No.13 / Mayo-Junio ISSN: 1251478, 1251477

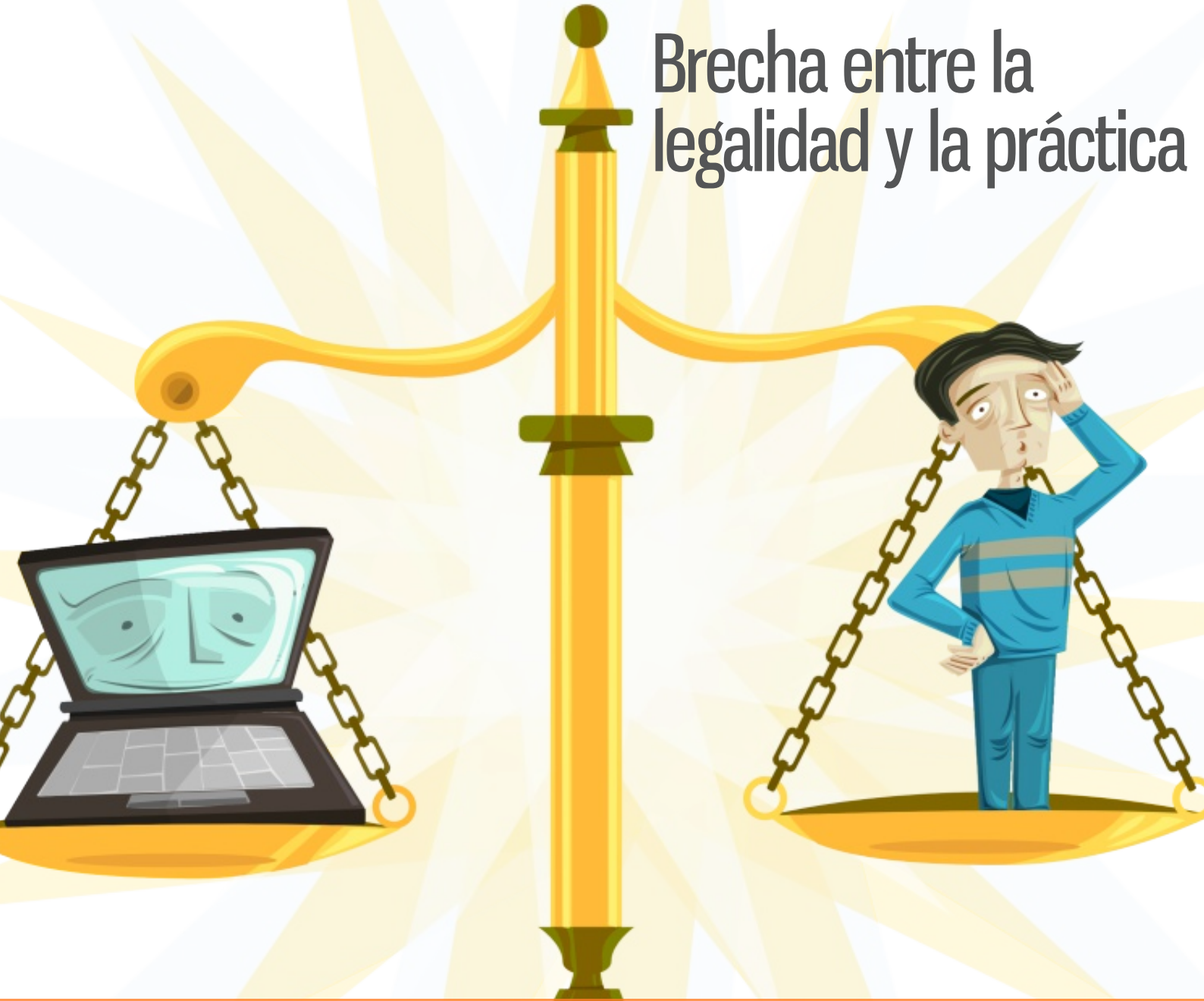
.Seguridad

Cultura de prevención para TI

13

Privacidad y Seguridad

Brecha entre la legalidad y la práctica



Hacking | DDoS | Protección Datos | Ley Federal Protección Datos | Protección Información | APT (Advanced Persistent Threat)

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Privacidad y seguridad
Brecha entre la legalidad y la práctica

En la actualidad, tanto usuarios como empresas intercambian datos personales como parte de sus actividades cotidianas dentro y fuera de Internet. Por lo que siempre existe una constante inquietud sobre qué hacer para proteger los datos que recibimos y enviamos todos los días.

En esta edición .Seguridad Cultura de prevención para TI reúne una serie de opiniones que ayudarán a aclarar el horizonte de la seguridad de datos. Por un lado, se muestra el panorama mundial en cuanto a la protección de datos, se dirige la brújula en el engorroso tema de las políticas de privacidad en las empresas; y se ofrece una serie de prácticas soluciones para la protección de nuestros datos como usuario final.

Asimismo, se abordan temas de actualidad como el futuro de los antivirus y su método de identificación; y se continúa con el tema del fraude en México y las alternativas de Pentesting, abordado en ediciones anteriores.

En esta ocasión contamos con la participación especial del INFOTEC con una acertada explicación de lo que implica un ataque DDoS.

Esperamos que este número llene tus expectativas, te invitamos a contactarnos por cualquiera de nuestros canales de comunicación para extender el diálogo de seguridad.

Bienvenido una vez más a .Seguridad

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

.Seguridad
Cultura de prevención para TI

.Seguridad, Cultura de prevención TI / Número 13 / Mayo-Junio 2012 / ISSN No. 1251478, 1251477 / Revista Bimestral

Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I

Isai Rojas González, Gabriel Sánchez Pérez, Linda Karina Toscano Medina,
María del Carmen Prudente Tíxteco, Gualberto Aguilar Torres

Introducción

La protección de datos personales se remonta a 1948, cuando la Asamblea General de las Naciones Unidas adopta el documento conocido como Declaración Universal de Derechos Humanos, en este documento se expresan los derechos humanos conocidos como básicos. En el artículo 12 se señala lo siguiente:

" Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

Actualmente, una gran cantidad de datos personales, incluyendo aquellos conocidos como datos biométricos, son almacenados en sistemas computacionales, factor que los hace susceptibles de sufrir ataques informáticos.

En varios países del mundo hay esfuerzos por crear legislaciones que establezcan los límites, permisos y castigos entorno al manejo adecuado de los datos contenidos en los sistemas de información, sobre todo de aquellos definidos como datos personales.

Esta investigación busca un precedente legal de cómo son considerados los datos biométricos por las leyes de protección de datos personales de distintos países en el mundo.

A continuación se describen algunos conceptos que son utilizados en este trabajo:

1. Dato personal

Se refiere a toda aquella información asociada a una persona o individuo que lo hace identificable del resto de las personas y/o como parte de un grupo determinado de individuos, por ejemplo: nombre, domicilio, teléfono, fotografía, huellas dactilares, sexo, nacionalidad, edad, lugar de nacimiento, raza, filiación, preferencias políticas, fecha de nacimiento, imagen del iris del ojo, patrón de la voz, etc. La idea central de este concepto es común en las legislaciones de protección de datos que distintos países han redactado. de la

voz, etc. La idea central de este concepto es común en las legislaciones de protección de datos que distintos países han redactado.

2. Datos personales sensibles

Comúnmente se refiere a todos aquellos datos que se relacionan con el nivel más íntimo de su titular y cuya divulgación pueda ser causa de discriminación o generar un severo riesgo para su titular. De manera general, se consideran datos sensibles aquellos que revelen características como origen étnico o racial, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual, pertenencia a sindicatos, creencias filosóficas y morales, entre otras. Esta clase de información debe ser tratada con mayor responsabilidad y establecer medidas de protección más estrictas.

La siguiente lista son algunos ejemplos de datos biométricos:

- Huellas dactilares
- Geometría de la mano
- Análisis del iris
- Análisis de retina
- Venas del dorso de la mano
- Rasgos faciales
- Patrón de voz
- Firma manuscrita
- Dinámica de tecleo
- Cadencia del paso al caminar
- Análisis gestual
- Análisis del ADN

3. Datos biométricos

Por definición común, los datos biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Aquellos sistemas informáticos en los que se mide algún dato biométrico, como parte del proceso de identificación y/o autentificación de un sujeto, son conocidos como sistemas de seguridad biométrica o simplemente sistemas biométricos.

Por definición y por su propia naturaleza, los datos biométricos son datos personales, sin embargo, la interrogante es ¿Cuál es la aplicación de las leyes de protección de datos personales con respecto a los datos biométricos?

Leyes de protección de datos en el mundo

En el mundo existen dos vertientes principales entorno a la protección de los datos personales: El modelo europeo busca proteger la información y la propiedad de la misma, en aras de conservar la honorabilidad de la persona aun cuando ésta hubiese fallecido, la motivación de este modelo

tiene base en los derechos humanos de los individuos. El modelo estadounidense pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto, el modelo surge derivado de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información. extinguirse con la muerte del sujeto, el modelo surge derivado de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información.

Diversos países han promulgado leyes de protección de datos personales y en cada país se ha buscado adaptar, a sus propias condiciones culturales, económicas y políticas, las bases de alguno de los dos modelos de protección de datos personales existentes. A continuación, se mencionan algunos casos relevantes sobre las leyes de protección de datos personales de distintos países, organizaciones y regiones del mundo:

1. Organización de Naciones Unidas (ONU). En 1948, adopta el documento conocido como Declaración Universal de Derechos Humanos, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.

2. Alemania. En 1970 fue aprobada la primera ley de protección de datos (Datenschutz). En 1977, el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.

3.Suecia. En 1973 fue publicada la que fue una de las primeras leyes de protección de datos en el mundo.

4. Estados Unidos de Norteamérica. La protección de datos tiene base en la Privacy Act de 1974.

5.Unión Europea. El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como "Convenio 108" o "Convenio de Estrasburgo". En los 90's, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

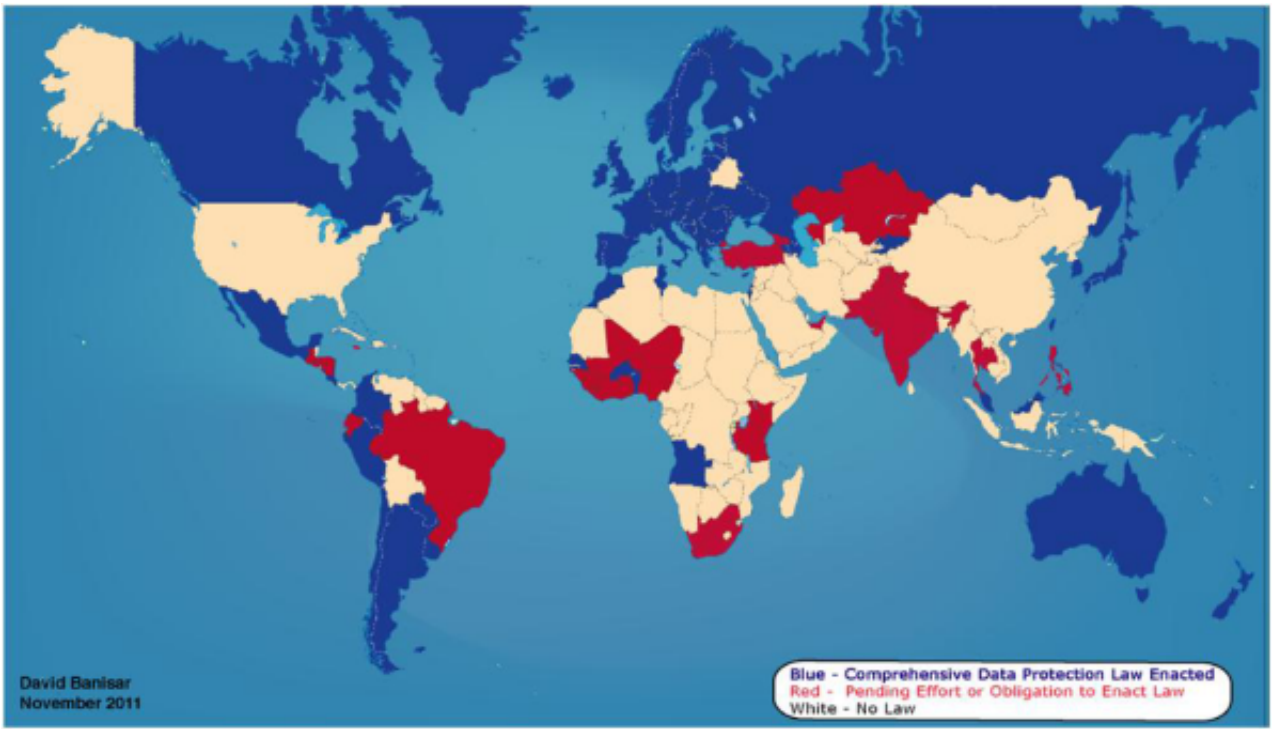


Fig. 1. Leyes de protección de datos en el mundo según David Banisar, David Banisar es un reconocido especialista en el campo de la política de la información, en particular en la intersección de los derechos humanos y las TIC.
http://cyberlaw.stanford.edu/profile/david-banisar.
http://ssrn.com/abstract=1857498

6. España. La ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Está ley ha sido importante para Latinoamérica porque se ha utilizado como firme referente del modelo europeo. se ha utilizado como firme referente del modelo europeo.

7. Latinoamérica. En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: En Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008).

8.Rusia. En el año 2006 fue aprobada una exhaustiva ley de protección de datos personales.

9.Perú. La ley 29.733 del 2 de julio de 2011 es la más reciente ley de protección de datos personales en el mundo.

10. México. La Ley Federal de Protección de Datos Personales en Posesión de Particulares fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, entró en vigor un día después y tiene efecto a partir de enero del año 2012.

Esta ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas, en ella se establecen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc.), son los denominados derechos ARCO: Acceso, Rectificación, Corrección y Oposición.

La ley también indica que los particulares deberán avisar, a cada persona de la que obtengan información personal, sobre el tratamiento que planean dar a sus datos. Lo anterior se debe hacer mediante un aviso de privacidad, el cual deberá ser respetado por el particular, y cada persona notificada tendrá la libertad de otorgar o no su consentimiento respecto al procesamiento de su información.

Mapa de protección de datos personales

David Banisar ha publicado un mapa con las leyes de protección de datos personales aplicadas en el mundo (Fig. 1). La clasificación de Banisar parece evaluar únicamente el modelo europeo de protección de datos personales, ya que no incluye

a los Estados Unidos como parte de los países con legislación sobre protección de datos personales.

Con esto concluye la primera parte de este artículo, en la segunda parte se hará mención de los riesgos asociados a los datos biométricos, de aquellas leyes de protección de datos personales, de distintos países del mundo, que incluyen en sus artículos la protección explícita de los datos biométricos.

Referencias bibliográficas (Parte 1)

[1] Ley Nº 19.628 (Chile). Sobre Protección de La Vida Privada O Protección De Datos De Carácter Personal

[2] Ley 25.326 (Argentina). Protección de los Datos Personales

[3] Ley Orgánica 15/1999 (España), de 13 de diciembre, de Protección de Datos de Carácter Personal.

[4] Gregorio C.G. Protección de Datos Personales: Europa Vs. Estados Unidos, todo un dilema para América Latina (p. 299–325)

[5] Ley Estatutaria 1266 . Colombia. (2008)

[6] Gregorio C.G. Protección de Datos Personales en América Latina – Juan Pérez ante la disyuntiva de progreso y bienestar. Disponible en http://www.iijlac.org/docs/juanperez.pdf

[7] Millan A. (2011). Retos de la protección de datos personales en México. Consultado en: http://www.lasillarota.com/index.php?option=com_k2&view=item&id=16493:retos-de-la-protecci%C3%B3n-de-datos-personales-en-m%C3%A9xico&Itemid=101

[8] Directiva 95/46/CE del Parlamento Europeo y del Consejo

[9] Travieso J.A. (2009). Seguridad física y lógica para la protección de los datos personales. CIBRA

[10] Luxemburgo. Protection Des Personnes À L'égard Du Traitement Des Données À Caractère Personnel

[11] Suecia. Personal Data Act (1998:204)

[12] Reyes O. P. (2004). Legislación extranjera sobre Derecho de Acceso a la información. Biblioteca del Congreso Nacional de Chile.

[13] Ley Nº 18.331 (Uruguay). Protección de Datos Personales y Acción de "Habeas Data"

[14] Ley Nº 29733 (Perú). Ley de Protección de Datos Personales.

[15] Ley de Datos de Suecia 1973

[16] Privacy Act, 1974. United State of America

[17] Ley de Protección de Datos de Hesse (1970)

[18] Ley Alemana Federal de Protección de Datos (1977)

[19] Loi 78-17 Du 6 Janvier (1978). Relative À L'informatique, Aux Fichiers Et Aux Libertés (Francia)

[20] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[21] Ley de Protección de Datos Personales de Paraguay

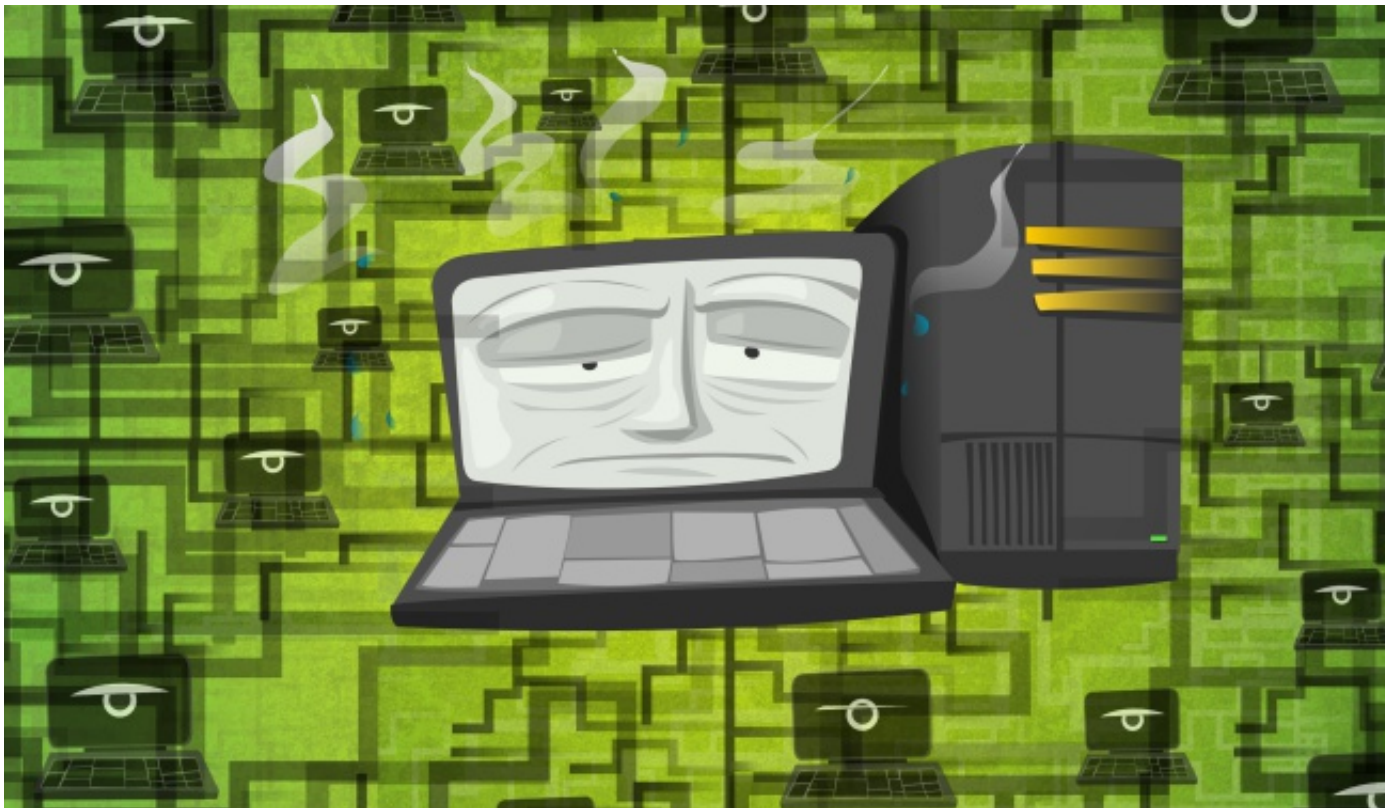
[22] Tratado de Estrasburgo. Convenio para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal.

[23] Banisar D., National Right to Information Laws, Regulations and Bills 2011 Map (November 22, 2011). Disponible en SSRN: http://ssrn.com/abstract=1857498

DDoS actualidad taxonomía y contramedidas

José Antonio Ruíz Alvarez

Una denegación de servicio o “DoS” (Denial of Service), es el vector de ataque que busca como objetivo principal, realizar la saturación o la explotación de alguna vulnerabilidad en un servicio que opere en equipos o infraestructuras de telecomunicaciones, dando como resultado la degradación, caída o falla del mismo. Una nueva modalidad de este vector de ataque es conocido como DDoS (Distributed Denial of Service), que por sus siglas en inglés se refiere a un ataque de denegación de servicio distribuido, el objetivo principal de este vector es la de utilizar un gran flujo de tráfico que es generada desde diferentes puntos de conexión, ya sea de internet o de una red de datos local con el mismo fin, la de deteriorar un servicio hasta hacerlo fallar.



Recientemente hemos escuchado sobre las operaciones grupos Hacktivistas, mismos que han realizado ataques de este tipo, principalmente hacia portales WEB de entidades gubernamentales y algunos cuantos del sector privado, es por este tipo de ataques que el INFOTEC se ha visto en la necesidad de incursionar e investigar estas nuevas tendencias de ataques, debido que nuestra visión es innovar y desarrollar servicios que puedan ser utilizados y aprovechados por ambos sectores ya sea gobierno o iniciativa privada.

En las operaciones cielito lindo, tequila, independencia y en la ultima llamada operación tranzas el principal objetivo de ataque ha sido el sector gobierno, entidades como la sedena, gobernación, el senado, la cámara de diputados por mencionar algunos, se han visto como victimas de este grupo de atacantes, que en momentos vemos como son superados los controles de seguridad por el gran número de atacantes; dejando en claro lo vulnerable y débil que son las infraestructuras y las arquitecturas de comunicaciones y seguridad en México. Lo que podemos notar, es que el modus operandi de estos grupos es de carácter político, religioso o social y el número de ataques aumenta hacia el

sector gobierno siendo esta de un 52% de ataques de este tipo, le sigue la iniciativa privada y al final y no por eso no ser atacadas, se encentran las instituciones académicas.

Entonces los ataques DDoS, representan una amenaza muy real para los negocios en línea, más aún cuando la disponibilidad del servicio es una función esencial del negocio. En la actualidad los firewalls tradicionales y dispositivos de protección perimetrales o controles de seguridad, pueden proporcionar un cierto grado de protección contra ataques de ancho de banda relativamente bajos, sin ser óptimos ni confiables. Cabe mencionar que es difícil defenderse de estos ataques, pero mediante una planificación cuidadosa y contando con el apoyo de especialistas y de los proveedores de servicios de internet (ISP), es posible proporcionar un nivel óptimo de protección frente a los ataques de denegación de servicio.

En conclusión, los ataques de denegación de servicios continúan siendo un problema y una gran preocupación para las empresas, gobiernos y proveedores de servicios, sobre todo en su forma distribuida (DDoS), principalmente por su fácil implementación, por lo devastador que puede ser el ataque y la mutación constante de sus procedimientos, pero no por eso es imposible detectarlos, mitigarlos, prevenirlos y detenerlos, si contamos con los especialistas, tácticas, proveedores y una infraestructura solida y en constante revisión lo podemos lograr, en INFOTEC ya contamos con casos de éxito vs DDoS/DoS, por lo que podemos apoyarte en la mitigación de este vector de ataque. INFOTEC su socio tecnológico.

José Antonio Ruíz Alvarez
Hacking SWAT Team Leader
Fondo de Información y Documentación para la Industria INFOTEC
Unidad de Seguridad de la Información
jose.ruiz@infotec.com.mx

¿Qué pide el reglamento de la ley?

Juan Carlos Carrillo D´Huerta

Desde el pasado miércoles 21 de diciembre de 2011 muchas personas me hacen la misma pregunta: "¿Qué pide el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares a las empresas como la mía?"

La respuesta, que no es simple, se encuentra en síntesis en 3 artículos del Reglamento de la Ley, los artículos 48, 60 y 61.

¿La Ley exige lo mismo para todas las empresas?

Ninguna ley, por naturaleza, puede exigir más o menos a las personas o empresas, por lo que la pregunta del nivel de exigencia es capciosa, pero el artículo 60 presenta elementos para que la carga sea acorde a las capacidades de los responsables (como pasa o debería pasar con los impuestos).

El artículo deja en libertad a los responsables en: "El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores"

Pero si nos marca las consideraciones necesarias para determinar las medidas de seguridad a implementar, explico dichas consideraciones:

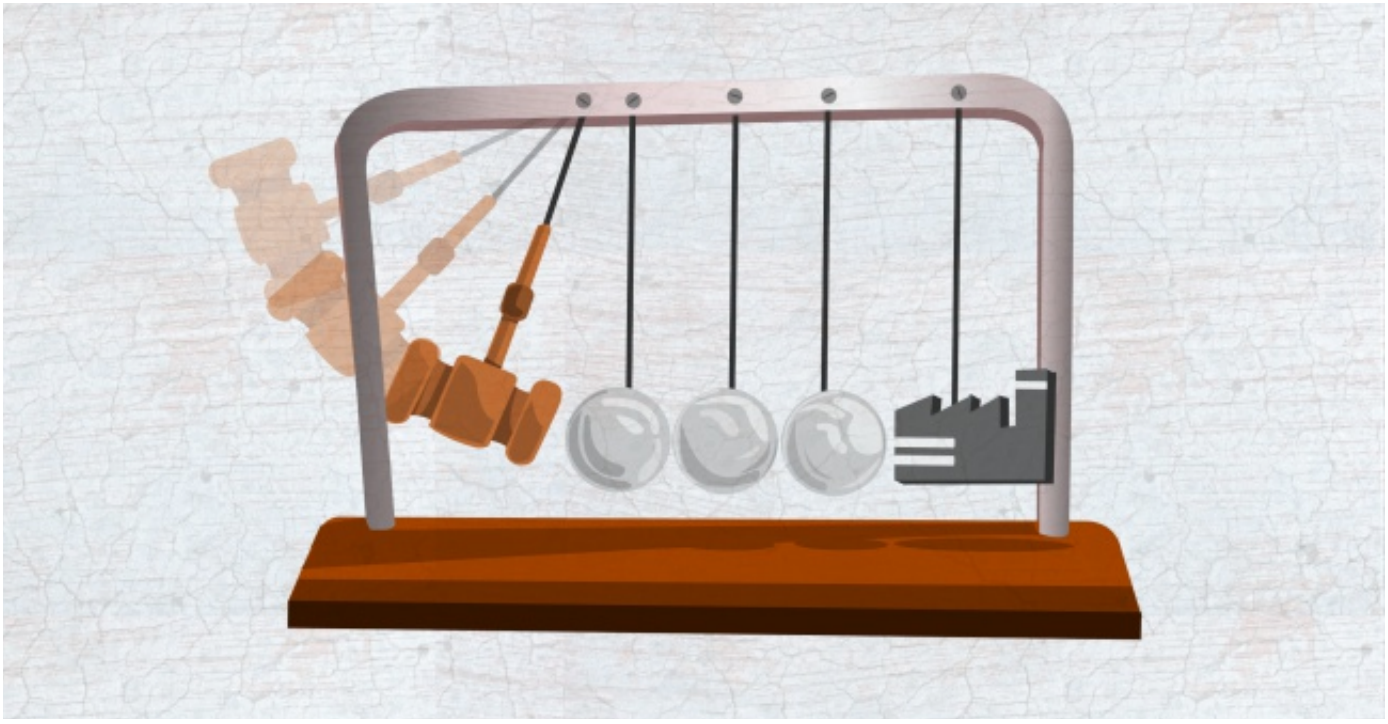
I. El riesgo inherente por tipo de dato personal. El riesgo es igual a la amenaza por la vulnerabilidad, por lo que es necesario realizar un análisis de riesgos (como lo insistirá el artículo 61).

II.La sensibilidad de los datos personales tratados. La sensibilidad derivada de la misma

Ley y definida en datos personales y datos personales sensibles, requiere que hagamos una clasificación de información para determinar la sensibilidad de los datos.

III. El desarrollo tecnológico. El estado actual de la tecnología, si no es conocido, deberá ser analizado con profundidad y relacionado con la sensibilidad de los datos, es decir no solo será conocer el desarrollo tecnológico general del responsable si no por el tipo de sensibilidad de los datos personales que se manejan.

IV. Las posibles consecuencias de una vulneración para los titulares. Históricamente, las organizaciones hemos valuado la información por el impacto que tiene al interior de la organización, bajo esta legislación debemos valorar el costo de los datos personales.



V. El número de titulares. Esta es la variable más sencilla. Es el volumen de datos personales que manejamos, básicamente de nuestros clientes (personas físicas) y de nuestros empleados.

VI. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento. Este es uno de los requerimientos más complejos, ya que por distintos reportes del Ponemon Institute sabemos que más del 85% de las empresas sufren al menos una vulneración a la seguridad al año, pero esto no se conoce o se decide ocultar. En el estado de California en los Estados Unidos existe desde 2003 una legislación únicamente para vulneraciones a la seguridad (California Senate Bill 1386) y que nos puede ayudar mucho en el manejo de estas situaciones.

VII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. Este punto nos pide que el análisis que hagamos de los datos personales no debe ser únicamente en su volumen sino en el riesgo de la reputación de los titulares afectados.

VIII. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares no exime del cumplimiento de otras legislaciones, por el contrario, suma a las variables de riesgo y cumplimiento dichas leyes o regulaciones, como pueden ser las solicitadas por el IMSS, SAT, INFONAVIT, etc.

Una vez que hemos entendido los factores que nos afectan en el tipo de medidas de seguridad a implementar, analicemos qué medidas son las que debemos implementar (artículo 48).

Img. 1 Medidas para garantizar el debido tratamiento de datos personales según el artículo 48

Medidas para garantizar el debido tratamiento de datos personales

El artículo 48 del reglamento nos explica las actividades que debemos realizar para poder garantizar que el tratamiento de los datos personales cumple con la legislación, estas medidas no son opcionales y todos los responsables deben cumplirlas.

Para explicarlo anterior, muestro una gráfica de los requerimientos, donde todo gira alrededor de políticas y programas de privacidad obligatorios, los cuales deben tener un fundamento en el conjunto de acciones técnicas y administrativas que permitan garantizar el cumplimiento de los principios y obligaciones derivados de la Ley y su Reglamento.

Lo complicado al mirar este esquema es que no existe una sola área dentro de las empresas que pueda tomar toda la responsabilidad para cumplir con la legislación, es por lo mismo que todos los responsables deben tener un comité de protección de datos personales donde al menos estén las áreas de tecnologías de información, recursos humanos, legal y comercial.

Hasta este punto, la mayoría del trabajo parece ser un trabajo de procesos y procedimientos propios de las empresas, pero el reglamento es muy específico al pedirnos que implementemos 9 acciones para asegurar los datos personales. El artículo 61 del reglamento lo explica de forma muy puntual.

¿Cómo aseguro los datos personales?

A continuación, dividiré las acciones de aseguramiento dentro de proyectos específicos para su mejor comprensión.

Clasificación de la información

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento.
2. Determinar las funciones y obligaciones de las personas que traten datos personales.
3.Realizar un registro de los medios de almacenamiento de los datos personales.

PIA (Privacy Impact Analysis)

4.Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.
5.Establecer las medidas de seguridad

aplicables a los datos personales e identificar aquellas implementadas de manera efectiva.

Plan estratégico de mejora

6. Realizar el análisis de brecha que consiste en: la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.
7.Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.

Auditoria y capacitación

8. Llevar a cabo revisiones o auditorías.
9.Capacitar al personal que efectúe el tratamiento.

El futuro no pertenece a los antivirus

Fausto Cepeda González.

Los antivirus cumplieron en su época (finales de los ochenta) una labor importante para proteger satisfactoriamente a los equipos de cómputo. Sin embargo, el reinado de los antivirus tal cual los conocemos está llegando a su fin, en gran parte por su antiguo y ya no tan efectivo enfoque de listas negras. Hoy en día una empresa que desee seriamente proteger sus equipos de cómputo Windows contra los códigos maliciosos no debe permitir que su seguridad descanse únicamente en los antivirus.

Aunque no son nuevas y ya han estado de alguna forma viviendo en las infraestructuras de TI, (por ejemplo en productos que previenen intrusos en sistemas) las soluciones de listas blancas han evolucionado y están evidenciando la mejora indiscutible en su enfoque para proteger a los sistemas de los cientos de códigos maliciosos o sus variantes que aparecen cada día. Dicho enfoque es sencillo y supone un cambio sutil, pero que hace la diferencia: enlistar lo que está permitido ejecutarse en un sistema (lista blanca) versus enlistar lo que se prohíbe ejecutar en una computadora (lista negra usada por los antivirus).

Si tuviéramos únicamente un puñado de software malicioso (virus, troyanos, etc.), entonces implementar una lista negra sería relativamente sencillo y efectivo. Cada semana que apareciera un par de virus o gusanos obtendríamos su huella (con la cual sabríamos cómo identificarlos), generaríamos la firma correspondiente y actualizaríamos el antivirus. Ésta era la situación que se vivía en los noventa.

Hoy en 2012 es otra historia, los antivirus han demostrado su punto débil ante la abrumadora cantidad y poder del nuevo malware que hay que detener. Sin mencionar la pobre labor para detectar a los llamados APT (Advanced Persistent Threat), que por su naturaleza son avanzados (indetectables por los antivirus al usar técnicas evolucionadas) y persistentes

(persiguen objetivos específicos y dirigidos, intentan incesantemente lograr sus metas).

Los APT representan una amenaza que impacta usando un enfoque diferente al código malicioso común y corriente. Estos últimos siguen la estrategia de reproducirse en el mayor número de equipos posibles en un tiempo relativamente corto e infectar así a una base amplia de sistemas (así se construyen por ejemplo, las botnets, que son una colección de sistemas infectados bajo control del atacante). Ahora bien, los APT como los que afectaron a RSA o los que se vieron durante la llamada operación Aurora son específicos en el sentido de que se desea afectar a una empresa en particular. No hay un interés en comprometer masivamente a equipos (la detección de amenazas masivas es donde los antivirus tienen su nicho). Para los APT que usan estrategias avanzadas y específicas como en el caso de StuxNet, los antivirus son burlados sin demasiada dificultad.

Ahora bien, uno podría pensar que al menos los antivirus proveen seguridad contra estos ataques genéricos donde se persigue una infección masiva. Sin embargo, aun en este escenario, la protección depende de que la compañía antivirus detecte al código malicioso, lo analice para generar la firma correspondiente y pueda empujarla a todos los clientes alrededor del mundo que tienen su producto. Es decir, transcurre un cierto tiempo entre que se identifica un virus y que finalmente nuestro antivirus cuenta con la firma apropiada para detectarlo y eliminarlo. Ese tiempo puede ser de horas o días, dependiendo de la rapidez para identificarlo, la prontitud para generar la firma y la importancia del bicho detectado, entre otros factores.

Cabe resaltar que los antivirus no se han quedado del todo estancados. Han mejorado diversas tecnologías usadas ya desde hace tiempo, como la llamada "heurística" que es una detección en base al comportamiento de archivos donde se trata de determinar si un ejecutable es potencialmente código malicioso nuevo.

Otra mejora a introducido al usar la famosa nube, para mejorar la identificación y reducir los bytes de las firmas, además de acelerar la detección de nuevo código malicioso. De esta forma han ayudado ciertamente a atacar el problema. Sin embargo a) no están resolviendo la problemática de raíz y b) los equipos de cómputo continúan infectándose. Cualquier administrador de un antivirus corporativo podrá confirmar que con todo y las mejoras, los sistemas se siguen contaminando, lo que hace necesaria una limpieza manual en varios casos; algunos incluso llegan a recomendar que

Img. 1 Gráfica Nivel de Confiabilidad

después de una infección, lo más apropiado sea formatear el equipo para reinstalar el sistema operativo.

Mientras los productos antivirus sigan requiriendo bajar diariamente actualizaciones de firmas, seguirá siendo evidente que la dependencia de éstas es un factor principal en su estrategia de detección. Lo anterior no solo se puede verificar en infraestructuras corporativas de TI donde frecuentemente aparecen infecciones en sistemas con antivirus actualizado, sino que también se han realizado pruebas donde se evidencia la contaminación exitosa de equipos que únicamente cuentan con este tipo de control basado en listas negras.

Las listas blancas no son un concepto nuevo, pero sí han madurado con el tiempo hasta llegar a convertirse en una solución suficientemente sólida como para ser usada en una corporación. Hace unos años estas listas blancas no eran un producto por sí solo sino que por lo general operaban junto con otra solución de seguridad. Trabajaban básicamente haciendo un hash de una aplicación y verificando que siempre que ésta solicitara salida a la red, contara con un hash válido. Y ciertamente, esta manera primitiva de administración no era nada cómoda para el administrador, quien tenía inicialmente que registrar cientos (o miles) de aplicaciones y averiguar si se podían catalogar como programas benignos. Pero la labor no termina ahí, ya que posteriormente se debían gestionar todos los cambios en las aplicaciones existentes (por ejemplo, por la aplicación de parches de seguridad o instalación de nuevas versiones) para darles el visto bueno y que pudieran seguir saliendo a la red, sin mencionar el registro de nuevas aplicaciones. Esto resultó ser un verdadero infierno administrativo y se optaba por hacer reglas genéricas, por lo tanto se reducía el poder para proveer seguridad.

El concepto no ha cambiado, pero sí la forma de administrar los registros de las listas blancas. Hoy en día existen soluciones más "inteligentes" en el sentido de que tratan de identificar por sí solas a las aplicaciones benignas, siguiendo ciertos criterios para establecer un "nivel de confiabilidad", por ejemplo, cuánto tiempo se ha visto presente a esa aplicación en la infraestructura, si el programa proviene de una fuente confiable de la red corporativa (como un servidor de distribución de software) y otros parámetros, como se muestra a continuación: (Imagen 1)

Actualmente, se requiere tener dos soluciones separadas en las infraestructuras de TI, una de antivirus y otra de listas blancas, con toda la carga administrativa que eso conlleva: diferentes

agentes instalados en los sistemas, un par de consolas de administración y servidores donde residen las soluciones. Es probable que en el futuro estas dos tecnologías converjan en un solo producto haciendo una labor preventiva (lista blanca) y reactiva (lista negra); de hecho algunas soluciones de listas blancas están tomando ya ese camino.

No sorprende que varias instituciones estén actualmente incorporando soluciones de listas blancas, como se ven el caso de la NSA en Estados Unidos. Cabe mencionar que existen diversas soluciones que podemos encontrar actualmente en el mercado y que están orientadas al control de aplicaciones por medio de listas blancas, por ejemplo:

• Bit9 con su producto “Parity Suite”.

• Lumension con su solución “Application Control”
.
• CoreTrace con su lista blanca llamada “CoreTrace Bouncer”.

Las listas blancas vienen a llenar los huecos de los actuales controles basados en listas negras que luchan contra el código malicioso. Por lo tanto, el futuro cercano no debe seguir perteneciendo a los antivirus como el control por excelencia para proteger de los virus, gusanos, troyanos y códigos maliciosos en general. Una estrategia contra este tipo de amenaza ya no está completa sin la participación activa de un enfoque basado en listas blancas.

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

El poder de proteger tu información

Miriam J. Padilla Espinosa

¿Has pensado qué una protección no adecuada de tus datos personales podría convertirte en una cifra más en las estadísticas de robo de identidad o afectar tu reputación en línea?

Los casos de robo de identidad en México y a nivel internacional van en aumento, esto como consecuencia de factores como el uso de nuevas tecnologías, el incremento en la demanda de compras por Internet y el uso de banca en línea, la falta de conciencia o tiempo destinado por los usuarios para la protección de sus datos personales o financieros y el desarrollo de técnicas más sofisticadas por los atacantes para la obtención ilícita de este tipo de información, quienes se aprovechan de Internet, de diversos medios digitales y sobre todo, de la falta de precaución del usuario para lograr sus objetivos.

La protección de los datos personales y financieros es una actividad fundamental que se debe realizar con absoluta responsabilidad y conciencia, para ello es necesario definir un conjunto de medidas que permitan proteger nuestros datos, estas deberán ser seleccionadas considerando las siguientes interrogantes:

a)¿Qué se desea proteger?

Es indispensable que el usuario identifique qué información pone en riesgo su identidad o su privacidad. Para poder hacerlo es necesario entender estas clasificaciones:

Dato personal: es toda información relativa a un individuo que lo identifica o que permite su identificación (origen, edad, lugar de residencia o cualquier tipo de trayectoria, ya sea académica, laboral o profesional).

Datos personales sensibles: son aquellos cuyo uso indebido representa un riesgo grave para el propietario, que daña su intimidad o que lo hace sujeto de algún tipo de discriminación (origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual).

Datos financieros: es la información que permite conocer la composición o variación del patrimonio económico de un usuario en un momento o periodo determinado (estados de cuenta, transacciones y transferencias, saldos, número de cuenta, usuario y contraseña para el acceso en línea, etc.)

b)¿De qué se desea proteger?

Una vez identificados los objetivos de protección, es preciso que el usuario conozca los principales riesgos a los cuales puede estar expuesta su información, tales como robo, divulgación no autorizada, alteración, modificación, extravío o eliminación. A su vez, debe estar consciente de las consecuencias que esto conlleva, como daño en la reputación en línea del usuario, ser víctima de agresiones psicológicas o discriminación, convertirse en una víctima de robo de identidad para cometer cualquier tipo de fraude, mal uso o la afectación del patrimonio financiero del usuario.

MEDIDAS PARA LA PROTECCIÓN DE DATOS PERSONALES Y FINANCIEROS	
1.	Asegúrate que las páginas donde ingresas tus datos cuenten con certificados de seguridad que avalen la autenticidad de la misma. Nunca ingreses tus datos de usuario y contraseña en links desconocidos o que te sean enviados por correo electrónico.
2.	Verifica que cuando proporciones tus datos personales a cualquier particular éste te muestre un aviso de privacidad en el cuál tú autorices la recolección y el tratamiento que le darán a tu información.
3.	Ante el extravío de documentos de identificación, levanta una denuncia ante las autoridades que correspondan, quedando esto como un antecedente para tu protección ante cualquier mal uso que se le de al documento extraviado.
4.	En las encuestas telefónicas nunca proporciones información comercial, financiera o personal.
5.	Evita realizar compras o transferencias electrónicas en lugares públicos tales como café Internet, lugares que no estén debidamente establecidos o de dudosa reputación.
6.	Es recomendable tener cuidado en el manejo de documentos con información personal o financiera en especial aquellos que tengan tu firma personal o huella digital. Evita dejarlos al alcance de cualquier persona o en cualquier lugar.
7.	Nunca compartas tú información financiera, esta debe ser confidencial y ser manejada con reserva.
8.	Tomate tiempo para revisar tus estados de cuenta donde podrás verificar las transacciones que has realizado, en caso de presentarse alguna irregularidad comunícalo de inmediato a tu banco.
9.	Mantén actualizado el antivirus de tu equipo de cómputo, cambia y revisa con frecuencia la complejidad de tus contraseñas.
10.	Revisa la información que publicas en Internet especialmente en redes sociales y modifica las configuraciones de privacidad que éstas tienen, con el objetivo de permitir sólo a personas conocidas ver tus perfiles.
11.	Cuida la información que publicas en Internet recuerda que actualmente la reputación en línea es considerada al momento de la contratación de personal en las organizaciones.
12.	Es indispensable para cualquier aclaración conservar los comprobantes digitales de todas las transacciones que sean realizadas en línea.

Tabla 1. Medidas para la protección de datos personales y financieros

c)¿Cómo protegerlo?

El usuario debe ser precavido cuando navega por Internet, debe cuidar la información que publica en las redes sociales o que ingresa en formularios o ligas enviadas por correo electrónico. De igual forma debe hacer valer sus derechos, tales como el acceso, la rectificación, la cancelación y la oposición, para que los particulares (personas físicas o morales de carácter privado, con excepción de los mencionados en el artículo 2 de la LFPDPPP1) protejan la información que de ellos se tiene almacenada.

Definir medidas para proteger nuestros datos personales y financieros nos permite actuar de forma proactiva, es decir, actuar antes de presentarse cualquier incidente que ponga en riesgo nuestra reputación, privacidad, intimidad, situación financiera o en casos más extremos la vida misma.

La Tabla 1 presenta un conjunto de recomendaciones que permitirá a los usuarios tomar medidas para proteger su información.

REGULACIONES PARA PROTECCIÓN DE DATOS PERSONALES, FINACIEROS Y SEGURIDAD DE LA INFORMACIÓN	
ESTÁNDARES INTERNACIONALES	
ISO 27001:2005	Estándar que contiene el conjunto de requisitos necesarios para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI)[2].
ISO 27002:2005	Estándar que contiene una guía de buenas prácticas donde se describen un conjunto de objetivos de control y controles recomendados para mantener e incrementar la seguridad de la información en cualquier organización.
ISO 27005	Guía de técnicas para la gestión de riesgos de seguridad de la información.
ISO 27011	Guía de gestión de seguridad de la información enfocada en el área de las telecomunicaciones.
ISO 27032	Guía relacionada con la ciber seguridad.
LEYES, CÓDIGOS Y REGLAMENTOS EN MÉXICO	
• Constitución Política de los Estados Unidos Mexicanos: Artículo 6, 16, 73 • Ley Federal de Protección de Datos Personales en Posesión de los Particulares Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares • Ley Federal de Acceso a la Información Pública Gubernamental *Capítulo III Información reservada y confidencial* • Ley Federal de Protección al Consumidor *Artículo 76 BIS, fracción I* • Código Penal Federal del DF ***Artículo 211 BIS*** • Código de comercio • **Código Civil y de Procedimientos Civiles** • Ley de Protección de Datos del Estado de Colima • Ley de Protección de Datos Personales para el Distrito Federal • Ley de Instituciones de Crédito • Ley para regular las sociedades de información crediticia • Ley General de Salud y Reglamento de la Ley General de Salud en materia de prestación de servicios de atención médica	

Tabla 2. Regulaciones para protección de datos personales, financieros y seguridad de la información

Actualmente, existen tanto en México como a nivel internacional iniciativas, leyes, códigos y reglamentos que consideran la protección de los datos personales y financieros, así como

estándares internacionales y buenas prácticas para protección de la seguridad de la información. Algunos de éstos se presentan en la Tabla 2:

Tomando en cuenta estos datos, es posible fortalecer la seguridad de la información y reforzar las prácticas que llevan a una cultura de prevención de delitos relacionados con los datos personales.

Es fundamental que los usuarios elijan medidas de seguridad para proteger su información personal y financiera. También es necesario considerar la importancia de difundir información a personas cercanas para fomentar la cultura de seguridad y protección de los datos personales. Con estas prácticas contribuiremos a reducir riesgos y cifras en las estadísticas de personas afectadas por amenazas de seguridad. Recuerda que la información es poder, que está en nuestras manos protegerla y así controlar la capacidad que damos a otras personas para usar nuestra información.

Referencias:

• Padilla Espinosa, Miriam J. Buenas prácticas para proteger datos confidenciales en las aseguradoras. Tesis de licenciatura, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2009, México D.F.

• Requerimientos para publicar documentos en la web. En http://www.contenido.ccs.ipn.mx/G-840-2011-S.pdf

• Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010). Consultado en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

• Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2011) Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

• Leyes y reglamentos de la Secretaría de Gobernación. Consultado en http://dof.gob.mx/ley-reg.php

• Guía práctica para generar el aviso de privacidad (2011) IFAI. Consultado en http://www.ifai.org.mx/PrivacidadGuia

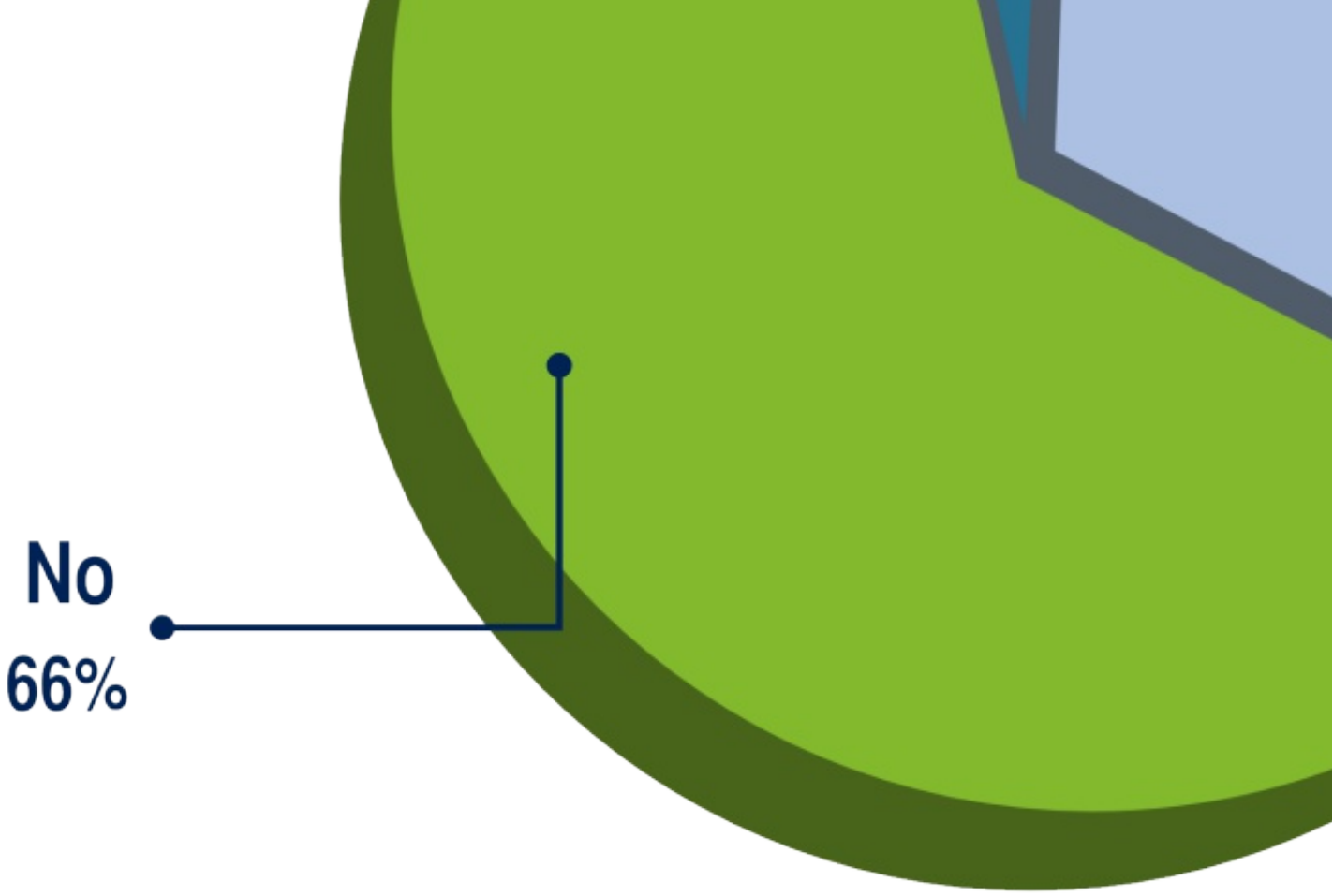
• ISO 27000 http://www.iso27000.es/iso27000.html

• Evento sobre la Ley y el Reglamento de Protección de Datos Personales (Presentaciones) Lex Informática. En: http://www.lexinformatica.com/blog/?p=129

• Navega protegido en Internet http://www.navegaprotegido.org/

1 LFPDPPP: Ley Federal de Protección de Datos Personales el Posesión de los Particulares.

2 SGSI: Sistema de Gestión de Seguridad de la Información. Concepto central sobre el que se constituye ISO 27001, su objetivo es garantizar que la seguridad de la información se gestione de forma correcta, basado en un proceso sistemático, documentado y con la participación de toda la organización, desde un enfoque de riesgo empresarial.



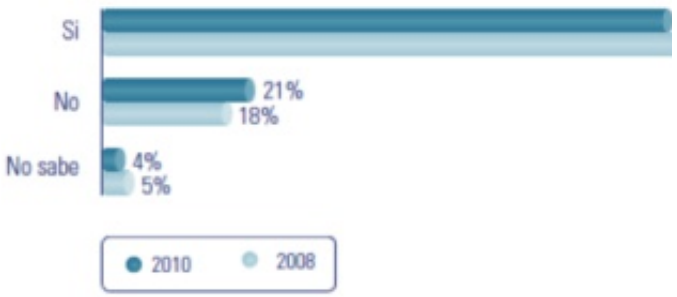
El hacking ético y la seguridad de la información de empresas en México

Anaid Guevara

En el artículo anterior revisamos qué es el hacking ético, cuál es su objetivo, quiénes trabajan en él y cuáles son sus alcances. Retomando esto último abordaré a detalle algunas razones para aplicar esta metodología en casos concretos como los fraudes y las fugas de información en países latinoamericanos, aunque enfocándonos específicamente en México.

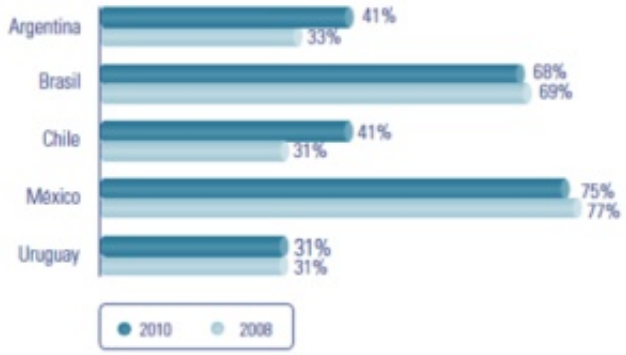
Desafortunadamente, hoy en día existe un bajo índice de inversión por parte de las organizaciones en auditorías pentesting, ya que no se le presta la debida importancia, y se prefiere invertir en otras áreas que puedan redituar a corto plazo, o simplemente las desconocen.

Este hecho ha propiciado el fraude de manera exponencial. Según un estudio realizado por KPMG referente a esta actividad en México durante el 2010, el nivel registrado de incidencia de fraudes para las compañías que operan en el país es de 75 por ciento, como lo muestra la siguiente gráfica:



Img. 1 Gráfica de Incidencia de fraudes en empresas que operan en México/ Fuente: KPMG. Encuesta de Fraude en México 2010

Esto significa que prácticamente 8 de cada 10 empresas que operan en México han padecido al menos un fraude en los últimos doce meses. Al comparar con otros países de la región, (Argentina, Brasil, Chile y Uruguay) se puede observar que México sigue presentando los niveles de incidencia de fraude más altos, pese a que en varios de estos países se registró un incremento en los mismos, tal y como lo muestra el siguiente gráfico:



Img. 2 Incidencia de fraudes en América Latina
Fuente: KPMG. Encuesta de Fraude en México 2010

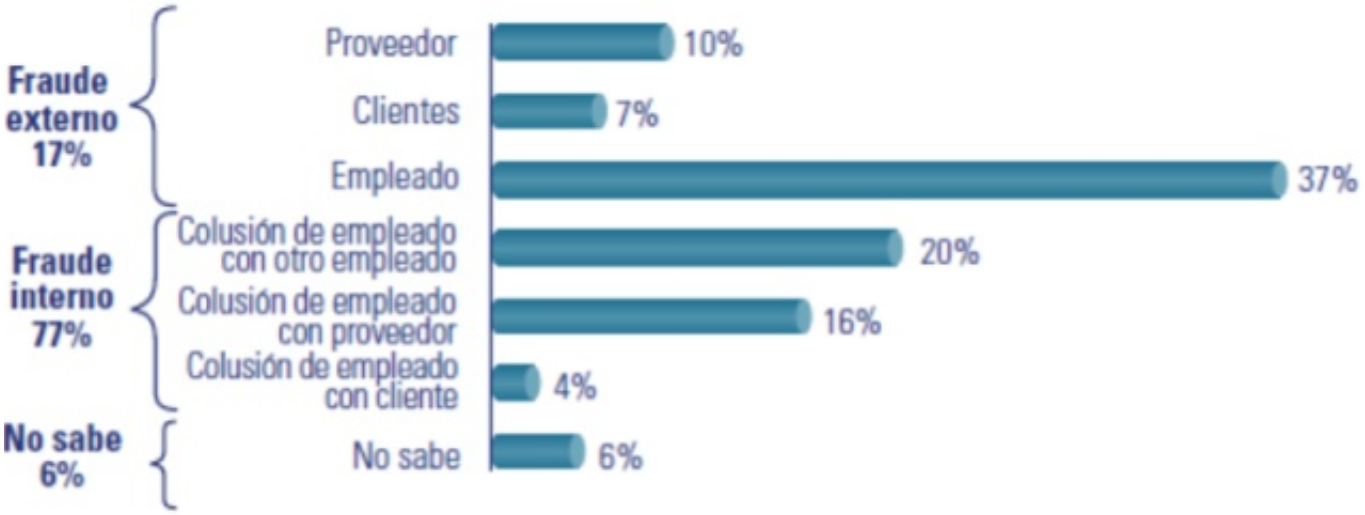
Si bien es cierto que el grado de incidencia de fraudes en general se ha mantenido prácticamente en el mismo nivel, también se pueden observar cambios significativos en el tipo de fraudes cometidos contra empresas que operan en México.

En términos de quién comete el ilícito, se pueden distinguir dos tipos de fraude: el interno y el externo.

El fraude interno es aquel que comete un empleado de la propia organización, sea de manera solitaria o en complicidad con alguna otra persona. Por el contrario, el fraude externo es el que realiza una persona ajena a la organización, como puede ser un proveedor o un cliente. Con base en esta clasificación, se puede observar que los fraudes que se han cometido en los últimos doce meses a empresas que operan en México son principalmente fraudes internos, un 77 por ciento, como se muestra en la siguiente gráfica: (Imagen 3)

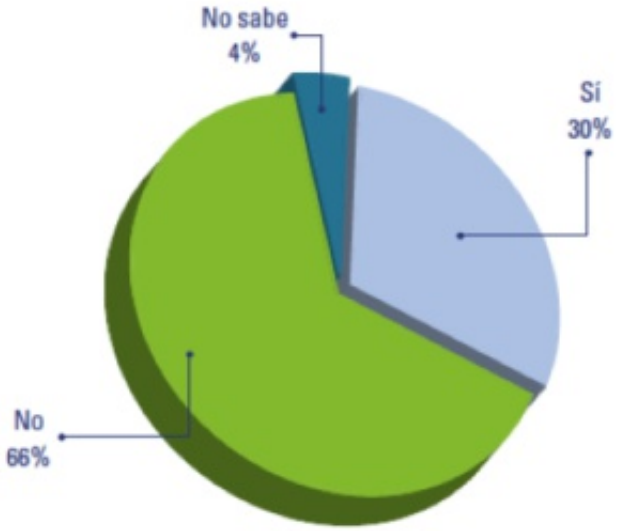
Por lo anterior, el control de una empresa debe tener base en un sistema permanente. No se puede dejar el patrimonio de la compañía al cuidado de la buena voluntad de los empleados, mucho menos en situaciones de crisis. No olvidemos que en situaciones como las que hoy se presentan, el principal objetivo de las empresas es mantenerse operativas e impedir mayores pérdidas. De ahí que, proteger a la empresa de posibles quebrantos se convierte, en buena medida, en un objetivo estratégico.

Para 2010, solo el 30 por ciento de las compañías que operaban en el país habían adoptado medidas de prevención de fraudes, las cuales pueden deberse a fallas en los sistemas, información divulgada consciente o inconscientemente por los trabajadores de las mismas, ataques informáticos, falta de cultura organizacional, etcétera.



Img. 3 Tipo de fraude por perpetrador del ilícito
Fuente: KPMG. Encuesta de Fraude en México 2010

La gráfica siguiente muestra la proporción de empresas que cuentan con medidas preventivas y las que reconocen no tenerlas. La alta relación de empresas que no cuentan con mecanismos de prevención de fraudes explica, en parte, el nivel de incidencia de fraudes en México, siendo uno de los más altos en América Latina.



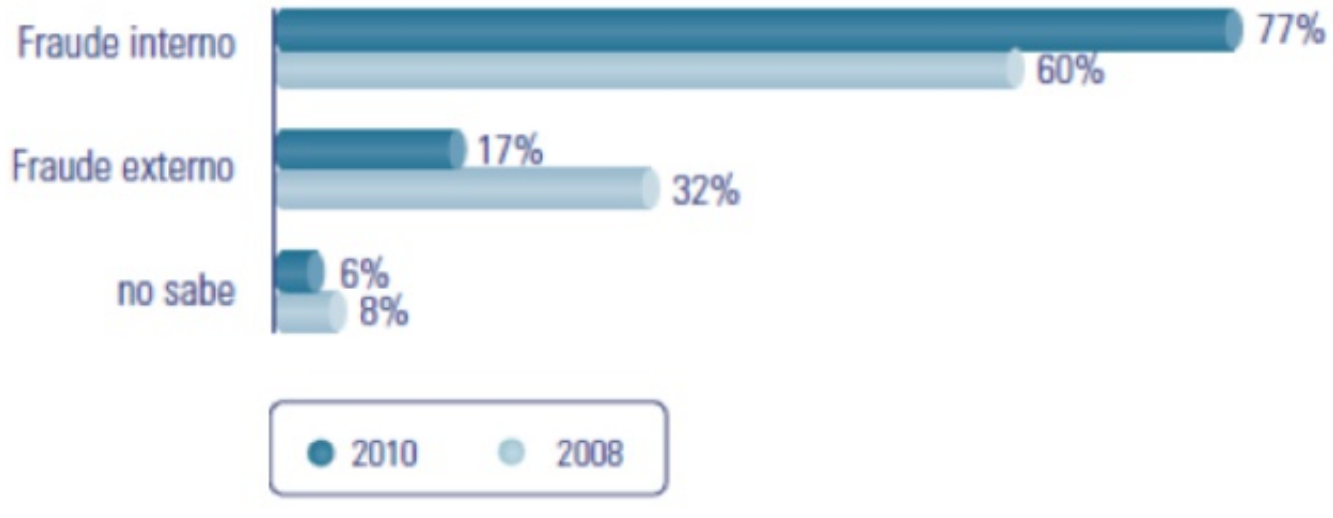
Img. 4 Porcentaje de empresas que cuentan con medidas de prevención de fraudes
Fuente: KPMG. Encuesta de Fraude en México 2010

Como se puede observar, solo el 30 por ciento de las empresas de nuestro país implementa medidas de prevención de fraude. Una mayoría, el 66 por ciento, no lo hace, y un 4 por ciento ni siquiera invierte en ello, no porque no quiera, sino porque desconoce las medidas preventivas que ayudan a mitigar la fuga de información confidencial, lo que trae como consecuencia grandes pérdidas monetarias y de reputación para la organización.

Finalmente, se expone la siguiente gráfica en la que, de acuerdo a estudios realizados en el 2010 por la Consultora KPMG, se hace un comparativo entre el índice detectado en 2008 y el 2010, respeto a los fraudes de índole interna en las empresas mexicanas.

Con estos antecedentes, queda claro que los empresarios y empleados deben ser conscientes de la gran cantidad de fraudes que acontecen a su alrededor, sobre todo con aquellos fraudes perpetrados por los propios empleados. También deben tomar conciencia de cuidar que los trabajadores que transportan información confidencial, no la revelen a terceros bajo ninguna circunstancia. En caso de que ocurra cualquier contingencia, prever para tener un plan de respuesta. Acciones como pruebas de penetración o hacking ético ayudarán a encontrar dichas fugas de información para así poder prevenir el mal uso de las mismas, y por consiguiente traer el fortalecimiento de la seguridad de la organización.

En conclusión, las pruebas de penetración o hacking ético son técnicas que arrojan resultados sustanciales a las empresas en cuanto a la detección y explotación de vulnerabilidades existentes en una infraestructura de red (Seguridad física, Seguridad en las comunicaciones, Seguridad inalámbrica, Seguridad en las tecnologías de Internet, Seguridad del resguardo de información, Seguridad de los procesos). Todo pentester (o hacker ético) ayuda a encontrar puntos



Img. 5 Comparativo de incidencia de fraudes
Fuente: KPMG. Encuesta de Fraude en México 2010

vulnerables realizando ataques informáticos, evitando que personas maliciosas (o crackers) causen daños, detectando previamente las vulnerabilidades y debilidades de la organización.

Es indispensable romper el paradigma de que lo relacionado con la palabra hacker es malicioso, permitiendo una mayor apertura a la aplicación de esta técnica en empresas en México ya que, como se expuso, el porcentaje de fraudes informáticos es muy alto, inclusive en relación con otros países latinoamericanos.

Referencias

• Anzola, S. Administración de pequeñas empresas (2003). México: McGraw-Hill.

• Barragán, J. et al. Administración de las pequeñas y medianas empresas, retos y problemas ante la nueva economía global (2002). México: Trillas.

• INEGI (1999). Instituto Nacional de Estadística Geografía e Informática.

• MARTÍNEZ Aguirre, Tania Guadalupe. Seguridad en el acceso a los sistemas de información. Celaya, Gto. Tesis de Licenciatura (Ingeniero en Computación- Universidad Lasallista Benavente, Escuela de Ingeniería en Computación), 2009.

Artículos

• Anonymous. Arm yourself against black hats. En: E-WORLD: Businessline. Chennai: Jul 12, 2010.

• Ronald I Raether Jr. DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure. En Business Law Today. Chicago: Sep/Oct 2008. Tomo 18, No. 1; Pág. 55 Ethical hacking on rise, Bill Goodwin. Computer Weekly. Sutton: Jan 31, 2006. Pág. 8 (1 página)

Estudios

• KPMG. Encuesta de Fraude en México 2010. México: KPMG. (2010). Recuperado de http://www.kpmg.com/MX/es/IssuesAndInsights/ArticlesPublications/Documents/Estudios/Encuesta_fraude_en_Mexico_2010.pdf