SEGURIDAD EN LA NUBE

1. RESUMEN

En este documento vamos a hablar de la seguridad que existe en la llamada nube, un servicio muy usado en la actualidad. Empezaremos definiendo el concepto de nube y nombrando las principales ventajas que nos aporta usar este novedoso servicio. Continuaremos hablando de factores importantes en este ámbito como es la disponibilidad y las copias de seguridad. Detallaremos los principales riesgos o amenazas que existen en la actualidad (según la conferencia RSA que hubo en San Francisco en 2013). Y por último hablaremos de muchos modos para evitar dichas amenazas y hacer de la nube un servicio más seguro a través de la autenticación múltiple, encriptación de datos, conexión segura para las redes (mediante protocolos de encriptación), antispam, firewall, backup y WAF.

Antes de meternos en el ámbito de la seguridad en la sube queremos dar una muy breve introducción de qué es la nube.

2. DEFINICIÓN Y FACTORES IMPORTANTES DE LA NUBE

¿Qué es la nube?

Es una metáfora empleada para hacer referencia a servicios que podemos usar a través de internet. Lo que normalmente tenemos almacenado en nuestro ordenador personal podemos pasarlo a servidores a los que se puede tener acceso desde internet.

¿Por qué usar la nube?

- Podemos tener acceso a nuestros datos almacenados desde cualquier sitio y a través de diferentes dispositivos conectados a Internet.
- Todo el software se encuentra en la nube, despojandonos la necesidad de tener que instalar los programas en nuestros equipos así como su mantenimiento.
- Se ahorra dinero en hardware. Con una sola copia almacenada en la nube, esta es compartida por diversos usuarios sin necesidad de gastar dinero en sistemas de almacenamiento.
- Son herramientas ideales para la comunicación y el trabajo en equipo.
- Pago en medida al uso que necesito hacer de la nube.

Ejemplos de servicios de computación en la nube hay muchísimos, como por ejemplo: Droxbox, Google Drive, Flickr, icloud, Google Cloud Platform, etc.

A día de hoy los servidores virtuales superan a los servidores físicos, y no solo eso, sino que se predice que en pocos años el 71% de servicios que den los servidores serán de servidores virtuales. Y este tipo de servidores es uno de los pilares del concepto de computación en la nube.

Disponibilidad

Hablemos ahora sobre **disponibilidad**, ya que es una de las principales ventaja que creemos tener al usar un sistema de nube. Al almacenar nuestros datos en un lugar virtual, cuando accedemos a ellos, nosotros pensamos que están en un lugar abstracto llamado nube, pero realmente no es tan abstracto. Los datos a los que accedemos se encuentran almacenados en un sistema de memoria parecido al que dispone un portátil común, con la diferencia de que esta copia se puede encontrar almacenada a la vez en diferentes sistemas de almacenamiento repartidos por diversas localizaciones geográficas. Los datos almacenados en estas localizaciones están disponibles para nosotros cuando los solicitamos. Bueno realmente no está tan disponible para nosotros cómo podemos llegar a pensar , y un ejemplo de esto es el caso de la caída de un Rayo en Dublín el 8 de agosto de 2014,sobre las instalaciones para la nube de Amazon. Tras el comunicado oficial de amazon: “Nuestro servicio cloud ha estado fuera de servicio en las últimas horas debido al impacto de un rayo en uno de los centros de control”. Por esta causa un gran número de webs europeas se vieron afectadas por la acción de este rayo ya que usaban este servicio de nube siendo cuestionada la garantía de disponibilidad que se tiene sobre el sistema.

Copias de seguridad
Como hemos mencionado antes, nuestros datos se encuentran almacenados en diferentes lugares, esto también es debido a que se realizan copias de seguridad de los datos con el fin de disponer de un método para recuperarlos en caso de pérdida. Estas copias son útiles ante eventos como pueden ser catástrofe natural o por ataques al servicio. El uso de estas copias tiene como fin restaurar la cantidad de archivos que hayan sido eliminados, corrompido, infectados por virus, etc. Las copias se utilizan a menudo ya que según un estudio el 66% de los usuarios de Internet han sufrido una seria de pérdida de datos en algún momento. Los usuarios debemos tener en cuenta las configuraciones por defecto de copias de seguridad de nuestro sistema cloud y un ejemplo de esto es que en *iCloud* de *Apple* muchos usuarios desconocen que por defecto se realizan 3 copias de seguridad de sus datos de forma automática. Esta es una de las razones por las que los hackers acceden a los datos que han podido ser borrados hace meses pero permanecen en la nube.

Al margen de donde están almacenados nuestros datos , se nos dirige a ellos de manera virtual. La manera de distribuir las peticiones que se realizan se denomina **equilibrio de carga**. Esta distribución de peticiones sobre los servidores disponibles es una medida importante de seguridad debido a que en momentos concretos se puede estar realizando un gran número de peticiones sobre un mismo nodo del sistema incrementando con esto el tiempo de respuesta para peticiones, o incluso no teniendo respuesta por parte del servidor. Si el mismo recurso que se solicita se encuentra ubicado en diferentes localizaciones es más eficiente acceder a través del nodo que se encuentra menos congestionado. **El equilibrio de carga puede implementarse a través de hardware o software**:

-En sistemas **hardware** tenemos como ejemplo uno de los sistemas más demandados. El equipo Big-IP de F5 Networks no es más que un PC dentro de una carcasa destinada a ser montada en un rack que corre un software específico, se comporta de cara a la red como un router, debiendo situarse entre dos redes con distinto direccionamiento. Para ello, dispone de dos conectores Ethernet, uno destinado a la red externa por donde entrarán todas las peticiones a los servidores Web, y otro para la red interna, en la que deben estar situados todos los equipos balanceado.

En los mecanismos de equilibrio de carga más sencillos son en el que se escucha en un puerto de red las peticiones de servicio, al llegar esta petición, el equilibrador de carga hace uso de un algoritmo de planificación para asignar donde enviar la petición, entre estos algoritmos los típicos en uso hoy en día son de turno rotatorio, turno rotatorio con prioridades, tiempo de respuesta más rápido por parte del nodo y asignaciones personalizadas entre otro factores…

La nube de Google: esta empresa tiene una gran inversión en infraestructura para su sistema, siendo su nube una de las más grandes del mundo hoy en día. Se calcula que el servicio de Google se ejecuta sobre un millón de servidores en todo el mundo, procesa un Billón de peticiones de búsquedas y genera veinte petabytes de datos al día. Aun así conseguimos tener una respuesta para una búsqueda de la palabra “cloud“ de aproximadamente 344.000.000 de resultados (0,21 segundos). Google tiene al menos 12 instalaciones principales en Estados Unidos y muchas más por todo el mundo. Estos centros se ubican en distintos sitio concretos por los siguientes motivos:
-menor coste de energía (lugares donde sea más económica la energía).
-ubicación relativa de otros centros para tener una menor latencia de respuesta entre diferentes lugares.
-Una fuente de agua (para temas de refrigeración).

Cuando nosotros hacemos una consulta en la nube esta consulta se envía a un servidor DNS el cual consulta los servidores DNS de Google, este examina qué direcciones están más cercana a nuestra posición geográfica y sobre las más cercanas usan un algoritmo de turno rotatorio para devolvernos una dirección IP sobre la que se realizará la petición del servicio solicitado. De esta manera google consigue un primer nivel de balanceo de carga.

Localización geográfica de los datos almacenados en la nube
Como los datos pueden estar almacenados en diferentes ubicaciones geográficas, de encontrarse almacenados en países distintos, las leyes que gobiernan la protección de los datos difieren de unos países a otros donde se encuentran almacenados los datos físicamente. Por lo que puede pasar que la protección legal de datos de su país no sea la misma que la del país donde se encuentran alojados. Por ejemplo, en España, todo lo relacionado con la protección de datos está recogido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos.

3. PRINCIPALES RIESGOS, AMENAZAS Y ATAQUES QUE SUFRE LA NUBE

Para poder entender mejor este problema, antes debemos de conocer cuales son las principales amenazas en torno a la seguridad que existen en la nube. Para ello vamos a detallar las 4 principales amenazas que existen en la actualidad según la conferencia RSA que hubo en 2013 en San Francisco.

A continuación describimos estas 4 principales amenazas:

- **1ª)** ***Violaciones de acceso a los datos****:* CSA puso a un grupo de investigación a manos de esta sección y obtuvieron resultados que describen que una máquina virtual puede utilizar la información de las claves criptográficas privadas en uso por otras máquinas virtuales en el mismo servidor. Un Hacker con mala intención no tendría mucha dificultad para conseguir este tipo de hazaña. Si una base de datos que da servicio en la nube no está correctamente diseñada, un solo defecto en la demanda que haga un cliente podría permitir a un atacante obtener no sólo los datos de ese cliente, si no los datos de cualquier otro cliente. Para solucionar esta violación se podrían cifrar los datos, pero si se pierde la clave de cifrado se perderían todos los datos.

- **2ª)** ***Pérdida de los datos a causa de terceros***: ver desaparecer sus valiosos datos sin saber como ha sucedido. Un Hacker con mala intención podría conseguirlo sin dejar rastro. Como hemos comentado hace un momento, eso se podría solucionar con un cifrado de datos, pero si se perdiese esa clave perderíamos todos los datos.

- **3ª)** ***Riesgo para la seguridad de la computación en la nube***: Si un Hacker consiguiese tener acceso a las credenciales de un usuario podría espiar sus actividades, manipular sus datos, enviar información falsificada… Un ejemplo de este riesgo es el que sufrió Amazon en el 2010 mediante un ataque de XSS en el consiguieron obtener credenciales para este sitio. Una solución para esto es poner dos fuertes técnicas de autentificación siempre que sea posible.

- **4ª)** ***Amenazas a interfaces y API´s inseguras***: generalmente las API´s son parte de la seguridad y disponibilidad de los servidores en la nube. A partir de aquí se pueden construir interfaces, esto deriva en una API por capas, que aparte de aumentar la complejidad, puede maximizar el riesgo ya que puede hacer falta facilitar sus credenciales a terceros. Como por ejemplo hay casos en los que el diseño no esta bien realizado y se puede acceder a través de la inserción de código en los datos, normalmente en formularios web (inyección SQL, que detallamos en este documento).

Aparte de estas amenazas, existen una serie de **ataques que puede sufrir un servidor de la nube**, de los cuales vamos a nombrar algunos a continuación:

-**Ataques DDOS**: Este tipo de ataque hace que el sistema sea inaccesible por los usuarios que solicitan su servicio. Consiste en realizar un gran número de de accesos al sistema servidor provocando la saturación del ancho de banda de la víctima o la sobrecarga de su sistema. El fin que persiguen este tipos de ataques es que el sistema no pueda seguir prestando sus servicios por la saturación que se le produce. Estos ataques se suelen producir desde un gran número de puntos de conexión y son muy usados por el colectivo de crakers Anonymous sobre webs gubernamentales.

-**Ataques de fuerza bruta**: Estos ataques consisten en ir probando todas las combinaciones posibles de contraseñas hasta encontrar la que nos permita el acceso. Como este procedimiento es muy costoso en relación a tiempo, se suelen utilizar combinandolos con un diccionario de contraseñas.

Imagen sacada de: http://administracionjlespinoza.blogspot.com.es/2012/11/confidencialidad-y-encriptacion-de-la_16.html

-**Ataques de inyección SQL**: Estos ataques se realizan sobre web´s que interactuar con bases de datos, si no se realiza un filtro de la información enviada por los usuarios, estos pueden insertar código SQL a través de los datos de entrada que se envían al servidor y que a través de este código insertado se podría acceder a información almacenada en el servidor. Esta inclusión de código consiste en poner caracteres especiales en los campos que se rellenan en formularios de la web, ejemplo de ello sería añadir en un campo contraseña : 1234 ' OR '1' = '1 , lo cual enviará al servidor el dato '1234 ' OR '1' = '1' lo cual sería una condición que siempre es verdadera. Un tipo de ataque es el llamado "Ataque a ciegas por inyección de SQL" este tipo de web se delata de ser vulnerables al no mostrar un mensaje de error al ejecutar una sentencia SQL errónea, pudiendo realizarse pruebas hasta encontrar el nombre o tablas sobre los que se pueden actuar. (NO PROBAR ESTA TÉCNICA, SOLO SE NOMBRA PARA EXPLICAR ESTE TIPO DE ATAQUE)
Entre las bases de datos susceptibles a estos ataques se encuentran:
MySQL, Oracle, Postgres o MS SQL.

Panel donde poder insertar código SQL
Imagen sacada de: http://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql

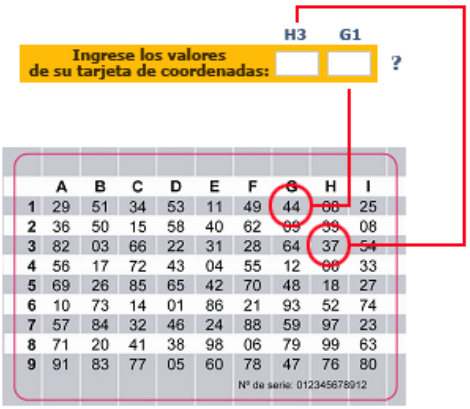
4. MANERAS DE GARANTIZAR LA SEGURIDAD EN LA NUBE Y EVITAR AMENAZAS

Para **garantizar la seguridad en la nube y evitar estas amenazas** descritas anteriormente y cualquier otro tipo de vulnerabilidad que haga que los datos no estén seguros en la nube hay empresas que se dedican a ello. Un ejemplo de estas empresas es *Safenet*. Uno de los numerables servicios que ofrece esta empresa es la **autenticación de factores múltiples**, la cual asegura que un usuario sea quien pretende ser, haciendo uso de más factores para la identificación del usuario. Cuantos más factores se sumen a esta identificación obtendremos mayor seguridad en la autentificación.

4.1 AUTENTICACIÓN MÚLTIPLE

Combinaciones de estos factores pueden ser:

- Algo que el usuario conoce: por ejemplo una contraseña, número de identificación o PIN.
- Algo que el usuario tiene en su poder: una tarjeta de coordenadas o firma digital.
- Algo que el usuario es (físicamente): por ejemplo reconocimiento de huella dactilar, facial…



El usuario tiene en su poder una tarjeta de coordenadas para el acceso.

Imagen sacada de: http://www.supervielle.com.ar/Personas/Bancaelectronica/tarjeta-coordenadas/

4.2 PRINCIPALES MEDIDAS DE SEGURIDAD

Otras medidas de seguridad son:

- **Encriptación de datos**.

Las bases de la encriptación de los datos es conseguir:

Confidencialidad: que solo pueda acceder a la información su destinatario.
Autentificación: que tanto el emisor como el receptor pueda confirmar la identidad de la otra parte.
Integridad: que la información no pueda ser alterada sin ser esto detectado.

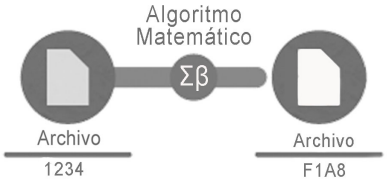
Tras un proceso de encriptación lo que se realiza es una transformación de un archivo mediante una clave o algoritmo para que sea ilegible sin este. Lo necesario para mantener la seguridad de todos los datos es encriptarlos antes de almacenarlos en los servidores, con lo cual, si alguien consiguiese acceder a uno de estos datos sería ilegible para él sin esa clave de cifrado que se le aplicó antes de almacenarlo. La mayoría de los algoritmos modernos de cifrado se basan en una de las siguientes categorías de procesos:

- Problemas matemáticos simples pero que tienen una inversa que es complicada de obtener. Esta es la que se usa para la mayoría de los métodos de cifrado de claves públicas.
- Secuencias que son en parte definidos por los datos de entrada. Esta sufre a menudo de correlaciones teóricas entre la entrada y la salida.

A continuación nombramos tres métodos de encriptación:

- Algoritmo HASH:

  Este algoritmo realiza unos cálculos matemáticos sobre los datos produciendo una secuencia de datos alfanuméricos único para ese archivo. Este cifrado es unidireccional y no se puede descifrar, siendo un uso común de este algoritmo el cifrado de contraseñas almacenadas en servidores. A las contraseñas introducidas en los campos de acceso para usuarios se aplican los mismos cálculos matemáticos y se comparan con el valor almacenado, de manera que si coinciden, la contraseña introducida es la correcta y, por tanto, el acceso será posible.

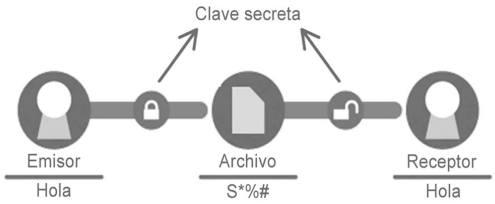


Realizada con herramientas de tratamiento de imágenes por nosotros

- Encriptación Simétrica:

  El emisor del archivo es el encargado de generar la clave. Este método se caracterizan por usar tanto para cifrar como para descifrar la misma clave, por ello hay que mantener esta clave en secreto. Este método es menos seguro por la necesidad de enviar la clave de cifrado, con el riesgo de poder ser interceptada por otras personas. Sus principales características son:

  ⇒ rápidos y fáciles de implementar.
  ⇒ usa la misma clave para cifrar y descifrar.
  ⇒ cada par de usuarios debe de tener una clave secreta compartida.



http://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura

- Encriptación Asimétrico (RSA):

Este algoritmo requiere de dos claves:

- una clave Privada (única y personal, sólo conocido por su propietario)
- una clave Pública.

El Destinatario se encarga de generar ambas claves. La clave pública es enviada a la persona que enviará posteriormente el archivo y es usada para el cifrado. La clave privada pertenece al destinatario del archivo y permite descifrar el archivo. Ambas claves están relacionadas por una fórmula matemática que garantiza que esta pareja de claves no se volverán a producir.

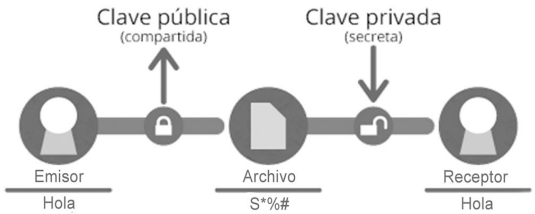


*Imagen sacada de:*http://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura

Ejemplos de software para encriptar archivos en la nube son:

-Secret Sync: es un software de encriptación que funciona solo sobre Dropbox. Crea un directorio llamado SecretSync en el que se sitúan los archivos que deseamos proteger. Acto seguido el programa crea un archivo ya encriptado en Dropbox en base nuestro archivo.

-Boxcryptor: soporta todos los principales proveedores de almacenamiento en la nube como Dropbox, Google Drive, Microsoft SkyDrive,SugarSync. Este sistema crea una carpeta cifrada en el ordenador donde los archivos son cifrados de forma local antes de ser subidos a la nube. Boxcryptor utiliza algoritmos de encriptación AES-256 y RSA,

Imagen sacada de:https://www.singlesplace.nl/gratis-veilig-daten-via-ssl

- **Conexión segura entre el usuario y la nube como medida de seguridad**

A Través de una conexión segura entre el extremo del cliente y la nube podemos evitar que el tráfico de datos que se realice sea interceptado por terceras personas. Para ello se puede usar protocolos como:

⋆**SSL (Secure Sockets Layer) :**Es un protocolo criptográfico que nos proporciona autentificación y seguridad de la información en las comunicaciones que se realizan en internet mediante el uso de criptografía.

⋆**TLS (Transport Layer Security)** :En español se podría traducir como Seguridad en la Capa de Transporte y es una evolución del protocolo SSL .

Tanto SSL/TLS realizan tres fases básicas:
Negociación: El extremo del cliente y del servidor negocian qué algoritmos criptográficos utilizarán para autenticarse y el cifrado de la información.

Autenticación y Claves: el cliente y el servidor se autentican mediante certificados digitales y realizan el intercambio de las claves para el cifrado.

Transmisión Segura: los extremos inician el tráfico de información cifrada y autenticada.

El protocolo SSL/TLS es usado por otros protocolos como:

- HTTP, que sobre SSL/TLS es HTTPS, ofreciendo seguridad a páginas web
- SSH, utiliza SSL/TLS por debajo.

A continuación, hacemos un pequeño inciso para nombrar un conocido caso de inseguridad sobre una librería que hace uso del cifrado SSL/TLS para asegurar los datos datos.

Caso Heartbleed *Imagen sacada de: http://heartbleed.com*

Se trata de un agujero de seguridad en el código de la biblioteca de OpenSSL en su versión 1.0.1f. Este agujero permitía a un hacker acceder a la memoria de un servidor. Empresas que usaban esta versión tras saber de su vulnerabilidad han descubierto que atacantes han accedido a datos almacenados en sus servidores a través de este agujero.

Este agujero fue causado por un estudiante de la universidad de Duisburg-Essen, el cual implementó una extensión para OpenSSL. Esta modificación fue revisada por una de las personas que desarrolló el núcleo de OpenSSL, Stephen N. Henson, el cual validó e introdujo el 31 de diciembre de 2011 esta implementación, sin notar el agujero. Un empleado de Google encontró el agujero de esta implementación el 1 de abril de 2014.

A través de este agujero se permitía obtener 64 kilobytes de memoria del servidor, esta información leída del servidor podría tratarse de información comprometida. Entre los datos que podían ser robados está la clave maestra del propio servidor, con la que se puede llegar a permitir a un atacante descifrar el tráfico de datos en el servidor o el almacenado. Al poder descifrar información enviada por el usuario esta podía tratarse de contraseñas y nombres de usuarios, con la cual se puede realizar una suplantación de identidad del usuario.

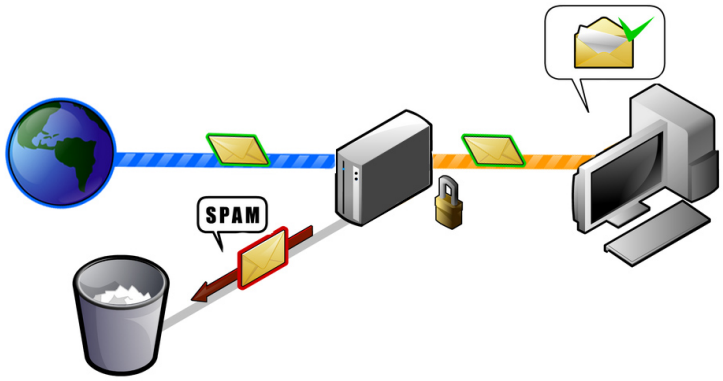


Imagen sacada de: http://www.gaffstrategy.it/5-motivi-per-non-comprare-liste-email/

- **Antispam**

Método destinado a evitar el correo electrónico basura en la bandeja de entrada. Este tipo de correos pueden llegar a saturar o colapsar servidores de correo electrónico dejándolos fuera de servicio. “El número de spam va en aumento, por lo que es necesario tener al alcance las herramientas necesarias para evitar este tipo de mensajes, como el antispam hosteado en la nube, que bloquea 99% de éstos”, así lo indicó, Gerardo Sandoval, director ejecutivo de IguanaHostig.com. Este tipo de servicios son muy importantes para las empresas debido a que sus empleados consultan frecuentemente el correo, llegando a dedicar importantes cantidades de tiempo en la eliminación de este tipo de correos. La productividad y rendimiento de la empresa pueden llegar a verse afectadas por esta causa.

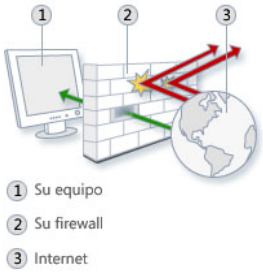
- **Backup (copia de seguridad)**

Una Backup es una copia exacta de los datos originales. Se hacen copias de seguridad de los datos para poder recuperarlos en caso de que se pierdan o se dañen los originales. Algunas de las causas que pueden suponer la pérdida de estos datos pueden ser por alguna catástrofe, por eliminación accidental, infección de nuestro sistema por un virus o cualquier otra causa que nos deje inservibles estos archivos originales.

- **Firewall**

Un firewall es un software o un hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.
Un firewall puede ayudar a impedir que hackers o software malintencionado obtengan acceso al equipo a través de una red . Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos a través de la red.

Imagen sacada de: http://windows.microsoft.com/es-es/windows/what-is-firewall#1TC=windows-7



- **WAF**

Es una aplicación firewall. Se trata de una herramienta para proteger su página web de peticiones con malas intenciones, analizando estas una vez han traspasado el **Firewall de red.** Tiene la opción de activarse y desactivarse desde el panel de control. El sistema WAF puede ser más o menos eficiente en base a las reglas que tiene para las peticiones permitidas sobre el servidor. Por contra este sistema puede dar falsos positivos sobre peticiones que cree ser ilícitas (no teniendo porqué serlo). El sistema en caso de dar positivo bloquea la dirección IP, la cual se añade en una blackList.
Cuando se detecta que una petición al servidor se considera ilícita, al cliente se le redirige a una página donde se verifica que no se trata de un robot.
Después de confirmarse que este usuario no se trata de un atacante, esta dirección IP se añade a una lista blanca para que no se vuelva a repetir su bloqueo.

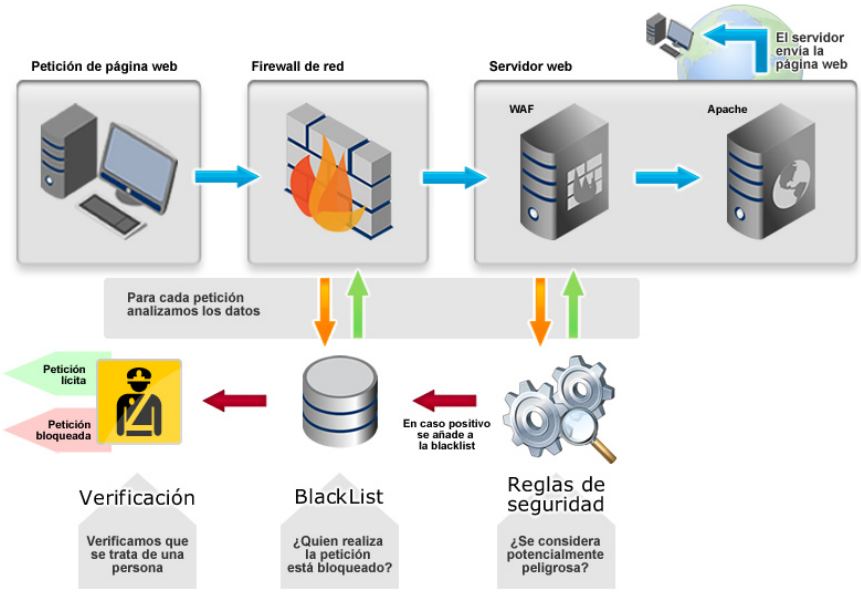


Imagen sacada de:
https://support.cdmon.com/entries/25196051-Firewall-de-Aplicaci%C3%B3n-Web-WAF-

5. BIBLIOGRAFÍA

- http://encripdedatos.blogspot.com.es
- http://www.safenet-inc.es/multi-factor-authentication/
- Libro : Cloud Computing, tecnología y negocio, Marta Beltran, Fernando Sevilano, capítulo 1 Qué es Cloud Computing
- Libro : Cloud Computing, tecnología y negocio, Marta Beltran, Fernando Sevilano, capítulo 2 Arquitectura hardware y software del Cloud
- Libro : Cloud Computing, tecnología y negocio, Marta Beltran, Fernando Sevilano, capítulo 5 Riesgos y beneficios de la migración en un entorno Cloud
- http://www.safenet-inc.es/data-protection/cloud-security/
- http://www.trendmicro.es/tecnologia-innovacion/nube/
- http://www.globbtv.com/microsite/33/Adjuntos/1_AMENAZAS%20Y%20CSA_LUIS%20BUEZO.PDF
- https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf
- https://www.gnupg.org/gph/es/manual.html
- Libro: ¿Que es la nube?El futuro de los sistemas informáticos, Barrie Sosinsky, capítulo 15 Trabajar con el almacenamiento basado en la nube
- Libro: Computación en la nube, Luis Joyanes Aguilar, capitulo 8.3 Aseguramiento de los datos en la nube.
- Libro: Computación en la nube, Luis Joyanes Aguilar, capitulo 8.8 Cumplimiento de regulaciones y estándares
- http://www.digitalattackmap.com/understanding-ddos/
- https://www.owasp.org/index.php/Web_Application_Firewall
- http://support.apple.com/es-es/HT1766
- http://www.segu-info.com.ar/malware/spam.htm
- http://php.net/manual/es/security.database.sql-injection.php
- http://pressroom.hostalia.com/wp-content/themes/hostalia_pressroom/images/inyeccion-sql-wp-hostalia.pdf