No.20 / abril-mayo 2014 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

20

Ambientes óptimos

De la incertidumbre a la acción segura

Internet profunda | Entornos virtuales | Vender seguridad | Prevención de copyright | Hablando correctamente | Seguridad en salud

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Ambientes óptimos
De la incertidumbre a la acción segura

En nuestro mundo digital, y también en el físico, estamos rodeados de múltiples entornos, lugares en donde aprendemos, crecemos profesionalmente, donde convivimos todos los días, sitios que nos falta conocer, otros a los que siempre volvemos, en fin. Un mapa que no podríamos navegar sin el uso de la tecnología y que, desafortunadamente, se encuentra en constante riesgo.

Es la naturaleza de nuestro tiempo, tratar de convertir esta simbiosis con lo digital en mejoras para nuestra vida. Es el reto que nos hemos propuesto en la edición 20 de la revista .Seguridad, hacer de lo cotidiano el mejor de los caminos, y de lo nuevo, una mejora constante. Probablemente, los temas que encontrarás en este número emerjan en una gran interrogante de fallas de seguridad de nuestros días, pero también, son una buena oportunidad para optimizar nuestro futuro.

Sin embargo, óptimo en los brazos de la seguridad, no quiere decir inquebrantable. Sabemos que pese a nuestro esfuerzo, no hay garantías totales para lo que cambia todos los días, pero sí existe la satisfacción de hacer de nuestro ambiente, lo mejor en favor de nuestra protección.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 20 / febrero - marzo 2014 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829

Seguridad informática en entornos virtuales

Enrique Sánchez Gallardo

La proliferación de nuevas tecnologías en las distintas áreas que conforman las soluciones actuales de TIC (tecnologías de información y comunicación), trae como consecuencia nuevos retos que las direcciones deben asumir y solventar llegado el momento de su instrumentación.

“Aun cuando el término virtualización ha sido acuñado en el contexto de los sistemas mainframe de IBM, introducidos en la década de los 60’s” (Polze y Tröger, 2012), uno de los retos actuales es el aseguramiento de este tipo de entornos, que a diferencia de la infraestructura física, plantea nuevos desafíos. En contraste con los entornos físicos, los entornos virtuales basan su operación en infraestructura física unificada, es decir, un servidor físico puede contener uno o varios sistemas operativos hospedados en una misma plataforma. Aquí el tema de seguridad de ambientes virtuales juega un papel importante.

Seguridad en máquinas virtuales

Las máquinas virtuales (virtual machines), a diferencia de un equipo físico, están reducidas a un simple archivo; que si bien representa flexibilidad para el administrador, también significa una vulnerabilidad que puede ser explotada para robar la máquina completa, incluyendo su contenido. Recordemos que en los entornos virtuales, varias máquinas virtuales pueden compartir una sola interfaz física (Figura 1), en consecuencia, dichos equipos pueden ser víctimas de diversos tipos de ataques entre una máquina virtual y otra residente en el mismo equipo físico, ante esta situación, el administrador debe estar prevenido.

Por otro lado, la seguridad virtual se extiende más allá de las máquinas virtuales, por ejemplo, los sistemas de almacenamiento en red se ven

expuestos a amenazas y constituyen otra línea de acción para los atacantes.

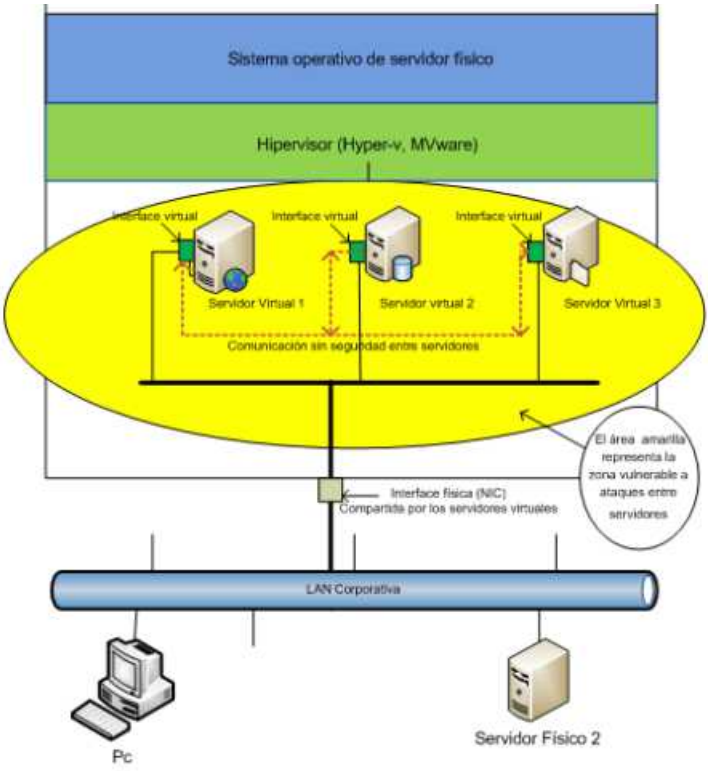


Figura 1. Servidores virtuales en un mismo servidor físico sin seguridad entre ellos.

Una recomendación es mantener los sistemas de almacenamiento separados del resto de las máquinas virtuales.

En un esquema virtual, en donde se utilizan equipos para ejecutar las tareas de procesamiento de las máquinas virtuales (y su almacenamiento se encuentra en un almacenamiento de red SAN[1]), es fácil ver cómo se ve comprometido todo el sistema de almacenamiento cuando no se contemplan este tipo de riesgos, sobre todo al momento de la instrumentación de entornos virtuales basados en sistemas de almacenamiento separado.

En este tipo de esquemas de operación, existe un servidor denominado “Servidor de procesamiento” que puede contener una o varias máquinas virtuales y un “Sistema de almacenamiento” (por ejemplo, uno del tipo SAN). Este sistema es un equipo físico separado del servidor de procesamiento, cuya función es alojar los archivos de cada una de las máquinas virtuales a través de interfaces, ya sea de tipo iSCSI[2] o Fiber Channel. Al interconectarse con el servidor de procesamiento, utiliza canales de comunicación que nuevamente quedan vulnerables ante cualquier posible ataque (Figura 2).

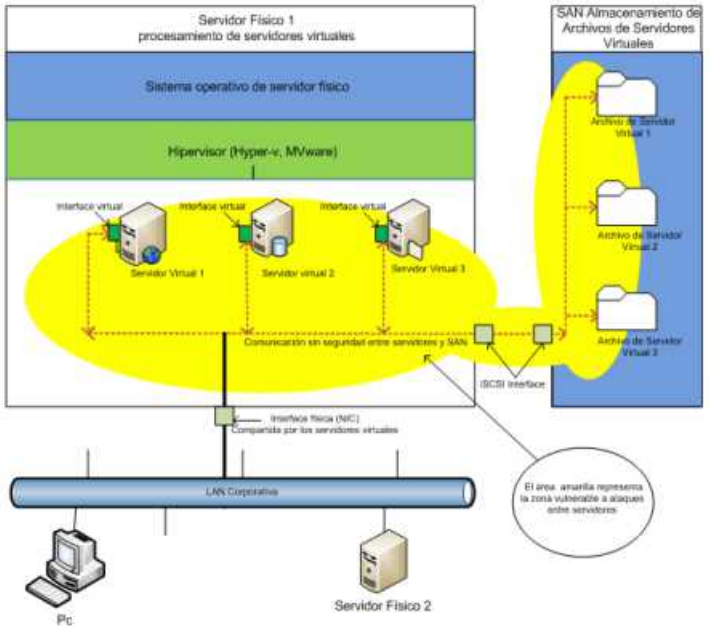


Figura 2.Esquema de servidores virtuales con procesamiento en un servidor y almacenamiento en una SAN.

En los entornos de cómputo en la nube, los cuales involucran sistemas operativos para el servidor físico, máquinas virtuales y aplicaciones, es necesario considerar el aspecto de seguridad para la virtualización.

Aplicación de seguridad en entornos virtuales

Sabnis, S., Verbruggen, M., Hickey, J. and McBride, A. J. (2012), hacen mención de algunos aspectos para la aplicación de seguridad en entornos virtuales al inicio de su diseño, por ejemplo: clasificación del tráfico e información real entre máquinas virtuales, mecanismos de autentificación y controles de acceso robustos, controles para el acceso y la operación, corrección de vulnerabilidades e instalación de actualizaciones de seguridad, así como configuración de auditoría y escaneo de vulnerabilidades.

Se debe considerar la utilización de VLANs[3] para la separación del tráfico entre máquinas virtuales, lo que permitirá cierto nivel de aislamiento entre cada una de ellas. La utilización de *firewalls* personales en cada una de las máquinas también constituye una línea de defensa, puede

administrar el tráfico de red permitido desde y hacia cada una de las máquinas. Otra opción es el empleo de switches virtuales, éstos pueden segmentar la red y controlar el tráfico, sobre todo cuando varias máquinas virtuales hacen uso de una sola interfaz física (Figura 3). Mantener actualizados los sistemas también representa un menor riesgo en ambientes virtuales.

Se puede hacer uso de herramientas comerciales para ayudar a resolver este tipo de problemas de seguridad virtual, tanto en entornos virtuales puros como en mixtos.

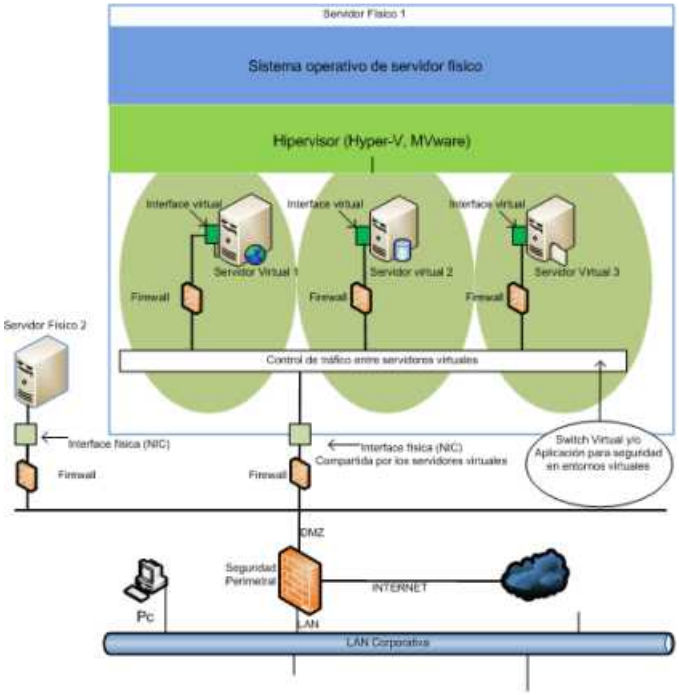


Figura 3. Esquema de servidores virtuales con mecanismos de seguridad instrumentados.

¿Qué hacer para asegurar los entornos virtuales?

Al igual que cualquier componente físico de TI, se debe comenzar con un plan de instrumentación de seguridad para los entornos virtuales, un buen punto de inicio es consultar a los principales proveedores de soluciones, los cuales son unos de los primeros involucrados en el tema debido a la relevancia que tiene la seguridad en ambientes virtuales.

Algunos documentos como VMWareSecurity BestPractices, Hyper-V Security BestPractices (2010) y otros disponibles en los diferentes portales, permiten a los administradores de TI evaluar el tema y comenzar, en el caso de no haber considerado antes la instrumentación de seguridad para sus entornos virtuales.

Ejemplos de soluciones aplicables a seguridad virtual

Shavlik Technologies: ShavlikNetChkConfigure es una solución para la gestión de configuraciones que audita y hace cumplir las configuraciones de seguridad en una red.

Sistema de respaldo BackupExec 12.5 de Symantec Corp.: Esta solución de Symantec permite el respaldo de servidores virtuales a través de la instalación de un cliente enfocado específicamente a entornos virtuales.

VMware: VMware vCloud Networking and Security Edge ofrece una puerta de enlace de servicios de seguridad para proteger el perímetro del centro de datos virtual.

Check Point: Secure Virtual Network (SVN) asegura las comunicaciones *business-to-business* entre redes, sistemas, aplicaciones y usuarios a través de Internet, intranets y extranets.

Microsoft: Microsoft integra servicios de seguridad a entornos virtuales, en algunos casos integrados a sus soluciones, por ejemplo en Hyper-v a través de Windows Authorization Manager y en otros, con la integración de soluciones de terceros.

Dado que la complejidad de los sistemas de tecnología va en aumento, se podría decir que la seguridad en entornos virtuales se ha colocado en la cima de dicha complejidad. Requiere, por parte de los administradores de sistemas, una interacción con los sistemas virtuales igual o mayor a la que demandan los ambientes físicos, pero con un nivel de abstracción superior. Los administradores requieren, en principio, de un buen o excelente entendimiento de los sistemas tradicionales para una mejor comprensión de los entornos virtuales.

Es importante mencionar que el tema de seguridad virtual tratado en este artículo es sólo una introducción a esta área de la tecnología, pues bien podría ser considerada como un área de especialidad para los administradores de sistemas. En tal caso se deben tomar en cuenta, entre otros aspectos: el análisis de vulnerabili-

dades en entornos virtuales, políticas, tecnologías y mejores prácticas, así como tomar en cuenta que este tipo de entornos no operan de igual forma que los físicos. Sin embargo, al igual que en éstos últimos, existen herramientas que ayudan a proteger y mantener la integridad de los entornos virtuales a través de una buena administración de la seguridad virtual.

[1]SAN (Storage Area Network), Sistema de Almacenamiento en Red
[2]Abreviatura de Internet SCSI: es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP
[3]Acrónimo de virtual LAN (red de área local virtual)

Referencias

Polze, A. and Tröger, P. (2012), Trends and challenges in operating systems—from parallel computing to cloud computing. Concurrency Computat.:Pract. Exper., 24: 676–686. doi: 10.1002/cpe.1903

Sabnis, S., Verbruggen, M., Hickey, J. and McBride, A. J. (2012), Intrinsically Secure Next-Generation Networks. Bell Labs Tech. J., 17: 17–36. doi: 10.1002/bltj.21556

Server virtualization security best practices. Recuperado de: http://searchservervirtualization.techtarget.com/tutorial/Server-virtualization-security-best-practices-guide
Shavlik Technologies. Recuperado de: http://totemguard.com/soporte/files/Shavlik_NetChk_Configure.pdf

Symantec Backup Exec 12.5 for Windows Servers. Recuperado de: http://ftpandina.atv.com.pe/ManualesIT/ManualLTo.pdf

Seguridad y cumplimiento normativo. Recuperado de: http://www.vmware.com/latam/cloud-security-compliance/cloud-security#sthash.wrmYQ5XX.dpuf

Check Point. Recuperado de: http://www.etekreycom.com.ar/tecno/proveedor/check_point.htm

Microsoft Virtualization. Recuperado de: http://www.microsoft.com/spain/virtualizacion/solutions/technology/default.mspx

Enrique Sánchez Gallardo

Director de TI de El Colegio de Michoacán, A.C., Centro Público de Investigación CONACYT.

Es miembro del Grupo de trabajo Maagtic-SI del Consejo Asesor en Tecnologías de Información del CONACYT. Candidato a Doctor en Ciencias de la Administración por la Universidad del Valle de Atemajac, Plantel León. Maestro en Computación por la Universidad del Valle de Atemajac, Plantel Guadalajara.

Es Licenciado en Informática por la Universidad de Zamora y docente Universitario en las áreas de Ingenierías, Mercadotecnia y Administración de la Universidad del Valle de Atemajac, Plantel Zamora.

Mitos y realidades de la Internet profunda

Juan Armando Becerra Gutiérrez

Leyendas urbanas

Un concepto como *deep web* o Internet profunda suele rodearse de misticismo, todo lo que suene profundo, oculto e invisible tiene esa facultad de estimular nuestra imaginación. A lo largo del tiempo, he escuchado historias y recibido cuestionamientos sobre la naturaleza de la Internet profunda: sobre sus múltiples capas, las realidades alternas que la contienen, comparaciones con *The Matrix* y sobre las "terribles cosas que se albergan en el fondo de la red".

Internet profunda, tecnologías de privacidad, e incluso mercado negro, son conceptos que se han entremezclado y que si bien, son igual o más sorprendentes que las mismas leyendas a su alrededor, se encuentran detrás de mucha niebla.

Red profunda

Deep web es una idea a la que recurrentemente se le compara con el océano, donde existe información en la superficie, fácilmente accesible para las redes de cualquier barco, e información que requiere más esfuerzo para ser adquirida y procesada. La *deep web* es toda la información de Internet no accesible por tecnologías basadas en indexado y rastreo web (*web indexing y web crawling*) de los buscadores como Google o Bing.

La red superficial, aquella que se accede por medio de las consultas a los buscadores, se basa en las ligas y relaciones existentes entre un sitio y los hipervínculos que alberga, esta acción dio origen al término navegar en la web, saltamos de una página web a otra porque existe una interrelación directa con cada sitio indexado en un buscador.

La red profunda, por su parte, es una porción de Internet a la que sólo se puede acceder a través de la consulta exacta dentro del contenido de alguna base de datos. Para visitar una página no indexada por un navegador, hay que conocer la dirección o ruta exacta de ese sitio en particular.

Existen varias razones para que un contenido, es decir, cualquier tipo de archivo y no sólo sitios web, no sea indexado y pertenezca a la *deep web*:

- Tiene mecanismos o interfaces poco amistosas con los bots de los buscadores.
- Es un contenido aislado, sin ligas que hagan referencia a otros sitios y viceversa.
- Son subdirectorios o bases de datos restringidas.
- Son contenidos no basados en html o codificados (por ejemplo, sólo contienen JavaScript, Flash, etc.)
- Es un contenido protegido por contraseña o cifrado.

A partir de estos conceptos, podemos ver que gran parte del contenido de Internet es *deep web* (se presume que alrededor del 90%), esta información no siempre está optimizada para el uso humano o está diseñada para ser explícitamente usada bajo ciertos protocolos y tecnologías. Por ello se han desarrollado herramientas como buscadores especializados o navegadores web con características especiales, permitiendo que disciplinas como *data mining, big data u open source intelligence* utilicen todos los datos disponibles y no sólo los más evidentes proporcionados por los buscadores tradicionales.

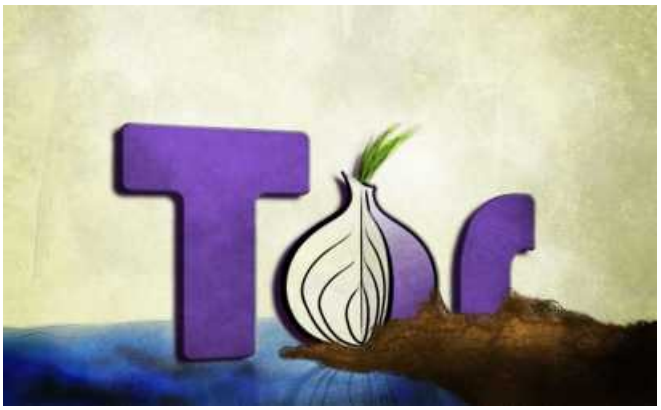
Red oscura

Dentro de la red profunda hay una clase especial de contenidos que han sido diseñados para permanecer ocultos o en secciones separadas de las capas públicas de Internet. Como se ha explicado anteriormente, una página sin una *URL* conocida permanece oculta de los buscadores. Por ejemplo la entrada de un blog sin publicar o un tuit en borrador son elementos que existen en Internet, pero que no pueden ser hallados debido a que la *URL* sólo es conocida por el creador de dicho contenido. Este tipo de datos son los que forman parte de la *red oscura, oculta o invisible.*

Las redes virtuales privadas (virtual private networks o VPN) son tecnologías que corresponden a esta clasificación de red oscura y de hecho, son sus principales representantes. Estas redes corresponden a infraestructura y contenidos que se pueden acceder únicamente a través de un software específico, uno de los ejemplos más representativos es TOR.

TOR, The Onion Router

TOR es un proyecto diseñado e implementado por la marina de los Estados Unidos, posteriormente fue patrocinado por la EFF (*Electronic Frontier Foundation*, una organización en defensa de los derechos digitales). Actualmente subsiste como TOR Project, una organización sin ánimo de lucro galardonada en 2011 por la *Free Software Foundation* por permitir que millones de personas en el mundo tengan libertad de acceso y expresión en Internet manteniendo su privacidad y anonimato.



TOR es una red de túneles virtuales que permite a los usuarios navegar con privacidad en Internet, a los desarrolladores, crear aplicaciones para el intercambio de información sobre redes públicas sin tener que comprometer su identidad, ayuda a reducir o evitar el seguimiento que hacen los sitios web de los hábitos de navegación de las personas y a publicar sitios web y otros servicios sin la necesidad de revelar su localización.

Si bien el objetivo de TOR es proteger a los usuarios de la vigilancia en Internet (por ejemplo, del análisis de tráfico), también se ha utilizado

para mantener ocultos diferentes servicios de dudosa legalidad.

La *red oscura* no trata formalmente de crimen, pero las propiedades de privacidad y anonimidad de tecnologías como TOR la han convertido en una esquina fangosa en el uso de la tecnología, a tal grado que *dark web* y mercado negro muchas veces pueden usarse como sinónimos.

Mercado negro y el abuso de la privacidad

Los objetivos de TOR como proyecto de software libre son admirables, han sido reconocidos por ello en múltiples ocasiones, sin embargo la posibilidad de navegar y crear servicios anónimos ha permitido el desarrollo de diferentes actividades, por ejemplo: pornografía infantil, venta de drogas, tráfico de información sensible o clasificada, lavado de dinero, armas, entrenamiento especializado en temas delictivos, entre otros. El mercado negro tradicional ha encontrado un lugar fértil para expandirse utilizando estas plataformas.

Pese a que no hay cifras exactas sobre el crecimiento o popularización de la red profunda como plataforma de intercambio, definitivamente hay un antes y un después con la utilización de *bitcoins*, una moneda electrónica descentralizada que tiene sus orígenes en 2009, pero que se ha vuelto todo un fenómeno desde 2012. *Bitcoin* (que hace referencia tanto a la moneda como a la red de intercambio) no está respaldada por ningún gobierno o emisor central, como suele ocurrir con cualquier otra moneda. Las transacciones con *bitcoins* son directas entre un usuario a otro, sin ninguna institución mediadora, los *bitcoins* se transforman en dinero de uso corriente (como dólares o pesos) a través de portales que hacen la transformación.

El comienzo de la utilización de *bitcoins* como medio de pago representa el gran cambio para el mercado negro digital. TOR proporciona una plataforma para que diferentes criminales den a conocer sus productos e intereses y los *bitcoins* han optimizado los medios de pago, permitiendo transacciones de difícil seguimiento.

Palabras finales

Este artículo ha ido avanzando desde las aguas más superficiales hasta algunas más turbias, tratando de mostrar que la *deep web* no es una región prohibida y mística de Internet, ni que la tecnología relacionada es malévola.

Si bien se ha abusado de herramientas como TOR (recientemente se arrestó al dueño de una compañía que proporcionaba almacenamiento para los servicios de TOR bajo cargos de pornografía infantil) también ha permitido a los ciudadanos mantener comunicación cuando los gobiernos totalitarios han restringido el uso de las comunicaciones. Por un lado, tenemos a las agencias antidrogas que afirman que los portales dentro de la red oscura serán un problema en el tema de narcotráfico y, por el otro, el número de personas que han descargado herramientas del proyecto TOR a raíz de los escándalos de espionaje de la NSA han aumentado drásticamente.

Más allá de las controversias sobre privacidad, la *deep web* es, principalmente, un cúmulo de

información que puede ser aprovechada por investigadores y entusiastas, un área de trabajo emocionante y poco entendida por el público en general debido a todas esas leyendas que giran alrededor de ella.

Referencias

Rodríguez Darinka, El lado oscuro del comercio en internet

https://www.torproject.org/ EFF

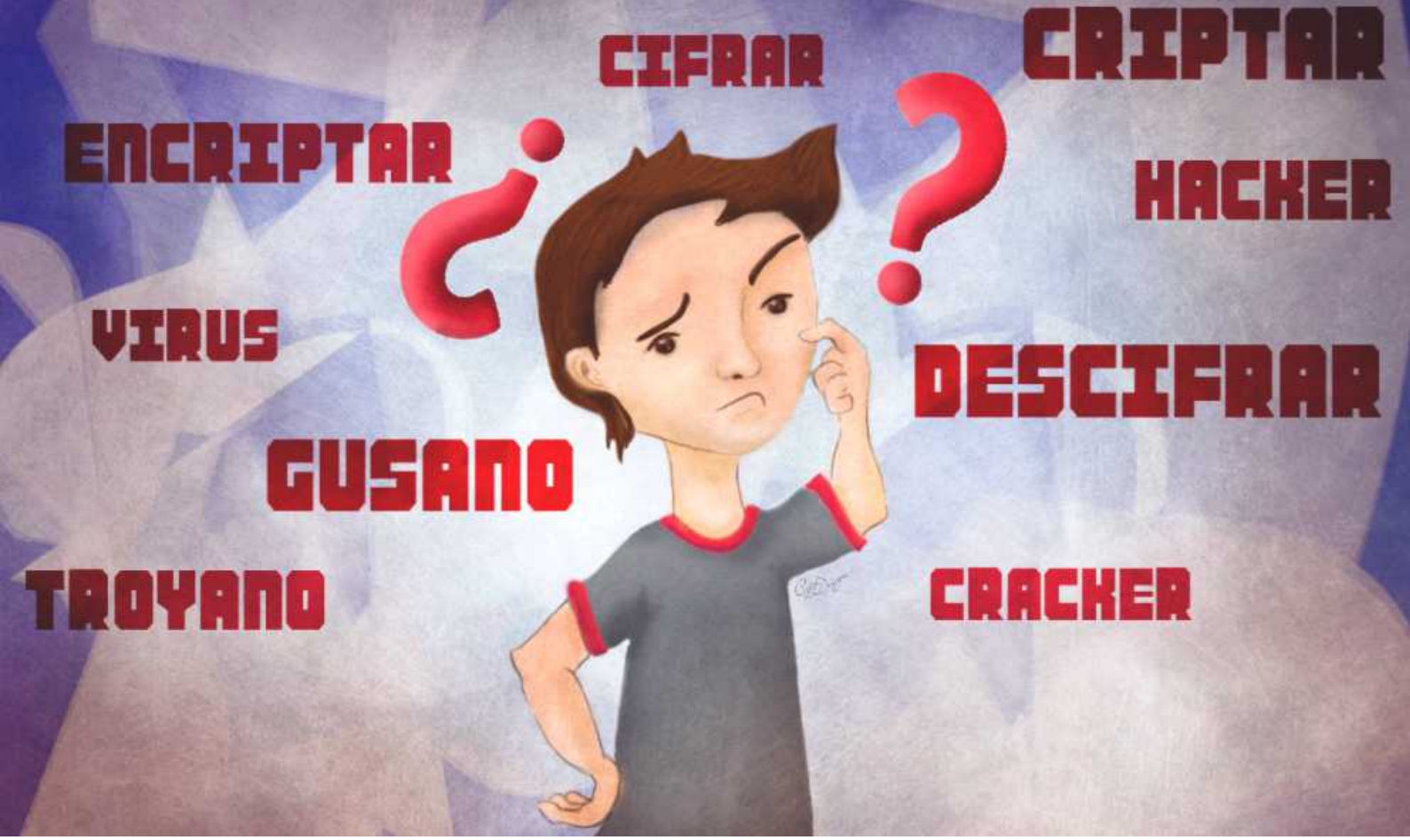
https://www.eff.org/ Deep Web Search

http://deep-web.org/

http://www.dineroenimagen.com/2013-08-22/24860

Juan Armando Becerra

Es ingeniero en telemática egresado de UPIITA del IPN, tiene experiencia en empresas de rastreo satelital, telecomunicaciones y desarrollo de software. Actualmente colabora en la Dirección General de Autorregulación del IFAI como consultor en seguridad, privacidad y protección de datos. Síguelo en Twitter como @breakpool



Hablando correctamente de seguridad de la información

José Luis Sevilla Rodríguez

En el ámbito de la seguridad de la información, el mal uso del lenguaje es una práctica que suele suceder al tratar de explicar cómo funcionan ciertos dispositivos, durante la elaboración de un artículo o documento; o simplemente conversando con otra persona sobre un tema en específico. Cuando hablamos de cosas relacionadas con seguridad de la información, se suelen utilizar términos con diferentes significados de manera indistinta o incorrecta. Es nuestro trabajo concientizar a los usuarios sobre la correcta utilización de algunos términos. En esta ocasión trataré de explicar la criptografía, el malware y las evaluaciones de seguridad de la información, así como también proporcionar los significados correctos.

"Errores que cometen especialistas, ingenieros, administradores, etc."

Encriptar y desencriptar

El principal error que cometen los especialistas de seguridad, ingenieros en computación, administradores de servidores, entre otros, es mencionar *encriptar* o *encripción* para referirse a la acción de **ocultar información sensible mediante un algoritmo de cifrado**. En el diccionario de la lengua de la Real Academia Española (RAE) dichas palabras no están registradas, aunque muchas fuentes en Internet manejan estos términos. En diversas conferencias y capacitaciones de seguridad de la información a las que he asistido, he escuchado los términos *encriptar* y *desencriptar*, además de otros que se utilizan como si fueran sinónimos. Mi teoría sobre estos errores radica en que las palabras en inglés para la acción ya mencionada es *encrypt* y su contraparte *decrypt*. Así, es posible que se quieran traducir como cognados debido a que la mayoría de la

información sobre temas relacionados a seguridad se encuentra en inglés.

El término encriptar está compuesto del prefijo *en* y de la palabra *cripta* (un lugar subterráneo en donde se puede enterrar a los muertos), es decir, significa enterrar en un cripta. Sin embargo, la etimología de la palabra *criptografía* viene del griego κρύπτος (kryptós), que significa oculto. Por tanto, la palabra encriptar no cumple con el significado de criptografía.

De acuerdo a la RAE, cifrar se refiere a "transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar". Por lo tanto, en el argot de seguridad y con base en mi experiencia, la forma correcta de referirse en español a la acción de ocultar y revelar información mediante un algoritmo de cifrado, es cifrar y descifrar.

Virus, gusano y troyano

Cuando un usuario detecta comportamiento inusual en su computadora suele atribuirlo a un *virus*, aunque el equipo de cómputo no haya sido revisado por un especialista o el antivirus no lo haya determinado. Lo más probable es que sea una víctima de **software malicioso**, existen muchos tipos distintos. Para entender con claridad el problema que tiene el equipo, es importante saber cuáles son las diferencias entre algunos términos.

Virus:

- Requiere la intervención del usuario para ejecutarse o propagarse.
- Se copia en el equipo sin el consentimiento del usuario para causar acciones maliciosas.
- Suele esconderse dentro de ciertos procesos del sistema operativo (por ejemplo svchost.exe o explorer.exe en Windows).

Gusano:

- Programa malicioso que se replica a sí mismo y se propaga sobre una red.
- Explota vulnerabilidades afectando a un gran número de computadoras.
- Puede enviarse de forma automática mediante correo electrónico.

Troyano:

- Programa malicioso que intenta suplantar un software legítimo.
- Tiene diversos propósitos malintencionados, como obtener estadísticas de actividad de exploración en Internet de la víctima, información sensible y acceso remoto.

Si nuestro equipo personal o estación de trabajo comienza a hacer actividades no autorizadas e inusuales, es posible que no sepamos si es un virus, gusano o troyano. Entonces, podemos decir que el dispositivo se encuentra infectado con malware (acrónimo de Malicious Software), éste es el nombre que se le da al conjunto de software listado anteriormente, aunque puede incluir a otros más.

Hacker y *cracker*

En diversos medios de comunicación podemos encontrar noticias sobre ataques informáticos, denegación de servicio, *defacement*, robo de información, entre otros, comúnmente estas acciones se atribuyen erróneamente a los *hackers*. El término *hacker* se refiere a una persona experta en tecnología, capaz de identificar fallas o explotar vulnerabilidades de sistemas, pero su interés es académico, educativo o de investigación. Cuando los *hackers* detectan un problema de seguridad, lo informan al dueño del activo vulnerable para que se solucione y así, evitar que sea aprovechado por un delincuente informático.

En la mayoría de los casos, los protagonistas de ataques cibernéticos son los *crackers*, individuos que aprovechan vulnerabilidades o comprometen sistemas informáticos de manera ilegal, su objetivo es obtener algún beneficio, como reconocimiento personal o remuneración económica. Por éste último, se han creado grupos criminales que buscan defraudar a usuarios y organizaciones.

Revisando el significado de los dos términos, te puedes dar cuenta de que la palabra *hacker* ha sido satanizada y mal empleada en muchos medios de comunicación, los *hackers* tienen un código de ética que no les permite utilizar sus conocimientos para afectar la información de otros, aunque hay distintos tipos de *hackers*.

Para no caer en confusión. Un *hacker* de sombrero negro es igual que un *cracker*, pero el primero buscará vulnerabilidades en tu infraestructura sin provocar algún daño (modificación o destrucción), tal vez podría reportarte las fallas de seguridad de tu organización mediante un correo anónimo; sin embargo, lo hace sin permiso, ésta es la diferencia con un *hacker* de sombrero blanco, que puede ser contratado para evaluar la seguridad de la empresa. Por otro lado, un *cracker* podría alterar, destruir o lucrar con la información obtenida a partir de un acceso no autorizado o mediante la explotación de una vulnerabilidad.

Evaluación de seguridad, *hacking* ético y pruebas de penetración

Estas tres frases frecuentemente se utilizan de manera indistinta; y aunque no significan lo mismo, tienen cierta relación entre ellas pues conforman un todo. En la imagen 1, se observa que las pruebas de penetración pertenecen al *hacking* ético y, a su vez, forman parte de una evaluación de seguridad.

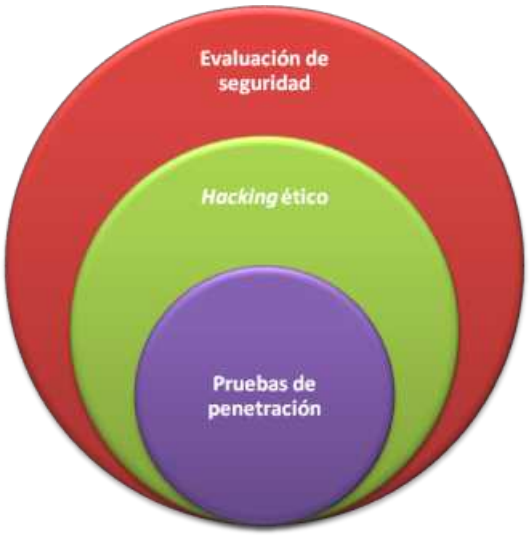


Imagen 1. Relación entre evaluación de seguridad, hacking ético y pruebas de penetración.

Una evaluación de seguridad de la información es un proceso para determinar el estado de seguridad actual del activo que se esté evaluando (computadora, sistema, red, etc.). Durante la evaluación de seguridad de una organización, se revisa una serie de documentos y archivos, tales como políticas de seguridad, bitácoras, configuraciones de seguridad, conjunto de reglas, entre otros; también es necesario hacer pruebas de penetración. Durante todo el proceso se documentan los hallazgos y se genera un reporte final que refleja la postura de seguridad de una organización.

Cuando se hace referencia al término *hacking*, se piensa en muchos significados, por lo regular las personas creen que se habla del robo de información digitalizada o de ataques hacia organizaciones para provocar fallas, es decir, siempre se ve con una connotación negativa.

En el contexto de la seguridad, *hacking* hace referencia a la manipulación de la tecnología para lograr que ésta haga algo para lo cual no fue diseñada. *Hacking* ético se refiere a usar técnicas de ataques para encontrar alertasde seguridad con el permiso del dueño del activo (por ejemplo, análisis de vulnerabilidades y pruebas de penetración), lo que se busca, es fortalecer la seguridad.

Según el NIST[1], las pruebas de penetración son una prueba de seguridad técnica en donde un evaluador simula ataques reales, su función es identificar los métodos para eludir las características de seguridad de una aplicación, un sistema o una red. De acuerdo con el SANS[2], las pruebas de penetración, como su nombre lo indica, son un proceso enfocado a penetrar las defensas de una organización, comprometer los sistemas y obtener el acceso a la información.

Analizando las dos definiciones anteriores, concluyo que las pruebas de penetración son un proceso intrusivo en donde se evalúan los mecanismos y configuraciones de seguridad de una organización mediante la utilización de métodos y técnicas para burlar la seguridad. Su función es penetrar los sistemas para conseguir información confidencial de la organización.

Existen más términos relacionados con seguridad de la información empleados como sinónimos o utilizados incorrectamente (payload, exploit, amenaza,riesgo), sin embargo, considero que en este artículo traté los que llegamos a escuchar de forma más cotidiana, cuando asistimos a una clase, conferencia, curso, taller o capacitación relacionada con la seguridad.

[1] SP 800-115, Technical Guide to Information Security Testing and Assessment.
[2] S/A, Network Penetration Testing: Planning, Scoping, and Recon, Maryland, SANS Institute, SEC 560.1, version 1Q09, 2008, 242pp. SANS SEC560.1: Network Penetration Testing: Planning, Scoping, and Recon.

Ing. José Luis Sevilla Rodríguez

Egresado de la Facultad de Ingeniería de la carrera de Ingeniería en Computación por la Universidad Nacional Autónoma de México, con módulo de salida en Redes y Seguridad.

Cuenta con las certificaciones Ethical Hacker (CEH) y Hacking Forensisc Investigator (CHFI) de EC Council.

Actualmente está implementando un Sistema de Gestión de Servicio de Pruebas de Penetración ofrecido por el Área de Auditoría y Nuevas Tecnologías. Además está impulsando proyectos para realizar pruebas de penetración en aplicaciones y dispositivos móviles.

Vender seguridad informática

Fausto Cepeda González

La venta de seguridad informática no es una tarea fácil. Incrementar el nivel de protección en las redes, sistemas y aplicaciones involucra un esfuerzo extra. Para lograrlo, el área de sistemas debe emplear a su personal en estas actividades y dejar de lado sus tareas cotidianas, así como dejar o suspender otras actividades con el fin de atender los pendientes de seguridad. En el peor de los casos, no sólo es tiempo, sino también presupuesto lo que interfiere.

Por lo tanto, atender a la seguridad se percibe como una carga extra tanto para usuarios como para administradores de sistemas. Es trabajo que probablemente no estaba contemplado y que es resultado de varias situaciones, aquí muestro algunos posibles escenarios:

• **Pentest interno o externo**. El resultado de estos ejercicios seguramente va a generar más de un hallazgo que tiene que ser solucionado. Son problemas que *"no se tenían que remediar"* anteriormente.

• **Consultoría de seguridad.** Es común que en el área de seguridad informática se contraten servicios de consultoría para atender alguna necesidad. Puede tratarse de poner en marcha un sistema de gestión de seguridad o para apegarse a un estándar. También serán las áreas de Tecnologías de Información (TI) quienes estarán involucradas en mantener esos procesos que antes no existían.

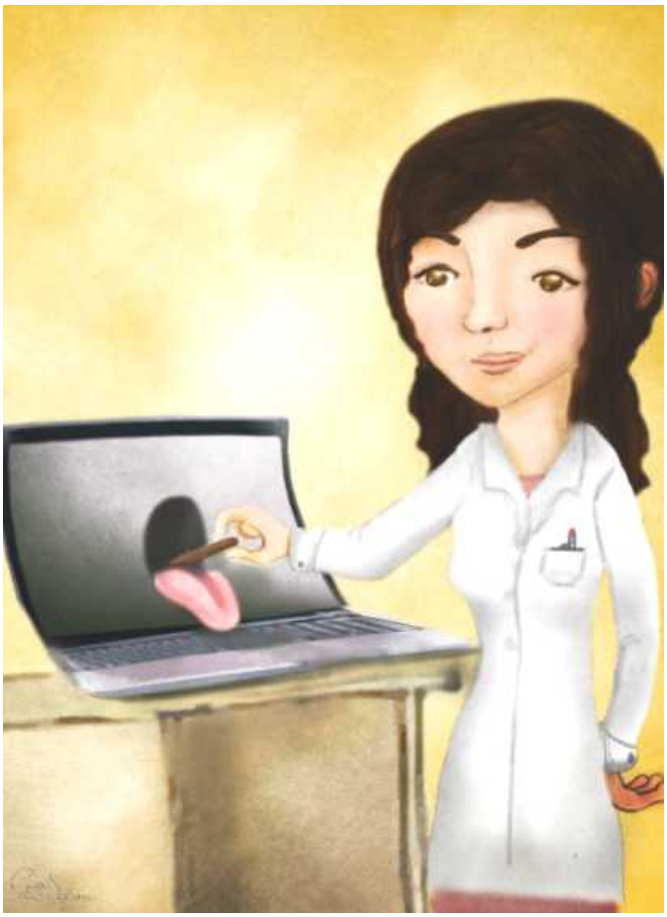
• **Nuevas tecnologías**. Para el siguiente año hay cambio de marca de *firewall* perimetral e instalarán por fin esa red inalámbrica que todos están esperando. Pero los de seguridad dicen que no se puede instalar nueva tecnología sin previa revisión. Esas *revisiones* agregarán otras tareas a esos proyectos de implementación.

• **Recientes problemas de seguridad**. A una tecnología usada en la organización que nunca había dado problemas, de pronto le aparecen vulnerabilidades por doquier y amenazas que aprovechan sus debilidades.

Es necesario cambiar esa tecnología y con eso, llega un nuevo proyecto.

• **Incidentes de seguridad**. Existe la sospecha de un incidente en la infraestructura de TI. El área de seguridad solicita bitácoras para revisarlas y tomar alguna acción. Durante esta investigación, se consume tiempo de las áreas de TI. Sin mencionar que las acciones correctivas también requiere que se involucren otros recursos.

• **Usuarios descontentos**. "El antivirus hace a mi computadora lenta", "no puedo entrar a sitios de Internet que necesito para mis labores porque están bloqueados", "no me llegan correos porque algo los detiene", "no puedo ejecutar una aplicación porque aparece un mensaje de seguridad". Seguramente estos usuarios estarían más felices sin los controles de protección. Menos seguros, pero más felices.



El reto es: ¿Cómo conseguir que exista interés por la seguridad? ¿Cómo lograr que los administradores destinen tiempo y recursos para temas de seguridad informática? ¿Cómo poner a la alta dirección del lado de seguridad? ¿Cómo persuadir a los usuarios para que cooperen?

La respuesta más fácil sería obligarlos. Pero eso presenta al menos dos problemas. El primero es que no deberías obligar a la alta dirección (tus jefes), esos son terrenos peligrosos. El segundo es que las quejas pueden multiplicarse tanto y venir de tantas áreas diferentes, que finalmente será el área de seguridad la que se verá obligada a modificar sus procedimientos y sus intentos de conseguir una *seguridad perfecta*.

Pues bien, la respuesta que yo propongo no es técnica. Es todo lo contrario, se trata de un tema puramente de *ventas* para ofrecerle a otra persona una idea atractiva. Esto es algo en lo que deseo puntualizar, porque la gente de seguridad informática es buena con los bits y bytes. Muchas veces ellos entienden mejor a las computadoras que a las personas y dominan el Metasploit, pero no el arte de convencer a un grupo de administradores o usuarios. Hacen presentaciones tan técnicas que parece que van a ir a BlackHat y no a una reunión con los *jefes*. De tal forma que el resto de la empresa los ve como entes *raros*, como si hablaran de términos oscuros, riesgos inentendibles y que dan trabajo extra a los demás. ¿Así es como quieres vender seguridad a tu empresa?

A continuación, enlisto tácticas concretas que podrían servir para *vender* seguridad a nuestra organización. No tienen garantía, porque insisto, no es un tema de ingeniería ni una cuestión técnica a resolver. Sin embargo, quiero recalcar que lo importante es intentar estas estrategias y, en caso de no funcionar, continuar insistiendo y creando otras ideas que puedan dar el resultado deseado. De otra forma, impulsar los temas de seguridad informática será una labor ardua, tortuosa y con resultados limitados.

I.- Demuestra de manera práctica las consecuencias. Llevar a cabo pruebas de seguridad internas (como pentest) es ideal para demostrar los riesgos de no incrementar las protecciones. Considero mucho mejor este método que dar una presentación en PowerPoint donde se expone "lo que podría pasar". Siempre es mejor demostrar la consecuencia de manera práctica y en vivo. Éstas quedan claras cuando se visualiza, por ejemplo, que es posible extraer

información de una base de datos importante desde Internet. Y por cierto, a nadie le va a importar la técnica usada, cuánto esfuerzo pusiste ni cómo funciona el *hackeo*. Habla de consecuencias.

II.- Prestar recursos a los departamentos de informática. Las áreas de TI se quejan de que les das más trabajo con cada revisión, consultoría o pentest que haces. ¿Estarías dispuesto a prestar una persona de seguridad informática a esas áreas? Este recurso les ayudará a solucionar un par de tus hallazgos. Dirán que les diste más trabajo, pero apreciarán que les ofrezcas un recurso humano tuyo para que ellos no distraigan tanto a los suyos. La idea es que en verdad prestes a tu recurso y que no sólo se quede en una buena intención.

III.- Proyección de la seguridad al resto de la empresa. No sólo hablo de las áreas de TI, sino del resto de tus usuarios. ¿Haces algo con ellos para explicarles los beneficios de tus controles de seguridad? ¿Conferencias, boletines, correos o artículos en la Intranet? ¿Armas seguido algún programa de concientización (*security awareness* por su término en inglés)? ¿Recabas los comentarios de tus usuarios por medio de encuestas? ¿Das cursos internos dirigidos a la seguridad informática del hogar de los usuarios? Evalúa la relación que tiene la seguridad informática con el resto de la organización.

IV.- Antes de instalar, avisa y trata de persuadir a tus usuarios. ¿Vas a poner un antivirus en cada computadora? ¿Un producto de listas blancas? ¿Un nuevo firewall a nivel aplicación? ¡Avisa! Informa con sobrada anticipación de lo que vas a implementar y de las ventajas de esa nueva herramienta. Explica si implicará algún trabajo extra para el resto de las áreas en el futuro. Haz presentaciones sobre el cambio y adelántate, como buen pastor, a persuadir a tu rebaño para que siga tu camino. No te vayas al extremo de pedirles las cosas a ver si las quieren; pero tampoco a que no estén enterados de tus planes. Siempre que puedas, evita poner el nuevo producto “de un día para otro”.

V.- Presenta con el afán de que te entiendan. No estás frente al público de *BlackHat*. Tampoco estás en *DefCon*. Estás en tu empresa. Presenta de tal manera que quede claro a tu público de lo que estás hablando. Explica cualquier término complicado. Como ya dije, habla de consecuencias. La cantidad de tecnicismos que uses debe reducirse conforme presentas a gente de jerarquías más altas. Tal vez valga la pena que vayas alguna vez a una junta o conferencia de economistas o de abogados. Cuando entiendas un 30% de lo que ahí se dice, sabrás cómo se sienten los demás en tus exposiciones.

VI.- Usar tecnicismos no te hace ver más inteligente. A propósito del punto anterior. ¿Usas términos como *buffer overflow, sql injection o cross site scripting*? ¿Crees que hablar así te hace ver superior porque no te entienden? Mal. Si no te entienden, el mensaje completo no llega al destinatario. Eso no es muy inteligente. Sobre todo si le estás explicando un riesgo a alguien que toma decisiones. No tendrá el entendimiento suficiente para impulsar tus iniciativas.

VII.- Ve más allá de vender, haz que te compren.
Ve al consultorio de un buen doctor. Siempre estará lleno. Los pacientes van a él. Es su salud. El doctor no les está llamando para que acudan a una visita. No tiene que ir a vender sus servicios de casa en casa, sus pacientes van y lo buscan. No vende, ya hizo que ellos compraran por sí solos. Obviamente es porque ofrece un buen servicio y es bueno en lo que hace.

¿Tú también puedes lograr que tus usuarios y administradores acudan a ti? ¿Que perciban que es mejor ir contigo que no ir y estar desprotegidos? Si lo logras, estarás más allá de la venta de la seguridad, habrás llegado a lo que yo considero el nirvana: que ellos compren la seguridad.

Fausto Cepeda González

Es Ingeniero en Sistemas Computacionales por el ITESM. Es Maestro de Seguridad de la Información por la Universidad de Londres (Royal Holloway). Actualmente labora en la Subgerencia de Seguridad Informática del Banco de México. También cuenta con las certificaciones de seguridad CISSP, CISA, CISM y CEH.

Seguridad de la información en salud, un sector olvidado

Miriam J. Padilla Espinosa

En un mundo hiperconectado, la incorporación de tecnologías ha evolucionado la forma en que se crea la información, en su intercambio, almacenamiento y difusión. Ha dado lugar a nuevas amenazas que afectan la confidencialidad, disponibilidad y la integridad de los datos, es decir, la seguridad de la información. Esta situación no es única de sectores como el financiero o el tecnológico, ni exclusiva de grandes empresas o instituciones.

El sector salud en México enfrenta grandes retos en materia de seguridad de la información, en los últimos años se han incorporado nuevas tecnologías como una medida para renovar y agilizar la prestación de servicios, esta situación se ha visto reflejada recientemente en las estrategias del gobierno mexicano.
La recién liberada Estrategia Digital Nacional tiene como objetivo mejorar el uso de la tecnología para contribuir al desarrollo del país, cinco objetivos son los que conforman dicha estrategia. En aspectos relacionados con la salud, el objetivo número cuatro, denominado Salud Universal y Efectiva, fue creado con la finalidad de aprovechar la incorporación de las tecnologías de información y comunicación como medio para aumentar la cobertura, el acceso y la calidad de los servicios de salud, otra de las finalidades es lograr el uso eficiente de la infraestructura y los recursos destinados a proveer el servicio de salud a la población.

Previamente, existían ya iniciativas de integrar los datos clínicos en un expediente electrónico, de hecho, algunas entidades ya lo han implantado, junto con algunas otras leyes en México que regulan en el sector público y privado, la protección de los datos personales, los datos personales sensibles y las Normas Oficiales Mexicanas (NOM) en materia de salud. Algunas de ellas son la NOM-004-SSA3-2012 del

expediente clínico, la NOM-024-SSA3-2010 de Sistemas de Información de Registro Electrónico para la salud y en cuanto a intercambio de información en salud, la NOM-035-SSA3-2012.

Todas estas iniciativas, si bien son de gran ayuda, deben ir de la mano con una estrategia en materia de seguridad de la información que considere la gestión de nuevos riesgos asociados a la incorporación de las TIC. Esta estrategia debe ser evaluada previamente, considerando la problemática a nivel organizacional que enfrenta el sector, la prevaleciente resistencia al cambio y la falta de conciencia sobre temas relacionados con la seguridad de la información. De no considerarse estos factores, podrían convertirse en una gran limitante.

Para identificar los retos en materia de seguridad de la información que enfrenta el sector salud en México, se realizó un análisis tomando como base el modelo de negocio para la seguridad de la información (veáse figura 1.1) desarrollado por el Dr. Laree Kiely y Terry Benzel en Institute for Critical Information Infrastructure Protection (Instituto de Infraestructura de Protección para la Información Crítica) en la escuela de negocios Marshall School of Business de la Universidad del Sur de California de EUA.

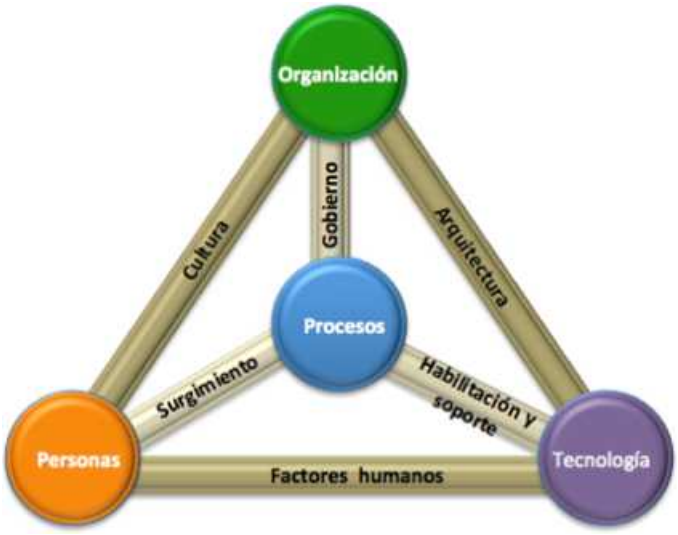


Figura 1. 1 Modelo de negocio para la seguridad información

El modelo se representa gráficamente como una pirámide conformada por cuatro elementos unidos mediante seis interconexiones dinámicas, todas las partes que integran el modelo interactúan entre sí. Si cualquiera de los elementos es modificado o gestionado de forma inadecuada, afectará el equilibrio del modelo. El resultado del análisis aplicado al sector salud en México se presenta a continuación:

1. Diseño y estrategia de la organización

El Sistema Nacional de Salud en México fue creado en cumplimiento al derecho a la protección de la salud que toda persona tiene, según lo establece el artículo 4º de la Constitución Política de los Estados Unidos Mexicanos, formalmente se encuentra definido en la Ley General de Salud.

Los principales objetivos de este sistema son: proporcionar servicios de salud a toda la población, colaborar con el bienestar social, dar impulso al desarrollo de la familia y comunidades indígenas, apoyar en la mejora de las condiciones sanitarias y promover el conocimiento y desarrollo de la medicina tradicional, principalmente. Para el cumplimiento de sus objetivos son considerados el Plan Nacional de Desarrollo y el Programa Nacional de Salud.

El Sistema de Salud de México se divide en dos sectores: el público y el privado. La siguiente tabla presenta las instituciones que forman parte de cada sector:
La estructura funcional del Sistema de Salud en México está integrada por tres niveles de atención, se describen brevemente en la Figura 1.2.

Sector público	Sector Privado
Instituciones de seguridad social: • Instituto Mexicano de Seguridad Social (IMSS) • Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) • Petróleos Mexicanos (PEMEX) • Secretaría de la Defensa (SEDENA) • Secretaría de Marina (SEMAR) **Instituciones para población sin seguridad social:** • Secretaría de Salud (SSA) • Servicios Estatales de Salud (SESA) • Programa IMSS-Oportunidades • Seguro Popular	• Compañías aseguradoras. • Prestadores de servicios que laboran en consultorios, clínicas y hospitales privados. • Servicios de medicina alternativa.

Fuente: Elaboración propia con información de González Guzmán, R Moreno Altamirano, L, & Castro Albarrán, JM. (2010). La salud pública y el trabajo en comunidad (M. G. Hill Ed. Primera Edición ed.).

México cuenta con una amplia red de atención médica, resultado de la inversión que el gobierno federal ha designado para mejorar la prestación de servicios de salud. Según datos del Banco Mundial, este hecho que se ve reflejado en un incremento del porcentaje del PIB destinado para gastos de salud, de un 5.8 % en el año 2008, a un 6.2 % en el año 2011. La decisión ha favorecido a las instituciones de salud en México, fortaleciendo la infraestructura y mejorando los recursos tecnológicos disponibles para la prestación de los servicios de salud a la población.

2. Personas

Es fundamental realizar mayores esfuerzos para lograr la capacitación y concienciación del personal administrativo y médico que labora en las instituciones de salud en México, sobre todo, en los aspectos relacionados con la seguridad de la información. Es importante que conozcan las amenazas, las vulnerabilidades y las principales técnicas de ataques que pudieran afectar, tanto la operación de la institución como la confidencialidad, integridad y disponibilidad de los datos clínicos.

Otro aspecto importante a considerar es la resistencia al cambio. En algunas instituciones ha sido una gran limitante que ha impedido la adopción efectiva de la tecnología para mejorar los procesos institucionales.

También es necesario considerar controles más rigurosos para los proveedores y personal externo que brinda productos o servicios a las instituciones de salud.

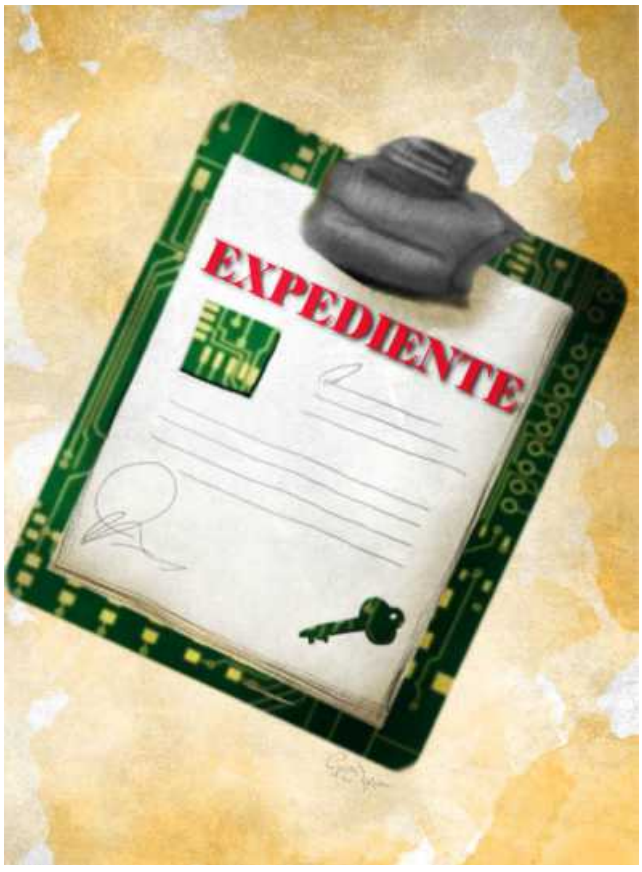
Interconexión	Resultados
Gobierno	Las instituciones de salud deben fortalecerse en este ámbito para garantizar el cumplimiento de los objetivos. Deben integrar o mejorar la gestión de sus riesgos de manera que les permita actuar de forma proactiva, así como mejorar las estrategias que actualmente se tienen implantadas para verificar el uso responsable de los recursos institucionales, reduciendo con ello los fraudes y eventos que puedan afectar la continuidad o causar daños en los activos.
Cultura	El gran reto en este rubro está enfocado en reducir la división que existe entre el personal médico y el administrativo, además de realizar programas efectivos de concienciación en materia de seguridad de la información para generar una cultura en la materia.
Habilitación y soporte	La labor en este aspecto se relaciona con llevar a cabo una reingeniería de procesos con el objetivo de mejorarlos en cada una de las instituciones de salud. El resultado será que éstos sean prácticos y fáciles de poner en marcha. Si son transparentes para el personal, podrán salir adelante de mejor manera. El fortalecimiento con buenas prácticas, normas, políticas y estándares no se debe dejar de lado. Si bien la mayoría de las instituciones cuentan con éstos a nivel documental, en algunas entidades no se encuentran realmente implementados.
Surgimiento	La resistencia al cambio ha impactado esta interconexión en el sector público de salud, que en gran parte ha sido el resultado de incorporar tecnología sin llevar a cabo de forma previa una evaluación sobre el impacto a nivel organizacional que dicho cambio traerá en consecuencia.
Factores humanos	Es necesario que los desarrollos y tecnologías a ser implantadas tomen en cuenta la experiencia de los usuarios de dichos recursos con el objetivo de reducir errores por desconocimiento o generados por la resistencia al uso de los recursos tencnológicos.
Arquitectura	Es fundamental que las instituciones de salud, una vez que identifiquen sus necesidades en materia de seguridad, incorporen una arquitectura que incluya los controles requeridos para la protección de sus activos, al tiempo que permita a las entidades de salud ser proactivas con sus decisiones de inversión en materia de seguridad.

De igual forma, se deben mejorar los controles de acceso. En algunas instituciones éstos son deficientes debido a la gran demanda del servicio, que sin duda se vuelve un asunto prioritario que deja para después los temas y controles relacionados con la seguridad de la información.

3. Procesos

Las instituciones de salud cuentan con diversos procesos para llevar a cabo sus actividades diarias, sin embargo, en la operación, los procedimientos asociados se exceden en trámites. Esta situación genera mayores tiempos de espera, descontento por parte de los usuarios del servicio y, en el peor de los casos, puede afectar la vida misma de los pacientes, resultado de errores en los procedimientos o exceso en los tiempos de espera.

Los procesos deben ser difundidos adecuadamente y se deben llevar a cabo acciones para monitorear su cumplimiento bajo un esquema de indicadores y métricas.
En cuanto a la estandarización de los procedimientos, las entidades de los estados de la república deben realizar sus actividades bajo condiciones similares, además, es indispensable



incorporar procesos y procedimientos en materia

de seguridad de la información en donde se definan claramente los roles y responsabilidades de los involucrados. Esta acción contribuirá a cambiar de un enfoque de respuesta reactivo a uno proactivo.

4. Tecnología

Con la finalidad de generar una mejora en la operación de este sector, se han incorporado nuevas tecnologías que permitan brindar el servicio a una cantidad mayor de usuarios, una de ellas, es la iniciativa de incorporar el expediente clínico electrónico.

En la actualidad, las instituciones cuentan con dos modalidades de expedientes, la versión física y la digital. La implantación de sistemas de información como éstos, desarrollados sin considerar la experiencia de los usuarios (médicos, administrativos o enfermeras) ha ocasionado una resistencia a su adopción o bien, información incompleta en los expedientes.

El Sistema de Salud en México enfrenta grandes retos, tanto a nivel organizacional como operativo, por un lado es necesario ampliar la cobertura del servicio y por otro mejorar la calidad y eficiencia de las instituciones que se encuentran actualmente en operación. Dado el crecimiento de la población, éstas se encuentran saturadas y con escasos recursos, complicando significativamente la prestación de servicios que garanticen la satisfacción de los usuarios.

Para dar una mejor respuesta a las necesidades de la población en materia de salud, es necesaria una planeación interinstitucional de largo plazo, con estrategias claramente definidas, una mejor administración de riesgos, así como el compromiso y corresponsabilidad entre instituciones. Además, es fundamental considerar los controles necesarios para garantizar la protección de la información que es creada, almacenada y transmitida en las instituciones de salud.

Como resultado de este análisis, podemos identificar grandes oportunidades para proponer, actuar y, como profesionales, contribuir por medio de conocimientos, tecnologías y personal calificado a mejorar la seguridad de la información

Referencias

Moreno Altamirano, L, & Castro Albarrán, JM. (2010). La salud pública y el trabajo en comunidad (M. G. Hill Ed. Primera Edición ed.).

Leal, Héctor Vázquez, Campos, Raúl Martínez, Domínguez, Carlos Blázquez, & Sheissa, Roberto Castañeda. Un expediente clínico electrónico universal para México: características, retos y beneficios.

Salvador Rosas, Griselda. (2007). La protección de los datos personales en expedientes clínicos, un derecho fundamental de todo individuo. (Licenciado en Derecho Licenciatura), UNAM.

Sánchez-González, JM, & Ramírez-Barba, EJ. El expediente clínico en México.

http://www.isaca.org/KnowledgeCenter/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09Research.pdf

http://www.presidenca.gob.mx/estrategia-digital-nacional-para-transformar-a-mexico/

http://bvs.insp.mx/rp/articulos/articulo_e4.php?id=002625

http://www.diputadosgob.mx/LeyesBiblio/pdf/1.pf

http://www.diputados.gob.mx/LeyesBiblio/pdf/142.pdf

http://dof.gob.mx/nota_detalle.php?codigo=5280848&fecha=30/11/202

http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2010_SistemasECE.pf

http://www.dof.gob.mx/nota_detalle.php?codigo=5272787&fecha=15/10/2012

http://pnd.gob.mx/

Miriam J. Padilla Espinosa

Ingeniera en Computación egresada de la Facultad de Ingeniería de la UNAM. Colaboró en la Subdirección de Seguridad de la Información (SSI/UNAM-CERT) en el Área de Auditoría y Nuevas Tecnologías como responsable del proyecto de implementación de ISO 27001. Actualmente es maestrante en Administración de la Tecnología del Posgrado de la FCA de la UNAM. Cuenta con experiencia en implementación de ISO 27001 y Gobierno de TI.

Copyright Prevent Copy: Protocolo BPS

Jesús Nazareno Torrecillas Rodríguez

Cada vez que vamos a un auditorio, salón de actos, cine, etc., presenciamos cómo las personas toman fotos o graban las sesiones y a nadie parece importarle esta situación pues, debido a las continuas *violaciones del copyright*, la mayoría de la gente piensa o cree que estas acciones no son ilegales.

Es bien conocido que muchos artistas, para poder sobrevivir, se dedican a dos profesiones ya que su actividad artística, incluso, llega a costarles dinero debido a los graves efectos de la piratería sistemática de sus producciones.

En general, la gente considera que el hecho de fotografiar a un artista, grabarle en un concierto, enviar fotos tomadas en un evento o subir a la red grabaciones domésticas, no es materia de delito. La realidad es distinta. De hecho, como está establecido judicialmente en la mayoría de los países: “El desconocimiento de la ley no exime su cumplimiento”. Lo que en palabras llanas quiere decir que las leyes están para cumplirlas, aunque se desconozcan.

¿Qué hacen los cines, salas de exhibición, salas de conciertos y auditorios (los responsables de los eventos) para evitar que el público filme, fotografíe y grabe en su paso por esos recintos? Poca cosa, ya que se podría afirmar que cada asistente a un evento porta un teléfono con cámara incorporada.

¿Cómo se defienden los artistas ante la sistemática violación del copyright de sus obras? Pareciera que a priori tienen la batalla perdida tras la incorporación, hace pocos años, de cámaras en los teléfonos móviles.

Sin embargo, la respuesta depende de muchos factores: Educación del público, costo de las actuaciones, nivel social de los asistentes, jurisprudencia del país, capacidad de la autoridad para prevenir estos delitos, interés de los empresarios en contribuir en la prevención de estas actividades, etc.

Una pregunta que yo me he planteado es, ¿son responsables los fabricantes de los teléfonos móviles del incremento de las sistemáticas violaciones del copyright? Esta pregunta es similar a decir que son los fabricantes de armas los responsables del aumento de los crímenes. Yo me atrevería a decir que directamente no lo son, pero indirectamente sí. Es muy posible que sin armas no hubiera tantos crímenes, entonces las armas, son hasta cierto punto, facilitadoras de delitos. Igual ocurre con los teléfonos móviles que cuentan con cámara de fotos y sistema de grabación incorporados.

Por ello, mí planteamiento es muy simple y versátil. Los fabricantes de telefonías móviles y de smartphones se pueden poner a trabajar en conjunto en lo que yo llamo un nuevo protocolo integrado en WIFI 4G. Se trataría de lo que yo he denominado Protocolo BPS (*Blocked Phone System*)

En muchos lugares, salas, auditorios, iglesias, y con el fin de evitar que el público asistente pueda perturbar la tranquilidad del lugar con llamadas telefónicas, se instala lo que se denomina bloqueadores telefónicos. Hay de dos tipos:

Dinámicos, cuando detecta emisión de frecuencias; y estáticos, es decir, siempre emiten una señal perturbadora que impide que el teléfono reciba o efectúe llamadas, creando lo que se conoce como zona de sombra. El problema de los perturbadores o bloqueadores telefónicos descritos es, que para que los teléfonos se queden sin señal, deben emitir una frecuencia igual a la de los teléfonos, pero con mucha mayor potencia. Esto es pernicioso a todas luces para la salud humana, ya que los teléfonos trabajan en frecuencias de varios gigahercios (microondas).

El BPS básicamente consiste en una combinación de estrategias por parte de los fabricantes de teléfonos y de los dueños de las salas de exhibición, cines, auditorios, etc. De acuerdo a lo siguiente:

1° Protocolo propiamente dicho. Se trataría de que todos los teléfonos aceptasen instrucciones en una frecuencia modulada FM del orden de pocos MHz en modulación PCM (Pulse Code Modulation).

2° Instalación de transmisores de muy baja potencia en lugares públicos que emitiesen en la frecuencia modulada FM de pocos MHZ en modulación PCM.

3° Como las frecuencias de pocos MHz en modulación PCM no se interfieren con las de GHz, los teléfonos podrían recibir instrucciones de la estación emisora local instalada en los auditorios con el fin de que el teléfono, al recibir la señal codificada, automáticamente desconectase sus funciones.

La situación sería la siguiente:
A medida que el público entre en la sala y sus teléfonos reciban la orden desde el transmisor FM-PCM podrían considerarse varias acciones:

1° Apagado automático del equipo. Cuando el usuario intentase reactivarlo, éste automáticamente se volverá a desactivar sin llegar al encendido operativo.

2° Bloqueo de algunas funciones del equipo, como llamar, tomar fotos, tomar vídeo, etc.
3° En el auditorio se podría indicar un semáforo o aviso óptico indicando a los asistentes que a partir de ese punto sus teléfonos quedarán

bloqueados interrumpiendo todas o algunas funciones.
4° Sólo en los tiempos de descanso del evento se podrían activar manualmente algunas funciones, como llamadas, pero no grabación ni captura de fotos.

Considero que es una buena solución de compromiso en eventos públicos.
Sin embargo, aún quedaría pendiente ver las implicaciones *jurídicas* y *operativas* de implementar este tipo de protocolos en el campo real.

5° Al reiniciar el evento se bloquearían de nuevo las funciones del teléfono.

6° A la salida del recinto los teléfonos volverían a su operación normal.

Correspondería al trabajo conjunto entre los operadores de eventos, las compañías de servicios telefónicos y los fabricantes de estos dispositivos, implementar una tecnología adecuada para al manejo de la privacidad en el campo de los eventos masivos. Asimismo, el trabajo se llevaría a cabo de la mano con el marco legal existente en cada uno de los países en donde se piense implementar una tecnología como esta.

Jesús Nazareno Torrecillas Rodríguez

Actualmente es CISO en la compañía Axtel. Graduado con Excelencia como Director de Seguridad de Empresa (D.S.E.) Por la Universidad Pontificia de Comillas en Madrid (UPCO). Realizó cursos de Ingeniería Técnica en Telecomunicaciones en la EUITT de Madrid. Ha estudiado Electrónica Digital y Microprocesadores orientados a robótica en diferentes centros de estudios privados en España.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.20 / abril-mayo 2014 ISSN: 1251478, 1251477