Magazcitum

El magazine para los profesionales de la seguridad de TI

¡Estamos de FIESTA!

¡Magazcitum versión IMPRESA!

Antología de números en línea

Lo único seguro es que somos vulnerables

Cómputo en la nube

¿el último grito de la moda o una necesidad ineludible?

El eslabón más débil

El control por sí solo no es suficiente

Seguridad en la VoIP

AÑO 1, NÚMERO 1
JULIO-SEPT. 2010
EJEMPLAR GRATUITO


BlueCoat®

Magazcitum

AÑO 1, NÚMERO 1. JULIO - SEPTIEMBRE 2010

Dirección General
Ulises Castillo

Editores
Héctor Acevedo
Gerardo Fernández

Consejo Editorial
Ulises Castillo
Antonio Fájer
Priscila Balcázar
Héctor Acevedo
Gerardo Fernández
Dinorah Valladares

Marketing
Dinorah Valladares

Colaboradores
Priscila Balcázar
José Ramírez
Marcos Polanco
Eduardo Patricio Sánchez
David Gutiérrez
Esteban San Román
Omar Alcalá
Osvaldo Hernández

Correctora de estilo
Adriana Gómez López

Diseño
Silverio Ortega

Magazcitum, revista trimestral de Scitum S.A. Año 1, número 1 julio-septiembre de 2010. Editor responsable: Héctor Acevedo. Número de Certificado de Reserva otorgado por el Instituto de Derechos de Autor: 04-2010-071512010500-102. Permisos ante SEGOB en trámite. Domicilio de la Publicación: Av. Paseo de la Reforma 373 piso 7, Col. Cuauhtémoc, delegación Cuauhtémoc, México DF 06500. Impreso en : Rouge & 21 S.A. de C.V. Av. Rómulo O'Farril # 520 int 5 Col. Olivar de los Padres México DF. Distribuida por Editorial Mexicana de Impresos y Revistas S.A. de C.V: Oaxaca 86-402 Col. Roma México DF. Magazcitum, revista especializada en temas de seguridad de la información para los profesionales del medio. Circula de manera controlada y gratuita entre los profesionales de la seguridad de la información. Tiene un tiraje de 5,000 ejemplares trimestrales.
Para cualquier asunto relacionado con esta publicación, favor de dirigirse a **contacto@magazcitum.com.mx**

contenido

» editorial

» opinión

» conexiones

» tips

¡Estamos de fiesta!

Héctor Acevedo
CISSP, CISA, CGEIT, ITIL, MCSE
hacevedoj@scitum.com.mx

Magazcitum impresa

A partir de este número lanzamos la versión impresa, enfocada a los profesionales de seguridad en TI, con un tiraje inicial de 5 mil ejemplares trimestrales y distribución gratuita. Para suscribirse visite nuestro sitio web y llene la forma correspondiente.

La versión impresa de la revista conservará las mismas secciones que hemos tenido hasta ahora:

» **Noticias**.
El objetivo de esta sección es, más que hacer una simple recopilación de sucesos del medio, abordarlos desde un punto de vista editorial y de opinión, de manera que los lectores tengan elementos que les permitan forjar el propio.

» **Tips.**
Consejos y sugerencias para el personal técnico que les permita aprovechar de mejor manera la infraestructura de seguridad disponible en sus organizaciones.

» **Opinión.**
Artículos principales en los que el autor habla de algún tema relevante para la industria. En este caso no sólo se expone un tema, sino que el autor habla de su experiencia al respecto, de manera que se aporte algo de nuestros conocimientos y experiencia..

» **Conexiones.**
Sección de textos más breves, pero permanentes en cada edición, en los que el autor habla desde una perspectiva todavía más personal del tema de su elección. Las “Conexiones” que tenemos son:

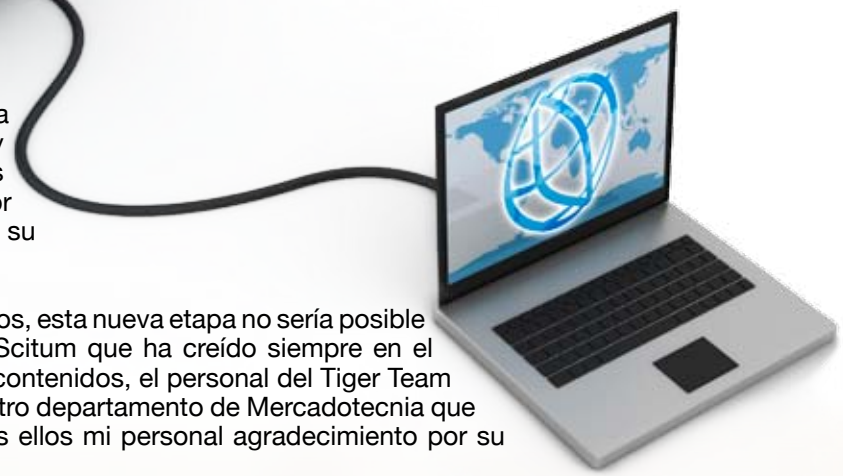
- **Departamento de defensa.**
- **Desde la trinchera.**
- **En el pensar de….**
- **Historias.**

» **Historias de éxito**
Descripción de proyectos que presentan alguna problemática de interés general, cuáles fueron los retos y cómo se abordó la solución para cada caso en particular.

Ilustración: Silverio Ortega

«El sexto número representa un hito importante en el crecimiento de Magazcitum y queremos compartir con todos nuestros lectores el enorme gusto que nos da tener un nuevo sitio web y lanzar la versión impresa de la revista.»

www.magazcitum.com.mx



Magazcitum en línea

Renovamos nuestra presencia en Internet con una interface más intuitiva, funcionalidad mejorada y fácil acceso a los artículos de cada edición. Los invitamos a visitarnos y a darse “una vuelta” por la nueva Magazcitum en línea, esperamos sea de su agrado.

Además de los colaboradores que publican sus textos, esta nueva etapa no sería posible sin mucha gente detrás: la Dirección general de Scitum que ha creído siempre en el proyecto, la gente que apoya en la revisión de los contenidos, el personal del Tiger Team que ayudó en la creación del nuevo web site y nuestro departamento de Mercadotecnia que coordina la logística de impresión y envío. A todos ellos mi personal agradecimiento por su esfuerzo y espíritu de colaboración.

Sin más por ahora, queda en sus manos esta sexta edición de Magazcitum con una mezcla de nuevos artículos y una antología de los artículos más leídos desde el inicio de la revista. Recuerden que son bienvenidas sus ideas y sugerencias acerca de los temas que deseen sean tratados, o incluso participando activamente publicando en la revista. No dejen de escribirnos al correo de cada uno de los colaboradores o a **contacto@magazcitum.com.mx**.

Como siempre, muchas gracias por su atenta lectura.

Cómputo en la nube: ¿el último grito de la moda o una necesidad ineludible?

Esteban San Román
CISSP, CISA y CEH
esanroman@scitum.com.mx

Los más recientes eventos de Tecnología han dado especial énfasis a tópicos relacionados con el cómputo en la nube, y es que en un entorno donde los recursos tecnológicos son cada vez más sofisticados y los presupuestos más escasos, se presenta una necesidad de explotar al máximo el ingenio a fin de buscar las mejores alternativas para apoyarse en lo que se va haciendo disponible.

La mayor parte de los analistas coinciden en que la revolución que se está gestando será un tema recurrente por los próximos diez años. Ante este escenario, los gerentes y directores de tecnología tratan de determinar hasta qué nivel se puede adoptar un atractivo esquema que, en principio busca disminuir drásticamente los costos de propiedad de la tecnología.

Ahora todos los recursos de información los vamos a acceder y manipular a través de aplicaciones que se encuentran en algún lugar en la nube.

Pero, ¿qué seguridad se esperaría obtener de esos esquemas? para muchos, esto representa el principal paradigma (no sé si la palabra sea paradigma, creo que la idea no es clara) a superar, porque el control (o parte de él) se está delegando a alguien más. Pareciera que establecer niveles de servicio específicos no sería suficiente porque el nivel de madurez de las soluciones hoy disponibles se enfocan a la disponibilidad de la información, cuando aún se divisan claroscuros en cuanto a la protección de los datos.

Por lo tanto, se presenta en principio la necesidad de crear nubes privadas donde entidades, como por ejemplo los bancos, puedan manejar sus recursos de información, y que posteriormente a través de acuerdos de niveles de operación interactúen con sus proveedores u otras entidades financieras para eventualmente crear los esquemas que faciliten la interacción a través de nubes públicas con otras organizaciones y con los usuarios finales.

Esta evolución es muy similar a lo que hoy tenemos con las redes privadas, las redes públicas y la Internet, con la diferencia de que ahora los recursos se suben a la nube y alguien más se encarga de los costos de mantenimiento y del crecimiento tecnológico.

Un panorama en principio muy atractivo para los proveedores de servicio, pero con muchas aristas como la virtualización, la proliferación de las redes sociales, las nuevas posibilidades de comunicación unificada, las redes inalámbricas metropolitanas y otras tantas que incrementan los niveles de complejidad, para no dejar nada fuera de los acuerdos contractuales.

A fin de comprender cuáles son los elementos que participan como ejes del cómputo en la nube, podemos mencionar que hoy las soluciones de la industria cuentan con:

a) Estándares abiertos y plataformas de programación, cuyo objetivo es el de crear aplicaciones mucho más apegadas a las necesidades del usuario y mejor compenetradas con el negocio.

b) Portabilidad, que permite que las aplicaciones desarrolladas puedan funcionar con independencia de la plataforma de hardware y software que se pretenda utilizar.

c) Evolución de nombres y registros, que conforman entornos de operación mucho más manejables para el usuario final. El inminente advenimiento de IPv6 amplía las posibilidades de direccionamiento de los recursos de información.

d) Transparencia, que con apoyo de tecnologías web le permiten a las organizaciones simplificar al usuario la interacción con las aplicaciones y permitirle enfocarse a las funciones específicas de su puesto, potenciando de esta forma la productividad y la eficacia en sus actividades cotidianas.

e) Soluciones de manejo de Identidades y autenticación, para facilitar y asignar adecuadamente el uso de los recursos al usuario, proporcionándole el acceso exclusivo a los recursos que este requiera, manteniendo un estricto control de qué se accedió y quién lo hizo, cumpliendo con las regulaciones a las que se debe apegar la organización.

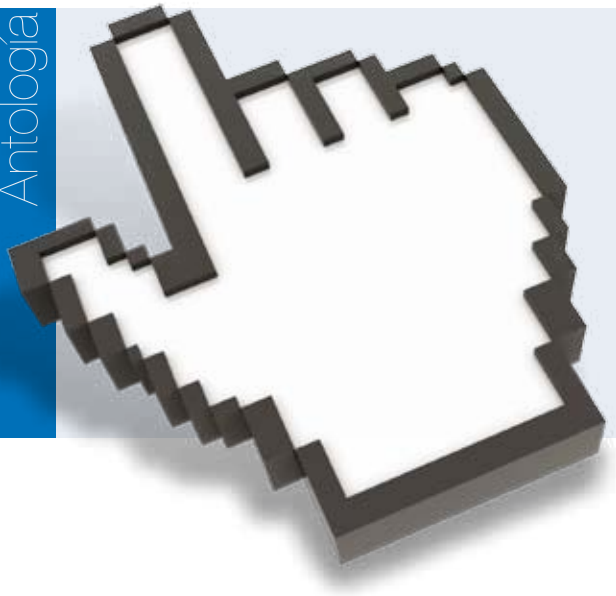
f) Elementos y soluciones móviles que se acoplan a la dinámica de los negocios de hoy, el usuario tiene comunicación y posibilidades de acceso a los recursos de información que se le asignan independientemente de dónde se encuentre.

g) Mejores metodologías de diseño de software, basado en prácticas que se comienzan a adoptar por parte de los creadores de aplicaciones para que éstas, desde su concepción se estructuren con un mínimo de defectos.

h) La centralización y sustentabilidad de la información, un área en la que los proveedores de Servicios de cómputo en la nube realizan su planeación e inversiones, buscando diferenciarse entre sus competidores. Estructurando planes muy detallados de continuidad de negocio y recuperación de desastres.

Así, el cómputo en la nube comienza a perfilarse como el recurso tecnológico sobre el que las organizaciones estarán apoyándose los próximos años, y la seguridad se mantiene como uno de los ejes principales para el éxito de este nuevo esquema de operación.

Al fin y al cabo, si dudamos de la seguridad de la nube, tendríamos que preguntarnos también ¿podemos permitirnos el no confiar en ella?



La seguridad en los tiempos del hipervínculo

Priscila Balcázar Hernández
CISSP, CISA y CGEIT
pbalcazarh@scitum.com.mx

Me da la impresión de que la comunidad informática a veces cree que la seguridad es una necesidad de la modernidad digital. Pero basta echarnos un clavado a la historia de la humanidad para localizar cientos de técnicas de protección de información y de activos, o hacer analogías con nuestra vida cotidiana para entender la seguridad informática.

Entonces, siendo la seguridad tan antigua, ¿qué es lo que ha obligado hasta ahora a las organizaciones a pensar seriamente en mecanismos de protección de su información? La respuesta la tienes en la punta de la lengua: lo vulnerable de nuestra era, hoy día con un simple clic en un hipervínculo podemos disparar un virus; podemos ser víctimas de suplantación de identidad en un banco y por tanto sufrir una estafa; podemos dar albergue a un caballo de Troya; también con un clic fácil y rápidamente podemos replicar, alterar, distribuir, borrar o almacenar cientos de miles de bytes con información.

En tiempos ancestrales cualquiera de estas acciones que hoy toman menos de un segundo, habría implicado el esfuerzo de uno o un grupo de hombres, tiempo considerable y técnicas de ocultamiento; por ejemplo para robar y replicar un largo manuscrito secreto.

Los intereses de los delincuentes digitales van desde mero entretenimiento, evasión fiscal, espionaje industrial, malversación de fondos, fraude, piratería, secuestro, obtención de información privilegiada, tráfico de drogas, hasta terrorismo, entre otros muchos.

Las prácticas de mal uso de información parecen tan creativas en la actualidad, que hasta suenan novedosas, pero la proclividad a ejercer el acto invasivo, tanto como la necesidad de preverlo y atacarlo, son tan antiguas como la historia misma.

La seguridad es como un modelo clásico, como el Volkswagen, la cola de caballo, los zapatos bostonianos o el Chanel N° 5: siempre está de moda. La historia de la humanidad nos ofrece múltiples ejemplos de cómo la información siempre ha sido del interés ajeno, lo mismo que guardarla siempre ha tenido sus buenos motivos. Ya los fenicios, los egipcios o los mayas, utilizaron métodos (que hoy llamamos muy coquetamente “controles” y que son los principios de la criptografía), para ocultar –cifrar- información clave o confidencial.

Por ejemplo, la caja de Julio César era un método para enviar mensajes ocultos sin que los mensajeros pudieran leerlos, o, en caso de ser capturados, tampoco pudieran hacerlo los enemigos. El método consiste en elaborar un mensaje con un número de letras que sea el cuadrado de un número natural n; es decir, que un mensaje válido es aquel que contenga 16, 25, 36, 49 letras, que son el cuadrado de n=4, 5, 6, 7 respectivamente; las letras del mensaje real se rellenan por n columnas y se emite el mensaje oculto por n renglones.

La creatividad no tenía límites. Por ejemplo se enroscaba un trozo de papel en un cilindro, se escribía el mensaje verticalmente en el papel y luego se desenrollaba el papel para enviarlo con el mensajero. El remitente y el destinatario habían acordado previamente cuál sería el diámetro del cilindro. Incluso se podía jugar con conos o figuras irregulares para despistar aún más.

Otro tipo clásico era la máquina Enigma, utilizada por los alemanes durante la segunda guerra mundial. Enigma se encargaba de cifrar y descifrar los mensajes de estrategias, a través de una clave, y funcionaba inicialmente con tres rotores. Los polacos, británicos y franceses lograron descifrarla con una máquina idéntica. Así, los alemanes fueron agregando rotores hasta llegar a ocho. Y, cuando sospechaban haber sido descubiertos, enviaban mensajes falsos para despistar al enemigo.

Este artículo apareció en el número 4

¿Qué tal en los deportes?, para muestra el béisbol: el coach se planta junto a la almohadilla y empieza a emitir al bateador y a sus corredores la estrategia de la jugada a través de una serie de señas que parecen un ataque al corazón. Las señas cambian jugada a jugada, ya que son rápidamente interpretadas por el pitcher, por ejemplo, un toque de bola.

Quien haya leído el libro o visto la película de El código Da Vinci recordará que la historia está llena de pistas ocultas en obras de arte, bóvedas de seguridad, y un artefacto curioso llamado cryptex que custodiaba un secreto (esto, claro, es una historia de ficción, pero nos refleja la necesidad permanente del hombre de guardar secretos). Para abrir el dispositivo, la combinación de componentes rotatorios tenía que estar en orden correcto. Si se abría de manera forzada, un mecanismo interno rompería un tubo con vinagre el cual disolvería el mensaje escrito en papiro. Este artefacto fue codiciado para buscar una verdad que había permanecido oculta por dos mil años y que afectaría creencias milenarias. Lo mismo sucede en La leyenda del tesoro perdido o en la solución de algunos de los problemas que se le presentan a Sherlock Holmes.

Así podríamos encontrar cientos de ejemplos sobre la importancia de la seguridad hasta llegar al día de hoy, donde el principal factor es lo vulnerable de la información digital. Para proteger este nuevo formato de la información, contamos con una serie de algoritmos y tecnologías altamente complejas que nos permiten resguardarla y los mensajes incluyen propiedades de confidencialidad, integridad autenticidad y no rechazo, a través de firmas digitales, recursos que incluso se encuentran ya legislados en algunos países.

« La historia de la humanidad nos ofrece múltiples ejemplos de cómo la información siempre ha sido del interés ajeno, lo mismo que guardarla siempre ha tenido sus buenos motivos »

Sin embargo, lo más interesante no es el ingenio que el ser humano ha desarrollado para cifrar: ¡hay que ver lo genial que resulta para descifrar! Cada vez existen técnicas más sofisticadas y mayor poder de cómputo para romper llaves, crackear contraseñas e introducirse sin autorización en la información confidencial de las organizaciones. Entre más largas las llaves de codificación, mayores retos para los hackers que encuentran al final una forma de romperlas. ¡Incluso se utilizan técnicas de ingeniería social para obtener información de viva voz de los empleados!

Entonces, ¿qué podemos hacer para ganar la carrera a estos pillos de la información? Algunas prácticas saludables para su organización son las siguientes:

- Clasifique su información, decida con claridad qué es lo confidencial, qué es lo sensible y qué es lo público.
- Sensibilice a sus empleados sobre la importancia de proteger la información, principalmente aquélla clasificada como confidencial.
- Utilice técnicas innovadoras que ayuden a sus usuarios a crear contraseñas robustas y a renovarlas periódicamente. ¡Recuerde a nuestros ancestros!
- Emprenda campañas de seguridad, con algún eslogan que fomente la seguridad como una constante, por ejemplo: “La contraseña es como el cepillo de dientes: debe ser fuerte, no se presta y se debe cambiar cada tres meses”
- Proteja su información crítica en todos sentidos: desde derechos de autor para secretos de marca hasta respaldos en cajas de seguridad bancarias.

Aún mejor: piense mal y acertará; póngase en los zapatos del enemigo, “¿qué se le ocurriría al otro para robar mi información…?” Siendo maliciosos, tendremos nuevas ideas para protegernos. ¡Permanezca a la moda, esté siempre seguro!

La invitación es a capitalizar todo este conocimiento que la humanidad ha atesorado en materia de protección de la información, para buscar ideas fáciles y analogías interesantes para los programas de concientización, además de buscar que los colaboradores compren la idea de que la seguridad es una tarea de todos y una responsabilidad compartida.

El eslabón más débil

El control por sí solo no es suficiente

Omar Alcalá
CISSP, CISA y CEH
oalcala@scitum.com.mx

Hace no mucho tiempo leía un hilo de las preguntas que se realizan en *Bugtraq*, una lista de distribución de temas de seguridad. La pregunta decía así: "¿Alguien podría decirme los métodos disponibles para evitar al *firewall* (hacerle "*bypass*") para cualquier tipo de tráfico?". La persona no colocó más contexto en torno a la pregunta.

Para ser honesto me preocupó. Por un momento quise pensar en que quien lanzó la pregunta quería realizar algún tipo de prueba de penetración o alguna prueba particular hacia un producto, pero nunca lo aclaró. Lo que sí me hizo reflexionar es que este tipo de interrogantes suceden en la vida cotidiana, muchas veces por personal no técnico, y muchas veces no buscan exactamente una prueba de seguridad sino transgredir las políticas de seguridad establecidas.

Es muy complicado para la mayoría de las personas técnicas comprender que las no técnicas definitivamente no tienen idea de lo que se les habla cuando entramos al mundo de las computadoras. A las personas no técnicas les importa su *e-mail*, sus redes sociales y su mensajería instantánea. Hay quienes van más lejos y buscan obtener programas, música o películas gratis. Y hay quienes todavía llegan más allá, tratando de burlar los elementos de seguridad implementados.

Afortunadamente este hilo habló de hacer esos *bypass* con túneles cifrados (SSH o SSL) y técnicas avanzadas de inyección de paquetes, lo cual responde la pregunta original con muchas complicaciones para personas no inmersas en la parte de tecnología, pero me surgieron dos preguntas:

¿Qué pasa cuando un responsable de seguridad quiere burlar la seguridad misma?

¿Qué pasa cuando una persona no técnica quiere acceder a recursos no autorizados?

Para la primera pregunta las respuestas en el hilo original fueron contestando: "soluciones técnicas, pero revisa tus políticas de seguridad", "debe ser para algo que sea justificado en tu trabajo" (léase, que no sea causa de recisión de contrato), o bien, cuidados de tipo legal (acceder a redes no autorizadas y ser atrapados en el acto). Incluso hubo una respuesta donde se le mencionó que si tenía una necesidad de uso de una aplicación y que el *firewall* no lo permitía, lo lógico y elemental sería solicitar los accesos; la petición legítima no podría ser negada.

Para la segunda pregunta el riesgo se diversifica. Sea un *firewall*, IPS, control de accesos, Filtrado de Contenido o lo que sea que exista en la red, siempre existirá el riesgo más por el factor humano que por otra circunstancia.

Debido a ello, la importancia de que los controles implementados sean entendidos por todos implica tener bases sólidas sobre los derechos y obligaciones de un empleado en cuanto a la información que maneja, además de los límites en el uso permitido de los recursos informáticos de la organización.

Las políticas de seguridad, los acuerdos de confidencialidad, la clasificación de la información (en cualquier modo en que ella exista) y las sesiones de concienciación y actualización en materia de seguridad siempre serán importantes y ninguna empresa puede obviarlas. La alta dirección debe estar comprometida con la seguridad para mantener al día, actualizados y en orden todos los documentos que establezcan las reglas que gobiernan la empresa.

El eslabón más débil en los controles mismos

Si bien hay individuos con capacidades impresionantes para crear, identificar o burlar los controles tecnológicos de los sistemas (llámense *hackers*), éstos son escasos a nivel mundial. Esto lo menciono porque hay quienes pueden argumentar que la tecnología está mal hecha, y podemos encontrar casos claros de aversión a marcas como Microsoft o el protocolo DNS, que son juzgados por presentar un pobre diseño en materia de seguridad.

Recuerdo en una asistencia al Defcon que se celebra anualmente en Las Vegas, Nevada, cómo Dan Kaminsky, reconocido profesional de tecnologías de la información, criticó duramente la arquitectura e implementación del protocolo DNS en su conferencia sobre *Cache Poisoning* (envenenamiento del caché en los servidores de DNS), e incluso habló de realizar evasiones a tecnologías de seguridad como las que fabrican ISS (ahora IBM) y Check Point. Éstos son ejemplos de acciones que pocas personas en el mundo pueden lograr, y sobre las que los propios fabricantes trabajan día con día para corregir errores que las herramientas pueden tener.

Los controles tecnológicos difícilmente serán 100% confiables puesto que, hasta donde se puede vislumbrar, serán diseñados por humanos, lo que obliga a la tecnología a ser inherentemente imperfecta. Pese a lo anterior, los controles creados hasta el momento realizan con alto grado de eficacia las funciones o contenciones para las que fueron diseñados.

La siguiente pregunta obligada es: Si tengo los controles en el lugar adecuado, ¿por qué continúan existiendo fallas de seguridad? Hay tres puntos importantes:

- **Administración operativa** (cambios, parches, versiones, incidentes, requerimientos, altas, bajas).
- **Monitoreo** (detección y contención de eventos).
- **Verificación de controles de seguridad** (evaluación de controles).

Esto me recuerda no pocos vicios en torno a cuando un control está establecido, pero si leemos detenidamente las viñetas anteriores, el control necesita de la interacción con el ser humano. Una vez más, estamos hablando de que es el mismo administrador, operador, consultor, usuario o responsable del sistema quien es más propenso a fallar.

El que el experto falle no necesariamente significa que realmente no conozca la herramienta, sino que es la operación diaria, mantener numerosas reglas, firmas, usuarios, políticas en los equipos, lo que hace que en algún momento "algo" quede fuera de lugar: un acceso no válido, un puerto no cerrado, una contraseña preconfigurada (por "*default*"), un servicio innecesario activado, entre otros. Es común ver cómo las reglas de un *firewall* van creciendo, cómo poco a poco surgen interrogantes sobre "la regla X, ¿es correcta?" o "¿el usuario Y todavía necesita estos permisos?". Y es donde podemos observar cómo el propio ser humano debilita el control tecnológico.

Como podemos ver, los controles tecnológicos apoyan el cumplimiento de la seguridad que la institución necesita, pero si no tomamos en cuenta el factor humano en todo momento, dichos controles disminuirán su utilidad y no se tendrán los resultados esperados.

«la importancia de que los controles implementados sean entendidos por todos implica tener bases sólidas sobre los derechos y obligaciones de un empleado en cuanto a la información que maneja, además de los límites en el uso permitido de los recursos informáticos de la organización»

El sentido de los controles

Hubo algo que me llamó mucho la atención respecto a este tópico, que puede ayudar a entender claramente por qué la seguridad gira en torno a las personas: alguien definió al *firewall* en términos humanos como "un dispositivo que aplica la política de seguridad [establecida]". Al final del día, la tecnología es sólo un control, y el factor humano es sobre quien reside el correcto uso y aplicaciones del control.

Todos los controles pueden venirse abajo si vemos que una asistente conoce las contraseñas de sus jefes, si personal de Finanzas comparte sus usuarios de acceso con otros, o si el DBA es compartido por personas de Bases de Datos, desarrolladores y programas por igual (esto es mucho más frecuente de lo que podría suponerse). Por ello la insistencia de que una política que defina los roles, responsabilidades, obligaciones, auditoría ("*accountability*") y sanciones debe ser parte integral de la seguridad.

Aunque a mucha gente no le gusta, el eslabón más débil somos nosotros mismos, y bajo esta premisa debemos considerar los controles de seguridad. La tecnología puede tener errores, pero esos a la larga son modificables; los humanos siempre seremos impredecibles y guiados por sentimientos, lo que tiende a hacernos irracionales por momentos, por lo que, independientemente del control, el ser humano siempre será una variable importante a considerar en el riesgo para la seguridad.

En el mismo evento del Defcon hay una playera que al frente dice en inglés "*Social Engineer Specialist*", que significa "Especialista en Ingeniería Social"; al reverso indica "*Because there is no patch for human …*". No puedo indicar la última palabra, pero lo traduciré como sigue: "Porque no hay un parche para la torpeza humana". Termino con una reflexión: No es que seamos torpes, así lo ven los *hackers*, simplemente no hay conciencia del daño que se puede causar por no cuidar algo tan valioso para el ser humano como lo es la información.

La importancia de la arquitectura de seguridad

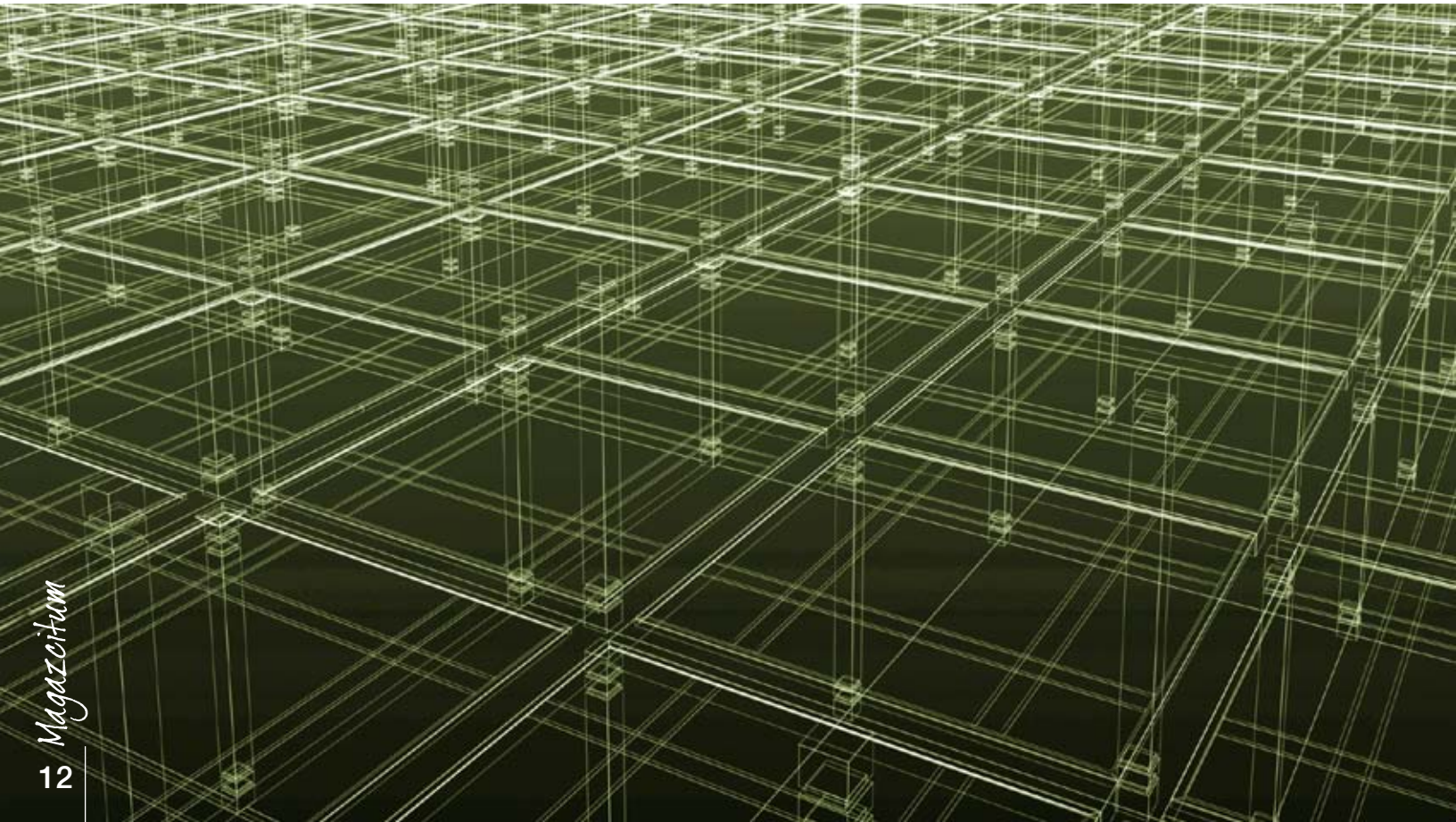
Esteban San Román
CISSP, CISA y CEH
esanroman@scitum.com.mx

> Una estrategia de seguridad de la información, apoyada en un diseño que combine una infraestructura propia de seguridad y un esquema de servicios en *outsourcing* adecuado, puede mejorar su posición de cumplimiento… y su tranquilidad.

Durante mucho tiempo las organizaciones han sido más reactivas que proactivas en el ámbito de la seguridad informática. La incorporación de elementos de seguridad se ha dado en ocasiones por moda y en otros momentos por una necesidad inminente de resolver un problema.

En una misma organización se pueden encontrar diversas plataformas de diferentes fabricantes haciendo que su infraestructura se asemeje a una auténtica exposición de tecnología. El cada vez más común recorte de presupuesto correspondiente a TI en las organizaciones hace más difícil mantenerlas actualizadas y en funcionamiento, incluso, yendo más lejos, hace mucho más compleja su interoperabilidad.

Es importante recalcar que en estos entornos se suele encontrar más de una plataforma que ofrece la misma funcionalidad, por lo que el administrador deberá desarrollar un proceso sistematizado que le permita evaluar de entre las distintas opciones la que mejor se adecúe a sus necesidades. En otros casos existen alternativas como los servicios administrados, que pueden economizar los gastos asociados con el monitoreo 7x24, el manejo de incidentes y la elaboración de reportes.



De acuerdo con lo anterior, esta estrategia de operación involucra la definición de un modelo a la medida de las necesidades de la organización, en el cual se puede tener una infraestructura básica de seguridad de la información con una inversión propia y apalancarla con un servicio en outsourcing de monitoreo que correlacione todos los eventos de seguridad.

El modelo de arquitectura de seguridad define esta estrategia. Así pues, el arquitecto de seguridad comenzará por realizar un análisis de riesgos donde determinará tanto el grado de exposición de la organización a amenazas como el balance adecuado de elementos y servicios de seguridad requeridos.

Para realizar este análisis de riesgos el arquitecto de seguridad debe tomar en cuenta la normatividad aplicable a la organización y hacer coincidir los objetivos de TI con los objetivos del negocio.

Como se puede inferir de lo anterior, cuando se habla de arquitectura de seguridad se están abarcando muchos campos de conocimiento: desarrollo, administración de sistemas, aplicaciones de escritorio, infraestructura de comunicación de datos, por lo que este concepto no se limita a elementos tan puntuales como lo pueden ser la constitución de un sistema o la conformación de un grupo de trabajo.

Entonces ¿por dónde empezar? A continuación sugerimos algunos pasos a seguir a fin de dar un enfoque metodológico a la arquitectura de seguridad:

- Apegarse a los lineamientos de las políticas de seguridad. Ha terminado la era de hacer las instalaciones con los valores por omisión. Si el administrador trabaja en las opciones y preferencias de la configuración de los programas puede crear una visión sistemática de la seguridad corporativa y permearla a todos los niveles de la organización.
- Cada decisión debe ser sustentada y acreditable. Cada inserción o eliminación de un elemento en la arquitectura global debe estar sustentada como mejora o depuración de alguna que haya sido previamente acordada.
- Respetar el principio del menor privilegio (*least privilege*). Cuando en una arquitectura de seguridad se respeta el que nada tenga más permisos de los necesarios, se disminuye la posibilidad de que en un ataque se puedan elevar privilegios y con esto se acota el daño potencial que se pudiese sufrir.
- Defensa en profundidad. Una adecuada arquitectura de seguridad considera varias funciones de seguridad operando en diferentes niveles, de manera que se evite manejar una sola plataforma que, en caso de ser vencida, deje expuestos los recursos de información.
- Incorporar elementos de auditoría. Con el fin de tener elementos de mejora continua hay que mantener historiales de todos los eventos de seguridad. Una de las primeras actividades de un *hacker* al hacer una intrusión a un sistema es ocultar sus huellas. Es muy importante desarrollar una estrategia de generación, protección y preservación de evidencias.

Adicionalmente, hay que tener en cuenta que un esquema de seguridad es tan robusto como su enlace más débil y que la tarea de fortalecer la arquitectura de seguridad es una etapa y no un destino. Hay que seguir informándose y mantener un sentido autocrítico con el fin de estar listo para tomar las decisiones y realizar los ajustes más apropiados.

ITIL
¿qué es y para qué sirve?

Héctor Acevedo Juárez
CISSP, CISA, CGEIT, ITIL, MCSE
hacevedoj@scitum.com.mx

Éste es un primer artículo de una serie que pretende explicar, desde un punto de vista pragmático, qué es ITIL y para qué puede ser usado en las organizaciones en la actualidad. En esta entrega se cubren algunos temas preliminares y se revisa un poco de la historia de ITIL.

Introducción

Si usted se dedica a algo relacionado con TI es altamente probable que haya escuchado de ITIL e incluso puede que sea de los afortunados (¿afortunados?) que ya están involucrados en un proyecto de implantación de ITIL.

ITIL está de moda en el mundo, todos hablan, bien o mal según les haya ido, de ITIL. En las revistas de auditoría ITIL, en las revistas de seguridad ITIL, por todos lados ITIL… pero, ¿qué es ITIL y para qué sirve? En esta serie de artículos trataré de dar respuesta a las preguntas anteriores, de tal manera que los lectores hagan un mejor uso de ITIL en sus organizaciones, sacándole el mejor provecho y sin pedirle que haga cosas que no sabe o no puede hacer.

Una aclaración importante: no pretendo hacer una revisión técnica con detalle de ITIL en cualquiera de sus versiones, así que si está buscando capacitación o profundización de sus conocimientos en ese sentido, este no es el texto adecuado (en una serie posterior de artículos prometo revisar la versión 2, la versión 3 y las diferencias entre ambas). La idea aquí es entender "la filosofía" de ITIL y dar algunas ideas de cómo, cuándo y por qué aplicarlo en la vida real. Así pues, emplearé la versión 2 para desarrollar mis ideas, aunque todos los conceptos aplican de igual manera si usted está pensando en la versión 3.

Dos temas preliminares

Antes de entrar en materia, es preciso hablar de dos temas relevantes y muy relacionados con ITIL:

1. Administración de servicios de TI.
2. Administración por procesos.

¿Por qué es necesario? Fácil, porque algunas de las premisas básicas de ITIL descansan en esos temas y, por lo tanto, entender ITIL implica, inevitablemente, entenderlos.

¿Qué es eso de administración de servicios de TI? Veamos: si reconocemos la creciente dependencia en las áreas de TI para el cumplimiento de los objetivos estratégicos, entonces esta dependencia implica una mayor calidad de los servicios de TI. Por ello, la calidad debe alinearse a los objetivos de negocio y a las necesidades de los usuarios, lo que nos lleva a un cambio de paradigma: las áreas de TI deben cambiar su visión de administradores de dispositivos a administradores de servicios de TI.

Tradicionalmente al preguntarle a alguien de TI "¿a qué te dedicas?", estamos acostumbrados a escuchar respuestas como "soy administrador de firewalls", "soy administrador de servidores", etc., pero, ¿cuál es el problema con ello? Si lo pensamos bien, los usuarios no piensan, como dicen los técnicos, en "cajas". Ellos pueden incluso no saber, ni les importa, qué es o para qué sirve un firewall, un *switch*, un *router*, etcétera. Lo que los usuarios quieren es hacer uso de ciertos servicios, los famosos servicios de TI, como el correo electrónico, el acceso a Internet, el servicio de impresión, etcétera.

Es precisamente esta dicotomía entre un área de TI y sus usuarios la que puede causar en muchas ocasiones que sus opiniones sean diametralmente opuestas en cuanto a lo que la primera ofrece: mientras que los técnicos se enfocan en "administrar cajas", sin darse cuenta que las relaciones entre ellas son relevantes, los usuarios lo que ven son servicios, los cuales se proporcionan a través de todo un conjunto de cajas diferentes, por lo que una falla o deficiencia en una de ellas se propaga por todo el sistema. Es así como, por ejemplo, llegamos a ver reportes de TI que presumen de 99.9999% de disponibilidad en el *firewall* de acceso a Internet, mientras que los usuarios se quejan de que el servicio de acceso a Internet es muy malo por lento, intermitente, o por otras razones.

¿Cuál es el meollo del asunto? Precisamente está en que un servicio de TI es entregado a los usuarios mediante un conjunto de cajas (tecnología), personas que manejan las cajas (gente) e instructivos y relaciones entre ellos (procesos). Es por ello que el área de TI debe entender que lo que administra y da a sus usuarios son servicios de TI, no dispositivos. El reto es lograr la integración eficiente de gente, procesos y tecnología para una mejor administración de los servicios de TI, optimizando el uso de los recursos y mejorando constantemente los niveles de servicio.

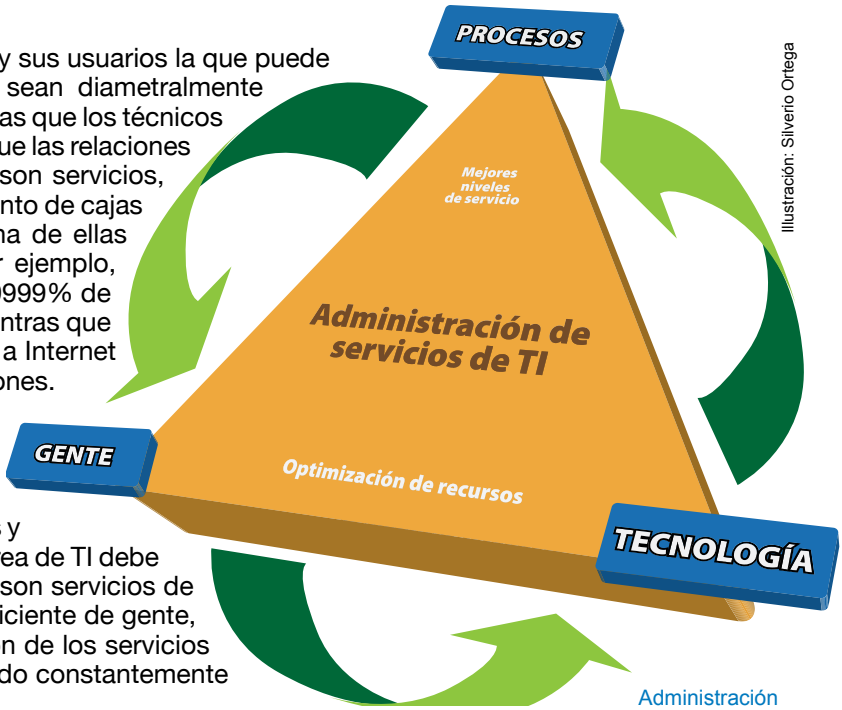


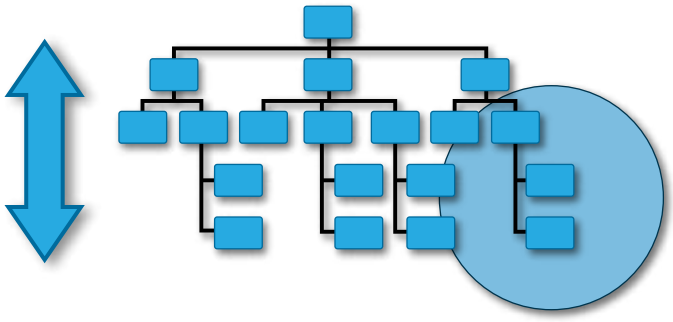
Ilustración: Silverio Ortega

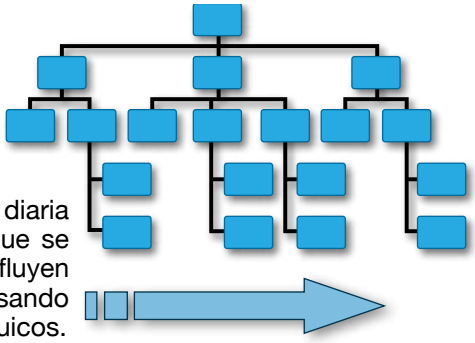
Administración de servicios de TI: integrando gente, procesos y tecnología

¿Y qué es la administración por procesos? Para facilitar la explicación, un poco de historia: tradicionalmente, las organizaciones se han estructurado con base en departamentos funcionales que dificultan la orientación hacia el cliente (por ejemplo, Dirección de Finanzas, Dirección de Producción, Dirección de Ventas y Dirección de Sistemas), con organigramas muy jerárquicos divididos en múltiples niveles. Normalmente este tipo de organizaciones adolece de dos grandes problemas:

a) La comunicación "oficial" fluye verticalmente y puede ser muy lenta. Incluso a veces propicia el conocido juego del "teléfono descompuesto". Por ejemplo, dos operarios de áreas distintas que requieren de un acuerdo oficial deben "subir" por el organigrama hasta la rama común, pasando por todos los niveles del mismo (operador A –> supervisor de A–> coordinador de A –> gerente de A -> director de A -> director de B -> gerente de B -> coordinador de B -> supervisor de B -> operador B).

b) Se crean "cotos de poder" e "islas ideológicas" que nada tienen que ver con la satisfacción de las necesidades del cliente final. Algunos ejemplos: El director de cierta área defiende a capa y espada sus privilegios y, en muchas ocasiones, más que colaborador de otros directores es un enemigo de ellos, y ellos de él. La gente de Finanzas sólo ve a la empresa desde su punto de vista (estados financieros, costos, gastos, etc.) y no considera otras variables y otros puntos de vista como satisfacción del cliente, clima laboral, etcétera.





Sin embargo, en la vida diaria de la organización lo que se tiene son procesos que fluyen horizontalmente, atravesando los organigramas jerárquicos.

Es por ello que surge la administración por procesos, que percibe la organización como un sistema interrelacionado de procesos que contribuyen conjuntamente a incrementar la satisfacción del cliente. La administración por procesos coexiste con la administración funcional, asignando "propietarios" a los procesos clave, haciendo posible una gestión interfuncional generadora de valor para el cliente y que, por tanto, procura su satisfacción; determina qué procesos necesitan ser mejorados o rediseñados, establece prioridades y provee de un contexto para iniciar y mantener planes de mejora que permitan alcanzar objetivos; y hace posible la comprensión del modo en que están configurados los procesos de negocio, de sus fortalezas y de sus debilidades.

Así mismo da la forma en que la organización administra y mejora continuamente los procesos de negocio para lograr sus objetivos y crear valor para sus accionistas, clientes y colaboradores. Al final, lo que la administración de procesos intenta cambiar es: ir de una organización orientada a productos (en la que existen procesos no coordinados ni administrados), por una organización que administra sus procesos en ciclos de mejora continua mediante el famoso ciclo de "*plan-do-check-act*" o PDCA, por sus siglas en inglés.

Historia de ITIL

Pues bien, parece que ya es hora de entrar en materia. Empecemos como los clásicos con una definición:

ITIL (IT *Infrastructure Library*, biblioteca de infraestructura de TI) = Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

¿Suena bien no? Pero para qué sirve y cómo se usa, eso es harina de otro costal y es lo que trataré de explicar en esta serie de artículos, pero antes veamos un poco de sus antecedentes: en 1987 la CCTA, un organismo del gobierno británico (ahora llamado la OGC) inició un proyecto llamado GITIMM (*Government IT Infrastructure Management Method*), en el cual involucraron a varias firmas de consultoría para investigar y documentar las mejores prácticas para planear y operar la infraestructura de TI. Poco después, conforme el proyecto evolucionaba de administración de infraestructura a administración de servicios de TI, se le cambió el nombre a ITIL.

Como marco de referencia, ITIL se creó como un modelo para la administración de servicios de TI e incluye información sobre las metas, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las áreas de TI.

Desde sus inicios ITIL fue puesta a disposición del público en forma de un conjunto de libros, de ahí su nombre, para que las organizaciones de todo el mundo pudieran adoptarlo.

La primera versión consistía de 10 libros principales que cubrían dos grandes temas: "Soporte al servicio" y "Entrega del servicio", amén de una serie de libros complementarios que cubrían temas tan disímbolos como la administración de la continuidad o cuestiones relacionadas con cableado. Posteriormente, en 2001 se hizo una reestructura importante que reunió los 19 libros principales en sólo 2, mientras que otros temas siguieron en libros separados, dando así un total de 7 libros para la segunda versión de ITIL:

- Soporte al servicio (1).
- Entrega del servicio (2).
- Administración de la seguridad (3).
- Administración de la infraestructura ICT (4).
- Administración de las aplicaciones (5).
- La perspectiva del negocio (6).
- Planeación para implantar la administración de servicios (7).

Precisamente con la versión 2, a mediados de los años 90, ITIL fue reconocido como un "estándar de facto" para la administración de servicios de TI, el cual, como siempre, tuvo que seguir evolucionando para considerar las nuevas escuelas de pensamiento y alinearse mejor a otros estándares, metodologías y mejores prácticas, lo que llevó en 2007 a la liberación de la versión 3 de ITIL.

ITIL V3 sólo consta de cinco libros, que están estructurados en torno al ciclo de vida del servicio:

- Estrategia de servicios.
- Diseño de servicios
- Transición de servicios.
- Operación de servicios.
- Mejora continua de servicios.

Esta nueva estructura organiza los procesos contemplados en ITIL V2 con contenido y procesos adicionales encaminados a una mejor administración del periodo de vida de los servicios de TI. Partiendo de esta observación, podemos afirmar que la V3 refuerza el foco en los servicios de TI, sin dejar de lado los procesos, pero haciendo patente que aunque los procesos son importantes son secundarios y sólo existen para planificar, entregar y dar soporte a los servicios.

Éste es el segundo artículo de una serie que pretende explicar, desde un punto de vista pragmático, qué es ITIL y para qué puede ser usado en las organizaciones hoy en día. En esta entrega revisaremos cómo está diseñado el modelo de procesos de ITIL, además hablaremos brevemente de las certificaciones disponibles y de qué versión de ITIL emplear.

Definiendo "las mejores prácticas"

Aunque existen diversas definiciones, para efectos prácticos podemos decir que las "mejores prácticas" son un conjunto de prácticas que alguien obtiene analizando y estudiando qué hacen y qué no hacen los mejores exponentes de un tema en particular. La idea es que al terminar el análisis se tendrá un conjunto de prácticas comunes a todos aquellos que están a la vanguardia, y es precisamente ese conjunto el que se recopila y se lanza como "las mejores prácticas" para un tema dado.

Así pues, las mejores prácticas no tienen un fundamento matemático o analítico puro, simplemente son obtenidas del mundo real y representan lo que "parece ser lo mejor" hasta el momento. Como tales, las mejores prácticas pueden cambiar con el transcurso del tiempo y, lo que también es muy importante, ser muy cuidadoso al establecerlas para no llegar a conclusiones erradas o ilógicas que lleven a unas "mejores prácticas" absurdas.

Entendiendo ITIL

Al final de la primera entrega de esta serie se revisó brevemente la historia de ITIL y se mencionó algo sobre la estructura de la versión 2 y la versión 3; pasaremos ahora a explicar con un poco de más profundidad la filosofía de ITIL y las características de cada versión.

Antes que nada, recordemos que ITIL es un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos. Pero ¿qué significa eso? Pues simple y sencillamente que los libros de ITIL listan una serie de procesos y funciones que se recomienda implantar para una mejor entrega de los servicios que las áreas de TI proporcionan a sus usuarios. La idea es que toda organización de TI opere con un enfoque de procesos para la administración de servicios de TI, empleando ITIL como una guía sobre qué procesos implantar y cuáles son las características principales de dichos procesos.

En ITIL 2 se definió un modelo de procesos cuyo núcleo lo constituyen los libros de "Soporte de servicios" y "Entrega de servicios", y juntos forman la "Administración de servicios":

Modelo de procesos de ITIL V2

De hecho, se hizo tanto énfasis en la administración de servicios que prácticamente todos los esfuerzos de implantación de ITIL V2 en realidad sólo se centran en esos dos libros, que listan 10 procesos y una función:

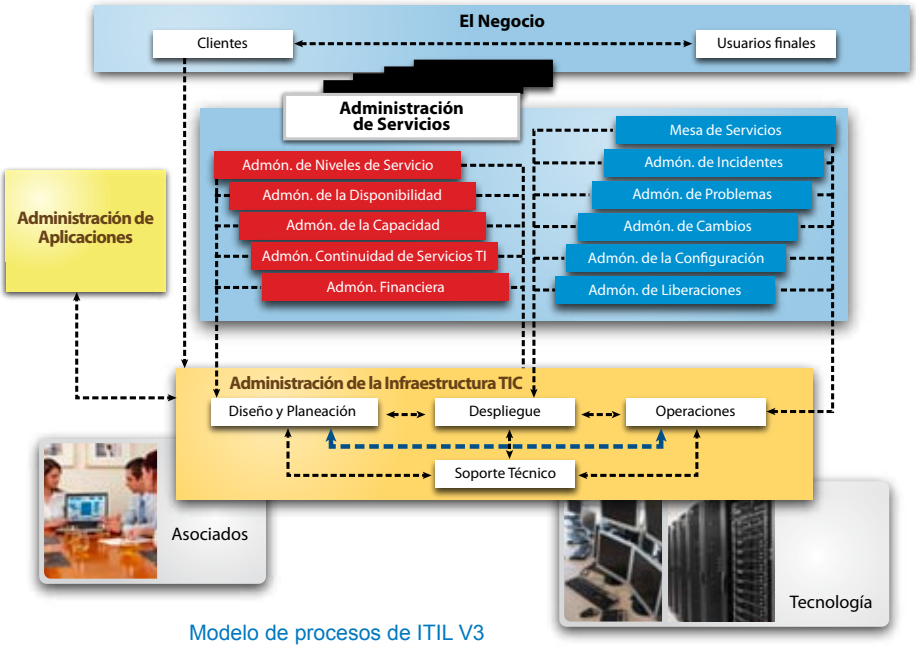
Soporte de servicios.

- Administración de la configuración: Proceso cuyo objetivo es lograr el "control de la infraestructura". La idea es tener claridad en los componentes de la infraestructura involucrados en la prestación de los servicios, la documentación (configuración) de los mismos y las relaciones entre ellos.
- Administración de incidentes. Enfocado a lograr, lo antes posible, la restauración de los servicios cuando éstos quedan inoperables o degradados a causa de un incidente.
- Administración de problemas. Proceso responsable de identificar la causa raíz de los incidentes para evitar su repetición y minimizar el impacto sobre las operaciones del negocio.
- Administración de cambios. Garantiza el uso de métodos estandarizados para la realización de cambios en la infraestructura, minimizando así el impacto de los incidentes relacionados con dichos cambios.
- Administración de liberaciones. Permite una visión integral de los cambios para asegurar que en su implantación se hagan las pruebas necesarias y se consideren tanto los aspectos técnicos como los no técnicos de la liberación.
- Mesa de ayuda. Función en el organigrama con actividades de gran importancia en la interrelación de TI con sus usuarios: es parte fundamental del proceso de incidentes al ser el punto único de contacto para aconsejar, guiar, y restaurar rápidamente los servicios normales de los clientes y usuarios.

Entrega de servicios.

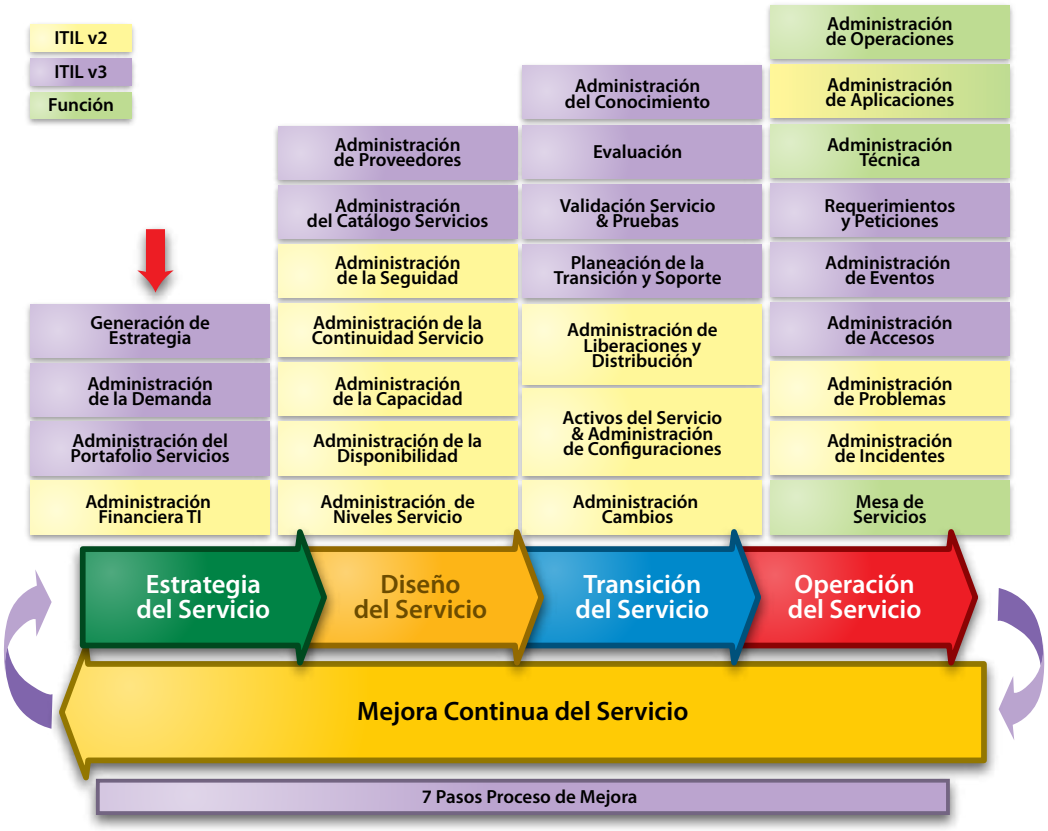
- Administración de niveles de servicio. Proceso encargado de mantener y mejorar la calidad de los servicios de TI mediante la definición, monitoreo y reporte de los niveles de servicio.
- Administración financiera de TI. Provee guías para la utilización eficiente, en cuanto a costos, de los recursos de TI.
- Administración de la capacidad. Proceso que asegura que la capacidad de los recursos de TI sea suficiente para cumplir las necesidades presentes y futuras del negocio, siempre a un costo adecuado.
- Administración de la disponibilidad. Permite ofrecer un nivel de disponibilidad sostenido en los servicios de TI, con un costo adecuado para que el negocio pueda alcanzar sus objetivos.
- Administración de la continuidad. Proceso que permite la continuidad de los servicios de TI para que, en caso de un desastre, se recuperen dentro de los tiempos y costos acordados.

Ahora bien ¿qué pasa con ITIL V3? Al igual que la versión anterior, define un modelo de procesos basado en la administración de servicios, sólo que ahora dichos procesos están supeditados al ciclo de vida de las aplicaciones y los servicios de TI



Modelo de procesos de ITIL V3

Como se dijo en al artículo anterior, la nueva versión organiza los procesos comprendidos en la V2 con contenido y procesos adicionales, reforzando el foco en los servicios de TI y sin dejar de lado los procesos, pero haciendo patente que aunque los procesos son importantes, son secundarios y sólo existen para planificar, entregar y dar soporte a los servicios (todo sometido a un ciclo de mejora continua):



Procesos y funciones considerados en ITIL V3

Así pues, al final podemos decir que ITIL se trata de definir, implantar y administrar los procesos y funciones de TI utilizando como guía los libros de ITL.

Certificaciones en ITIL

Dado que ITIL no es un estándar, es importante comprender que una empresa no puede certificarse en ITIL. Lo más que puede obtenerse es una especie de diagnóstico en el que alguna empresa de consultoría puede opinar que, desde su punto de vista, cierta organización "está alineada" con ITIL. Las únicas certificaciones disponibles actualmente son para personas, que de esta manera reciben un aval sobre sus conocimientos de parte de los organismos que desarrollan ITIL.

En ITIL V2 existen tres niveles de certificación:

- ***Foundations.*** Diseñada para asegurar el entendimiento de los principios, la termin ología y el contenido de los libros de Administración del servicio (Soporte de servicios y Entrega de servicios).
- ***Practitioner.*** Enfocada a aquellos responsables de diseñar e implantar los procesos de Administración del servicio en una organización. Existen varias certificaciones, de acuerdo a las diversas áreas cubiertas en la administración de servicios según ITIL:
  - ***5 Practitioners de soporte de servicios*** (administración de cambios, administración de configuraciones, administración de problemas, administración de liberaciones, administración de incidentes y mesa de ayuda).
  - ***5 Practitioners de entrega de servicios*** (administración de la disponibilidad, administración de la capacidad, administración financiera de TI, administración de la continuidad de servicios de TI, y administración de niveles de servicio).
  - ***4 Practitioners*** combinados (mesa de ayuda, administración de incidentes y de problemas -IPSR-, administración de cambios, configuración y liberaciones -IPRC-, administración financiera y de niveles de servicio -IPAD-, y administración de disponibilidad, de capacidad y de continuidad de servicios de TI -IPPI-).
- ***Service Manager.*** Destinada a consultores y administradores que deben tener conocimientos profundos de todos los temas relacionados con la administración de servicios de TI de acuerdo a ITIL V2.

Por su parte, ITIL V3 considera cuatro niveles de certificación:

- ***Foundations.*** Asegura el entendimiento de los principios, la terminología y el contenido de los procesos y funciones considerados en ITIL V3.
- ***Nivel intermedio.*** Diseñada para reforzar las habilidades para analizar y aplicar los conceptos de ITIL. Es análoga a la certificación ***Practitioner*** de V2, por lo que existen varias opciones:
  - 5 de ciclo de vida de los servicios (estrategia de servicios, diseño de servicios, transición de servicios, operación de servicios y mejora continua de servicios).
  - 4 de Capacidad (Soporte y análisis operacional -OS&A-, oferta y acuerdos de servicios -SO&A-, liberación, control y validación -RC&V- y planeación, protección y optimización -PP&O-).
- ***ITIL Expert.*** Destinada a aquellos que requieren consolidar el conocimiento obtenido en los niveles de certificación anteriores.
- ***ITIL Master.*** Es el nivel máximo de certificación en V3 y se enfoca en asegurar la habilidad para analizar y aplicar los conceptos de ITIL en nuevas áreas. Aún está en desarrollo.

Continúa en página 19

Ya sea que busque proteger a su organización contra las amenazas del correo entrante o reducir los riesgos legales, financieros y normativos relacionados con el correo electrónico saliente, necesita tener confianza en la solución que elija.

Basado en su análisis de nuestra visión y capacidad para ejecutarla, la firma de analistas Gartner, Inc. ha posicionado a Proofpoint en el cuadrante de líderes dentro del "2010 Magic Quadrant for Secure Email Gateways" (anti-spam, anti-virus, filtrado de contenido saliente, cifrado de correo electrónico, prevención de intrusiones).

Vea una copia gratuita del "2010 Magic Quadrant for Secure Email Gateways" en:

www.proofpoint.com/2010mq

proofpoint™

Control tomorrow's email risks today

¿ITIL V2 o ITIL V3?

Esta es una pregunta que surge con frecuencia y hay mucha confusión en el mercado. Dado que la nueva versión es una simple evolución de la anterior no debería haber tanto problema. A continuación algunas recomendaciones de acuerdo al estado de implantación de ITIL en su organización.

- No hay trabajo anterior sobre ITIL. Si su organización apenas va a adoptar ITIL, definitivamente la mejor opción es iniciar con la versión 3, de esta manera evitará después tener que adecuar para cumplir con V3 desde algo diseñado para cumplir con V2.
- Implantación inicial de V2. En caso de que se lleve poco tiempo trabajando con V2, de tal manera que apenas se está en la fase de diseño o hay muy poco trabajo de implantación, sería recomendable hacer un alto en el camino y evaluar el nivel de esfuerzo necesario para saltar a una implantación de la V3, dependiendo de los presupuestos disponibles, el nivel de conocimiento de la gente y la complejidad de su organización.
- Implantación avanzada de V2. Definitivamente conviene continuar con la implantación pero dedicar un pequeño esfuerzo para ver en qué momento será conveniente cambiar a la siguiente versión de ITIL.

Recordemos que nada de lo que se haga en V2 sale sobrando, todo será "reutilizado" cuando se migre a la versión 3. La decisión de cambiar o no de versión debe ser por cuestiones de negocio y no de moda o deseos de los equipos encargados de regular la adopción de ITIL.

Implantando ITIL: más que tecnología, un cambio organizacional

Ya sabemos un poco de la historia de ITIL, de su estructura y de algunas de las características de las versiones 2 y 3. Antes de puntualizar algunas ideas sobre cómo implantarlo, preguntémonos ¿por qué implantar ITIL?

Es indudable que ITIL está de moda y cada día son más las organizaciones que se embarcan en esfuerzos para que sus áreas de TI proporcionen servicios mediante procesos alineados a ITIL pero, y aquí algo muy interesante, al mismo tiempo se tienen presiones de todos lados para alinearnos a otros estándares, regulaciones y mejores prácticas como ISO-20000, CobiT, SOX, ISO-27001, regulaciones bancarias, PCI, y un largo etcétera.

¿Cómo proceder entonces? Lo mejor siempre es hacer un alto en el camino, si no es que ya se hizo, e iniciar con una revisión de qué se quiere, debe y puede implantar. Además, esta revisión debe estar dictada por el negocio y las necesidades de cumplimiento regulatorio, no por una visión únicamente técnica. En otras palabras, el famoso Gobierno de TI debe encauzar y supervisar el análisis.

Uno de los principales productos del análisis antes mencionado es la "declaración de aplicabilidad" (SOA, por sus siglas en inglés), que no es otra cosa que un documento en el que se plasma la hoja de ruta de lo que se quiere implantar. Así, por ejemplo, para cierta organización la declaración de aplicabilidad contendrá una combinación de ITIL, ISO-27001, CobiT y regulaciones bancarias, según lo requiera el negocio .

Dado que la generación del SOA está fuera del alcance del presente artículo, por ahora simplifiquemos y supongamos que se requiere la implantación de procesos de ITIL, entonces, ¿por dónde empezar?

Como ya se mencionó en las entregas anteriores, existe una gran cantidad de procesos de ITIL y una de las primeras cuestiones a dilucidar es cuál implantar primero. Normalmente, y así es recomendable para la inmensa mayoría de los casos, debería iniciarse por la implantación de procesos de soporte al servicio ya que dichos procesos son lo que están "más de cara" a los clientes y usuarios, lo que permite que pequeñas mejoras a los procesos de TI sean percibidas de inmediato e impacten favorablemente en los servicios de TI. Continúa en página 20

Preparando el proyecto de implantación

Ahora bien, antes de revisar los detalles sobre cómo implantar ITIL, es importante recordar que un proyecto de esta naturaleza NO es una cuestión técnica, sino que involucra tecnología, procesos y gente, sobre todo gente. Y precisamente aquí radica una de las cuestiones fundamentales (y uno de los motivos más comunes para que muchos proyectos hayan resultado insatisfactorios o se convirtieran en verdaderos desastres): ITIL se trata, antes que nada, de un programa de cambio organizacional. Si usted busca que la implantación de ITIL sea un éxito es muy importante que desde la planeación misma se tenga en mente el cambio organizacional que permita a todos los involucrados poder llevar a cabo los cambios de paradigma necesarios (véase el recuadro "Logrando el cambio organizacional" para algunas ideas interesantes al respecto).

Además de la gran planeación y análisis para lograr un adecuado cambio organizacional, un proyecto de implantación de ITIL debe tomar en cuenta los siguientes aspectos:

a) Requiere un alto compromiso de la alta gerencia. Mucho se ha hablado de que el compromiso de la alta gerencia es relevante para proyectos importantes en cualquier organización, incluso se considera uno de los primeros requisitos en el establecimiento de sistemas de gestión para los diversos estándares de ISO como el 9000, 27001, 2000, etcétera.

   Sin el apoyo, involucramiento y patrocinio de la alta gerencia, este tipo de proyectos casi siempre está condenado al fracaso o, en el mejor de los casos, sólo logrará resultados parciales en un pequeño grupo de personas alrededor de los entusiastas que quieran afrontar el reto, siempre que estén dispuestos a trabajar muchísimas horas más allá de su horario laboral y a tomar dosis extras de medicina contra la frustración.

b) Se requiere que sea un proyecto formal, con todas las implicaciones que ello conlleva. Es necesario asignar los recursos humanos, materiales y económicos suficientes. No basta con un apoyo moral, es necesario entender claramente que, sobre todo al inicio, habrá muchas tareas extra que realizar además de la operación normal, y entre ellas las más comunes son:

   - Administración del proyecto, de preferencia a través de metodologías probadas como la del *Project Management Institute*.
   - Actualización de la documentación de los procesos actuales, si es que existe dicha documentación. Si no, habrá que documentarlos desde cero.
   - Revisión y análisis de los procesos para alinearlos a ITIL, tanto desde el punto de vista documental como de la propia operación, que incluso puede llevar a la adopción de nuevas herramientas y sistemas que deberán implantarse y ponerse en funcionamiento mientras se mantiene la operación normal del negocio.
   - Establecimiento y seguimiento del plan de comunicación interna del proyecto.

c) Hay que ser pacientes y no dejarse llevar por el canto de las sirenas (consultores internos y externos) que prometen una implantación completa en meses o semanas: La implantación completa de los libros de soporte al servicio y entrega del servicio puede llevar años, aunque deberían empezarse a ver mejoras en la operación y en la satisfacción de los clientes después de tres o cuatro meses.

d) Hay que hacer un esfuerzo importante en capacitación a todos los niveles. No basta, como es común, con mandar a certificar a un pequeño grupo de personas que se convertirán en los gurús de ITIL dentro de la organización. Dado que se trata de una nueva manera de ver el mundo, es necesario capacitar a mucha gente de todos los niveles de la organización.

   Y no se trata de mandar a 300 personas a certificarse en el nivel básico y otras 40 en el máximo nivel. Se trata de tener un pequeño núcleo de gente capacitada externamente que entienda muy bien lo que es ITIL para que sirvan como guías de la organización y como entrenadores, de tal manera que como parte del proyecto se tengan desde cursos internos de varios días hasta sesiones de entrenamiento de una hora, según requieran los diferentes roles de la organización.

e) Requiere de participación a todos los niveles. Así como es vital el involucramiento de la alta dirección, también es vital que toda la gente que vaya a ser parte del cambio esté involucrada, informada y participe. Recuerde que un proceso es como una maquinaria, basta con que cualquier componente falle o no realice bien su trabajo para que todo se venga abajo. Asegúrese de que la planeación del cambio organizacional, el plan de comunicación interna, las sesiones de capacitación y el diseño de los nuevos procesos contemple a todos.

Continuará…

Logrando el cambio organizacional

Lograr el cambio organizacional es una de las tareas más difíciles y complicadas en cualquier organización. Todos los humanos por nuestra propia naturaleza tendemos a aferrarnos a lo conocido y rechazamos el cambio, aun en aquellos casos en que incluso pudiera ser beneficioso. Es por ello que los encargados de implantar ITIL, o de cualquier otra iniciativa que implique una "sacudida" a los cimientos de la organización, deben tener en cuenta las etapas en el proceso de cambio, para poder establecer estrategias y acciones que permitan un tránsito más fácil por las diferentes etapas del proceso de cambio:

Nivel 1. Falta de claridad e incertidumbre.
Cuando se establece oficialmente el cambio, no todo queda claro al principio y la gente estará insegura de qué va a pasar y qué no va a suceder.

Nivel 2. Negación.
En esta etapa empiezan las dudas y la gente se cuestiona si el cambio funcionará, con una fuerte tendencia a suponer que la única opción es el fracaso.

Nivel 3. Resistencia.
En el nivel 3 puede observarse tanto resistencia consciente como inconsciente, lo cual casi siempre tiene un impacto negativo en el desempeño ("las cosas empeorarán aún más antes de mejorar"). Es importante entender que es parte del proceso normal de aprendizaje.

Nivel 4. Beneficios.
Conforme la gente se acostumbra a las nuevas reglas, empieza a ver los beneficios inherentes del cambio y el desempeño empieza a recuperarse.

Nivel 5. Equilibrio.
En esta etapa se logra el equilibrio entre lo positivo y lo negativo. El cambio empieza a operar realmente.

Nivel 6. Reflexión y aprendizaje.
Hay una reflexión interna sobre lo que aprendimos durante el proceso de cambio.

Nivel 7. Autorregulación.
En esta etapa la gente y la organización se preparan para el futuro estableciendo la nueva situación como normal y quedando listas para vivir un nuevo cambio.

Etapas en el proceso de cambio

Ahora bien, ¿cómo facilitar a la organización el tránsito por estas etapas? Mucho se ha escrito sobre qué cosas considerar para lograr un cambio organizacional exitoso. John Kotter, uno de los autores más reconocidos en el tema, definió ocho factores críticos de éxito para el cambio organizacional:

1. **Establecer un sentido de urgencia.**
   Las organizaciones que saben manejar el cambio productivamente crean un sentido de urgencia entre la gente más importante. De esta manera se demuestra que hay una gran necesidad de cambio y se motiva a la gente a buscarlo en lugar de permanecer en el estado actual.

2. **Crear una coalición de liderazgo.**
   Sin liderazgo es imposible cualquier cambio y dicho liderazgo debe ser ejercido por un equipo multidisciplinario que posea las habilidades, conexiones y autoridad necesarias. Un equipo líder fuerte facilitará el cambio.

3. **Desarrollar una visión y una estrategia.**
   Es imprescindible crear una visión que muestre cómo será la organización después del cambio, además deberán desarrollarse un conjunto de estrategias que permitan alcanzar dicha visión.

4. **Comunicar la visión del cambio.**
   Toda la organización debe entender la visión y las estrategias para llegar a ella. La comunicación es uno de los mejores facilitadores para el cambio.

5. **Facultar a una base amplia para la acción.**
   El cambio debe ser logrado por toda la organización y por ello es menester propiciar que todos sus integrantes actúen, lo cual requiere que mucha gente tenga la autoridad suficiente para ir atacando cada obstáculo que pueda surgir.

6. **Obtener victorias a corto plazo.**
   Lograr pequeños éxitos parciales rápidamente proporcionará credibilidad y validará los cambios. La idea es ganar impulso rápidamente para que el cambio a largo plazo sea autosustentable y para mantener el entusiasmo de todos los involucrados en el proceso.

7. **Consolidar las ganancias para ganar impulso.**
   Es importante mantener éxitos y consolidar el cambio constantemente, lo cual hará posible contar con los recursos y el entusiasmo de la gente a largo plazo.

8. **Arraigar el nuevo enfoque cultural.**
   La idea final es que la organización “olvide” cómo actuaba antes del cambio y el mañana se convierta en la nueva manera natural de hacer las cosas. Si no se arraiga el cambio, la gente (y la organización) irremediablemente regresarán a la manera antigua de conducirse, con lo que se anulará cualquier beneficio logrado y sólo se tendrá un enorme desperdicio de recursos y tiempo.

En resumen: lograr el cambio organizacional no es una cuestión de conocimientos o herramientas, es una cuestión de lograr modificar el modo de actuar de la gente. En la experiencia de Kotter, 50% de los esfuerzos de cambio fallaron justo en lograr modificar el modo de actuar de las personas.

Scitum

Mantenga su red segura y confiable.

con Servicios de Seguridad Administrada

SOC

- Servicio de Seguridad Perimetral
- Seguridad en Aplicaciones y Bases de Datos
- Servicio de Seguridad en Redes Internas
  (LAN, Wireless, VoIP)
- Seguridad en el Escritorio
- Monitoreo y Correlación de Eventos
- Security Dashboard

NOC

- Servicios de Optimización de WAN
- Servicios de Entrega de Aplicaciones
- Servicios de Monitoreo de LANs y PCs
- Monitoreo End to End

www.scitum.com.mx

Cd. de México
Av. Paseo de la Reforma # 373 - Piso 7,
Col. Cuauhtémoc, C.P. 06500, México D.F.
Tel: +52 (55) 9150.7400 / Fax: +52 (55) 9150.7478

Monterrey
Blvd. Antonio L. Rodriguez #1884,
Oficinas en el Parque, Torre 1 - Piso 16, Col. Santa María,
Monterrey N.L. CP 64650. Tel.+ 52 (81) 4624.4500

Lo único seguro es que somos vulnerables

Priscila Balcázar Hernández

CISSP, CISA y CGEIT
pbalcazarh@scitum.com.mx

Las generaciones que crecimos en los años 60, 70 y aún en los 80, no tenemos palabras para describir la revolución digital que hemos atestiguado y de la que estamos siendo protagonistas. Me atrevo a pensar que sólo la incorporación de la imprenta pudo haber traído tantos cambios como esta ola de tecnología e información.

Hoy muchas personas vivimos "en línea" en mayor o menor grado. Estamos permanentemente con el celular en la mano o en la mesa, no importando si comemos con un cliente, con la pareja, con amigas o con los hijos. Estamos revisando constantemente los correos, actualizando el estado en el *twitter* (¡no vaya a ser que mis amigas no se enteren de que estoy comiendo en la mesa de al lado de la de Valentino Lanus!), viendo las nuevas fotos que subió la vecina en *Facebook*, rechazando o aceptando invitaciones, platicando en el messenger con un compañero de trabajo que se sienta a dos lugares, viendo en el *Skype* a los sobrinitos y ahora también realizando operaciones financieras desde el móvil.

Cuando éramos niños salíamos a andar en bici, a jugar canicas, muñecas, a la maestra o a la mamá. ¡Éramos libres!, hoy somos presos de un manojo de *bytes* que nos dan identidad y somos sus esclavos en la medida que los alimentamos.

Los datos personales son oro puro para la delincuencia organizada pues utilizan esta información para trazar nuestras rutas, sitios frecuentes, relaciones, información financiera, y, en particular, cosas que "nadie sabía".

¿Estuviste preocupado por enviar tu CURP al RENAUT porque no sabías cómo se va a proteger tu información? Pero ¿has pensado toda la información que cargas contigo diario?, ¿cómo la proteges?

Analicemos un poco lo que traes en tu móvil (por favor marca las casillas que te apliquen):

- ☐ **Correo personal**: información sensible que has compartido sobre tu familia: a dónde vas de vacaciones, a qué escuela van tus hijos, en qué gimnasio estás inscrito, etcétera.
- ☐ **Correo de la oficina**: información confidencial, desde un sueldo hasta una estrategia de negocio y datos de tus clientes.
- ☐ **Calendario de citas**: dónde, a qué hora y con quién te encontrarás durante la semana.
- ☐ **Agenda**: direcciones de correo de clientes, amigos, compañeros de trabajo; domicilios de familia y amigos, probablemente algunos sean altos ejecutivos ¡blancos excelentes para la delincuencia!
- ☐ **Fotos**: familia y amigos, ¡etiquetadas para que se identifiquen perfectamente!
- ☐ **Mensajes**: desde un inofensivo "me gustas" hasta "t deposite 40,000 pa enganche de coche, tvo en la agencia".
- ☐ **Celulares**: números identificados sin lugar a duda: "mama", "amorcito", "hijita".
- ☐ **Llamadas**: últimas llamadas recibidas y realizadas.
- ☐ **Notas**: números de cuenta bancarios, contraseñas, CURP, RFC y pago de impuestos.
- ☐ **Internet**: tus sitios más visitados, información personal en Facebook, twitter, etcétera.
- ☐ **Música**: incluyendo las canciones más tocadas, ¿por qué es esto peligroso? Un secuestrador puede dar la "prueba de vida" diciendo: "la víctima me dice que su canción favorita es 'Rosas Rojas'", cuando probablemente no tengan al familiar, sólo su móvil.



Los delincuentes están ávidos de todo este tipo de información, que puede ser la punta de la madeja para armar un escenario completo, apoyados en técnicas de ingeniería social.

Las técnicas más sofisticadas de seguridad no son suficientes cuando de proteger nuestros datos se trata. El factor más importante es el propio peso con que ponderemos nuestra información, de ahí que como cultura cotidiana recurramos a las siguientes reflexiones y hábitos al usar el móvil:

- Lo que estoy escribiendo ¿es relevante?, ¿es necesario?, ¿es urgente?
- En caso de que sea confidencial ¿estoy seguro que del otro lado única y exclusivamente lo verá mi receptor? (¡recuerda que existen casos de intromisión en correos ajenos!),
- Al cambiar de teléfono, ¿quién usará este aparato? Asegúrate de borrar absolutamente todos los datos que tenías almacenados. Si no conoces el detalle técnico de cómo hacerlo, solicita apoyo y asegúrate personalmente de que quedaron eliminados de manera definitiva.
- Utiliza claves para bloquear tu teléfono y para proteger información sensible.
- No prestes tu teléfono o dispositivo móvil.
- Mantén un código básico para comunicarte con tu familia. Por ejemplo: en lugar de escribir “ya estamos en casa”, puedes codificarlo de manera divertida: “cruz azul juega de local”.

« Vivimos “en línea” en mayor o menor grado. Estamos permanentemente con el celular en la mano o en la mesa, no importando si comemos con un cliente, con la pareja, con amigas o con los hijos. »

Aprovechemos al máximo las bondades de la movilidad tecnológica y de estar “siempre en línea”, pero tengamos mucho cuidado con la información que dejamos a nuestro paso. Creo que de aquí en adelante no volveremos a estar seguros, ya somos vulnerables por esta naturaleza digital de nuestro nuevo estilo de vida, así que ¡administra tus riesgos!



Illustración: Silverio Ortega

Desde la trinchera

Marcos Polanco
CISSP, CISA y CISM.

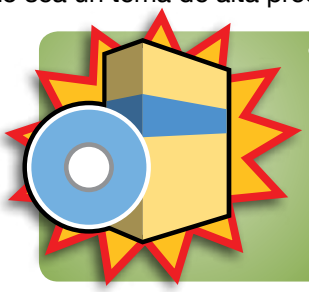
La seguridad de los menores en Internet, una importante tarea aún pendiente.

En este nuevo número de **Magazcitum**, con el que se inicia una etapa donde además del habitual número en formato electrónico ahora se tendrá también en formato impreso, he querido tomarme la libertad de hablar de un tema que, si bien está relacionado con asuntos de la seguridad informática, no incide directamente en los aspectos empresariales o corporativos, sin embargo, es, o al menos debería ser, un tema central de preocupación a nivel sociedad y si no por lo menos a nivel individual (sobre todo para aquellos que somos papás).

Me refiero a la protección de los menores en Internet. Dado que es un tema muy amplio que no sólo considera aspectos tecnológicos, sino también aspectos sociales, educativos, legislativos, etc., intentaré abarcar algunos de los más notables.

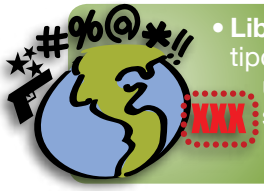
Primero analicemos los factores que influyen en que esto sea un tema de alta preocupación:

- **Anonimato.** Uno de los aspectos que ocasionan grandes problemas es el anonimato dentro de la red y la facilidad de tener una identidad falsa.



- **Nuevos tipos de aplicaciones.** Por otro lado el auge de las redes sociales y aplicaciones de la **Web 2.0** (*blogs, chats*, etc.) ha permitido que muchos niños estén utilizando de forma muy activa dichas aplicaciones, con los riesgos inherentes que esto conlleva.

- **Desconocimiento.** También se debe destacar que existe un gran desconocimiento por parte de los involucrados (niños, papás, profesores y autoridades) sobre los riesgos existentes.



- **Libertad de contenidos.** El acceso a todo tipo de contenido en Internet, siendo ésta una de sus principales características, supone también una de las principales preocupaciones.

- **Falta de control.** Por último, y no menos importante, es la falta de leyes y controles sobre los contenidos y actividades dentro de la red que, en combinación con los demás factores expuestos, tornan riesgosa esta experiencia, sobre todo para los más indefensos.

Ahora analicemos algunos de los riesgos a los que están expuestos los menores que utilizan Internet. Los he clasificado en cuatro grandes bloques con el objeto de simplificar, sin embargo se podrían identificar riesgos particulares para cada tipo de actividad que se realiza en Internet (*chats, blogs, online gaming*, redes sociales, correo, etc.).

1. **Conductas inapropiadas.** Se han identificado algunas conductas inapropiadas que ocurren de igual forma en el mundo online y en el mundo "normal"; una de ellas es el *Bullying*, que es el acoso u hostilidad verbal, psicológica, o física, repetitiva realizada por una persona o grupo de personas con el objetivo de molestar a otros. Ahora el *Cyberbullying* es lo mismo pero utilizando las nuevas tecnologías como Internet (correos, chats, redes sociales, etc.), celulares, mensajes SMS, etcétera. Otra es el denominado *Sexting*, término que viene de la combinación de las palabras en inglés "*sex*" y "*texting*" y se refiere al hecho de mandar mensajes o fotos con sexo explícito por medios electrónicos, principalmente por telefonía celular.
2. **Contenido dañino.** *Malware* a través de descargas de software, juegos, imágenes, música, películas o a través de correo *spam*. Los niños pueden entrar en contacto con contenido no adecuado con tan sólo poner una palabra en un buscador o al entrar a una página normal que maneja anuncios de cualquier tipo, incluyendo por ejemplo temas sexuales.
3. **Contactos inapropiados.** El *Grooming*, que se define como el intento de llevarse bien e influenciar a un niño a través de *chats* o aplicaciones similares con la intención de cometer abuso sexual.
4. **Actividades inapropiadas** que el niño puede realizar en la red con o sin intención como apuestas en línea, violación de los derechos de autor, etcétera.

Si bien las alternativas y estrategias de protección son múltiples, a continuación menciono algunas que considero fundamentales, utilizando como referencia (y no de forma restrictiva) el concepto de palancas de control definido por Robert Simons para agruparlas de una forma estructurada.

» **Sistemas de creencias.** El objetivo es establecer de manera básica los valores que servirán como guía. Establecimiento de un marco de comportamiento (valores). Enseñar a los niños que no necesariamente todo el contenido de Internet es apropiado, así como a buscar múltiples fuentes y compararlas, tratando siempre de usar fuentes reconocidas.
Generar un ambiente de confianza para que el niño consulte con los papás o con algún adulto cuando cierto contenido le resulte dudoso, confuso o incómodo.
Comportarse en el mundo *online* como lo haría en el mundo "normal".
Respeto a los demás al no publicar imágenes de otras personas sin su autorización, sobre todo si éstas pueden ocasionar algún tipo de daño (imagen, reputación, autoestima, etc.).
Recuerden aquel anuncio de hace muchos años (a lo mejor los más jóvenes no sabrán de qué hablo pero los que somos papás seguramente lo recordamos), que decía "Mucho ojo". Transmitamos esta misma idea a los niños pero trasladado al mundo *online*.

1. **Sistemas de límites.** El objetivo es establecer las restricciones en el comportamiento, definición de reglas, etcétera.
2. Establecimiento de reglas. Así como solemos poner reglas para otros aspectos de la vida familiar, es importante establecerlas para el uso de Internet. Por ejemplo, la computadora deberá estar en un lugar común de la casa (con la pantalla dando hacia la circulación de dicho espacio), no en el cuarto del niño, esto hará más fácil la labor de supervisión y será más difícil el hacer cosas a escondidas. Enseñar a los niños reglas básicas como no compartir contraseñas y a usar contraseñas robustas.

» **Sistemas de control diagnóstico.** Se centran en la vigilancia y enfocan la atención en lo que se debe hacer.

a) **Uso de herramientas.** Contar con herramientas para filtrar páginas, filtrar contenido, además de las típicas de protección informática como antivirus, antispam, *antispyware*, etcétera.

b) Contar con herramientas que ayuden a discriminar qué sitios son "buenos" y cuáles no (por ejemplo: Finjan *Secure Browsing*, Siteadvisor de McAfee). Utilizar como referencia las páginas de asociaciones que analizan miles de sitios con contenido educacional y ayudan a orientar respecto a cuáles son adecuadas, como protegeles.com, u organizaciones que contribuyen a concienciar y a educar sobre los riesgos, y a proponer estrategias de acción como inhope.org, saferinternet.org,

c) Mantener los equipos actualizados con parches, firmas del software de antivirus, y con cualquier otra herramienta de protección.

d) Configurar las restricciones de privacidad de los perfiles en redes sociales con todo cuidado y mantenerse al pendiente de cambios en las políticas de privacidad de dichos sitios y de cambios en los mecanismos de control y parámetros de configuración de privacidad.

e) Auditar. De vez en cuando es recomendable revisar que no se estén ejecutando actividades inusuales o indebidas.

» Sistemas de control interactivo. Su objetivo es estimular el aprendizaje, principalmente a través de la interacción y la enseñanza hombro con hombro.

» Interactuar. Mantener interacción mientras el niño navega, haciendo de esto una actividad familiar.

» Concienciación. Concienciar a los niños, a los padres, a los profesores, sobre los riesgos concomitantes, así como sobre mejores prácticas a tomar en cuenta.

» Enseñar. Navegar juntos hasta estar seguros del desarrollo en el niño de un criterio de discriminación (al menos elemental).

En conclusión, considero que si bien hay mucho por hacer, hoy en día podemos disponer de diversas herramientas para ayudar a evitar situaciones indeseables; sin embargo, creo que lo más importante es que como padres tomemos el control y estemos cerca de nuestros hijos y al pendiente de lo que hacen en Internet, y que los eduquemos para que sepan lidiar con las situaciones y problemáticas tanto en el mundo online como en el mundo "*normal*".

Departamento de Defensa

David Gutiérrez
CISSP y CISA.
dagutierrez@scitum.com.mx

Regulación sobre la notificación de incidentes de seguridad

En las teorías económicas liberal y neoliberal, las fuerzas del mercado son suficientes para controlar el buen desarrollo de las empresas y servicios, ya que todos aquellos que sean francamente malos, caerán de la preferencia de los compradores y poco a poco desaparecerán, quedando únicamente aquellas empresas que, por su valor y "bondad", hayan captado el mayor número de ventas.

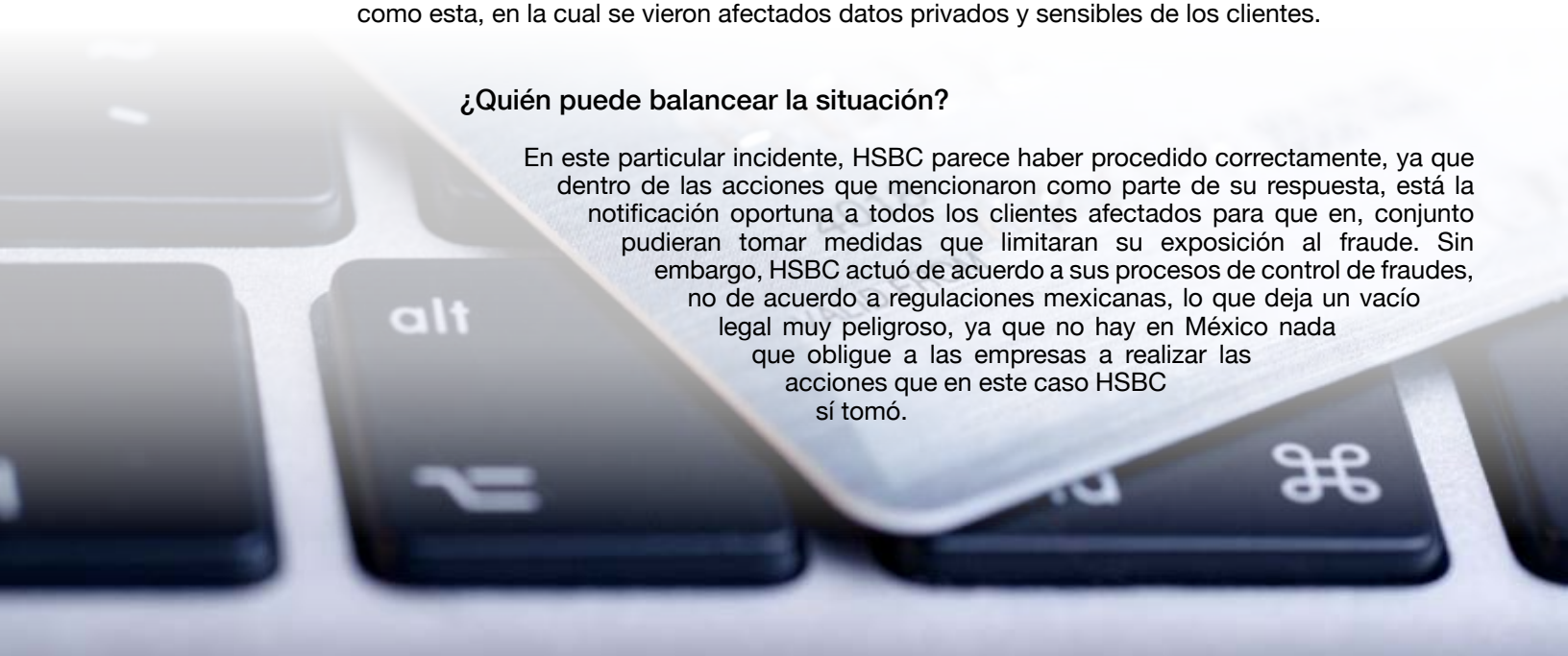
Es entonces, de acuerdo con este modelo, el incentivo económico el que obliga a las empresas a tomar decisiones en un sentido o en otro. Precisamente esto es lo que podemos observar en la realidad.

Resulta evidente que el hecho de admitir que a una organización le ha ocurrido un incidente de seguridad (y me refiero a incidente de seguridad como está definido en los documentos de la serie ISO 27000) no le va a traer a ésta ningún beneficio económico; por el contrario, la reputación de la empresa quedará dañada y habrá que realizar gastos para recuperar lo perdido. Por lo anterior, es evidente que difícilmente habrá un incentivo económico para reportar incidentes de seguridad, y por tanto, el mercado, por sí mismo, no podrá garantizar la supervivencia de las empresas que aseguren mejor sus datos.

Y la seguridad de los datos, ¿le es interesante al mercado?

¿Es de interés para los consumidores que las empresas resguarden sus datos correctamente?, ¿es también de interés para los consumidores que las empresas reporten sus incidentes de seguridad?, ilustraré la respuesta con un caso reciente: En enero de 2010 la institución bancaria HSBC tuvo que realizar una campaña muy fuerte para controlar los daños derivados de una "clonación masiva"[1] de tarjetas de débito en el estado de Jalisco, México, en la cual centenas de personas fueron víctimas de fraude al hacérseles cargos con las tarjetas clonadas. En posteriores notas[2], ejecutivos del banco declararon que estaban reembolsando a los clientes los cargos no reconocidos, que el incidente no había sido derivado de un "*hackeo*" ni abuso interno y que estaba circunscrito a un número "limitado de ataques a cajeros automáticos".

En el feliz supuesto de que el banco haya reembolsado las cantidades defraudadas a todos y cada uno de los cuentahabientes afectados, continúa siendo una pérdida importante, especialmente para los consumidores que recibieron un susto mayúsculo y la imposibilidad de usar sus fondos por al menos 48 horas. Es claro que existe un enorme interés del consumidor en que sus datos se resguarden correctamente y en que los incidentes se reporten de manera oportuna, cuando menos en situaciones como esta, en la cual se vieron afectados datos privados y sensibles de los clientes.



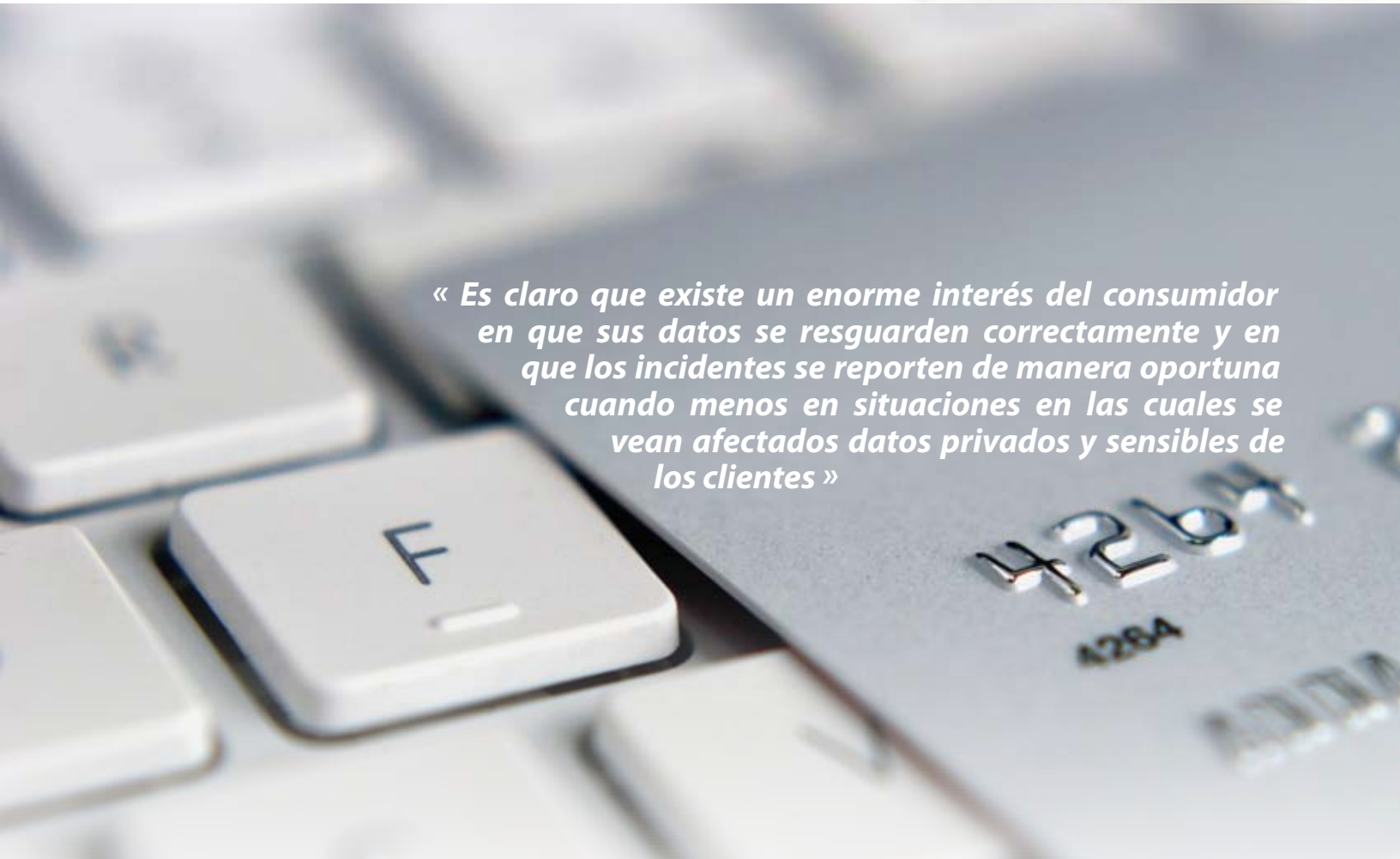
¿Quién puede balancear la situación?

En este particular incidente, HSBC parece haber procedido correctamente, ya que dentro de las acciones que mencionaron como parte de su respuesta, está la notificación oportuna a todos los clientes afectados para que en, conjunto pudieran tomar medidas que limitaran su exposición al fraude. Sin embargo, HSBC actuó de acuerdo a sus procesos de control de fraudes, no de acuerdo a regulaciones mexicanas, lo que deja un vacío legal muy peligroso, ya que no hay en México nada que obligue a las empresas a realizar las acciones que en este caso HSBC sí tomó.

Las autoridades gubernamentales son las indicadas para darle mayor peso al interés de los clientes en que se brinde protección a su información sensible y además que se les informe oportunamente en el caso de que la organización que la maneja haya sufrido algún incidente de seguridad que exponga tal información. La manera de hacer contrapeso al mero interés económico es mediante la regulación de las prácticas en materia de seguridad de la información, sobre todo aquellas que, como el robo de información de tarjetas de débito, entrañan un potencial daño a la sociedad.

En los Estados Unidos de América prácticamente todos los estados consideran en sus legislaciones normatividad relacionada con el reporte de incidentes de seguridad que involucren información personal[3], y al parecer, también la Unión Europea está cercana a contar con su propia legislación en la materia[4].

México cuenta ya con algunas leyes que abordan delitos informáticos, pero definitivamente no hay mucho relacionado con la notificación obligatoria de incidentes de seguridad. Me parece claro que hay mucho que ganar y poco que invertir al promulgar en México una ley de notificación de incidentes de seguridad basada en las que se han promulgado en EE.UU.; realmente no es necesario ser innovadores y pioneros en este tema, y sí lo es por otra parte, el actuar de manera diligente para proteger a la sociedad de los nuevos riesgos que conlleva este mundo interconectado.



« Es claro que existe un enorme interés del consumidor en que sus datos se resguarden correctamente y en que los incidentes se reporten de manera oportuna cuando menos en situaciones en las cuales se vean afectados datos privados y sensibles de los clientes »

1. CNN Expansión, ver nota publicada en http://exp.mx/n0028NP
2. Periódico Milenio, ver nota relacionada en http://impreso.milenio.com/node/8707272
3. Listado de estados en EE.UU. que cuentan con legislación sobre la notificación de incidentes de seguridad en http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx
4. Revista ZDNet Reino Unido, ver nota relacionada en http://www.zdnet.co.uk/news/security-management/2010/04/27/data-breach-notification-law-coming-says-watchdog-40088780/

En el pensar de...

Eduardo Patricio Sánchez
CISSP, GCIH, CISM y CEH
epsanchez@scitum.com.mx

Open Source Intelligence (parte II)

Para retomar el tema, me gustaría recordar la definición de *Open Source Intelligence* (OSINT), que se refiere a aplicar técnicas de inteligencia a la información que se puede extraer de fuentes públicas como son Internet, medios de comunicación tradicionales y no tradicionales, libros, etcétera. Todo con el fin de obtener información sensible.

Si las organizaciones y los individuos estuviéramos consientes que la información que ponemos en lugares públicos puede convertirse en huecos de seguridad, todos tendríamos más cuidado con lo que publicamos.

La serie de notas que publicaré a partir de ahora mostraran algunas de las técnicas que se usan para identificar información en Internet. Al finalizar dicha serie mostraré como toda esta información puede ser utilizada para crear un vector de ataque que permita a una persona mal intencionada comprometer información más crítica de las organizaciones, también daré algunas recomendaciones para evitar exponer información de más en sitios públicos[1].

Casi cualquier organización moderna tiene contacto con Internet; este contacto deja un rastro el cual puede seguirse y al seguir este rastro podemos encontrar información que en su conjunto podría considerarse sensible o incluso puede ser usada perpetrar algún ataque.

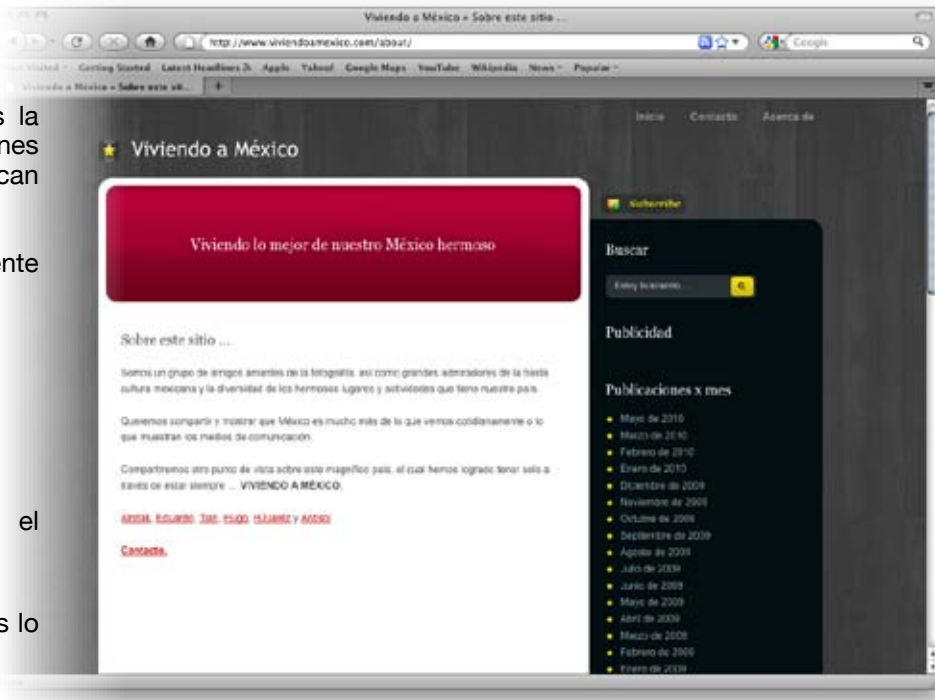
A continuación una lista del tipo de información que se puede identificar:

- Nombre de la organización.
- Ubicación física y lógica.
- Organigrama con nombre y puestos.
- Noticias relacionadas a la organización.
- Contactos de la compañía.
- Proveedores.
- Directivas de seguridad.
- Arquitectura y topología de red.

etcétera.

Investigando una organización

Lo primero que se intenta detectar es quien es la organización, cuánto tiempo tiene de existir, quienes son dueños. La mayoría de las empresas publican esta información en su sitio *Web* corporativo.



Del sitio Web de la organización se busca la siguiente información:

- Nombre completo de la organización.
- Giro.
- Ubicación física de sus oficinas.
- Teléfonos de contacto.
- Correos electrónicos publicados en el sitio *Web*.

Al ingresar al portal de la organización detectamos lo siguiente:

1. Los ejercicios que se mostraran durante el artículo se realizaron sobre una organización no lucrativa, con el respectivo permiso para mostrar los resultados obtenidos.

Después de ver la información nos dimos cuenta que:

» 5 personas son parte de la organización.

» 2 de ellos usan seudónimos.

» 2 de ellos, Hugo y Antisol, tienen páginas personales hospedadas en otros sitios.

Con el nombre del dominio de la organización (viviendoamexico.com), trataremos de detectar información sensible de la organización en medios públicos. Para ello recordemos que como parte del proceso de registro de cualquier dominio, los dueños deben proporcionar ciertos datos que son almacenados en un base de datos que se llama "*Registration transacction information*" conocida como WHOIS. Esta base puede ser consultada desde diversas páginas Web o incluso algunos sistemas operativos como Linux tienen un cliente que se conecta a ella.

Al realizar la consulta WHOIS sobre el dominio tenemos la siguiente salida:

```
whois viviendoamexico.com

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to
http://www.internic.net
for detailed information.

   Domain Name: VIVIENDOAMEXICO.COM
   Registrar: GODADDY.COM, INC.
   Referral URL: http://registrar.godaddy.com
   Name Server: NS.NIMROD.COM.MX
   Name Server: NS2.NIMROD.COM.MX
   Updated Date: 01-dec-2009
   Creation Date: 05-feb-2009
   Expiration Date: 05-feb-2011

Administrative Contact:
   Name:          Eduardo Sanchez
   City:          Mexico
   State:         Distrito Federal
   Country:       Mexico

Technical Contact:
   Name:          Alejandro Aranda
   City:          Mexico
   State:         Distrito Federal
   Country:       Mexico

Billing Contact:
   Name:          Eduardo Sanchez
   City:          Mexico
   State:         Distrito Federal
   Country:       Mexico
```

¿Qué sabemos a partir de la consulta?:

» El contacto administrativo es Eduardo Sánchez, este mismo nombre apareció dentro del portal.

» El contacto técnico es Alejandro Aranda.

» Uno de sus proveedores de servicio es Godaddy.

» Los servidores de DNS se relacionan con el dominio nimrod.com.mx. Al realizar las mismas consultas sobre este dominio, se detecta que el dueño de los dominios es la misma persona.

A partir de lo anterior podemos realizar búsquedas especializadas en diversos sitios de Internet, con el fin de obtener más información de la organización. Algunos de los sitios que podemos consultar son los siguientes:

Nombre	URL	Tipo	Objetivo
Google	www.google.com	Buscador de Internet	Google es posiblemente el buscador de Internet que permite realizar las búsquedas mas personalizadas. Cuenta con su propia sintaxis que permite detectar información muy puntual en Internet. Un poco más adelante en el artículo daré un pequeño repaso a estas búsquedas especiales.
Bing	www.bing.com	Buscador de Internet	Bing es otro de los buscadores especializados para realizar búsquedas de información.
Apestan	www.apestan.com	Buscador de reputación de organizaciones	Se trata de un sitio *Web* en el cual las personas cuando publican quejas e inconformidades respecto a alguna organización o proveedor. Contar con esta información nos puede permitir medir el nivel de reputación de la organización.
Monster	www.monster.com/geo/siteselection.aspx	Portal de búsqueda de empleo	El propósito de consultar sitios de empleo tiene dos objetivos: 1. Detectar información sensible a partir de las ofertas de empleos publicadas. 2. Al realizar búsquedas de currículos de personas que hayan laborado en la organización podemos detectar información sensible. Entre la información que podemos detectar está la siguiente: 1. Clima organizacional 2. Cultura organizacional 3. Tecnología usada en la organización
Laborum	www.laborum.com	Portal de búsqueda de empleo	

Continúa en página 17...

Continúa de página 17...

Nombre	URL	Tipo	Objetivo
Google groups	groups.google.com	Compendio de diversos grupos de discusión	*Google Groups* es una serie de grupos de discusión de diversos temas. Su buscador también permite realizar búsquedas en foros que no pertenecen a Google, con lo cual es posible detectar información sensible. ¿Qué tipo de información podemos encontrar? Si una persona de la organización en alguna ocasión solicito soporte en un foro de tecnología, es muy probable que aquí lo encontremos. La mayoría de las personas cuando pregunta en foros, da más información de la requerida.
Netcraft	www.netcraft.com	Pagina Web de consulta	*Netcraft* es una página *Web* de una compañía Inglesa que de dedica a la seguridad informática. Entre sus servicios cuenta con una barra de herramientas que almacena información de los sitios *Web* que los usuarios que la instalan visitan. Esta información es guardada en una base de datos pública donde se puede consultar, entre otras cosas, el historial de ISP (*Internet Service Provider*) y el tipo de servidor *Web* de portales.
Archive	www.archive.org	Archivo de Internet	*Archive* es una base de datos historia que recolecta información diversa, entre la información que podemos encontrar es el historias de páginas *Web* de organizaciones.

Búsquedas con Google

Google se considera uno de los buscadores de Internet más poderosos, ya que integra una serie de parámetros que nos permiten afinar las búsquedas que realizamos, algunos de los más usados son:

- ***Intitle*:** Permite realizar búsquedas en los títulos de las páginas *web*.
- ***Inurl*:** Se usa para realizar búsquedas en los URL de las páginas.
- ***Filetype*:** Empleado para definir las búsquedas de ciertos tipos de archivos.
- ***Site*:** Permite definir la búsqueda en sitios concretos.
- ***Cache*:** Con este parámetro se pueden realizar búsquedas en el *cache* de Google y aunque las páginas ya no existan, se puede encontrar información.
- **Info:** Se usa para obtener información relacionada con nuestra búsqueda.
- **Autor:** Empleado para buscar información que ha publicado un autor en especifico.

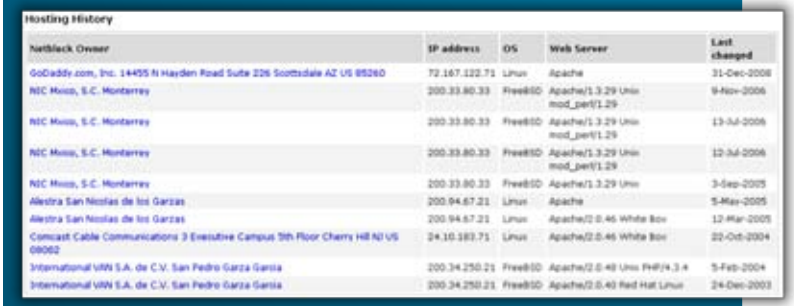
Estos parámetros se pueden combinar para realizar búsquedas muy específicas. Muchas personas consideran que las búsquedas de información mediante Google son un arte al cual le llaman "*Googling*". Johnny, quien es considerado el maestro del "*Googling*" mantiene una base de datos[2] con búsquedas especializadas que permiten encontrar desde configuraciones de equipos hasta contraseñas de sistemas. Esta información es publicada en Internet por errores o desconocimiento de los administradores o dueños de la información y mediante Google puede ser detectada.

2. http://www.hackersforcharity.org/ghdb/

Regresando al sitio en estudio, estos son algunos resultados de los sitios *Web* sobre el dominio viviendoamexico.com:

Bing: Dominios que comparten la misma dirección IP.

***Netcraft*:** Historial de tecnologías e ISP de dominio **nimrod.com.mx**



Como mencioné, estaremos analizando este sitio en varias entregas. En la próxima edición se mostrará cómo, mediante la información detectada, se pueden descubrir los servicios expuestos por la organización, así como su topología e incluso el tipo de plataforma usada. Todo esto sin generar ningún tipo de actividad sospechosa en dispositivos de seguridad.

Que su red esté segura NO implica que sus BASES de DATOS también lo estén

Protección y Aseguramiento de Bases de Datos

de Scitum

www.scitum.com.mx

Cd. de México

Av. Paseo de la Reforma # 373 - Piso 7,
Col. Cuauhtémoc, C.P. 06500, México D.F.
Tel: +52 (55) 9150.7400 / Fax: +52 (55) 9150.7478

Monterrey

Blvd. Antonio L. Rodriguez #1884,
Oficinas en el Parque, Torre 1 - Piso 16, Col. Santa María,
Monterrey N.L. CP 64650. Tel.+ 52 (81) 4624.4500

Historias

Jose Ramírez Agüero
jramireza@scitum.com.mx

Seguridad en la VoIP

Hace algunos años leí una noticia que decía “Descubren vulnerabilidades en voz sobre IP, las fallas pueden ocasionar la denegación total del servicio de Internet o de telefonía en la oficina. Ya está disponible la solución”.

En nuestro artículo anterior, hablábamos de cómo la Voz sobre IP inició y empezó a crecer a raíz del Internet y, sobre todo, de la tecnología de banda ancha, y que empresas como *Skype* tienen éxito en el uso de este tipo de servicios y, combinado con el crecimiento de las redes inalámbricas, pueden mover esta tecnología desde las empresas a los pequeños negocios y el mercado *SOHO* (*Small Office Home Office*, por sus siglas en inglés). Desafortunadamente, como cualquier nueva tecnología, trae consigo problemas respecto a la seguridad y se tienen que tomar en cuenta otras tecnologías para proteger y dar el servicio de voz y datos. Los servidores de “VoIP” (*Voice over IP*, por sus siglas en inglés) actúan como puertas de enlace, por lo que ruteadores, teléfonos, nuevos protocolos y sistemas operativos forman parte de esta innovadora tecnología y en la medida en que éstos se extienden y generalizan, su peligro y los factores de riesgo se incrementan, tal y como pasa con el resto de aplicaciones y servicios de Internet que son blancos de vulnerabilidades y ataques.

Las amenazas

Existen numerosas amenazas que están al acecho de los servicios de “VoIP”, muchas de las cuales pasan desapercibidas para la mayoría de los usuarios. Como decíamos anteriormente: los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su *software*, todos son vulnerables.

Por ejemplo, en la actualidad hay técnicas para que el servicio de “VoIP” pueda ser comprometido en un servidor de gestión de llamadas o “*call manager*”, y se use para configurar o dirigir llamadas del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Utilizando esta información un atacante puede obtener un mapa detallado de todas las llamadas realizadas en la oficina o negocio, creando grabaciones completas de conversaciones y datos de los usuarios.

Como pueden ver, la conversación es lo primordial en un servicio de “VoIP”, y es el objetivo de cualquier atacante, y si alguno de éstos consigue entrar a una parte clave de los dispositivos que conforman la infraestructura de voz, como por ejemplo una puerta de enlace de VoIP (*gateway* de voz), podrá capturar e instalar paquetes con los cuales podrá escuchar la conversación, inclusive y peor aún, grabarla y más tarde reproducir todas las conversaciones que pasan en la red.

Otro de los posibles ataques es el secuestro de llamadas (muy de moda en nuestro país); en este escenario, el atacante puede interceptar la conexión y manipular la configuración de la llamada de manera que una persona A marca el número telefónico de una persona B, llamada que es secuestrada por el atacante quien contesta y se hace pasar por la persona B. Es un ataque que causa temor, ya que los usuarios no notan el cambio y los atacantes usan técnicas de ingeniería social para ejecutar suplantación de identidad y robo de información confidencial, entre otros.

La disponibilidad del servicio de “VoIP” es otro punto importante. En tecnologías analógicas la disponibilidad no era realmente un problema. Pero en el mundo “IP” es mucho más sencillo *hackear* y dejar inoperante una red “VoIP”. Todos estamos familiarizados con los efectos de los ataques de denegación de servicio: si un atacante se dirige a puntos clave de la red puede causar la imposibilidad de comunicarte vía voz o datos.

Los servidores y teléfonos “IP” son vulnerables por sí mismos. Aunque parezcan simples teléfonos en realidad son pequeños equipos de cómputo con *software*. Obviamente, como todos sabemos, el *software* es vulnerable a los mismos tipos de “*bugs*” o huecos de seguridad que hacen que un sistema operativo pueda estar a plena disposición de un atacante.

La prevención

Ya hemos hecho énfasis en los principales peligros a los que se enfrenta la tecnología de "VoIP". Resumiendo, destacan los problemas de Denegación de Servicio (*DoS*), que afectan a la disponibilidad del servicio de "VoIP"; o los Accesos No Autorizados que pueden terminar afectando la confidencialidad del servicio (escuchar de forma no autorizada, suplantación de identidad, robos del servicio de voz, redirección, etc.). En este sentido, el uso no autorizado del servicio es factible que genere un impacto económico elevado al realizar llamadas internacionales o de larga distancia.

Desafortunadamente, al inicio del diseño de *hardware, software* y protocolos para voz, la seguridad no era una prioridad, pero como todos sabemos esto es lo que siempre pasa cada vez que aparece una nueva tecnología☺. A pesar de ello y para bien común, algún tercero siempre soluciona este problema; examinemos algunas opciones que previenen las amenazas sobre esta tecnología.

Una técnica común para mitigar las vulnerabilidades en el servicio de "VoIP" es la protección perimetral (IPS, *firewalls*, análisis avanzado de protocolos), la cual debe actualizarse para incorporar un nivel de seguridad proactivo adecuado frente a estas amenazas en los servicios de "VoIP"; inclusive hoy existen tecnologías de protección perimetral especializadas en VoIP. Los servidores de llamadas están abriendo y cerrando puertos de manera constante para las nuevas conexiones; este elemento dinámico hace que su manejo sea más difícil, pero el costo lo vale por la cantidad de beneficios que se obtienen, así que es aconsejable perfeccionar los controles de acceso aunque se nos dificulte un poco. Un IDS/IPS monitorea la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores, y recordemos: no hay mejor defensa que estar prevenido para el ataque.

Otro punto que debemos tener en mente en los servicios de "VoIP" es el cifrado. Aunque parezca un poco oneroso capturar y decodificar los paquetes de voz, se puede hacer, y cifrar es una de las formas de prevenirse ante un ataque, sobre todo alguno que atente contra la confidencialidad de las conversaciones. Existen varias técnicas de encriptación tales como: VPN (*Virtual Private Network*), el protocolo *IPsec* (IP segura) y otros protocolos como SRTP (*Secure Real-Time Transport Protocol*). El punto importante es elegir un algoritmo de encriptación rápido, eficiente, y emplear tecnologías dedicadas para cifrado. Otra opción manejada actualmente es QoS (*Quality of Service*, por sus siglas en inglés); los requerimientos para "QoS" aseguran que la voz se maneje siempre de manera óptima, reduciendo la pérdida de calidad y haciendo menos probable un ataque de denegación de servicio.

Es sustancial el proceso de asegurar todos los elementos que componen la solución de "VoIP": servidores de llamadas, ruteadores, *switches*, y teléfonos. Es necesario configurar cada uno de esos dispositivos para asegurar que están alineados con los procesos de seguridad de la empresa. Por ejemplo, los servidores pueden ejecutar pequeñas funciones y tal vez sólo deben estar abiertos los puertos que realmente se utilizan. Los ruteadores y *switches* deben estar configurados adecuadamente, con listas de control de acceso y filtros. Algo ya conocido es que todos los dispositivos deben estar actualizados en términos de parches y actualizaciones. En otras palabras, se trata del mismo tipo de precauciones que se toman cuando se adicionan nuevos elementos a la red de datos; lo que sucede ahora es que se debe extender este proceso a la parte que le compete al servicio de "VoIP".

Algo primordial que ya se ha mencionado y que se debe considerar es la disponibilidad del servicio de "VoIP". Es necesario tomar en cuenta que una pérdida de energía puede provocar que la red se caiga y este tipo de fallas son importantes, por lo que se debe asegurar que exista un sistema de redundancia, sobre todo en compañías que dependen del servicio de telefonía para sus procesos sustantivos.

Ilustración: Silverio Ortega

Algo interesante

En la *WEB* me encontré algunos términos y conceptos que se usan en las amenazas del servicio de "VoIP", aquí algunos:

- ***Eavesdropping***, que se traduce literalmente como escuchar secretamente, es el término con el que se conoce la escucha de conversaciones "VoIP" por parte de un intruso. El *eavesdropping* en "VoIP" es algo diferente del *eavesdropping* en las redes tradicionales de datos, pero el concepto es el mismo. *Eavesdropping* en "VoIP" requiere interceptar la señalización y los *streams* de audio de una conversación. Los mensajes de señalización utilizan protocolos separados, es decir, "UDP" o "TCP". Los *streams* normalmente se transportan sobre "UDP" utilizando el protocolo "RTP". Algunos podrían pensar que este tipo de ataque podría eliminarse con el uso de *switches Ethernet* que restringen el tráfico *broadcast* en la red, porque se limita quién puede acceder al tráfico. Sin embargo, este argumento deja de ser válido cuando se introduce el "ARP *spoofing*" o envenenamiento de la *caché* ARP como mecanismo para llevar a cabo una intrusión.
- **ARP *spoofing***. El concepto básico es que el atacante envía a los usuarios avisos con la MAC falseada y, por lo tanto, consigue que los paquetes IP lleguen a su *host*. Por medio del "ARP *spoofing*", un atacante puede capturar, analizar y escuchar comunicaciones "VoIP".
- **Oreka**. Es un *sniffer* de "VoIP" que captura conversaciones y registros y que soporta los protocolos más utilizados: *Bidirectional* "SIP", SCCP de Cisco, *Bidirectional Raw* "RTP". Tiene una licencia "GPL" y está disponible tanto para sistemas Windows como GNU/Linux.

  Es un sistema modular que está formado por los siguientes demonios:

  - » Orkaudio. Es el demonio encargado de escuchar conversaciones "VoIP" y decodificarlas a archivos WAV.
  - » Orkweb. Proporciona una interfaz de administración *WEB*.
  - » Orktrack. Es el servicio encargado de registrar las conversaciones "VoIP" en MySQL.

Así pues, hay que ser precavidos a la hora de implantar soluciones de VoIP porque las amenazas para las empresas han aumentado; por ello es importante conocer algunas de las técnicas y herramientas que usan los atacantes en la actualidad.

¿Se puede aprovechar la nube sin crear tormentas?

we **ca**n

ca technologies

Tips

Osvaldo Hernández
CCSA, ITIL
lhernandez@scitum.com.mx

¿Cómo crear un "rulebase" efectivo para Firewall Checkpoint NGX-RXX?

Siguiendo las mejores prácticas usted podrá tener un mejor rendimiento, desempeño y facilidad de gestión de cualquier Firewall Checkpoint NGX-RXX que administre, aquí publico algunas de las mejores prácticas generales que deben seguirse para crear un rulebase efectivo para el control de seguridad de nuestro *firewall*:

1. El rulebase de nuestro *firewall* deberá ser tan simple como sea posible, es decir el menor número de reglas concretas y específicas dará un mayor desempeño al equipo. Busque permitir el acceso sólo a lo que sea necesario.
2. Evite el uso arbitrario de "*Any*" para el campo de servicio; dichos servicios deberán ser específicos por cada regla.
3. Utilice "objetos de red" en lugar de muchos "objetos" individuales.
4. Utilice grupos de objetos donde sea posible y combinar reglas similares en una sola regla. Esto ayudará a mantener la base de reglas corta y simple, por lo tanto se reducirá la carga en el *firewall*.
5. Configure la funcionalidad de "Anti *spoofing*" en cada interfaz del *Firewall*.
6. Ponga las reglas más utilizadas o accedidas en las primeras posiciones de la base de reglas. Cuando un paquete llega al *firewall*, se verifica contra las reglas del *firewall* en orden de arriba hacia abajo (*top down*). Una vez que encuentra una coincidencia puede ser aceptado, negado, o se toma la acción definida en la regla. Por esta razón es mejor poner al principio de la base de reglas las que tienen más coincidencias con el tráfico en la red. Esto sirve para que no tenga que recorrer una gran cantidad de reglas hasta encontrar una coincidencia; hacerlo decrementará la carga de trabajo en el *firewall*.
7. Utilice nombres concretos para sus objetos (*hostname*, dirección IP, etc.).
8. Implemente la regla "*stealth*" o "furtiva", la cual bloquea los intentos de conexión hacia el módulo del *firewall* directamente (*src=any dst= firewall action= drop*).
9. Utilice "*drop*" en lugar de "*reject*" para algunos servicios, esto mejora el desempeño del equipo.
10. Implemente la regla '*clean up*' o una regla de *ANY* a *ANY*, acción *DENY*. Se recomienda habilitar el *log* para esta regla. Esto nos permitirá analizar los paquetes que sean descartados por no coincidir con ninguna regla de la base. Lo anterior es útil para detectar ataques o para la resolución de problemas.
11. No utilice el "objeto de dominio" en el *rulebase*. Dichos objetos pueden causar conflictos y problemas de desempeño como cuellos de botella.
12. Deshabilite el campo "*decrypt on accept*" si no se utiliza VPN.
13. Si la red está utilizando VPN, utilizar de preferencia AES128 como algoritmo de cifrado. Este tipo de cifrado genera menor carga y menos problemas de rendimientos a *firewalls* como Checkpoint.
14. Mantenga las bitácoras ("*logs*") al mínimo necesario. Ejemplo: Si la organización cuenta con dos servidores *Web* con mucho tráfico, entonces si el *firewall* tiene que registrar cada conexión de http, esto puede ocasionar una carga adicional al *firewall* y llenar el espacio del servidor de bitácoras rápidamente. Evalúe, sin embargo, si deshabilitar las bitácoras no conlleva ningún riesgo de perder información importante para una investigación digital.
15. Trate de implementar un esquema de alta disponibilidad o '*high availability*' si el presupuesto lo permite. Esto reducirá los tiempos de interrupción al servicio de red considerablemente. Si un *firewall* se cae, eso implica que la mayoría de las operaciones en ese segmento se detendrán. En cambio, si se tiene implementado '*high availability*', el *firewall* secundario puede salir al rescate. También existe la opción de '*firewall clustering*' que proporcionará redundancia y balanceo de cargas.

Continúa en página 42

El cumplimiento en tiempo real genera confianza en tiempo real cuando las TI y el control trabajan como uno.

Cada segundo de cada día hay miles de eventos a través de la red. Las soluciones de Administración del Cumplimiento de Novell® monitorean continuamente esta actividad en búsqueda de inconsistencias, generarando una vista holística en tiempo real de quién está accediendo qué y si están autorizados—todo mientras se integra con la infraestructura actual de tecnología. Así que en vez de documentar los riesgos después del suceso, puede confiar que el cumplimiento está activo, que la información está segura y que los costos de administración son reducidos. Obtenga cumplimiento en tiempo real y permita que Novell haga que las TI trabajen como una para su empresa.

Para mayor información contáctenos al (55) 5284 2700
o visite www.novell.com/compliance

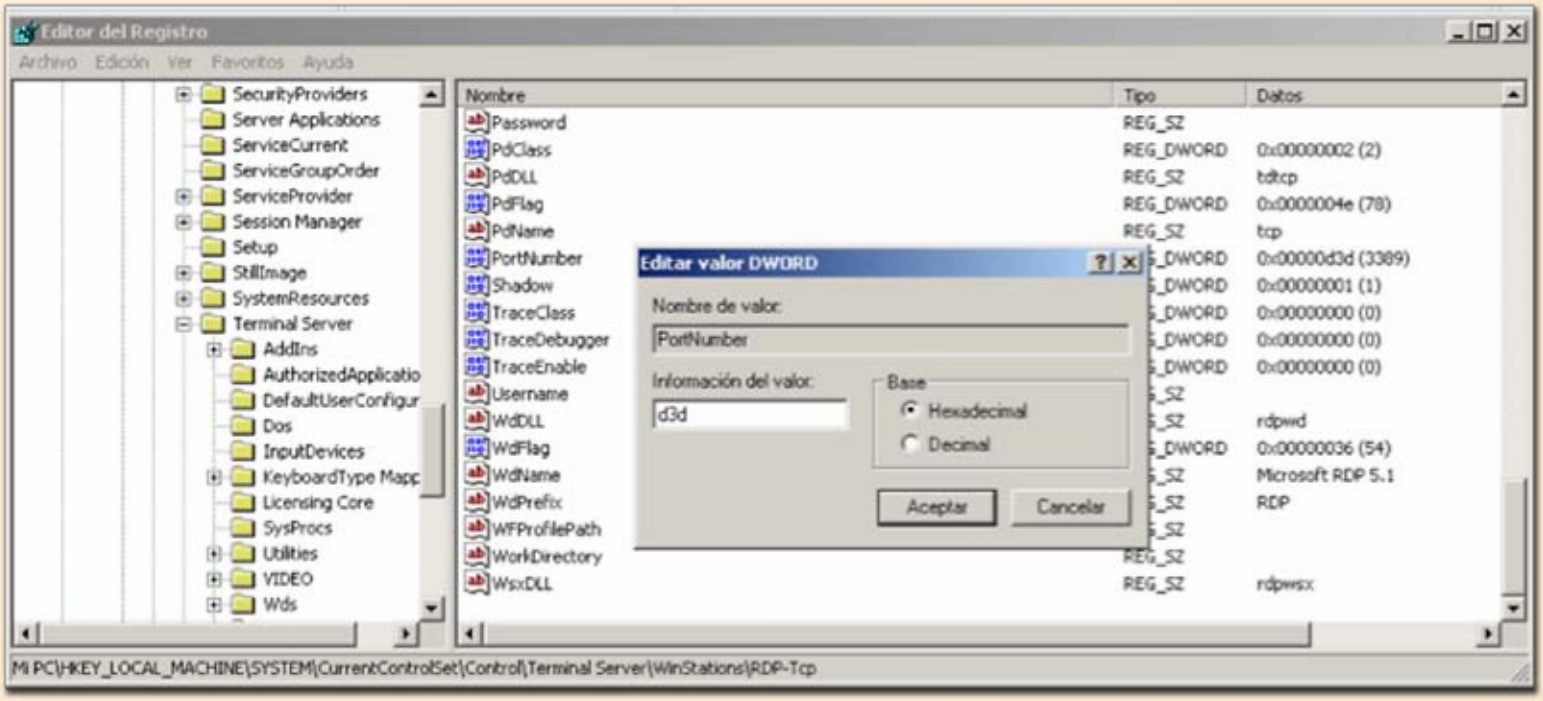
Novell®
Making IT Work As One™

¿Cómo evitar ataques de fuerza bruta al utilizar escritorio remoto (puerto 3389) en Windows 2003/XP/ Vista/7?

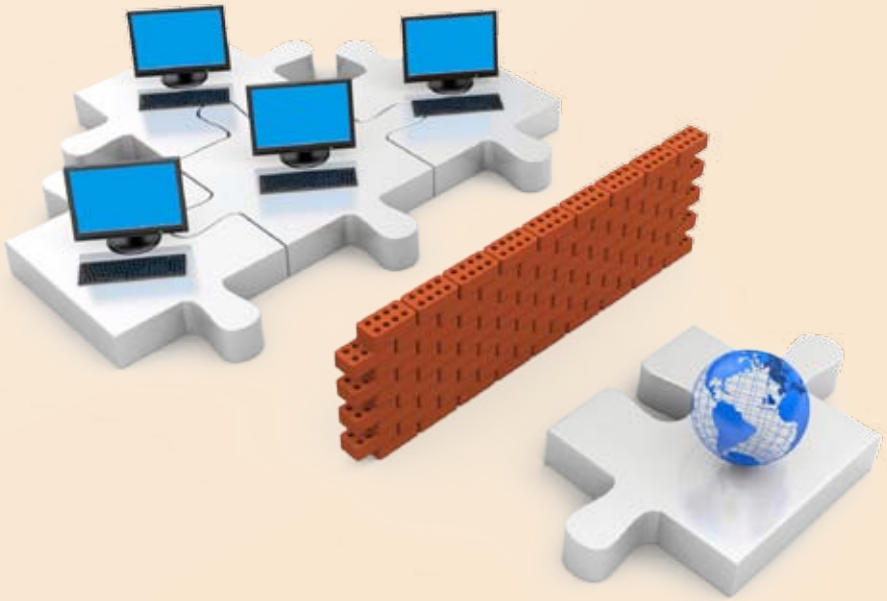
La mayoría de los ataques de fuerza bruta para obtener las cuentas de administrador en servidores Windows se presenta hacia el servicio de escritorio remoto, ya que los atacantes utilizan el escaneo de puertos para ver si se está ejecutando un servicio RDP (escritorio remoto). Es aconsejable cambiar el puerto default 3389 a un número diferente (revisar asignación de puertos http://www.iana.org/assignments/port-numbers) ya que la mayoría de los escáners de puertos (incluyendo nmap), escanean los puertos altos dando prioridad a los que ya tienen servicios asignados y conocidos (como el RDP en el puerto 3389), ya que si escanearan los puertos en orden secuencial, los resultados se darían en una forma muy lenta.

Cambiar el puerto disminuirá la probabilidad de que su servidor pueda convertirse en blanco de ataques de fuerza bruta a través del protocolo RDP. Aquí describo una manera para ocultar el servidor de rastreos al puerto 3389:

1. Inicie el editor de registro (*regedit*).
2. Buscamos la siguiente llave en el registro: `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`
3. Abra la subclave *Portnumber*:



4. Elija la opción decimal y cambie el numero de puerto (de preferencia arriba de 1024) y aceptar el cambio.
5. Cierre el editor de registro y reinicie el servidor.
6. No se olvide de realizar los cambios en sus políticas de *firewall* para permitir el nuevo puerto.



Espero que les sea de utilidad.

¿Sabías que

Scitum

es el primer Centro de Entrenamiento autorizado en México?

(ISC)² EDUCATION AFFILIATE Authorized Provider

Por lo que ahora puedes:

1.- Tomar el Seminario Oficial de CISSP de (ISC²) del 30 de agosto al 3 de septiembre de 2010, a un precio especial de $1,500.00 Dlls. + IVA
2.- Presentar el exámen de certificación CISSP el 23 de octubre de 2010, cuyo costo es de $549.00 Dlls.

La sede tanto del seminario como del examen es:
Oficinas de Scitum, Cd. de México.
Av. Paseo de la Reforma No.373
Col. Cuauhtémoc
C.P. 06500 México D.F.

Más informes, comuníquese al 9150 7496, lunes a viernes de 9:00 a 18:00 hrs. o bien al correo electrónico: capacitacion-isc2@scitum.com.mx

CAMBIANDO LA CARA DE LA PREVENCIÓN DE INVASIONES

con Check Point IPS Software Blades

Protección Total • Performance sin **Comparación** • Precio **Competitivo**

Presentamos Check Point IPS Software Blades

El Blade integrado de IPS de Check Point un cambio en la manera de hacer prevención de intrusiones y seguridad de la red como es conocido hoy en día. Las empresas tienen que escojer entre precio, desempeño y niveles de protección. La revolucionaria prevención de intrusiones trae protección de redes sin comparaciones, desempeño sin igual en el mercado, mientras reduce los costos significativamente- **hasta el 90% en comparación a las demás soluciones del mercado.**

Protección Total
Millares de firmas, protecciones por comportamiento y preventivas.

Performance lider de la industria
Hasta los 15GBps para el IPS y 25GBps para el trafico de firewall.

El más bajo TCO
Ahorros nunca vistos con un bajo valor de adquisición, instalación y operación.

Scitum

Check Point®
SOFTWARE TECHNOLOGIES LTD.