un constante monitoreo de seguridad sobre todas las aplicaciones, incluyendo el tráfico que hace uso del protocolo HTTP, además es necesario tener alojado en el sistema operativo un antivirus con supervisión constante del comportamiento de los archivos para detectar intentos de infección al equipo. Finalmente, es importante que las aplicaciones desarrolladas para trabajar en la web, desde su código fuente deban incluir seguridades que impidan un fácil acceso a la base de datos o a cualquier otra instancia del servidor.

Para prevenir este tipo de ataques se debe implementar sistema de Prevención de Intrusos IPS, definido por Panda Security (PANDA SECURITY, 2017), es el que ejerce el control de acceso en una red informática para proteger a los sistemas

computacionales de ataques y abusos. Está diseñado para analizar los datos del ataque y detenerlo en el mismo momento en que se está gestando y antes de que tenga éxito.

Las soluciones basadas en la nube, como Kona Site Defender, ofrecen escalabilidad integrada y alcance global para defenderse contra los tipos de ataques DoS más comunes, además de ataques contra aplicaciones web (inyecciones SQL, scripting entre sitios, etc.) y ataques directos al origen.

DoS Kona Site Defender mitiga los ataques DoS por medio de la absorción del tráfico DoS dirigido al nivel de aplicación, el desvío de todo el tráfico DoS dirigido al nivel de red, como inundaciones SYN o inundaciones UDP, y la autenticación del tráfico válido en el extremo de la red. Esta solución de protección integrada está "siempre activada" y únicamente se permite tráfico en el puerto 80 (HTTP) o el puerto 443 (HTTPS). Se pueden limitar los servicios asociadas al tráfico DoS y la función de almacenamiento en caché flexible maximiza la descarga del origen. (AKAMAI.COM, 2017)

El manejo de esta herramienta de seguridad permite mantener la disponibilidad de los sitios web sin redirigir el tráfico y sin que el rendimiento se vea afectado, ya que posibilita manejar Tb//s de tráfico diario.
Las capacidades de mitigación de DoS se implementan en la ruta para proporcionar protección solo a un salto de red del punto de solicitud del servidor en la nube.
Es una solución flexible, que configura un número ilimitado de reglas personalizadas para protección de aplicaciones en la nube.

Kona Site Defender incluye una completa colección de protecciones de firewall predefinidas, pero configurables, para la capa de aplicación, que mantiene periódicamente con actualizaciones en distintas categorías como: protocolo, infracciones de políticas de HTTP y de límite de solicitudes, robots maliciosos, ataques genéricos y de inyección de comandos, troyanos de puerta trasera y fuga de contenido saliente.

Esta solución es más eficiente que las actuales IDS, sistema de detección de intrusos, actúan reactivamente. Evitando mayores pérdidas económicas a las empresas que optan por un sistema IPS.

Se mencionan algunas ventajas sobre los servicios IDS:
• Sencilla integración con la infraestructura de TI existente.
• Maximización del tiempo de actividad y de la disponibilidad durante los ataques DoS.
• Defensa de la infraestructura de aplicaciones web.
• Escalabilidad.
• Mantenimiento del rendimiento incluso en caso de ataque.

En el Ecuador se está iniciando la implementación de estos sistemas de prevención de ataque, con el fin de evitar el crecimiento de intrusiones a nivel de servicios provistos a través de servidores en la nube, tal es el caso de servicios bancarios, compras en línea, servicios de comercialización vía web en general.

IV. Conclusiones.

1. El objetivo de los ataques DDoS es intentar bloquear sitios web e infiltrarse en ellos mediante la inundación del servidor de origen del sitio con solicitudes falsas, desde varias ubicaciones y redes.

2. A nivel mundial se están incrementando en un 28% aproximadamente los ataques de denegación de servicios, DoS, de acuerdo a la información de mapeo presentada por el portal www.digitalattackmap.com, si se toma como referencia las cifras de China y EEUU, principales países destino de este tipo de ataques.

3. En el Ecuador se debe prevenir el crecimiento de este tipo de ataques que en el año 2016, se presentó el 14.34% del total a nivel mundial, con la implementación de soluciones en la nube para el desvío del tráfico DoS.

4. Debido al creciente número y la escala de los ataques DoS, los proveedores de servicios en la nube, deben considerar dentro de sus políticas empresariales la planificación de detección y mitigación de los ataques DoS, así como la implementación sistemas de defensa para proteger al servidor de nombres de dominio frente a sobrecargas y ataques de denegación de servicio.

5. Para las empresas con servicios en la nube y elevado volumen de ventas al consumidor, transacciones empresa a empresa, usuarios de aplicaciones de SaaS y juegos online. Es imprescindible que adopten soluciones de seguridad cloud que les permitan protegerse y garantizar el acceso ininterrumpido a sitios web y aplicaciones.

6. Es indispensable para mitigar este tipo de ataque la implementación de herramientas como Kona Site Defender, para proteger los sitios web y las API de ataques sofisticados con un conjunto de herramientas multicapa. Las funciones de defensa contra DoS siempre están activas, por lo que no es necesario redireccionar el tráfico antes de que comience el proceso de mitigación.

V. Bibliografía.

AKAMAI.COM. (Enero de 2017). *https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp*. Recuperado el 22 de Mayo de 2017, de

https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp: https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp

AppArmor.com. (Octubre de 2016). *wiki.ubuntu.com/AppArmor*. Recuperado el 17 de Mayo de 2017, de wiki.ubuntu.com/AppArmor: wiki.ubuntu.com/AppArmor

Brito, N. (2009). *Manual de Desarrollo Web con GRAILS.* Imaginaworks.

Clamav.net. (Octubre de 2016). *https://www.clamav.net/documents/installing-clamav*. Recuperado el 17 de Mayo de 2017, de https://www.clamav.net/documents/installing-clamav: https://www.clamav.net/documents/installing-clamav

Gartner. (Febrero de 2017). *http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/*. Recuperado el 15 de Mayo de 2017, de http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/: http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/

Gartner. (Febrero de 2017). *http://www.gartner.com/it-glossary/software-as-a-service-saas/*. Recuperado el 15 de Mayo de 2017, de http://www.gartner.com/it-glossary/software-as-a-service-saas/: http://www.gartner.com/it-glossary/software-as-a-service-saas/

MODSECURITY. (Noviembre de 2016). *https://modsecurity.org/about.html*. Recuperado el 17 de Mayo de 2017, de https://modsecurity.org/about.html: https://modsecurity.org/about.html

Nixory. (Noviembre de 2013). *http://nixory.sourceforge.net/about.html*. Recuperado el 17 de Mayo de 2017, de http://nixory.sourceforge.net/about.html: http://nixory.sourceforge.net/about.html

PANDA SECURITY. (Enero de 2017). *http://www.pandasecurity.com/spain/support/card?id=31463*. Recuperado el 22 de Mayo de 2017, de http://www.pandasecurity.com/spain/support/card?id=31463: http://www.pandasecurity.com/spain/support/card?id=31463

Reimche, T. (2013). Tecnology Briefing. *Alberta Goverment*.

statista.com. (Octubre de 2016). *https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/*. Recuperado el 15 de Mayo de 2017, de https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/: https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/

TI, D. (2017). *Diario Ti.* Obtenido de diarioti.com.