

Deloitte.

Panorama de Ciber Seguridad en México para 2016-2017

Sergio Solís
Gerente Senior
Cyber Risk Services

0101010100101
1010001011100
0101010101011
1010001010010



Agenda

- Antecedentes de ciber seguridad en México 3
- Un vistazo a los eventos relevantes del 2015 en el mundo 7
- Hacia dónde va el mundo en ciber seguridad 13
- ¿Qué es lo que viene para nuestro país? 21

México

Antecedentes de ciber seguridad



Antecedentes de ciber seguridad en México

“El pueblo que no conoce su historia, está condenado a repetirla”

- En México cada vez se presentan más incidentes relacionados a la ciber seguridad.
- En los medios se destacan algunos, debido a su contenido de interés, sin embargo, la gran mayoría nunca salen a la luz, incluso dentro de las mismas empresas.
- Aún existe una gran falta de conciencia en las organizaciones, mientras algunas intentan minimizar el riesgo, argumentando frases como **“eso nunca ha pasado (pasará) en la empresa”**, **“nosotros tenemos la tecnología para detener cualquier ataque”** o **“nuestra organización no está en la mira de los delincuentes”**... lo cierto es que todas organizaciones, y las personas, están expuestas a un ciber ataque.



Antecedentes de ciber seguridad en México

Política y Gobierno

- El **espionaje** en México parece ser una realidad, y la ciber seguridad se ha vuelto crucial para llevar a cabo las actividades relacionadas; esto quedó evidenciado con los registros que fueron revelados después del robo de información a la empresa **Hacking Team**.
- Por otra parte, entidades de gobierno como el SAT son objetivo de múltiples ataques; recientemente el SAT reveló que reciben **al menos un ataque por día**.

The collage features three main news snippets:

- EL ECONOMISTA**: "Vulneración a Hacking Team confirma abuso de espionaje en México". A table lists damages in Euros for various Mexican dependencies.
- proceso.com.mx**: "Hackean el sitio web de la Secretaría de Cultura de la Ciudad de México".
- ECONOMÍA**: "Tiran sitio web del SAT".
- EL UNIVERSAL.mx NACIÓN**: "Hackean el twitter del INE".

DEPENDENCIA	EUROS
Centro de Investigación y Seguridad Nacional (CISEN)	1,390,000
Gobierno del Edo. de México	783,000
Gobierno de Querétaro	234,500
Gobierno de Puebla	428,835
Gobierno de Campeche	386,296
Gobierno de Tamaulipas	322,900
Sección de Planeación y Finanzas*	371,035
Gobierno de Yucatán	401,788
Gobierno de Durango	421,397
Gobierno de Jalisco	748,003
PEMEX	321,120
TOTAL	5,808,875

*NO SE ESPECIFICA SI ES DE ALGUNA DEPENDENCIA

Antecedentes de ciber seguridad en México

“El que no conoce su historia, está condenado a repetir los mismos errores”

- El **robo de identidad** se ha vuelto una de las amenazas más fuertes en nuestro país, y aunque los principales afectados son los particulares, existen fuertes multas para las organizaciones que no protegen de forma adecuada la información... además, si pueden robar información personal, **¿por qué pensar que no se llevarán más información?**

EL FINANCIERO
HOME ECONOMÍA EMPRESAS NACIONAL TECH AFTER OFFICE

Robo de identidad se incrementa 40% en el primer semestre del año

Santander, Banamex y HSBC registran el mayor número de reclamaciones, ya que concentran el 76% del total, informó la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

Jeanette Leyva 14.09.2015 Última actualización 14.09.2015

INAI exige facultades para perseguir robo de identidad

Las comisionadas destacaron la importancia de que el delito de robo de identidad sea tipificado en el Código Penal Federal, con el propósito que los estados tengan una base mínima para reformar o adicionar sus códigos.

Foto: Facebook

Redacción AN
enero 29, 2016 12:34 pm

Me gusta 225

Compartir Email 31

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) demandó facultades para poder cooperar con otras autoridades en la persecución del robo de identidad, en la Ley General de Protección de Datos Personales cuyo proyecto está en análisis en el Congreso de la Unión.

EXPANSION
EN ALIANZA CON OM

DINERO

DE 1,800 MDP, EL MAYOR DAÑO POR ROBO DE IDENTIDAD EN MEXICO

Personas robaron la identidad de una joven para darla de alta como comerciante para vender alcohol; las autoridades multaron a la persona con 1,800 millones de pesos antes de descubrir el hurto.

Miércoles, 20 de enero de 2016 a las 9:58 PM



Fuente: Banco de México

Mundo

Un vistazo a los eventos relevantes del 2015



Un vistazo a los eventos relevantes del 2015 en el mundo

Datos personales y agencias de noticias

- El **robo de datos personales** ha impactado en todo el mundo, y podemos esperar que más organizaciones sigan siendo vulneradas, afectando a todos sus clientes / usuarios.
- Asimismo, las **agencias de noticias** están siendo objetivo de ataques, aprovechando el alcance que tienen hacia las masas, debido a su popularidad y/o prestigio periodístico.



Credit: [Jeremiah Izay](#)
Based on the images released, it looks as if the person responsible has full access to the newspaper's servers

Un vistazo a los eventos relevantes del 2015 en el mundo

Vulneraciones permiten visualizar alcance de riesgos

Millions of Americans Use Medical Devices That May Be Vulnerable to Hacking

W I R E D SUBSCRIBE

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

COMPUTERWORLD RESIDER Sign In | Register

NEWS ANALYSIS
Researchers hack a pacemaker, kill a man(nequin)

W I R E D

IS IT POSSIBLE FOR PASSENGERS TO HACK COMMERCIAL AIRCRAFT?

Credit: CME Healthcare

Researchers decided you don't need to be a pen tester to wirelessly hack a pacemaker, to successfully launch brute force and denial of service attacks that can kill 15 simulated humans.

- Algunos de los eventos permitieron al mundo observar vulneraciones de ciber seguridad que sólo se habían vislumbrado en la ciencia ficción, **rompiendo paradigmas** sobre la imposibilidad de vulnerar tecnologías como las de los automóviles, dispositivos médicos y aviones.

Un vistazo a los eventos relevantes del 2015 en el mundo

Política y seguridad de estado

- Los gobiernos de varios países fueron víctimas de múltiples eventos de **robo de información**, impactando en múltiples ámbitos, tomando relevancia incluso a nivel global.
- Algunos de los incidentes han logrado **exponer información** relacionada a secretos de estado, información derivada de espionaje e incidentes relacionados al terrorismo.

Anonymous Reveals ISIS Plot to Attack Paris, Indonesia, Italy, and Lebanon

Posted By: [Hacker News](#) | Posted in: [News](#) | Time Posted: Novem

Hackers leaked 43 GB of Syrian Government data online

April 10, 2016 The White Cat 0

Cyber Justice Team a group of hackers w
of data online, which contained informati
Government.

Anonymous Hacks Philippines Election Commission, Leaks 55 Million Voter Data

By [Wagas](#) on April 9, 2015 [Email](#) [@hackread](#)

[ANONYMOUS](#) [HACKING NEWS](#)

WIKILEAKS IS PUBLISHING THE CIA DIRECTOR'S HACKED EMAILS

ANDY GREENBERG SECURITY 10.21.15 5:52 PM

Hackear un marcapasos es posible (y Cheney lo sabía)

Matar a alguien con marcapasos es posible para un buen hacker informático. Eso es algo que hemos visto en la ficción pero que el que fuera vicepresidente con Bush supuso y se adelantó pidiendo que quitaran el WiFi a su dispositivo.

Like Share Tweet G+ D t in 0 Comentarios



Dick Cheney, exvicepresidente de EEUU | Foto: Wikimedia commons

Un vistazo a los eventos relevantes del 2015 en el mundo

Las principales amenazas en brechas confirmadas

1. **Phishing**
2. **Uso de credenciales robadas**
3. **RAM scraper o memory parser** (captura de datos de memoria volátil)
4. **Ataques de negación de servicio**
5. **Exportación de datos a otros sitios/sistemas**
6. **Uso de backdoors**
7. **Malware desconocido**
8. **Acceso remoto**
9. **Spyware/Keylogger**
10. **Hackeo desconocido**
11. **C2 (Command and control)**
12. **Captura de datos almacenados en disco**
13. **Downloader** (descarga a través de actualizaciones de software u otro malware)
14. **Escaneo de redes** (footprinting)

Fuente: "The Top 25 VERIS Threat Actions"

Un vistazo a los eventos relevantes del 2015 en el mundo

Las principales amenazas en brechas confirmadas (2)

15. **Password dumper** (extracción de hashes)

16. **Abuso de privilegios en el sistema**

17. **Skimmers** (para tarjetas de pago)

18. **Adminware — Utilerías del sistema/de red** (e.g., PsTools, Netcat)

19. **Rootkit** (mantener privilegios locales, de forma sigilosa)

20. **SQL injection**

21. **Exploit de vulnerabilidades en código** (por falta o debilidad de configuración)

22. **Desactivación de controles de seguridad**

23. **Ataques de fuerza bruta**

24. **Uso de hardware o dispositivos no autorizados**

25. **Packet sniffer** (captura de datos en la red)

Fuente: "The Top 25 VERIS Threat Actions"



Mundo

Hacia dónde va el mundo en ciber seguridad



Hacia dónde va el mundo en ciber seguridad

Ante un mundo cada vez más digital, los riesgos se incrementan



Los ciber ataques van a seguirse incrementando en el mundo, con distintos objetivos, destacando algunos como:

- Denegación / Interrupción de servicios
- Robo de propiedad intelectual
- Robo de datos de usuario
- Robo de identidad
- Secuestro de bases de datos
- Ciber guerra / terrorismo

México es el 2º país con mayor actividad de ciber ataques en América Latina* – aunque mayormente no es el generador de los mismos.

Hacia dónde va el mundo en ciber seguridad

Aspectos políticos y de seguridad de estado

El **crimen organizado** y el terrorismo están adoptando recursos tecnológicos para llevar a cabo sus actividades, y las autoridades están respondiendo en múltiples frentes, desarrollando sistemas especializados en sus agencias de investigación y cuerpos de defensa a nivel militar.



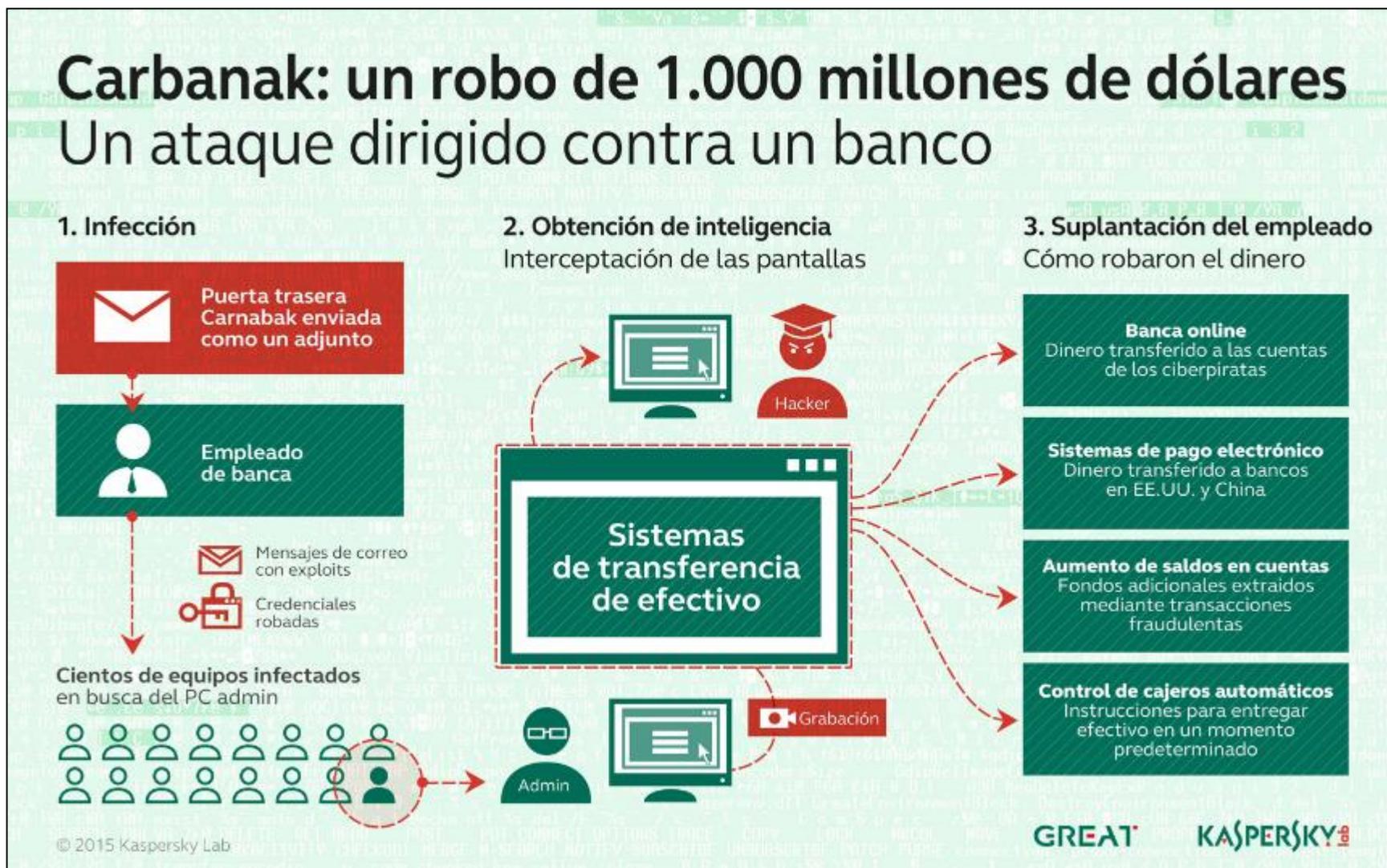
U.S. MILITARY LAUNCHES CYBERATTACKS AGAINST ISIS

BY ANTHONY CUTHBERTSON ON 3/2/16 AT 9:



Hacia dónde va el mundo en ciber seguridad

Los ataques de tipo APT rebasan los mecanismos básicos de seguridad



Hacia dónde va el mundo en ciber seguridad

“Conoce a tus enemigos y conócete a ti mismo, y podrás pelear un ciento de batallas sin algún desastre” – Sun Tzu

Existe un cambio global en los vectores, patrones y capacidades de ataque:

- Los **vectores de ataque** son cada vez más dirigidos a la gente y menos a la tecnología
- Los **patrones de los ataques** cada vez parecen más de “comportamiento normal”
- Las vulneraciones pueden estar en modo inactivo, y activarse sólo de forma temporal, haciendo **más difícil su detección.**
- Las redes criminales, los gobiernos e incluso los grupos hacktivistas están desarrollando **redes de inteligencia** cada vez más robustas
- Las capacidades de ataque se vuelven difíciles de estimar al existir plataformas de **“crime-as-a-service”** en lugares como la DarkWeb
- Las vulneraciones a través de la **cadena de suministro** o de los **socios de negocio** se hacen cada vez más frecuentes

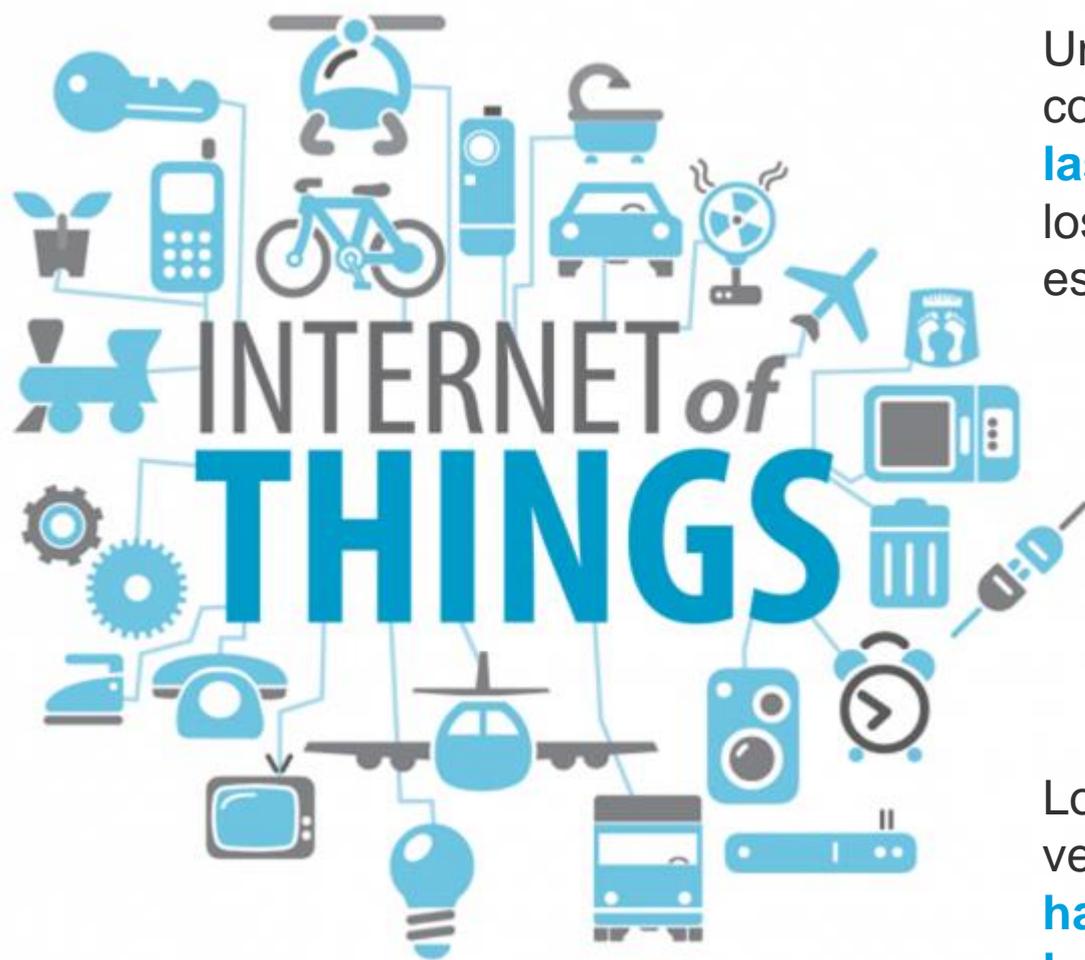


74% de las empresas esperan recibir un ciber ataque en el 2016.

Fuente: “State of Cybersecurity – Implications for 2016” de ISACA/RSA

Hacia dónde va el mundo en ciber seguridad

La mayor evolución en las redes aún está por venir



Uno de los principales cambios, viene con la inminente llegada del **Internet de las Cosas** a nuestra vida diaria; durante los próximos años (2016-2020) se espera:

- 4 billones de personas conectadas
- +25 millones de aplicaciones
- +50 trillones de GB de datos
- +25 billones de sistemas integrados e inteligentes

Los puntos de acceso a una red cada vez más grande y con menos fronteras, **harán crecer de forma exponencial los riesgos** de ciber seguridad.

Fuente: IDC

Hacia dónde va el mundo en ciber seguridad

“Locura es hacer lo mismo una vez tras otra y esperar resultados diferentes” – Albert Einstein



El rol del CISO requiere evolucionar a un enfoque balanceado, a través de cuatro rostros que habilitan a la función de seguridad de información para **maximizar el valor** entregado a la organización.

México

¿Qué es lo que viene para nuestro país?



¿Qué viene para nuestro país?

10 principales retos de ciber seguridad para las organizaciones

- La mayoría siguen careciendo de una **cultura/conciencia de riesgo** organizacional
- Aún existen muchos **sistemas legados** que no han sido asegurados / parchados
- Operan sin tener **políticas y estándares** de seguridad centralizados
- Enfoque ha sido, principalmente, en asegurar el perímetro – **defensa en profundidad**
- Pocos cuentan con **defensas antimalware**, y las que existen son insuficientes
- Las capacidades de **respuesta a incidentes** son deficientes, o no existen
- Con frecuencia se ignoran o no se consideran las **amenazas de internos**
- Alta dependencia/confianza en tecnología, sin considerar **procesos/procedimientos**
- No se consideran las amenazas/vulnerabilidades en la **cadena de suministro**



75% opinó que la mayor brecha en el personal de CS está en la falta de habilidades para entender el negocio

Fuente: “State of Cybersecurity – Implications for 2016” de ISACA/RSA

¿Qué viene para nuestro país?

Entorno regulatorio

Uno de los principales recursos utilizados las empresas para **impulsar la seguridad** es el cumplimiento regulatorio, el cual ha sido parte de la agenda del sector financiero desde hace décadas (ej. CUB), sin embargo, el resto de los sectores de industria se han visto incluidos en otras regulaciones. Algunos de los **principales marcos** que las empresas deben considerar:

- Ley Federal del Trabajo (retención de evidencia electrónica)
- LFPDPPP (medidas técnicas, físicas y administrativas)
- LFPIORPI (integridad de información)
- RSIM / PCI-DSS (seguridad en sistemas de pago)

De forma reciente, se publicó la **nueva regulación para el sector bancario**, la cual establece un marco normativo para el manejo de transferencias en dólares y los requisitos de seguridad y gestión de riesgo que se deben atender en el sistema correspondiente (SPID).

Adicionalmente, se espera que el ámbito regulatorio se siga fortaleciendo en todas las industrias, lo cual es parte de la estrategia nacional del gobierno federal sobre la **transformación digital**.

¿Qué viene para nuestro país?

La profesionalización en seguridad de información

La **falta de personal calificado** no será resuelta de forma rápida, sin embargo, ya hay universidades que están desarrollando profesionistas a nivel diplomado, licenciatura y maestría, lo cual aportará a las empresas recursos con la **formación básica** para desarrollar las funciones.

The collage features three screenshots of the UANL website and a vertical poster. The top-left screenshot shows the 'Licenciaturas' page for 'Seguridad en T.I.' with a keyboard image and an objective to form professionals in IT security. The top-right screenshot shows the 'Maestrías' page for 'Ing. en Seguridad de la Información'. The bottom-right screenshot shows a 'Becas' poster for the 'Programa de Becas de Formación en Tecnologías de Información y Comunicación' for 'Seguridad informática', with a start date of August 8, 2016, and a document delivery period from February 26 to May 20. The poster also includes contact information for DG TIC and the website www.tic.unam.mx.



28%

28% de las empresas tardan 6 o más meses en cubrir una posición de seguridad de información

¿Qué viene para nuestro país?

La certificación “no técnica”, orientada al proceso

Adicionalmente, existen **asociaciones profesionales** como ISACA que han visto de forma clara las tendencias y necesidades actuales, tales como las siguientes:

- Falta de profesionales capacitados
- Falta de certificaciones “no técnicas” para formar al personal.

Con base en lo anterior, desarrollaron un programa específico para el sector de la ciber seguridad (CSX), volviéndose parte central de su estrategia.



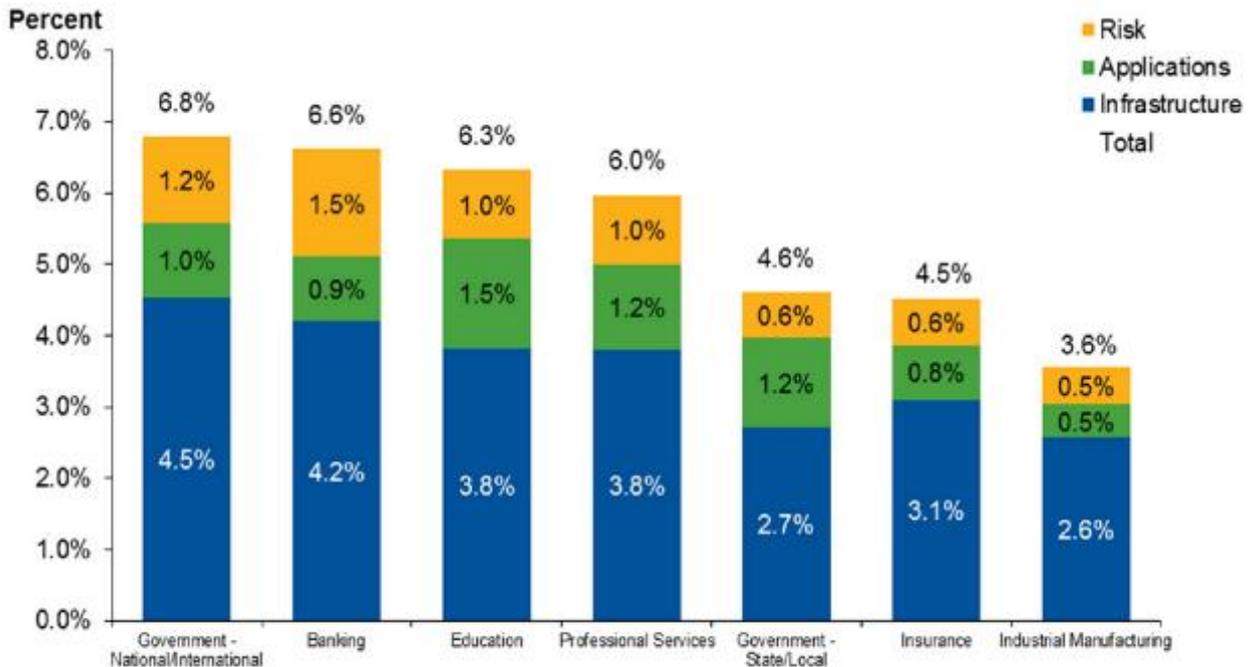
¿Qué viene para nuestro país?

El gasto en seguridad seguirá creciendo

Año con año, el **gasto en seguridad de información** ha seguido aumentando, lo cual se hace aún más complejo, si consideramos los factores económicos en el país.

Una buena práctica es realizar comparativos (**benchmarks**) de acuerdo a factores como:

- Tipo de industria
- Tamaño de la organización
- Cantidad de personal (FTE's)



Source: Gartner IT Key Metrics Data (December 2015)

El gráfico en esta página muestra el gasto en seguridad de información como un porcentaje del gasto total en el área de TI.

¿Qué viene para nuestro país?

El apoyo de la Alta Dirección será cada vez más crítico para la CS



Un programa de ciber seguridad efectivo requiere **compromiso continuo y proactivo** de la Alta Dirección

¿Qué viene para nuestro país?

“Si fallas al prepararte, te preparas para fallar” – Benjamin Franklin

Las organizaciones con **programas maduros** de ciber seguridad están realizando inversiones con base en la identificación oportuna y el reporte adecuado de los riesgos a los niveles ejecutivos / Alta Dirección, de acuerdo a lo siguiente:

- Cambiando el enfoque reactivo por un **enfoque proactivo**
- Reforzando los fundamentos de **gente y procesos** (no sólo tecnología)
- Ampliando las capacidades de **ciber inteligencia** para anticipar los vectores de ataque e identificar las vulneraciones de forma eficaz
- Reportando los riesgos identificados a los niveles directivos **con base en números...** entiéndase, dinero (ej. Cyber VaR)
- Extendiendo sus programas de ciber seguridad para llegar a toda su **cadena de suministro y socios de negocios**
- Integrando capacidades extendidas a través de servicios de tipo **“Security-as-a-Service”**
- Buscando todo el tiempo contestar una sola pregunta: **¿estamos vulnerados?**

Preguntas



¡Gracias!

Sergio Solís
sesolis@deloittemx.com
Tel. (81) 8152-7825



Deloitte se refiere a Deloitte Touche Tohmatsu Limited, sociedad privada de responsabilidad limitada en el Reino Unido, y a su red de firmas miembro, cada una de ellas como una entidad legal única e independiente. Conozca en www.deloitte.com/mx/conozcanos la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios profesionales de auditoría, impuestos y servicios legales, consultoría y asesoría, a clientes públicos y privados de diversas industrias. Con una red global de firmas miembro en más de 150 países, Deloitte brinda capacidades de clase mundial y servicio de alta calidad a sus clientes, aportando la experiencia necesaria para hacer frente a los retos más complejos de negocios. Los más de 225,000 profesionales de Deloitte están comprometidos a lograr impactos significativos.

Tal y como se usa en este documento, “Deloitte” significa Galaz, Yamazaki, Ruiz Urquiza, S.C., la cual tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría, consultoría fiscal, asesoría y otros servicios profesionales en México, bajo el nombre de “Deloitte”.

Esta publicación sólo contiene información general y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro, ni ninguna de sus respectivas afiliadas (en conjunto la “Red Deloitte”), presta asesoría o servicios por medio de esta publicación. Antes de tomar cualquier decisión o medida que pueda afectar sus finanzas o negocio, debe consultar a un asesor profesional calificado. Ninguna entidad de la Red Deloitte, será responsable de pérdidas que pudiera sufrir cualquier persona o entidad que consulte esta publicación.