
TS TeleSemana.com
Ciberseguridad y
Protección de Datos
No es sólo una obligación, es un posible negocio

Retos que enfrentan los operadores

- Económicos: cambio monetario, intereses, acceso a financiación
- Incremento en la competencia, otros operadores y nuevos jugadores digitales (OTTs)
- Mayor velocidad en la innovación de nuevas tecnologías, cambios en los ciclos de inversión
- Regulación y cambios en la legislación inesperados o situaciones políticas inestables, por ejemplo EU General Data Protection Regulation, GDPR (riesgos de subcontratar el guardado de datos)
- Transformación digital y reestructuración interna para hacerle frente

Retos que enfrentan los operadores

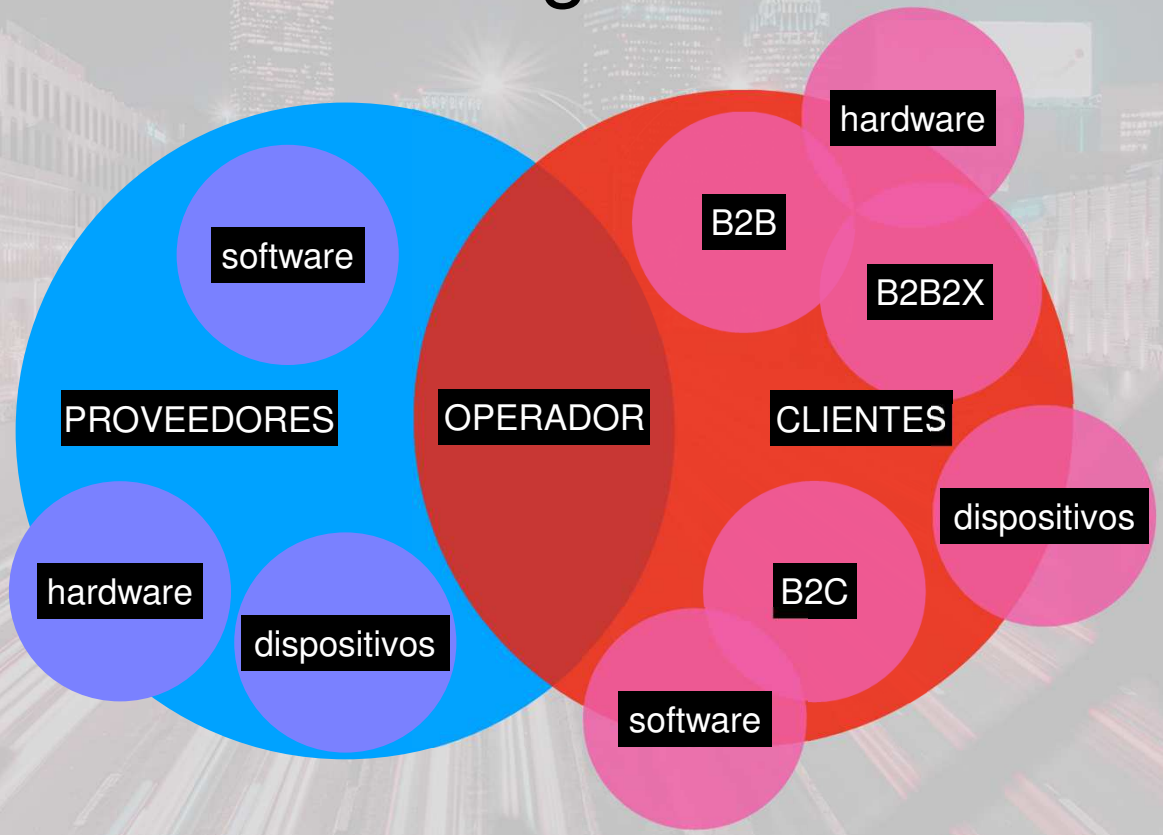
- Económicos: cambio monetario, intereses, acceso a financiación
- Incremento en la competencia, otros operad
  jugadores digitales (OTTs)
- Mayor vol

Cibercrimen, ciberataques, ciberseguridad y protección de los datos

- ión inesperados o situaciones
  jemplo EU General Data Protection
  R (riesgos de subcontratar el guardado de datos)
- Transformación digital y reestructuración interna para hacerla frente

¿Por qué aparece este nuevo riesgo?

En medio de la presión de la ciberseguridad



En medio de la presión de la dad

La mayor aportación del software: oportunidades y riesgos

- **PROS** - El software es el gran aliado de los operadores para su transformación digital: mayor innovación, escalabilidad, “menor costo”, agilidad, mejor respuesta a las necesidades del mercado

- **CONS-** Se incrementa la vulnerabilidad, Según una encuesta realizada 2018 en la comunidad DevSecOps por **Sonatype**, se produjo un incremento del 55% en agujeros de seguridad por culpa de vulnerabilidades del **código abierto**

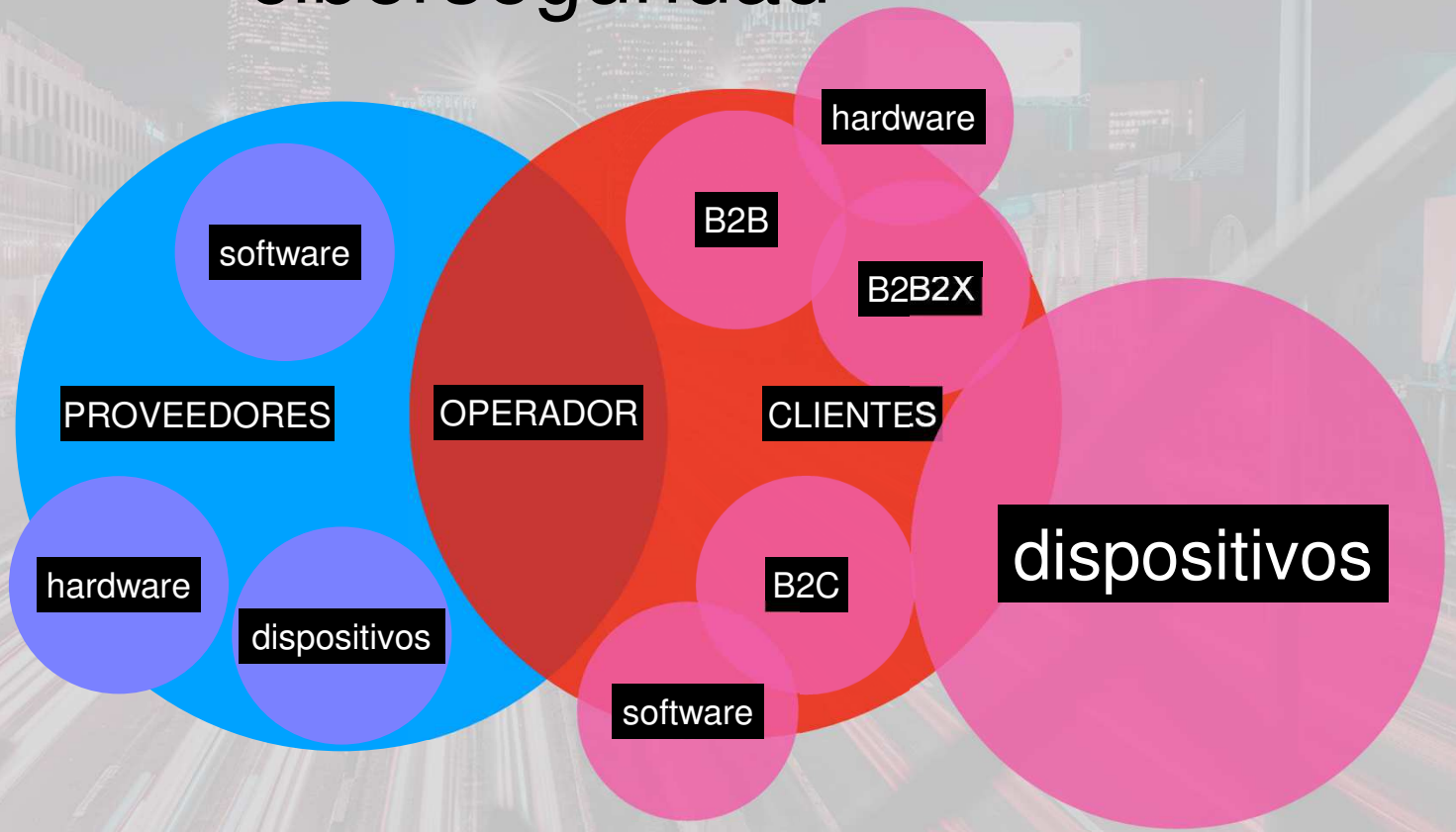
La mayor aportación del software: oportunidades y riesg

- **PROS** - El softwar
para su

EL CÓDIGO ABIERTO VA A SER DOMINANTE EN EL MUNDO DEL SOFTWARE, TAMBIÉN EN TELECOMUNICACIONES

DevSecOps por
iento del 55% en agujeros
pa de vulnerabilidades del **código**

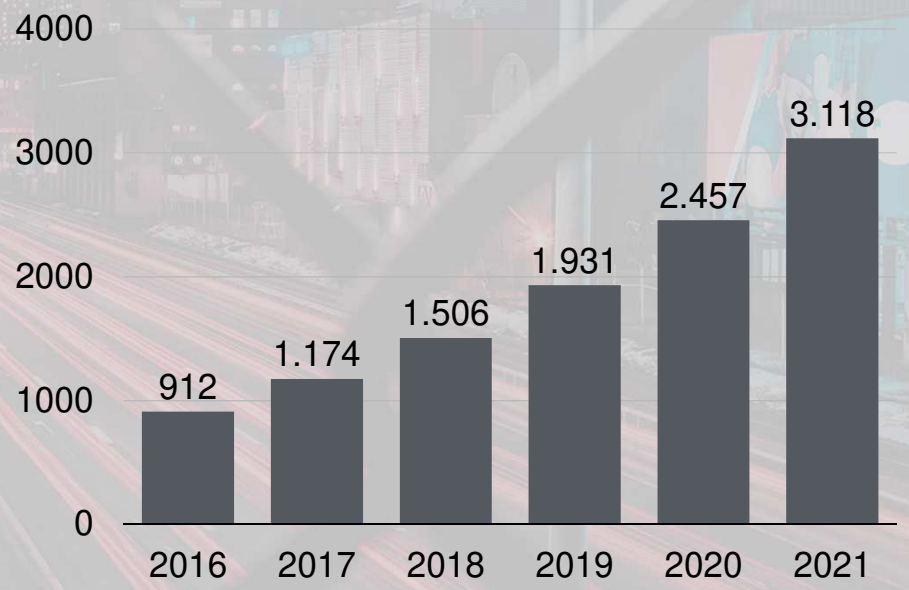
En medio de la presión de la ciberseguridad



IoT masivo

- 20% de las organizaciones sufrieron por lo menos un ataque IoT en los últimos tres años (Gartner)
- Aún no existe una coordinación para hacer que la mayoría de dispositivos IoT sean seguros, la seguridad se implementa después por el departamento de TI de la empresa que los adquiere
- La regulación jugará un papel fundamental para evitar la laxitud de algunos fabricantes

Proyección del gasto mundial en seguridad IoT (en millones de US$)



Fuente: Gartner, Marzo 2018

¿Donde pueden perder el control de la seguridad los operadores?

- En la oferta de sus proveedores de infraestructura, existentes o nuevos con las nuevas tecnologías (ej. caso Huawei)
- En la conexión a su red a dispositivos cuyos fabricantes han sido laxos en las medidas de seguridad
- En los acuerdos con otros proveedores de servicios en la nube para servicios gestionados o SaaS
- En su interacción con otras redes
- Errores humanos o fraudes desde dentro de las propias organizaciones
- Usuarios poco educados en los riesgos del uso de sus dispositivos conectados

¿Por qué el riesgo crece sin control?

- Múltiples redes 2G, 3G, 4G y pronto 5G (múltiples protocolos, SS7, SIGTRAN, Diameter, SIP, GTP)
- Multiples conexiones entre múltiples redes (fijas, móviles, locales, internacionales)
- Múltiples dominios donde se encuentran las aplicaciones
- Múltiples dispositivos (IoT)
- Múltiples tipos de usuarios según casos de uso
- Automatización e Inteligencia Artificial
- Todo muy nuevo, rápido y sin tiempo a una educación adecuada de las empresas y los usuarios

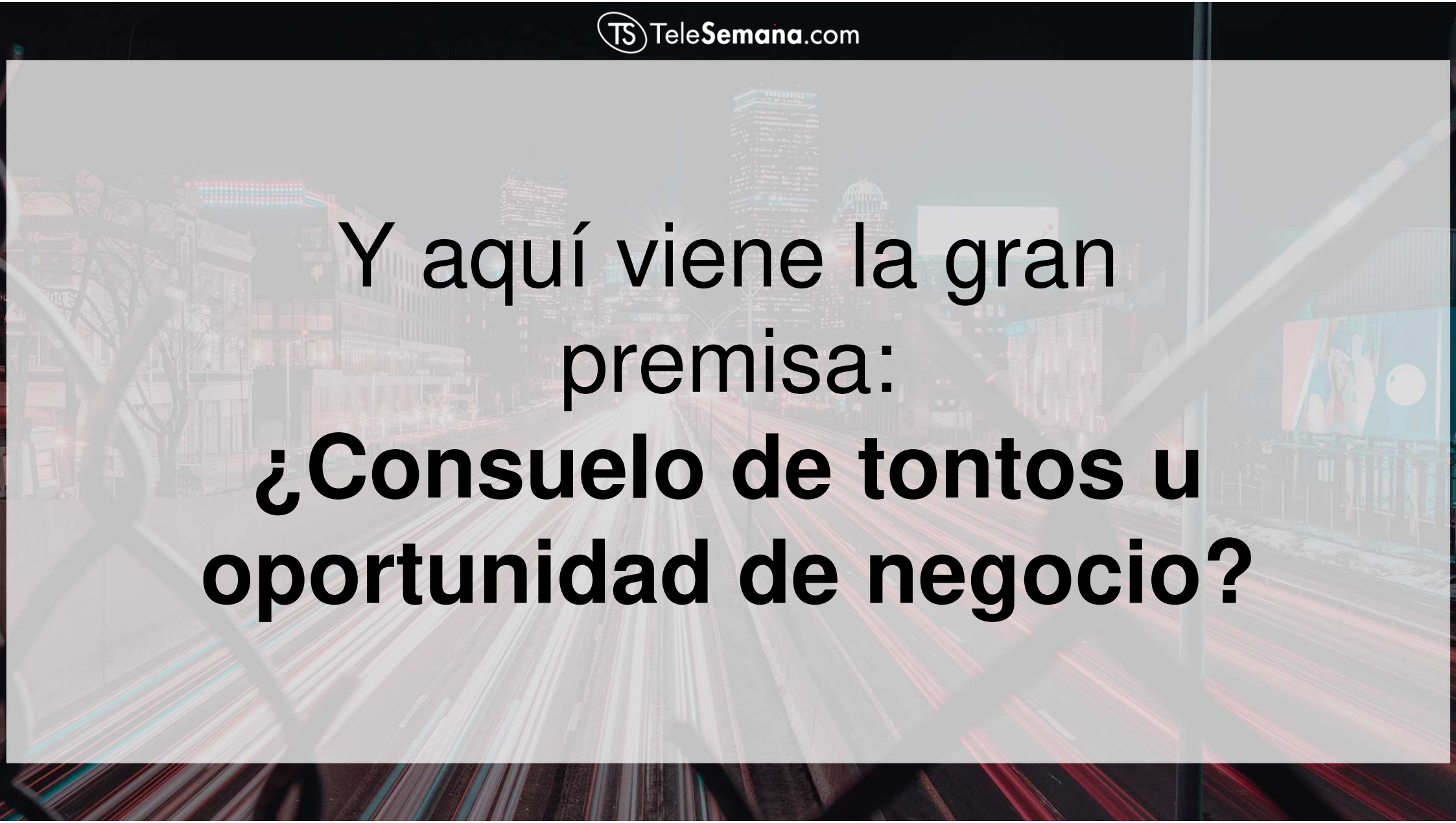
Los operadores cada vez acumulan y gestionan más datos

- Con la llegada de la 5G y el IoT masivo el volumen de datos y su gestión de multiplicará de forma exponencial

- El uso de Big Data y Analytics deberá ser uno de los pilares del negocio de los operadores a futuro, negocio basado en la capacidad de guardar y analizar grandes volúmenes de datos y a la vez asegurar mediante SLAs la transmisión de datos críticos (central nuclear vs. termostato en el hogar)

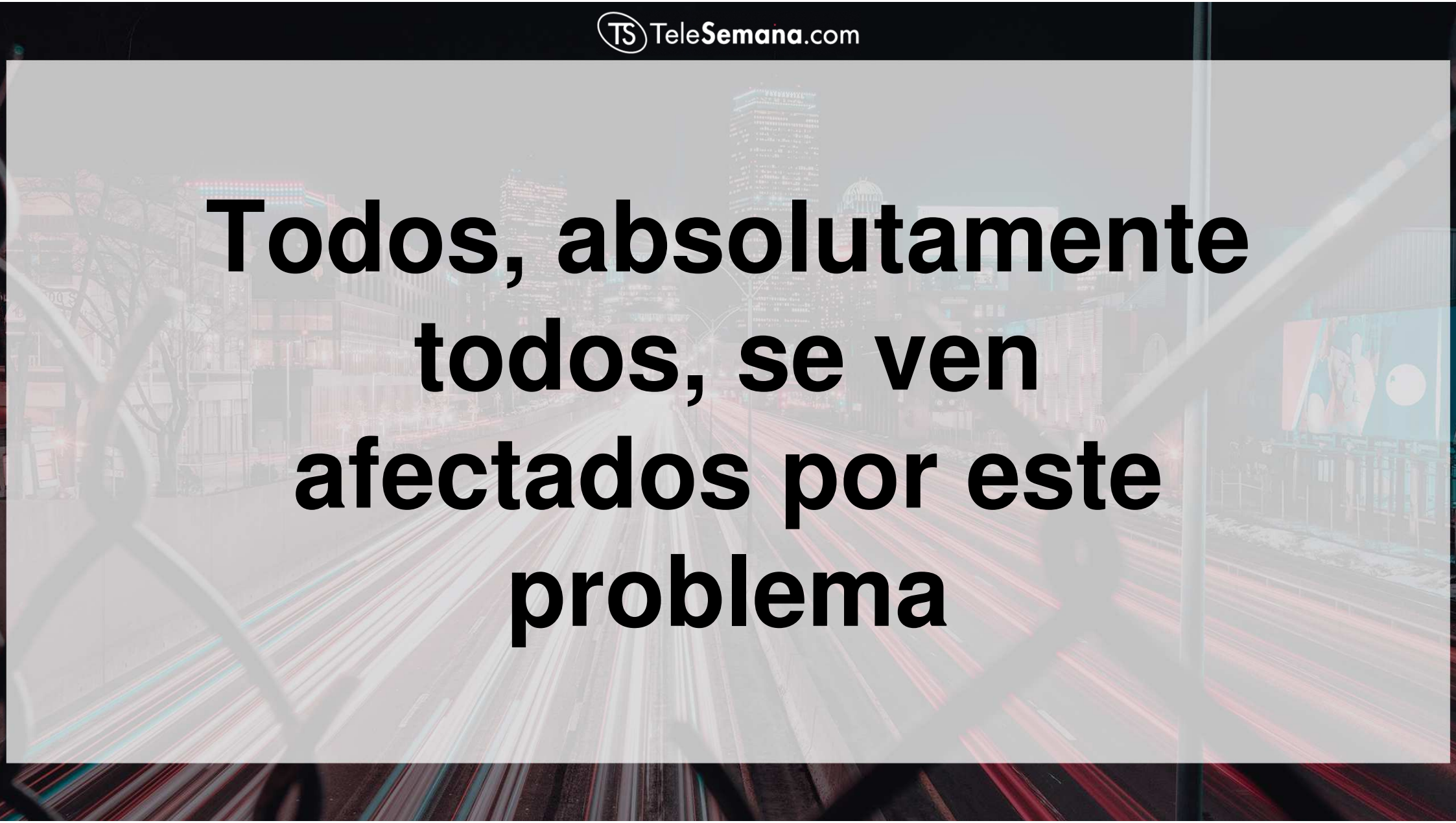
- Estos datos deben estar protegidos y asegurados para que el negocio pueda ser confiable

- Un estudio de Del EMC revela un incremento del 569% de los datos que gestionan las organizaciones en todo el mundo. Pasaron de gestionar 1,45 PB en 2016 a 9,70 PB en 2018



Y aquí viene la gran premisa:

¿Consuelo de tontos u oportunidad de negocio?



Todos, absolutamente todos, se ven afectados por este problema

Todos, absolutamente todos, se ven afectados por este problema

HACKED

Bell Canadá

- Cuenta con más de 22 millones de clientes
- Enero de 2018 alertó que 100.000 cuentas de email, teléfono, nombre, apellidos habían sido hackeadas. **NO PARECE HABER INDICACIÓN DE ROBO DE DATOS BANCARIOS O TARJETAS DE CRÉDITO**
- 8 meses antes el operador ya había anunciado el hackeo de 1,9 millones de emails

HACKED

Three UK

- Cuenta con más de +10 millones de clientes
- En marzo de 2017 reportó que las cuentas de más de 200.000 usuarios habían sido hackeadas, robando nombres, números telefónicos, direcciones, fechas de nacimiento, métodos de pago y correos electrónicos

T-Mobile

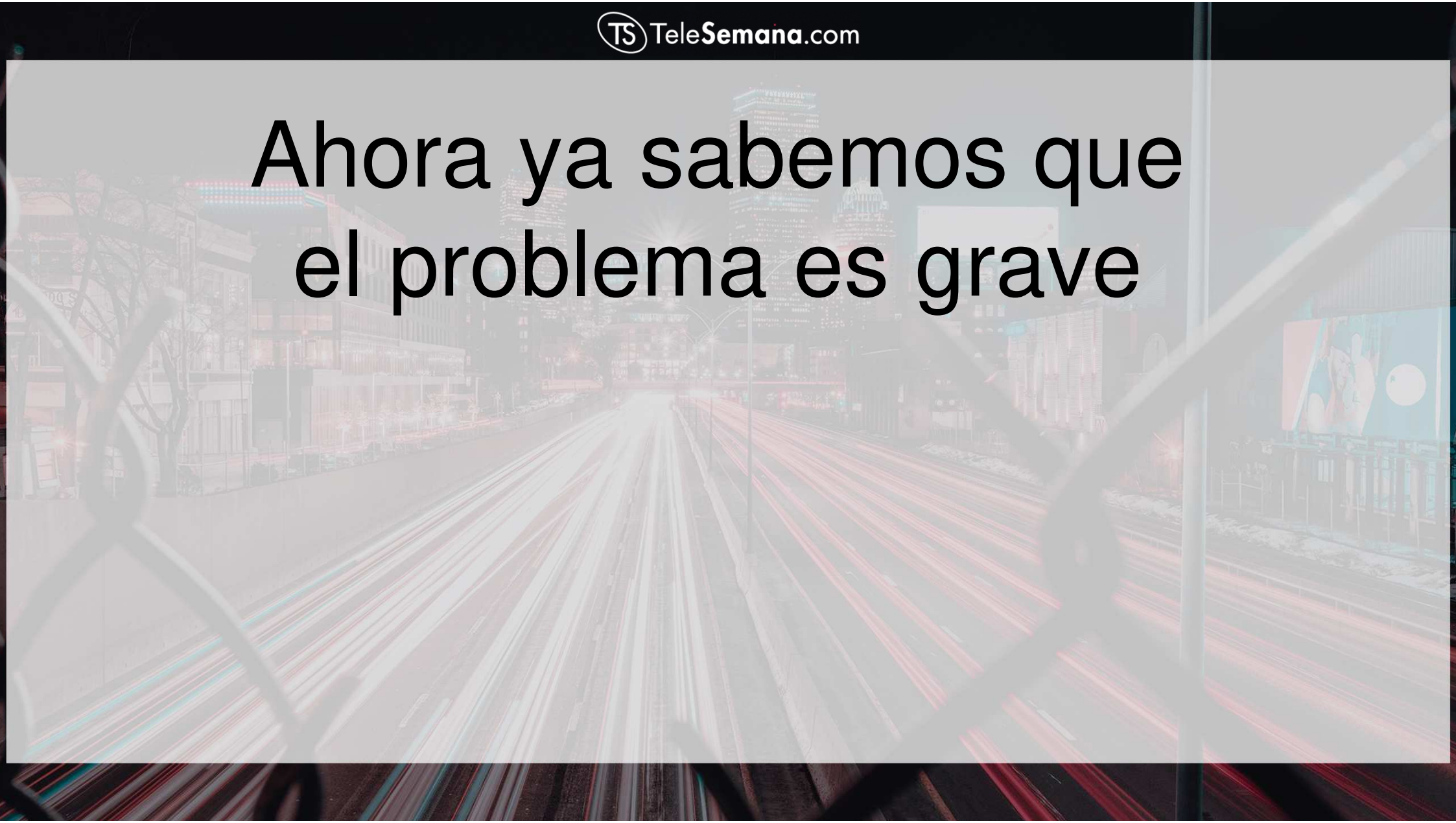
- Cuenta con más de 80 millones de clientes
- En agosto de 2018 el operador anunciaba que había sufrido un robo de datos de sus usuarios, se especuló que podría afectar a más de **2 millones**
- Los hackers accedieron a la información de los usuarios a través de un API del operador

Los OTTs también lo sufren

- Cuentas de email de **Microsoft** fueron hackeadas para robar criptomonedas a los usuarios
- **Yahoo** tuvo agujeros masivos en 2013 y 2014, el primero con 1.000 millones de usuarios y el segundo con 500 millones y se comprometió a pagar a las víctimas
- **Instagram** fue hackeado dejando a 49 millones de usuarios expuestos
- Cuentas bancarias de 100 vendedores de **Amazon** fueron hackeadas

La amenaza de IoT

- Kaspersky Lab divisó más de 30.000 ataques a dispositivos IoT en América Latina en 2018.
  - Los dispositivos IoT fueron atacados con más de 120.000 variantes de malware durante el primer semestre de 2018. La cifra es el triple de la cantidad de malware IoT revelada en 2017.
    - Routers y cámaras de videovigilancia, los más afectados.
- Propuesta de regulación de seguridad de routers en Alemania
- California (EEUU): A partir del 1 de enero de 2020, cualquier fabricante de un dispositivo que se conecte “directa o indirectamente” a Internet debe equiparlo con funciones de seguridad “razonables”, diseñadas para evitar el acceso no autorizado, la modificación o la divulgación de información

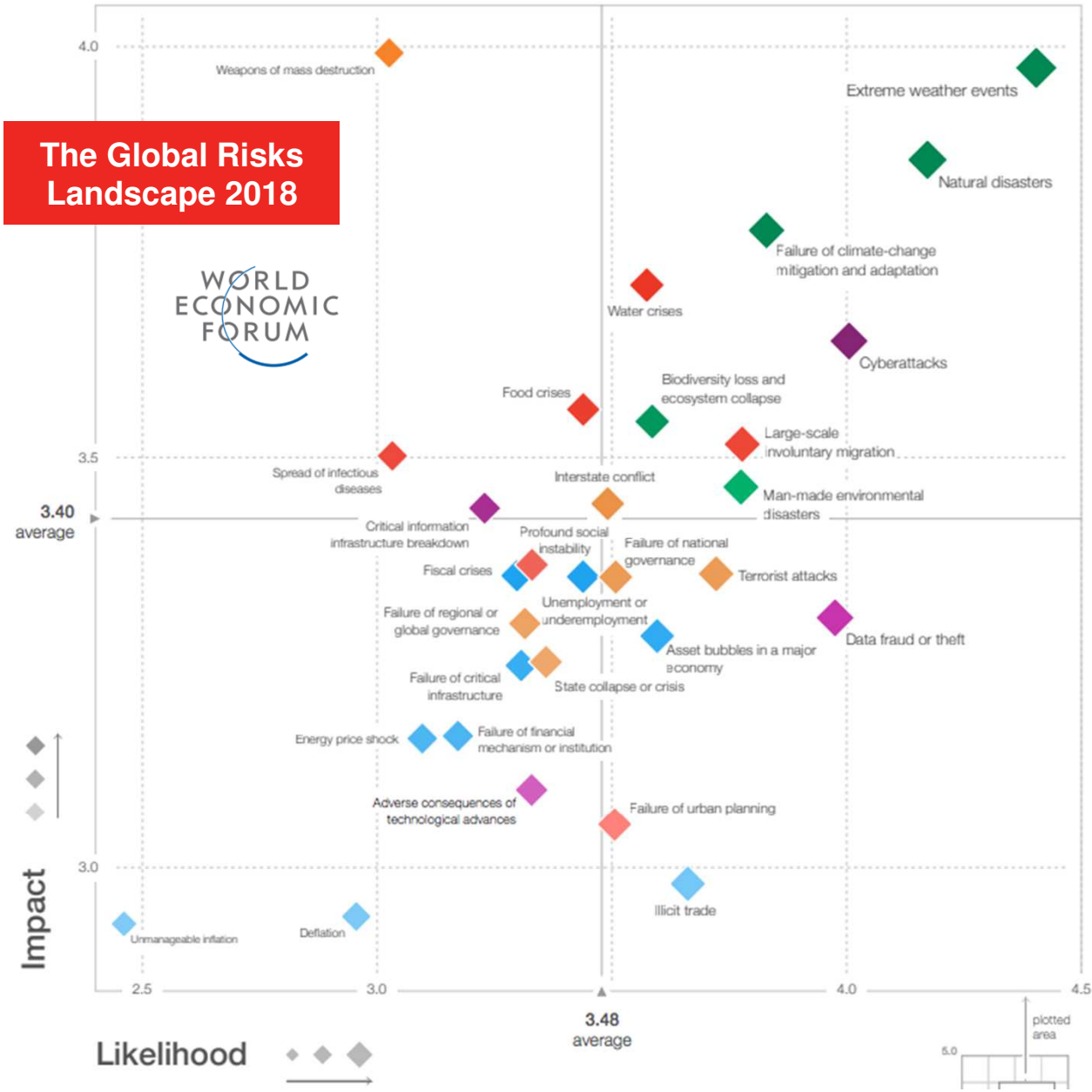


Ahora ya sabemos que el problema es grave

Ahora ya sabemos que el problema es grave

¿Pero cuán grave es el problema de la ciberseguridad?


TeleSemana.com
Ayuda a Wally
¿Donde está la ciberseguridad?


The Global Risks Landscape 2018
WORLD ECONOMIC FORUM
Weapons of mass destruction
Extreme weather events
Natural disasters
Failure of climate-change mitigation and adaptation
Water crises
Cyberattacks
Biodiversity loss and ecosystem collapse
Food crises
Large-scale involuntary migration
Spread of infectious diseases
Interstate conflict
Man-made environmental disasters
3.40 average
Critical information infrastructure breakdown
Profound social instability
Failure of national governance
Fiscal crises
Terrorist attacks
Unemployment or underemployment
Failure of regional or global governance
Data fraud or theft
Asset bubbles in a major economy
Failure of critical infrastructure
State collapse or crisis
Energy price shock
Failure of financial mechanism or institution
Adverse consequences of technological advances
Failure of urban planning
Illicit trade
Unmanageable inflation
Deflation
Impact
Likelihood
4.0
3.5
3.0
2.5
3.0
4.0
4.5
3.48 average
plotted area
5.0

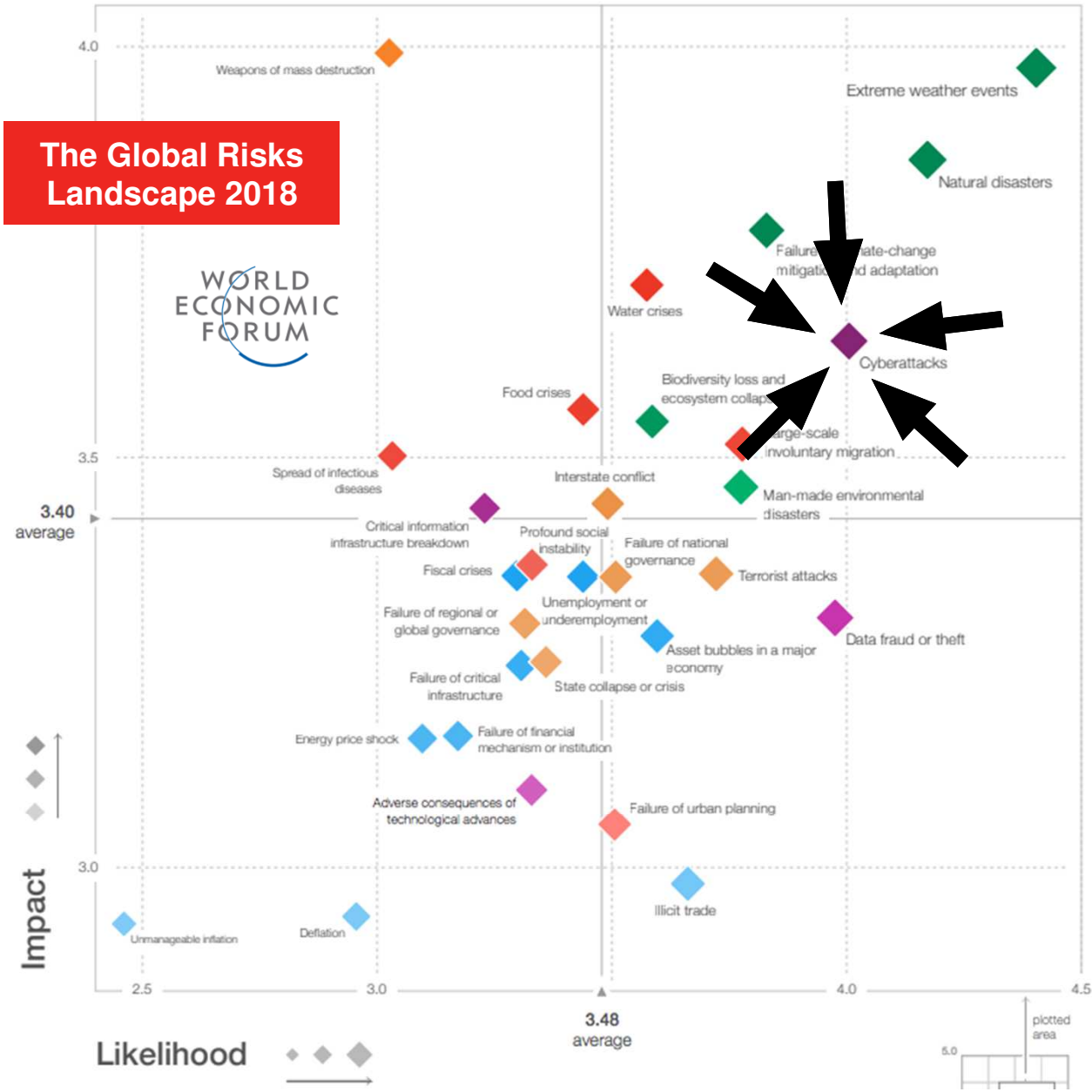
TeleSemana.com

Ayuda a Wally

¿Donde está la ciberseguridad?

The Global Risks Landscape 2018

WORLD ECONOMIC FORUM



Seguridad como negocio

verizon

orange™

COMCAST

Global Cyber Security Alliance

etisalat

Singtel

Telefónica

SoftBank

AT&T

La cooperación entre operadores puede ser un arma muy poderosa para estos jugadores

Conclusiones

- Los ataques de ciberseguridad y robo de datos van a ir en aumento
- Los operadores pueden convertir este desafío en un negocio
- Para ello tendrán que estar atentos a sus proveedores, a sus clientes y a los clientes de sus clientes
- Este es un problema complejo, quien lo resuelva obtendrá una ventaja competitiva sustancial