Deloitte.

Panorama de Ciber Seguridad en México para 2016-2017

Sergio Solís
Gerente Senior
Cyber Risk Services

Agenda

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.**

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 Usuari Servicios Financiero.

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

Me gusta 225

Compartir Email G+1 34

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.


EXPANSIÓN

EN ALIANZA CON CNN

DINERO

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

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.

Un vistazo a los eventos relevantes del 2015 en el mundo

Vulneraciones permiten visualizar alcance de riesgos

- 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.

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

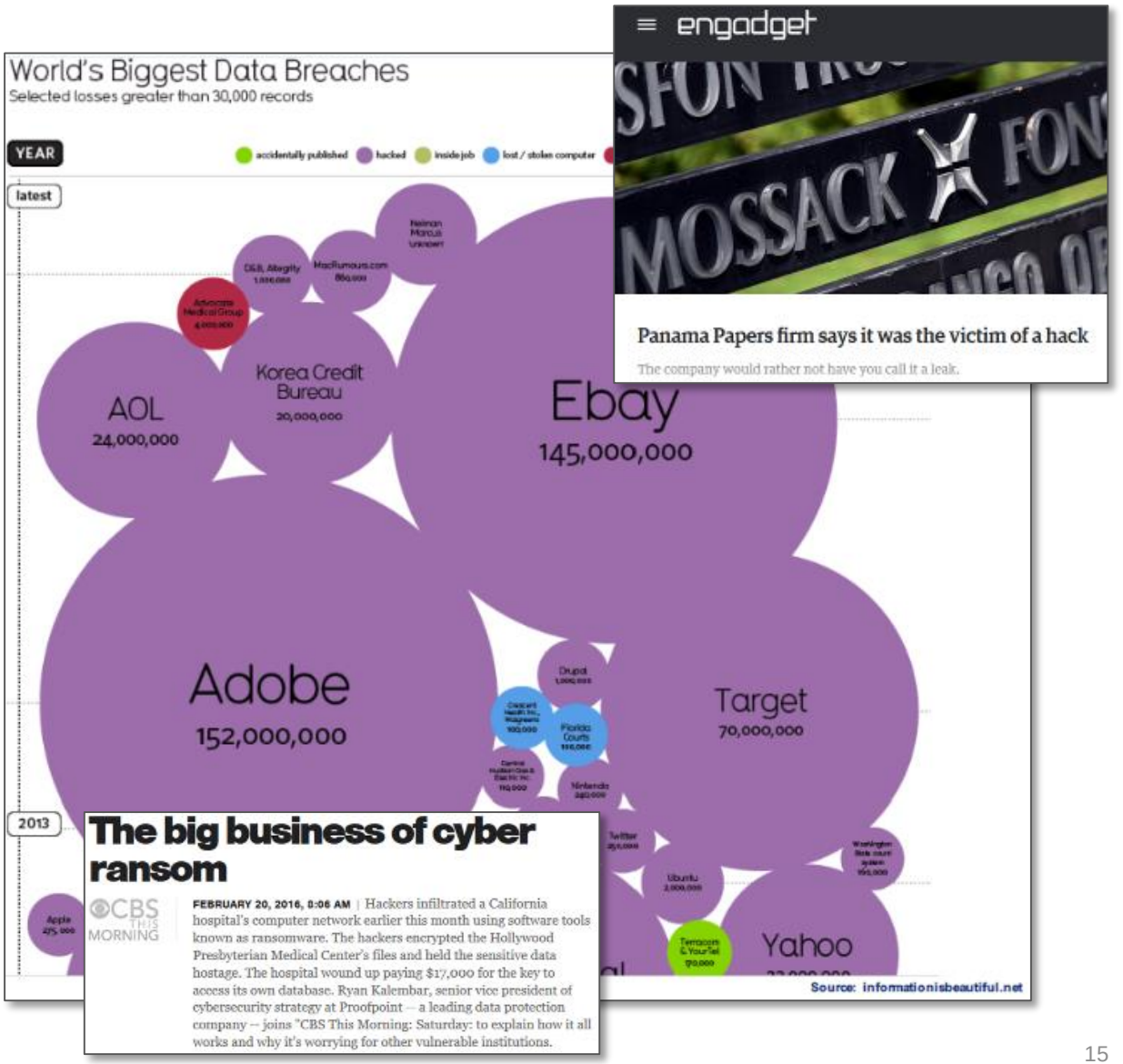
México es el 2º país con mayor actividad de ciber ataques en América Latina* – aunque mayormente no es el generador de los mismos.

Fuente: Nexusguard

Hacia dónde va el mundo en ciber seguridad

La información se ha convertido en el principal objetivo de los atacantes

- Aun y cuando ninguna organización está exenta de tal riesgo, **el robo de información seguirá creciendo** en sectores como el detallista y el financiero, afectando a millones de usuarios en el mundo.
- Las extorsiones relacionadas pueden llegar a tener grandes impactos, tales como los generados por el **ciber secuestro de datos y la revelación de información confidencial.**



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.

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:

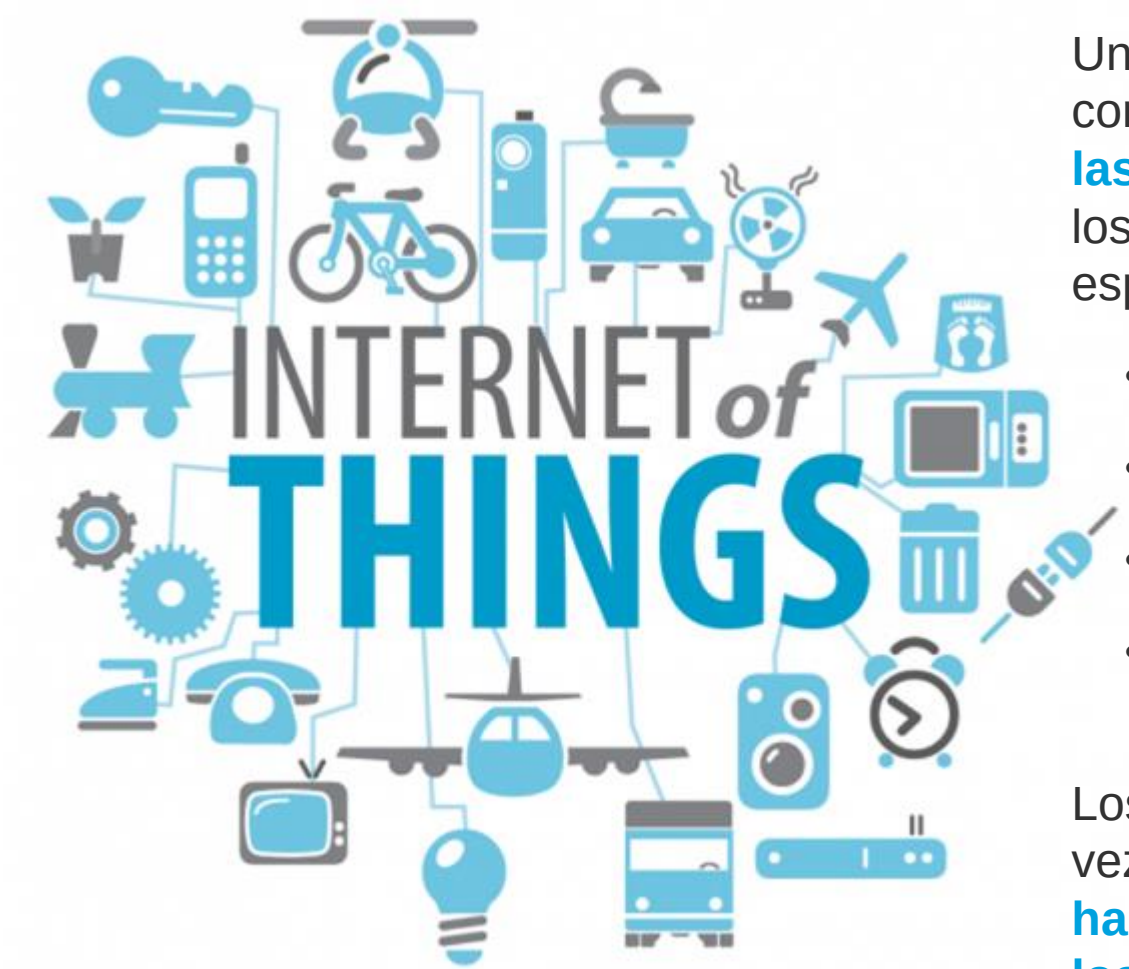
- Los **vectores de ataque** son cada vez más dirigidos a la gente y menos a la tecnología
- Los **patrones de los ataques** cada vez parecen más de “comportamiento normal”
- Las vulneraciones pueden estar en modo inactivo, y activarse sólo de forma temporal, haciendo **más difícil su detección.**
- 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.

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

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

¿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.

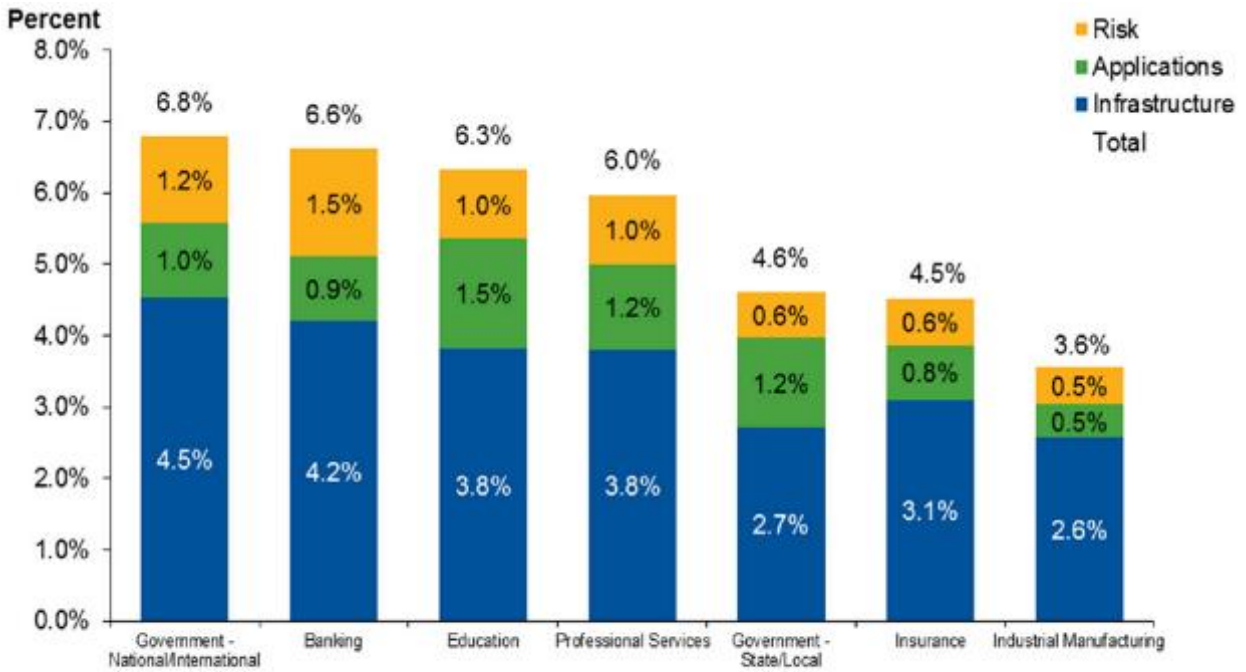
¿Qué viene para nuestro país?

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

CS requiere **'tone at the top'** incluyendo conciencia y responsabilidad

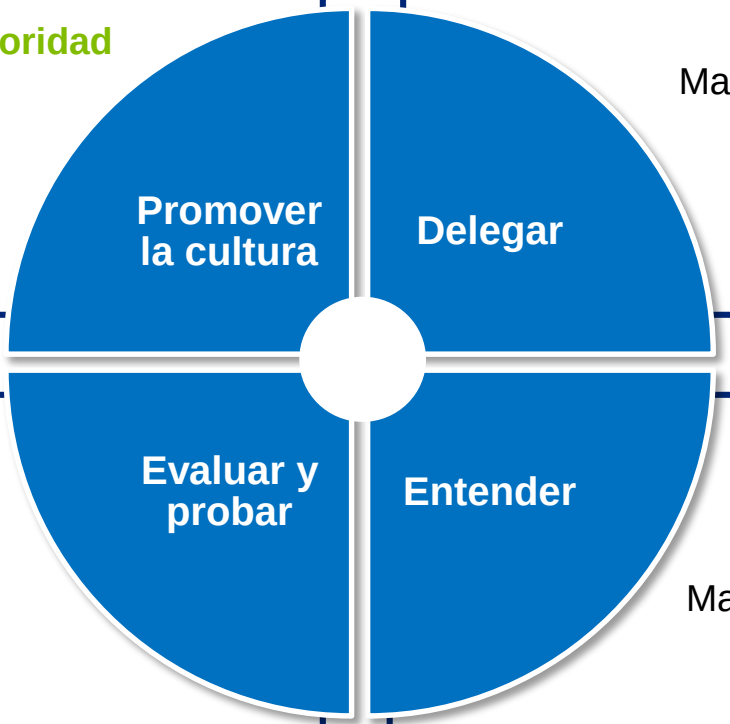
Importancia de CS como **prioridad** organizacional

Claro **gobierno**, políticas y monitoreo

Asignación clara de **responsabilidades y rendición de cuentas** para programa de CS

Manejo de las **expectativas** y la rendición de cuentas

Adecuación de recursos, financiamiento, y enfoque



Reporte de Incidentes y riesgos críticos

Resiliencia Organizacional

Políticas de CS de alto nivel

Evaluación independiente de programas y controles de CS

Revisión periódica de riesgos de CS

Cumplimiento **Regulatorio**

Manejo adecuado de **terceros**

Auditoría y pruebas de CS

Estructura de métricas y reportes para **filtrar riesgos críticos**

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

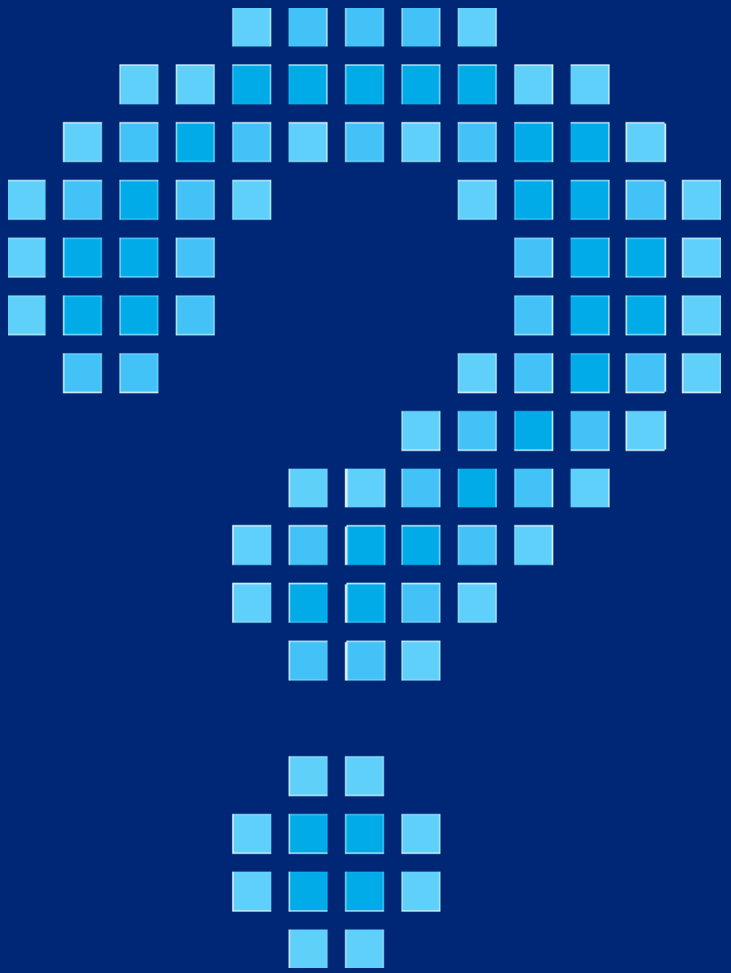
¿Qué viene para nuestro país?

“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.