

Deloitte.

Information •
Security
Community

Lucio Adame / Henoch Barrera
4 de diciembre 2014



Contenido

Ciber Inteligencia	4
<i>Honeynet</i>	8
Proyecto Munin	10



Nuevos horizontes en la generación de ciber inteligencia



Entendiendo una necesidad: Ciber Inteligencia

La administración tradicional de seguridad, sin el entendimiento adecuado de los riesgos a los que la organización se encuentra expuesta, no es suficiente para protegernos.



Entendiendo una necesidad: Ciber Inteligencia



**LA SEGURIDAD
ES UN ASUNTO
DEL NEGOCIO**

**INVERSIÓN
INTELIGENTE**



CIBER INTELIGENCIA ¿LA NECESITO?

El conocimiento y estudio de nuestros ciber adversarios se ha vuelto fundamental para el direccionamiento de nuestros esfuerzos y capacidades de defensa contra sus ataques.

**NUESTROS
ATACANTES
GENERAN
INTELIGENCIA**



Un asunto de negocio

Determinar proactivamente las capacidades, psicología y motivaciones de nuestros atacantes, permitirá a nuestra estrategia de riesgos y seguridad, prevenir y anticipar ataques reales en su infraestructura; y por lo tanto diseñar y mejorar sus sistemas de detección y respuesta adecuadamente.



Un asunto de negocio

**UN RETO TÉCNICO,
PERO TAMBIÉN DE NEGOCIO**

1



**EL CONOCIMIENTO DEL
NEGOCIO ES VITAL**

2



**NECESITAMOS EL
PATROCINIO DEL “C-CHAIR”**

3



Una inversión inteligente

Los productos de seguridad estándar basados en firmas, mantienen un enfoque genérico de solución que no es capaz de detener ataques de naturaleza dirigida.



Una inversión inteligente

01/ EVITEMOS UNA FALSA SENSACIÓN DE SEGURIDAD



Invertir únicamente en dispositivos de seguridad tradicionales puede darnos una falsa sensación de seguridad.

02/ ENFOCANDO NUESTROS ESFUERZOS



La generación de ciber inteligencia no significa gastar gran cantidad de recursos, sino invertir estratégicamente.

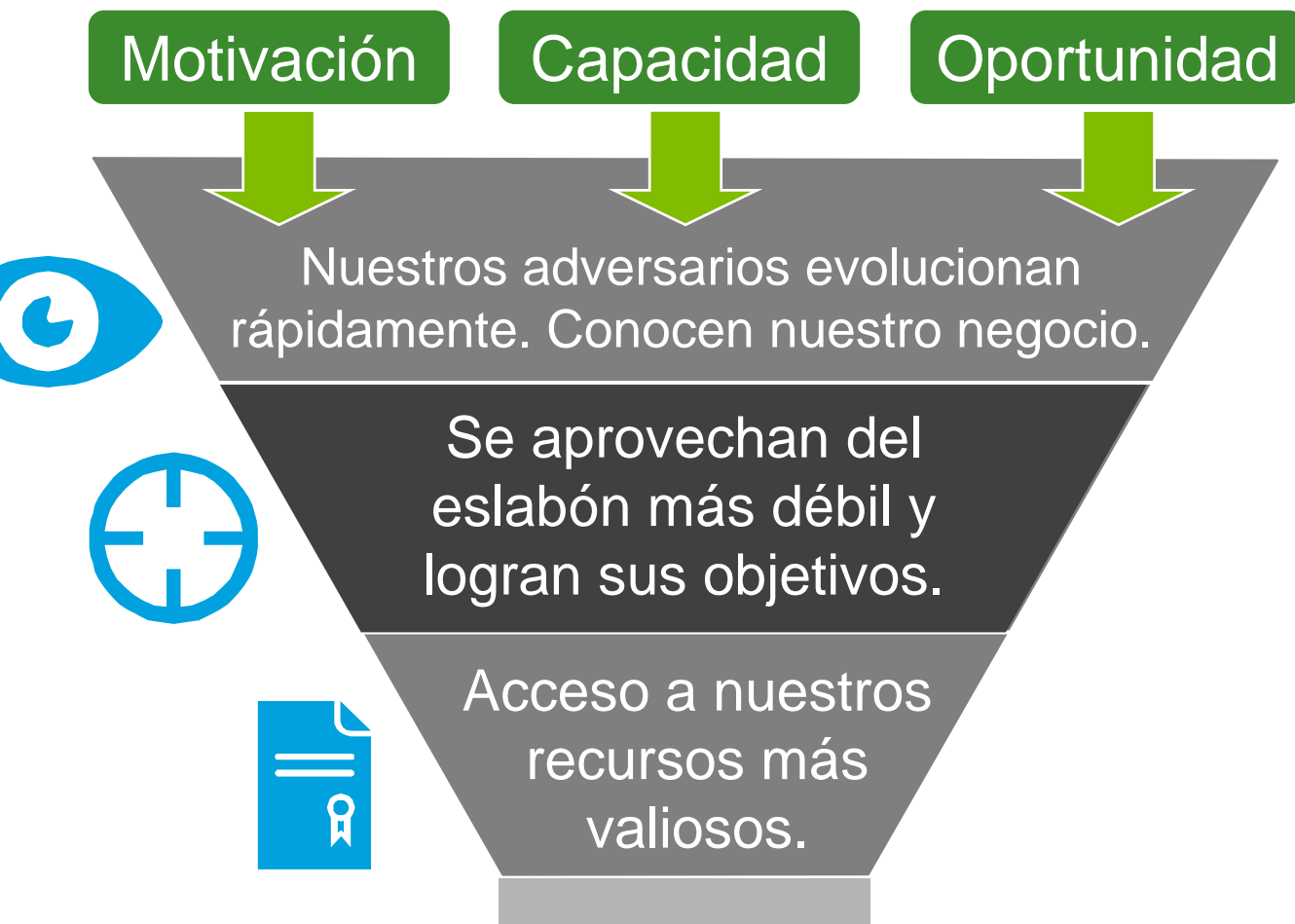
El costo del ciber crimen en México se estima en .17% del PIB (\$28 mil millones de pesos anualizados); sin embargo sólo el 30% de las compañías está dispuesta a invertir en ciber seguridad.

Conociendo a nuestros atacantes antes de que nos conozcan.

Actualmente los ciber ataques más costosos son minuciosamente planeados y dirigidos a compañías altamente perfiladas. Identificar patrones de comportamiento en nuestros sistemas podría indicarnos si somos o hemos sido objetivo de un ataque.



Conociendo a nuestros atacantes antes de que nos conozcan.



Las ciber amenazas pueden atacarnos en cualquier momento y desde cualquier lugar.

Pero estos ataques pueden ser identificados y prevenidos incluso antes de que se concreten.

Mientras que nuestra capacidad de detección disminuye ante lo que desconocemos.



Honeynet

Un punto de partida



Recolectar alertas de seguridad y *logs* es el inicio, obtener información relevante de ellos es un paso, transformar datos crudos en información significativa es un arte; un arte necesario para afrontar nuestras amenazas actuales.

Honeynet

Un punto de partida



HONEYNET

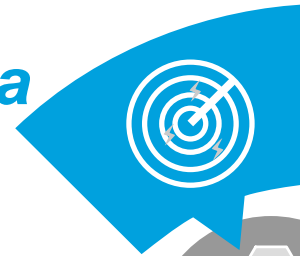
Es un recurso de seguridad cuyo valor reside en “**la información de ciber inteligencia que genera**”.

Es una red corporativa vulnerable, que emula o simula servicios críticos del negocio.

Pueden ser **el punto inicial para generar ciber inteligencia**.

Se publica como la “carnada” para los ciber atacantes, buscando ser:

Sondeada



Comprometida



Atacada



Honeynet

Beneficios de una Honeynet

Todos los servicios que se publican en internet son un objetivo, pero una *honeynet* nos permite saber cuándo es que nos convertimos en una víctima.

Beneficios de una Honeynet

La inclusión de una *honeynet* tiene amplios beneficios, destacando:

- Detección y alerta temprana
- Identificación de tendencias de ataque a nuestro negocio
- Predicción y prevención de ataques a la red corporativa real
- Conocimiento de nuestros atacantes
- Transferencia de conocimiento



Recibir información durante los **primeros 60 segundos** de un ataque, puede disminuir hasta en **40%** el impacto de un compromiso.

Proyecto “Munin”

El aprendizaje está basado en la experiencia, obtener información de compromisos reales es el camino para generar conocimiento de nuestros atacantes y nuestras debilidades.

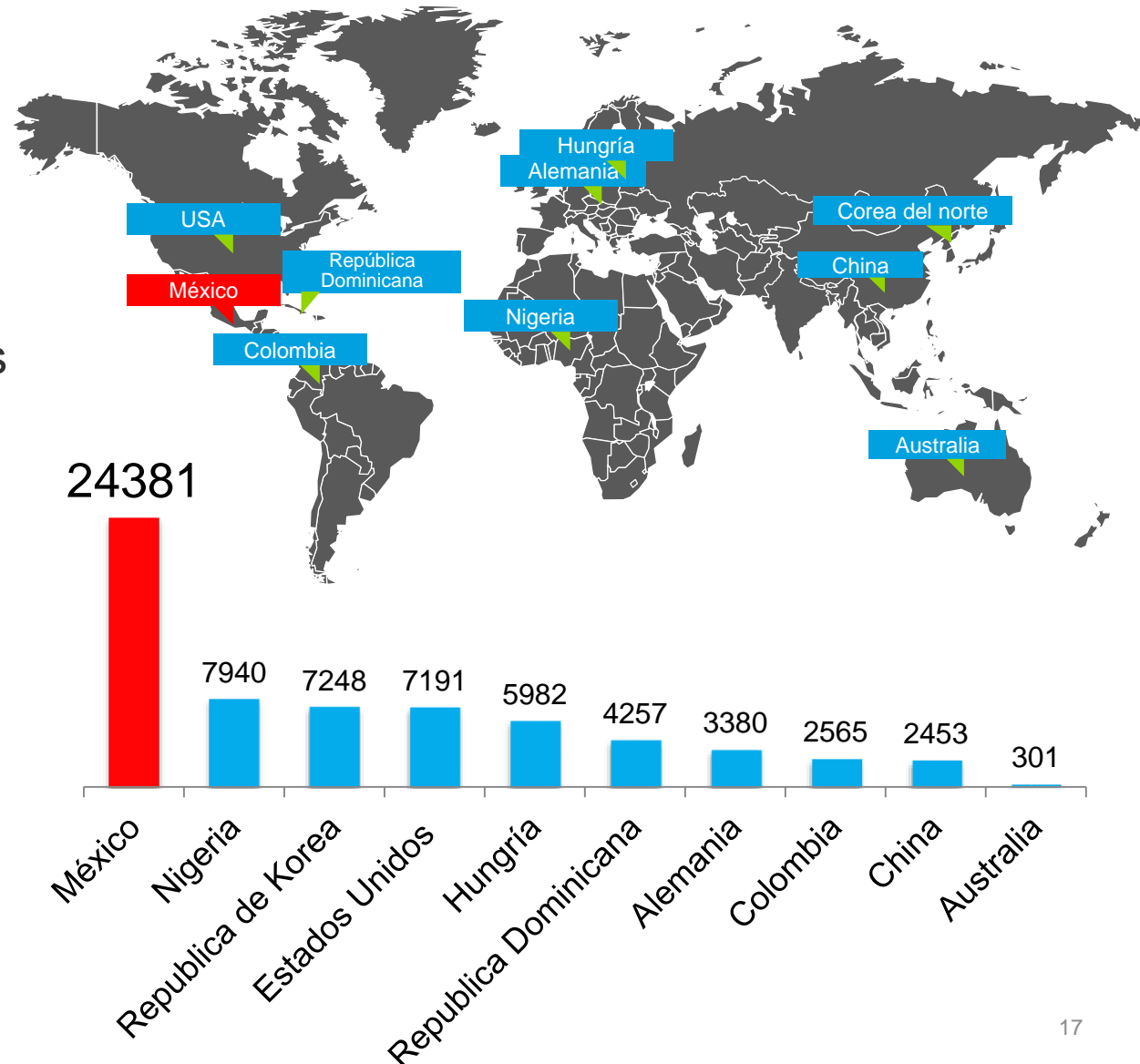


Proyecto “Munin”

En mayo de 2014, Deloitte México inició en operación la Honeynet – “Munin”.

- Se simula una compañía ficticia en México con sistemas operativos, servicios y un sitio *web* vulnerables
- Facilita la investigación de: Generación de *exploits* y análisis de *malware*
- Se identifican tendencias de ataques
- Se graba en tiempo de real cada ataque

Países con mayor número de ataques realizados

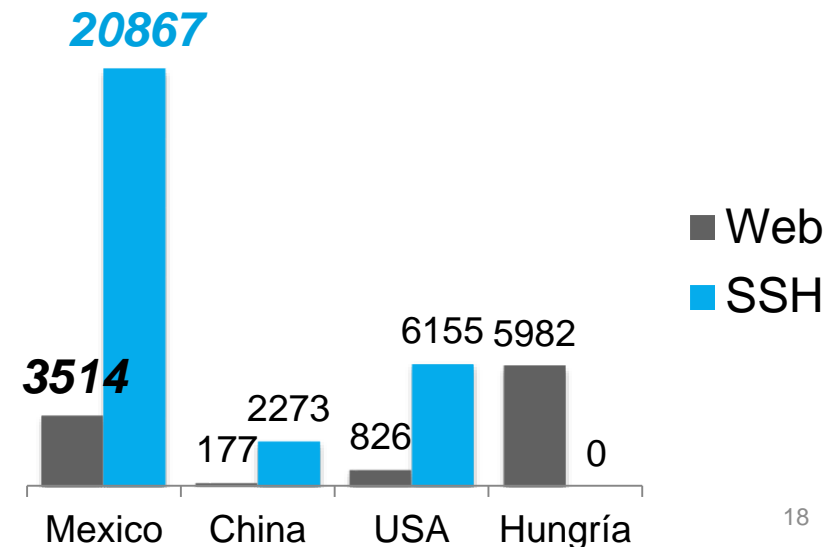
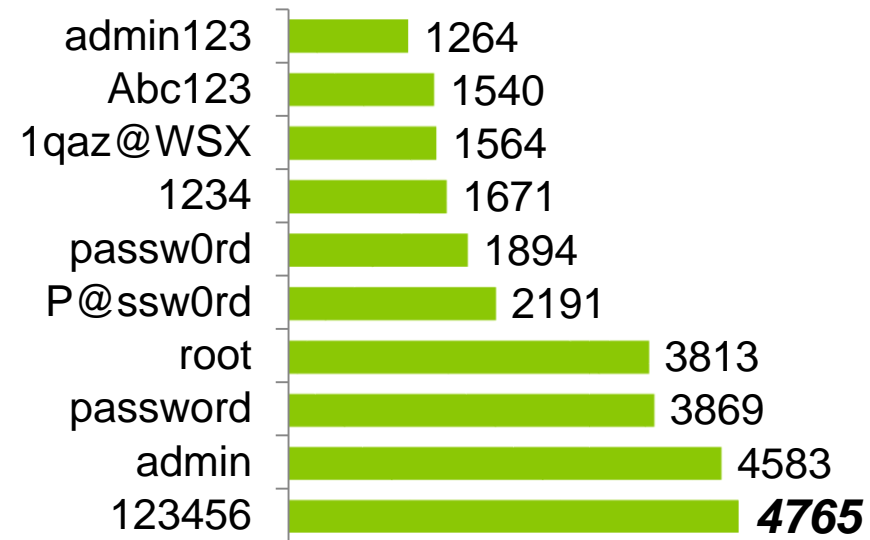


Lecciones aprendidas

“Un general sabio se ocupa de abastecerse del enemigo” – Sun Tzu

- Se han recibido más de 130,000 ataques (35,000 exitosos)
- Los tipos de ataque y motivaciones varían dependiendo de cada país:
 - México: SSH y Páginas *web*
 - China: SSH
 - USA: SSH y SMB
- Contraseñas débiles y/o por defecto es aún uno de los mayores vectores de ataque
- Se han obtenido 50 archivos maliciosos consideradas piezas de malware, **ninguno ha sido detectado como *malware* por firma de antivirus**
- Los países con mayor número de intrusiones exitosas:
 - China
 - USA
 - Hungría
 - México

Top 10 contraseñas

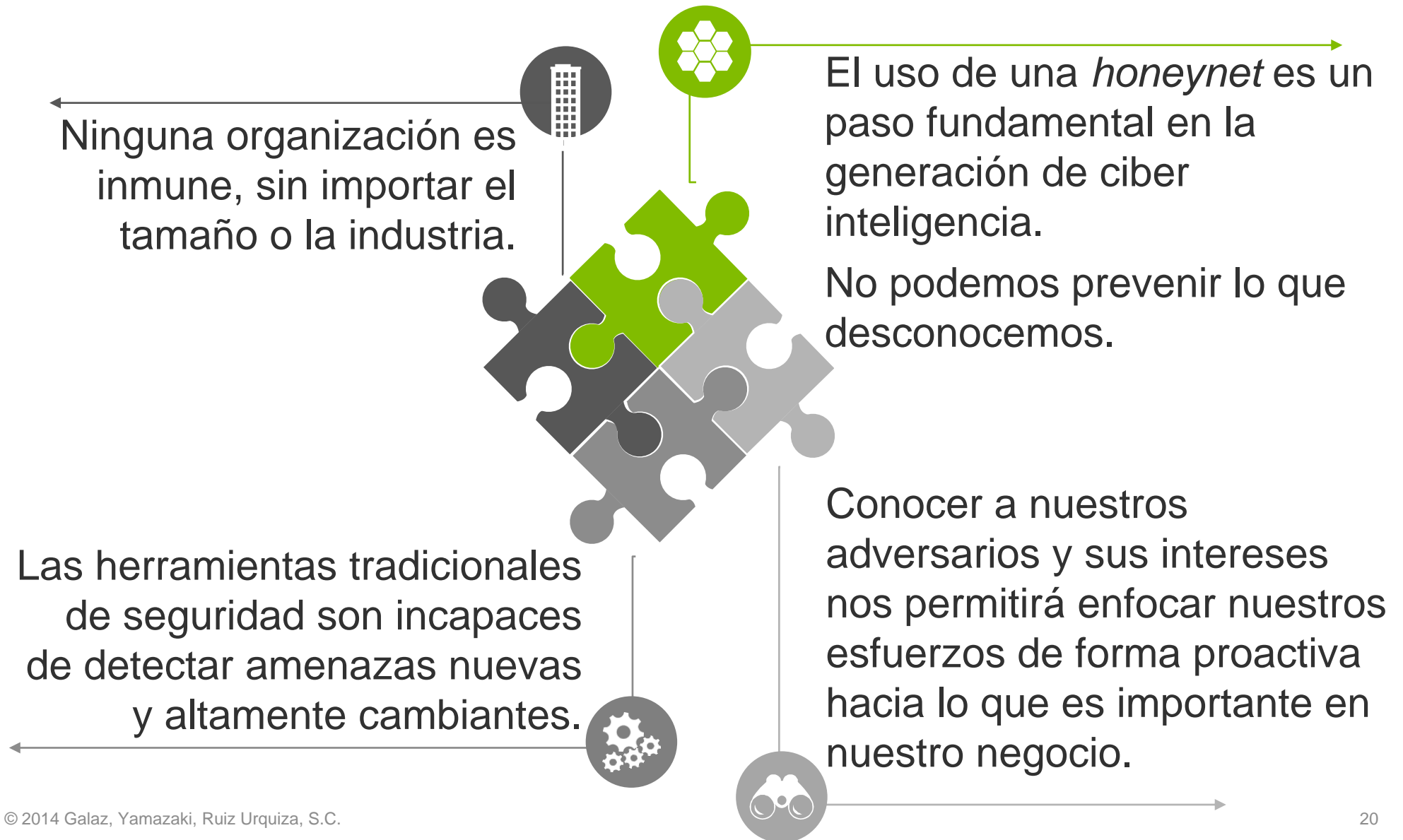


Lecciones aprendidas

No podemos evitar ser víctimas de un ciber ataque y los mecanismos de defensa no pueden prevenir todos los ataques que recibimos, debemos estar listos para ser comprometidos y tener capacidades de detección y de respuesta oportunas.



Lecciones aprendidas





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, consultoría y asesoría financiera, 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 los negocios. Cuenta con más de 210,000 profesionales, todos comprometidos a ser el modelo de excelencia.

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 financiera 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.