Instituto Tecnológico de Chihuahua 2. Ingeniería Informática. Programación en Ambiente Cliente/Servidor. **Medidas de seguridad en servicios web y locales.** Presenta: Nohemí Berenice Varela González, 13550649. 29/08/17.

MEDIDAS DE SEGURIDAD QUE PUEDEN IMPLEMENTARSE EN SERVICIOS DE LOS PROVEEDORES PRIVADOS:

1. AWS

Estas han sido las cinco claves para un uso eficiente y seguro de la nube:

* 1. Aplica seguridad en todas las capas: En lugar de emplear simplemente un firewall en el los límites de la infraestructura, sitúa firewalls en cada una de las redes virtuales que crea el escritorio.
  2. Habilita la rastreabilidad y refuerza los privilegios del administrador: Emplea etiquetas para indicar qué usuarios han creado y accedido a qué archivo y cuándo; define también los permisos que tienen cada usuario para según qué funciones. Emplea el acceso más estricto posible para cada cambio de configuración, añade necesidad de autorización y necesidad de autentificación para las funciones más importantes.
  3. Monitoriza y exige registrarse como usuario para todas las acciones y cambios del escritorio: Programa alarmas para que en caso de haber actividad inusual sea detectada dentro de los registros.
  4. Crea plantillas personalizadas de las imágenes de los servidores virtuales: Emplea estas imágenes automáticamente cuando un nuevo servidor esté disponible. El servicio AMI de Amazon creará automáticamente modelos re usables para cualquier instancia EC2 (el servicio de instancias de la compañía)  de manera que aparezcan con los ajustes de seguridad ya pre instalados. El fin es crear un entorno que se maneje completamente mediante modelos ya prestablecidos.
  5. Encripta toda la información sensible: Si lo desean, los usuarios pueden encriptar sus datos según su propia configuración y así enviar solo información encriptada a la nube; de este modo, el cliente puede guardar las llaves de la encriptación detrás de sus firewalls empleando el Hardware Security Module de AWS.

1. BLUEMIX

Descripción de las Medidas de Seguridad

* Este Servicio de Cloud puede utilizarse para procesar contenido que contenga datos personales si el Cliente, como responsable del tratamiento de datos, determina que las medidas de seguridad técnicas y organizativas son apropiadas para los riesgos presentados por el procesamiento y la naturaleza de los datos a proteger.
* El Cliente reconoce que este Servicio de Cloud no ofrece prestaciones para la protección de datos personales sensibles o datos sujetos a requisitos regulatorios adicionales.
* El Cliente acepta que IBM no tiene conocimiento de los tipos de datos que se han incluido en el contenido y no puede hacer una evaluación de la idoneidad de los Servicios de Cloud o las protecciones de seguridad que están en vigor.
* El componente de pasarela segura opcional proporciona la capacidad de permitir a los usuarios conectarse a las aplicaciones locales dentro de su propio firewall.
  + El uso del componente de pasarela segura está sujeto a una limitación de uso de 1 GB al mes.
  + El componente de pasarela segura proporciona una conexión cifrada entre el sistema local y el entorno de Servicio de Cloud para una transmisión más segura de los datos entre una aplicación local y el Servicio de Cloud.
  + El uso del componente de pasarela segura opcional corre a cuenta y riesgo del Cliente.
  + El Cliente se compromete a mantener a IBM indemne frente a sus daños y frente a cualquier reclamación de un tercero que surja o esté relacionada con el uso de este componente por parte de un Cliente o con su decisión de utilizar comunicaciones no cifradas o no seguras entre dispositivos/aplicaciones y el Servicio de Cloud.

1. GOOGLE
   1. Todas las conexiones a Google Drive se cifran mediante el protocolo de transporte SSL, no importa si accedemos desde el navegador web, las aplicaciones de escritorio o las móviles.
   2. Una vez alojados en los servidores de Google, todos los datos son cifrados, y aunque los de Mountain View no son muy dados a pregonar los algoritmos y configuraciones que utilizan, se entiende que cumplen con los estándares que marca la industria.
   3. Ahora Google Drive, viene configurada por defecto para cifrar también los documentos sin conexión que se almacenan en la memoria del teléfono, además de ofrecer la opción de descifrado de flujo -o cifrado de stream-, suponemos para facilitar el uso del servicio en modo colaborativo o acelerar el acceso a los contenidos.

MEDIDAS DE SEGURIDAD EN SERVIDOR EN ARQUITECTURA LOCAL

Estos son algunos de los puntos más importantes que tendríamos que revisar en nuestras redes para saber si cumplimos con los mínimos de seguridad que una red debe disponer:

1. Tener un servidor de datos, en el cual guardamos todos los datos relevantes de la instalación y con su consiguiente proceso de copias bien definido.
2. Tener montado en dicho servidor un DOMINIO, para la correcta administración de permisos de usuarios y facilidad de administración de la red local.
3. Tener cortafuegos (físico o por software) para separar red local de la red de internet y tener control sobre los accesos a datos relevantes e internet por parte de los usuarios de la red local.
4. Tener programa de antivirus “ACTUALIZADO” en todos los puestos de la red local, incluso en el servidor, para estar protegido casi al 100% sobre amenazadas de virus.
5. Todos los puestos de la red deben tener sistema operativo profesional (xp, vista o win7), para la correcta validación de los usuarios en el “Active Directory” (dominio).
6. Tener una política de contraseñas adecuada, cada usuario de la red local con su contraseña personal y además que esta caduque cada cierto tiempo (se puede definir).
7. Tener una política de copias de seguridad definida y externalizada para posibles “desastres extremos” (robo, fuego….)
8. Llevar un correcto mantenimiento de los pc´s, actualizaciones de software y hotfix que van surgiendo (serviPack´s de Windows).
9. Tener a alguien de la empresa o externalizada que controle los procesos de copia para detectar posibles problemas, actualización de antivirus, centralizar incidencias de la red local y así poder avisar a servicio técnico y llevar control sobre la resolución de las mismas.
10. Tener localizadas todas las licencias de programas instalados en la red por posibles inspecciones por la autoridad competente (BSA)

Fuentes:

<http://www.computerworld.es/tendencias/cinco-claves-de-seguridad-para-tu-cloud-aws>

<http://www-03.ibm.com/software/sla/sladb.nsf/pdf/7764-01/$file/i126-7764-01_06-2017_es_ES.pdf>

<http://muyseguridad.net/2012/04/26/seguridad-google-drive/>

<https://www.clavei.es/blog/2011/los-10-mandamientos-para-tener-una-red-local-segura/>