

---

## II Reunión de Ciberseguridad -2a Parte “La concientización en materia de Ciberseguridad”

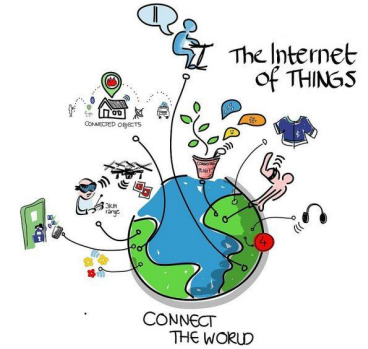
# Transferencia de Riesgos de Ciberseguridad

Dra. Erika Mata Sánchez, CISM, CISA, CISSP  
[erika.mata@gmail.com](mailto:erika.mata@gmail.com)

- ❖ Introducción
- ❖ Contexto de la Seguridad
- ❖ Transfiriendo riesgos - Ciber-Seguros
- ❖ Algunos pensamientos

# Introducción

- Vivimos una nueva ERA de conectividad, en donde digital y lo físico se combinan muy rápidamente



- Transformación Digital - nuevos modelos de negocio y ecosistemas
  - Cloud, mobile, SaaS y DevOps
  - Dispositivos físicos y sistemas de todos tipos están conectados a la red, programables, y crean nuevas oportunidades
  - En 2019 se espera más de 9 billones de dispositivos IoT
  - 90% de las organizaciones tienen corriendo alguna aplicación en la nube
- Esta transformación digital es también la nueva superficie que defender ... y está explotando ??

# Introducción

- 2016 - grandes momentos en el mundo de la ciberseguridad:
  - Distributed denial of service (DDoS) attack - DYN 1.2Tb p/seg
  - Phishing attack on a United States presidential candidate's campaign,
  - ransomware attacks (4000 ataques diarios según US-CERT)
  
- 2017 - aún no termina
  - nation-state cyber attacks
  - ransomware - RaaS, ransomworms
  - DDoS attacks - DDoS-for-hire tools and services.
  - Internet of Things
  - social engineering & human error
  - Reverse Deception Tactics – cybercriminal use
  - Sophisticated Phishing Campaigns
  - Strategic Use of Information Operations – espionage and disruption activity
  - Alternative



Crypto-Currencies

# Introducción

- El costo de no estar preparado va en aumento y las empresas en general están considerando mitigar riesgos.
- La industria de seguros puede jugar un papel importante en la administración de Ciber-riesgos



## RETO

- entendimiento de amenazas y cuantificación de daños
- rango y diversidad de ciber-amenazas
- costo de ciber-ataques y brechas de datos

## Contexto de la Seguridad y algunos datos

### XIV Encuesta Global de Seguridad de la Información - E&Y 2017

63% de los encuestados en México y el 72% a nivel global observan un **aumento en el nivel de riesgo** debido al aumento de amenazas externas.

- Sólo una cuarta parte de los encuestados en México (26%) y el 68% a nivel global han actualizado su **estrategia de seguridad de la información** en los últimos 12 meses para responder a dicho aumento en las amenazas.

- ❑ El **86%** de los directivos consultados afirma que los **mecanismos de seguridad de sus empresas no cumplen con los requisitos necesarios**.

Cerca del **50%** de las organizaciones han identificado mayores **amenazas dentro de sus propias organizaciones**.

Principales vulnerabilidades detectadas:

- Posibles descuidos de los empleados (**55%**),
- Acceso sin autorización a datos e información (**54%**).

Las mayores amenazas para las empresas encuestadas son:

- ataques como el malware o software malicioso (**52%**),
- el phishing y suplantación de identidad (**51%**).

## Contexto de la Seguridad y algunos datos

El Estudio de Seguridad de la Información en México 2017 de PWC indica que la principal fuente de incidentes de seguridad es “interno”.



A nivel global -

**En México**  
**44%**

atribuye estos incidentes a ex empleados.



**En México**  
**31%**  
 de las organizaciones creen que los incidentes de seguridad son causados por sus competidores.

87% de empresas en México que participaron en el estudio han tenido incidentes de seguridad.

## Contexto de la Seguridad y algunos datos

- México fue en 2016 el segundo país más atacado de América Latina, con un impacto de 5,500 MDD. (125 mil MDD a nivel mundial)  
Fuente: Informe sobre Amenazas para la Seguridad en Internet de Symantec, 2016
- A mayo 2017, un informe de Kaspersky Lab indica que empresas en México pierden hasta 17 mdp por incidente de ciberseguridad

The screenshot shows the homepage of EL ECONOMISTA. The main navigation bar includes: DINERO, TUS FINANZAS, TERMÓMETRO, EMPRESAS, ESTADOS, TECNOLOGÍA, POLÍTICA, INTERNACIONAL, FONDOS, OPINIÓN. Below this is a secondary bar with: RIPE, DEPORTES, ARTE E IDEAS, RANKINGS, EL ECONOMISTA TV, MULTIMEDIA, EDICIÓN DIGITAL. The main content area features a grid of news items:

- SEP 27, 2017 | 00:18: Argentina descarta aumento en precio de combustibles
- SEP 26, 2017 | 19:02: EU impone arancel de 220% a aviones de Bombardier
- OCT 1, 2017 | 21:18: **México gana relevancia para Ecolab en Latam**
- SEP 27, 2017 | 10:41: Inventarios de crudo en EU caen por reinicio de refinarias: EIA
- SEP 26, 2017 | 00:40: Construirán casas con PET para damnificados

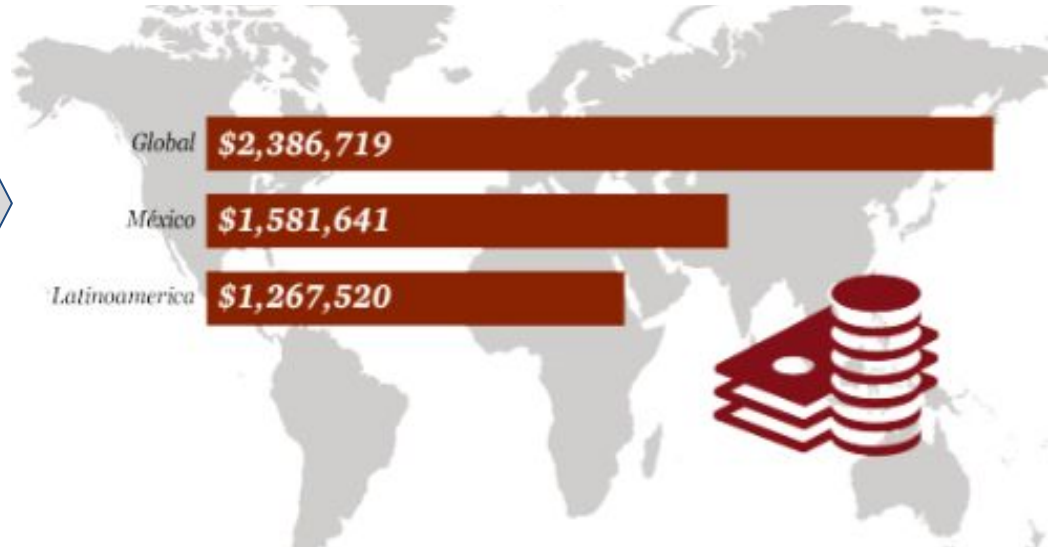
The featured article is titled "México es el quinto país con más ciberataques: Fortinet". The sub-headline reads: "México es el quinto país con más ciberataques en el mundo, reveló la empresa de seguridad Fortinet." The article is dated SEP 7, 2017 | 10:42. A "PUBLICIDAD" placeholder is visible on the right side of the page.



## Contexto de la Seguridad y algunos datos

	Global	Latinoamérica	México
Presupuesto de seguridad de la información para 2016?	5,060	4,772	5,020

El costo promedio de un incidente de seguridad a nivel mundial es el **32%** del presupuesto de seguridad de la información



## Contexto de la Seguridad y algunos datos

- Desde 2012, la inversión media que las empresas dedican a seguridad de la información en el mundo ha pasado de 2,8 a 5,1 millones de dólares y permaneció estable en 2016.



**59% de directivos de empresas a nivel mundial indica que la digitalización es el factor impulsor de la inversión en Seguridad**

Fuente: Encuesta Mundial sobre el Estado de la Seguridad de la Información 2017,

## Contexto de la Seguridad y algunos datos

### • Tendencias en Seguridad y Privacidad

Incremento en la colaboración entre áreas de Negocio, Seguridad, TI, y Digital - **57 %**.

Arquitectura y protección del negocio Digital - **46%**.

Nuevas necesidades en materia de seguridad en los negocios (Inteligencia ante las amenazas) - **46%**

Seguridad del Internet de las Cosas (IoT) - **46%**.

Biometría y autenticación avanzada - **43%**.

**74%**

Reducir el riesgo de incidentes de privacidad

**60%**

Cumplimiento con las regulaciones de privacidad

**56%**

Mejorar la confianza en la marca

Fuente: Encuesta Mundial sobre el Estado de la Seguridad de la Información 2017, PWC

# ¿Por qué continúan los incidentes de seguridad?

y en aumento



# Transfiriendo riesgo

- Definiciones diversas sobre mismos conceptos

- Ciber-riesgo
- Ciber-ataque
- Ciber-exposición
- Ciber-seguro



- ISO/IEC AWI 27102 - Information technology -- Security techniques -- Information security management guidelines for cyber insurance
- FFIEC
- CRO Forum
- Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions
- International Association of Insurance Supervisors - IAIS

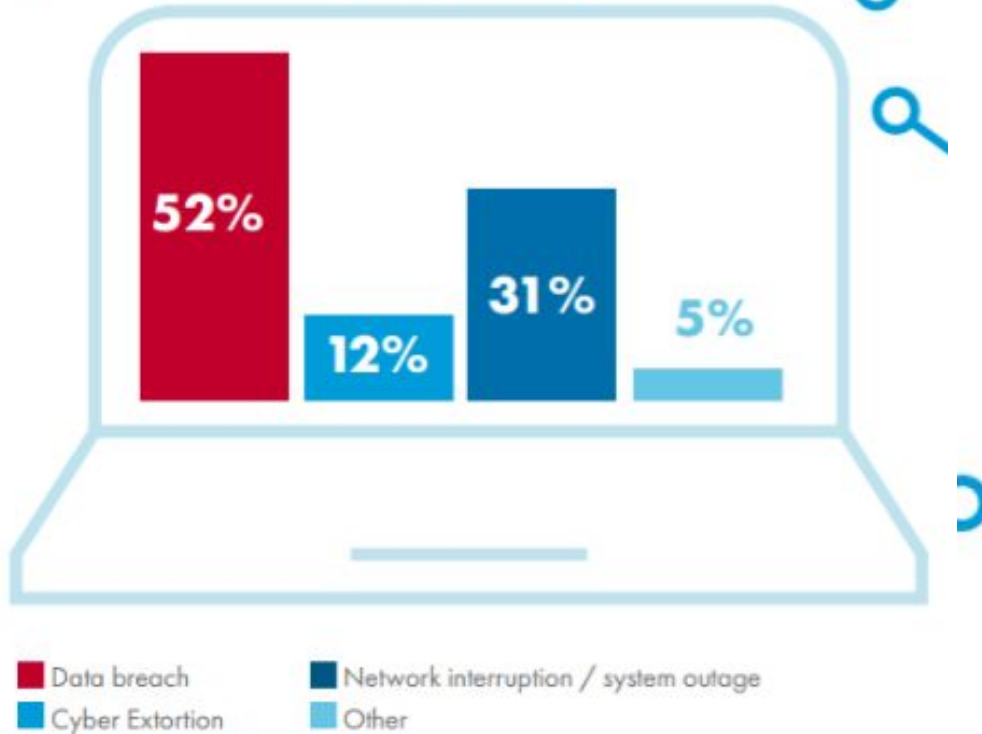
## Transfiriendo riesgo

- **Cyber-seguro** - Transferencia de riesgo financiero asociado con incidentes en la red, computadoras, sistemas a un tercero (aseguradora, proveedor de servicios - ICT, seguridad)



# Transfiriendo riesgo

Which cyber risk scenarios present the greatest risk to buyers/your organisation?



Which element of cyber insurance is most important to buyers/your organisation?

**64%**

**Post-loss incident management services**

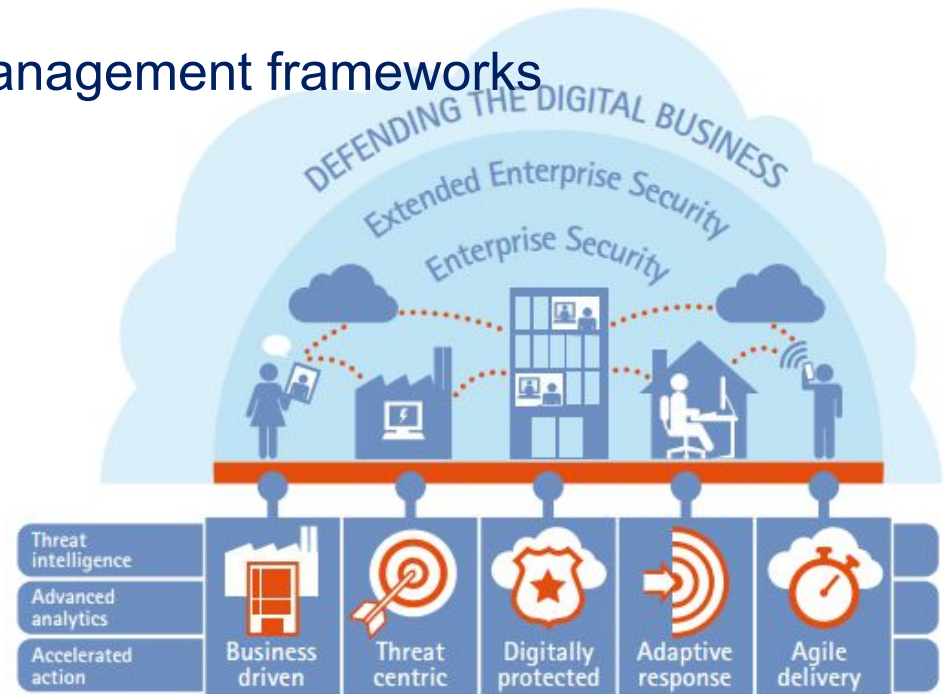
27% Insurance indemnity payments

8% Pre-loss risk mitigation services

AIG UK - 2015

# Transfiriendo riesgo

- Cuándo transiero riesgo?
  - Paso natural después de una administración de riesgos
  - transferencia de algunos riesgos residuales
  - **Proceso de Respuesta a incidentes**
  - **Foco en procesos y nivel de exposición de la empresa**
- Implantación de Cyber-risk Management frameworks
  - NIST CSF
  - ISO 27000 (familia)
  - etc..





- **Ciber-Seguros**
  - Modelos de leyes modernas de lado de reguladores de seguros
    - insurance information and privacy protection
    - privacy of consumer and health information
    - data breach notification
    - information sharing program: guiding principles, FS-ISAC. real time information of potential breaches or breaches in the sector
  
- **Metricas? - coberturas?**
  
- **Costo de Ciber- seguridad → prevención, no después de ataques**

# Transfiriendo riesgo

- Grandes retos - preguntas!!
  - Who's really responsible for new products and innovation that are vulnerable?
    - sw companies, IoT, mobile tech, ..
- No existe una solución real o respuesta ... pero SI un diálogo en el cómo se tratarán los issues y retos de amenazas e impactos que hoy no se miden realmente



# Recomendaciones

---

- Tener un Plan de Respuesta a incidentes de seguridad robusto, maduro y probado es un elemento clave en la mitigación de exposición y grandes impactos a la organización
- Administración efectiva de riesgos de seguridad
- Seguridad es un requerimiento de negocio y los procesos asociados se vuelven cada vez más parte del corazón del negocio
- Un modelos de Seguridad Inteligente pareciera el adecuado integrando la transformación digital y nuevos modelos de negocio

# Referencias

- Managing Cyber Risk and the Role of Insurance conference, Center for Strategic and International Studies (CSIS), September 10, 2015.
- Modeling Cyber-Insurance: Towards a unifying framework. Rainer Böhme and Galina Schwartz; Workshop on the Economics of Information Security (WEIS), Harvard, June 2010
- Cyber-insurance exposure data schema. AIG Cyber Insurance Seminar; Survey of 60 – 64 attendees. Banking Hall, November 2016.
- Issues paper on cyber risk to the insurance sector. Accenture Security Report Identifies Top Cyber Threats of 2017
- Un modelos de Seguridad Inteligente pareciera el adecuado integrando la transformación digital y nuevos modelos de negocio



# GRACIAS!

