

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING



PROTECCIÓN DE DATOS PERSONALES Y CIBERSEGURIDAD



PROTECCIÓN DE DATOS PERSONALES: ¿DÓNDE ESTAMOS Y HACIA DÓNDE VAMOS?

Oscar Montezuma Panez

Internet - 2007

iPhone

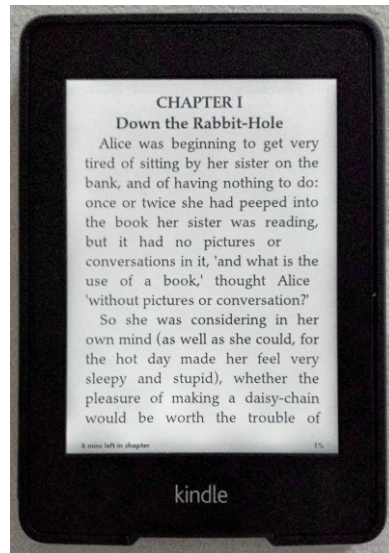
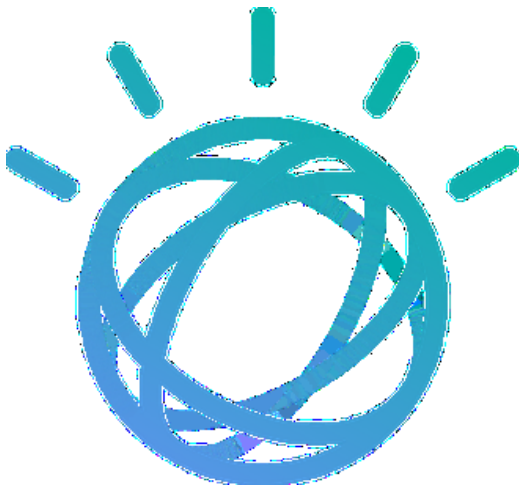
ANNOUNCED:
January 9, 2007

RELEASED:
June 29, 2007

KEY FEATURES:
3.5-inch diagonal
screen; 320 x 480
pixels at 163 ppi;
2-megapixel camera

PRICING:
4GB model, \$499; 8GB
version, \$599 (with
a two-year contract)





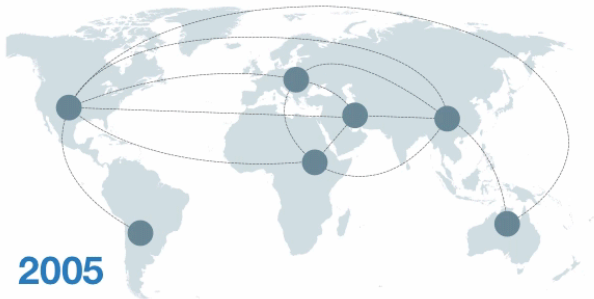


Sin embargo la revolución digital... recién empieza

Global flow of data and communication

Used cross-border interregional bandwidth, in gigabits per second

≤1,000 >1,000 2,000 5,000 10,000 15,000 20,000 24,405



Total used cross-border bandwidth,
in thousands of gigabits per second

Intraregional 3.1
Interregional 1.6

4.7
2005

McKinsey&Company | SOURCE: TeleGeography; McKinsey Global Institute analysis

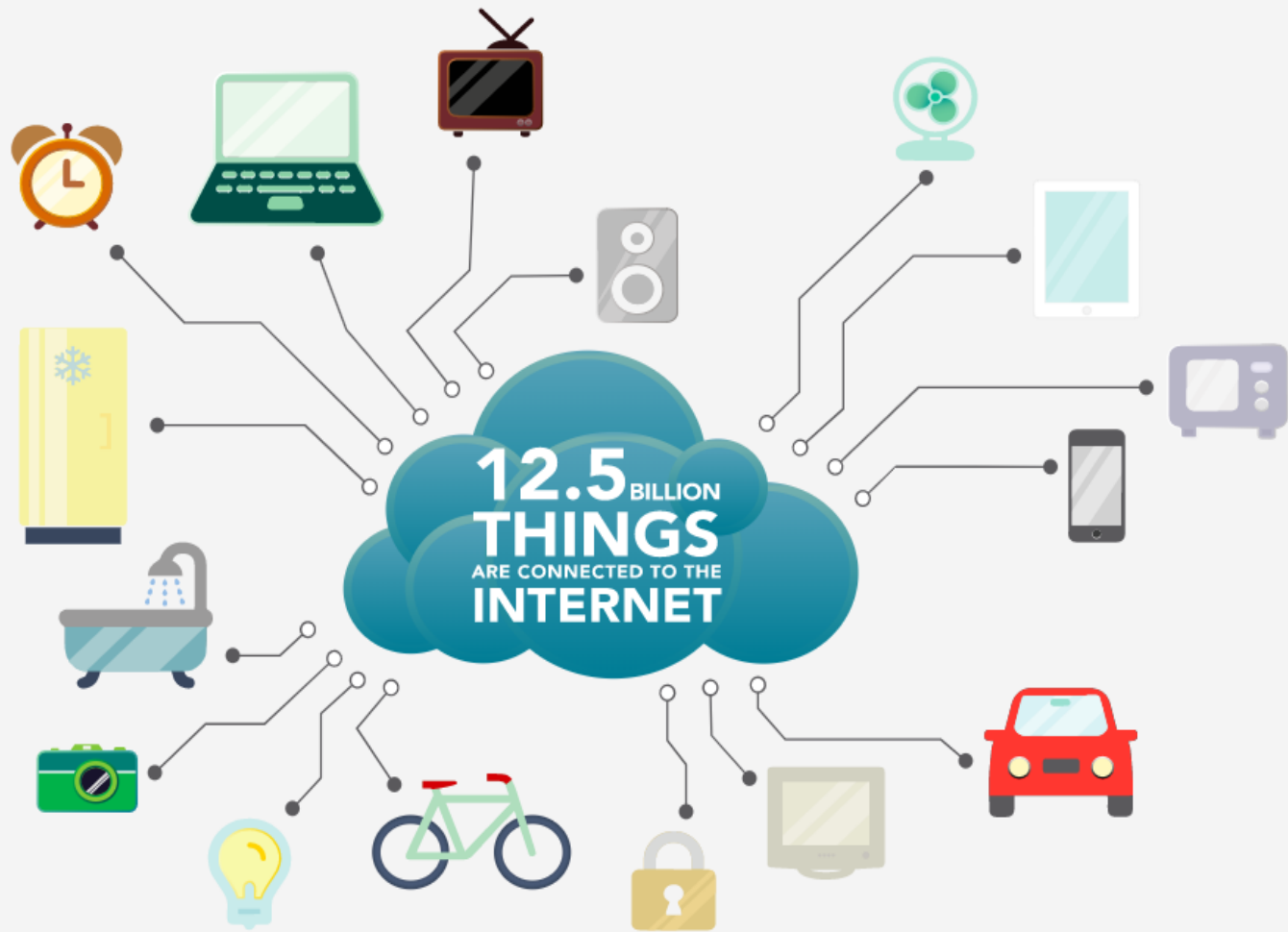
Se han creado más datos en los últimos 2 años que en toda la historia de la humanidad

El Big Data crece a una velocidad nunca antes vista, y se estima que para 2020 cada individuo creará 1,7 megabytes de información nueva por segundo

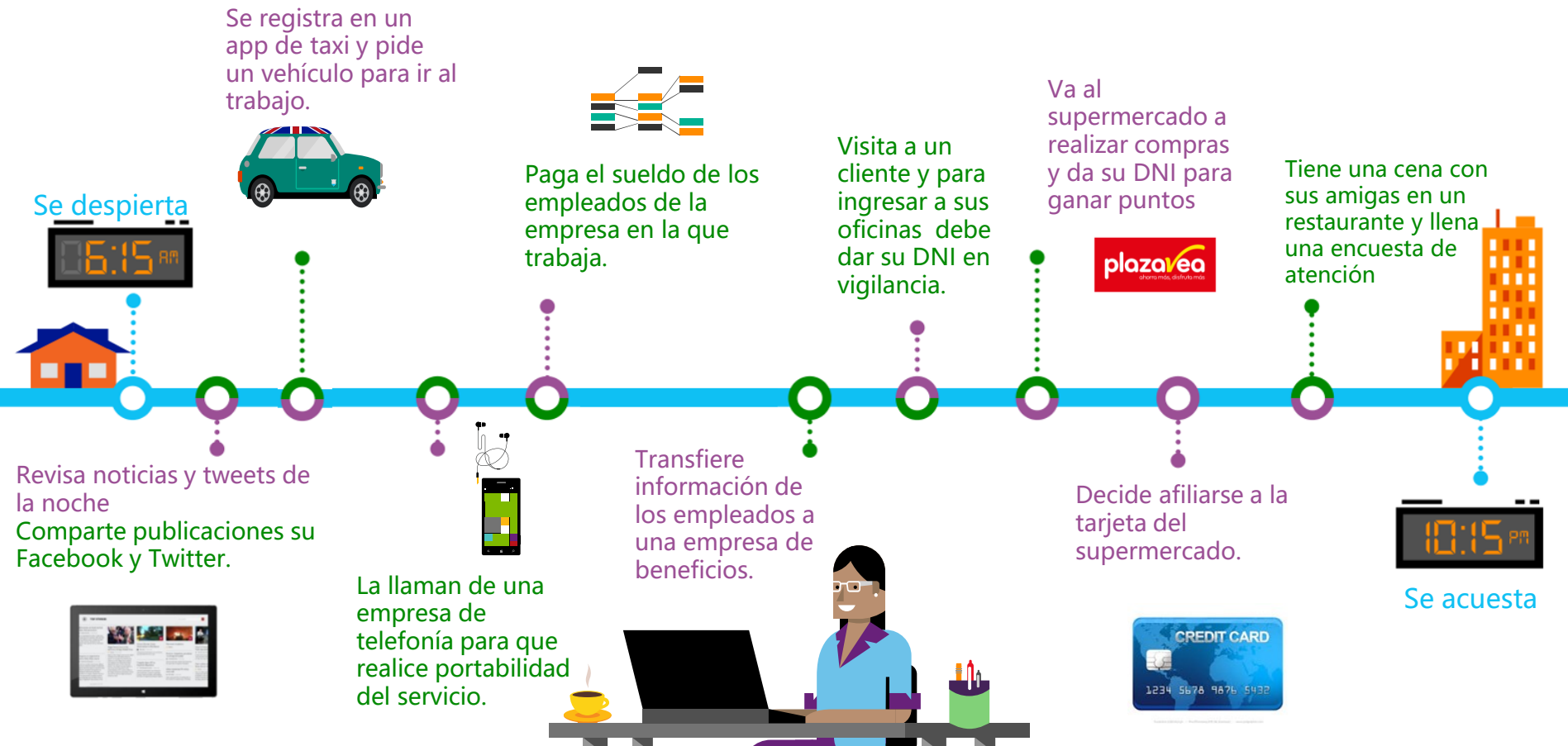
Para 2020, nuestro universo de datos pasará de **4.4 zettabytes** que existen actualmente a **44 zettabytes** (44 billones de gigabytes).

De momento solo se analiza y utiliza el 0,5% de todos los datos que existen, por lo que debemos considerar el potencial que este mercado presenta.

Global Report Cisco Systems 2016



Vivir en digital no es más una opción



MODELOS REGULATORIOS



Regulación sectorial

- ❖ No hay autoridad central
- ❖ Control posterior

MODELOS REGULATORIOS



- ◊ Regulación general y sectorial
- ◊ Autoridad central
- ◊ Control previo

Protección de datos personales

**LEY DE PROTECCIÓN DE DATOS
PERSONALES (LEY 29733)(2011)**

**REGLAMENTO DE LA LEY DE
PROTECCIÓN DE DATOS PERSONALES**
(Decreto Supremo 003-2013-JUS)(2013)

**Se crea Autoridad Nacional de Datos
Personales (MINJUS).
DIRECTIVA DE SEGURIDAD 2013.**



Objeto

Artículo 1. Objeto de la Ley

La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, **a través de su adecuado TRATAMIENTO**, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Tratamiento de datos personales.
Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

Objeto

En síntesis:

Tratar la **información personal (PN)** con debido respeto a ciertos parámetros.

La ley prescribe **ciertas normas y reglas** que se ocupan de:



Recopilación y el uso de información.



Calidad y la seguridad de la información.



Derecho de las personas con respecto a la información sobre sí mismos.

Definiciones importantes

Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.



Definiciones importantes

Banco de datos personales. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.



Definiciones importantes

Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Encargado del banco de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.



Regla general: el consentimiento

- 1 LIBRE, PREVIO, INFORMADO, EXPRESO E INEQUIVOCO.
- 2 Datos sensibles requieren consentimiento escrito u otro mecanismo que garantice carácter inequívoco.
- 3 En entornos digitales: Política de Privacidad



Directiva de Seguridad

- Orienta sobre las **condiciones, los requisitos y las medidas técnicas** para el cumplimiento con la Ley de Protección de Datos Personales
- Los requisitos y las medidas a implementar pueden ser variables y **dependerán de las categorías de tratamiento de datos** (básico, simple, intermedio, complejo, crítico)

Medidas de seguridad técnicas (Ley y Reglamento)

- Seguridad para el tratamiento de la información digital (Art. 39 Reglamento)
 - Incluir un control de acceso
 - Generar y mantener registros (trazabilidad de los accesos).
 - Identificación y autenticación.
- Conservación, respaldo y recuperación de datos personales (Art. 40 del Reglamento)
 - Respaldo verificando la integridad de los datos.
- Transferencia lógica de datos personales (Art. 41 del Reglamento)
 - Cifrado.
- Almacenamiento de documentación no digital (Art. 42 del Reglamento)
 - Acceso físico seguro (puertas, llaves).
- Copia o reproducción (Art. 43 del Reglamento)
 - Bajo control de personal autorizado.
 - Destrucción de copias o reproducciones deshechadas.
- Acceso a la documentación (Art 44 del Reglamento)
 - Sólo a personal autorizado.
- Traslado de documentación no automatizada (Art. 45 del Reglamento)
 - Impedir acceso y manipulación.

Medidas de seguridad técnicas (Directiva)

- Procedimientos documentados.
- Control de accesos.
- Gestión y uso de contraseñas.
- Pruebas de recuperación de datos.
 - Fecha y hora de la prueba.
 - Nombre de la persona que realizó la prueba.
 - Banco de datos personales recuperado.
 - Archivo recuperado y fecha de los datos recuperados.
 - Tiempo de recuperación
 - Resultados de pruebas.
 - Acciones tomadas en caso de pruebas insatisfactorias.
- Registro de incidentes de seguridad.
- Auditorías

GDPR



**Data Protection
Officer (DPO)**



Compliance



25 May 2018



Data Breaches



Personal Data



YO! DUDE...
BACK
HERE



CYBER
SECURITY



WHAT WILL THE
WARRIOR-GUARDIAN
OF THE FUTURE
LOOK LIKE?

Otras iniciativas internacionales



Cyber Security Law of the
People's Republic of
China (2017)



Política Nacional de Seguridad Digital
(2016)



The Comprehensive National
Cybersecurity Initiative (2008)



Política Nacional de
Ciberseguridad (2017)

¿Qué ocurre en el Perú?



Informe de la OEA y el Banco Interamericano de Desarrollo (BID), publicado este año, analizó la situación de 32 países latinoamericanos. En el caso peruano, si bien se destaca la existencia de normas importantes, entre ellas, la Ley 30096 de delitos informáticos y la **Ley 29733 de protección de datos personales**, también se resalta que “la ausencia de una estrategia y una cadena de mando clara sigue impidiendo el fortalecimiento de la seguridad cibernética en el país”.



CIBERSEGURIDAD: UNA NECESIDAD CRECIENTE PARA LAS EMPRESAS

Carlos Quintero – IT Manager RSM Perú

¿Qué es la ciberseguridad?

Objetivo

La ciberseguridad sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos.



INFORMATION AND
DATA SECURITY

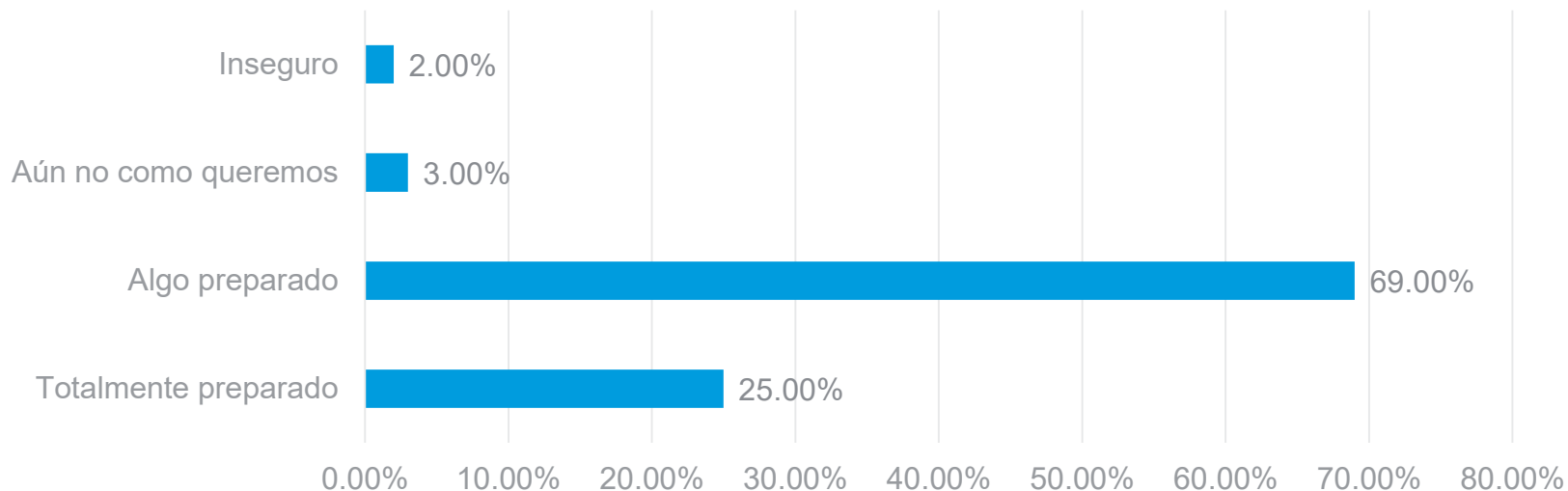
Delitos y fraude en internet

Los casos de fraude en Internet y otros delitos relacionados con los datos han aumentado de manera espectacular

Se han vuelto progresivamente sofisticados. Los ciberataques en las organizaciones a través de las lagunas de seguridad han aumentado más del 80% en los últimos dos años a medida que los intrusos buscan robo de información industrial o de identidad.

¿Cómo estas preparado?

Cómo está preparada su empresa para un ciberataque



¿Estamos preparados? El **72%** de los CEO dice que no están completamente preparados para un evento cibernético.

Ciberataques dirigidos

Los ataques dirigidos son cada vez más comunes ...

En un estudio de 1200 empresas, la empresa de investigación de seguridad FireEye identificó:

24 % → 97 %

de estas empresas con
experiencia en eventos
que coinciden con los
patrones de una ataque
dirigido

de estas empresas fueron
violado.

Casos recientes de ciberataques

Titulares de noticias recientes de The New York Times, The Washington Post, Computer World y Krebs on Security.

N.Y. Firm Faces Bankruptcy from \$164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole \$465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR \$50,000 CYBER HEIST

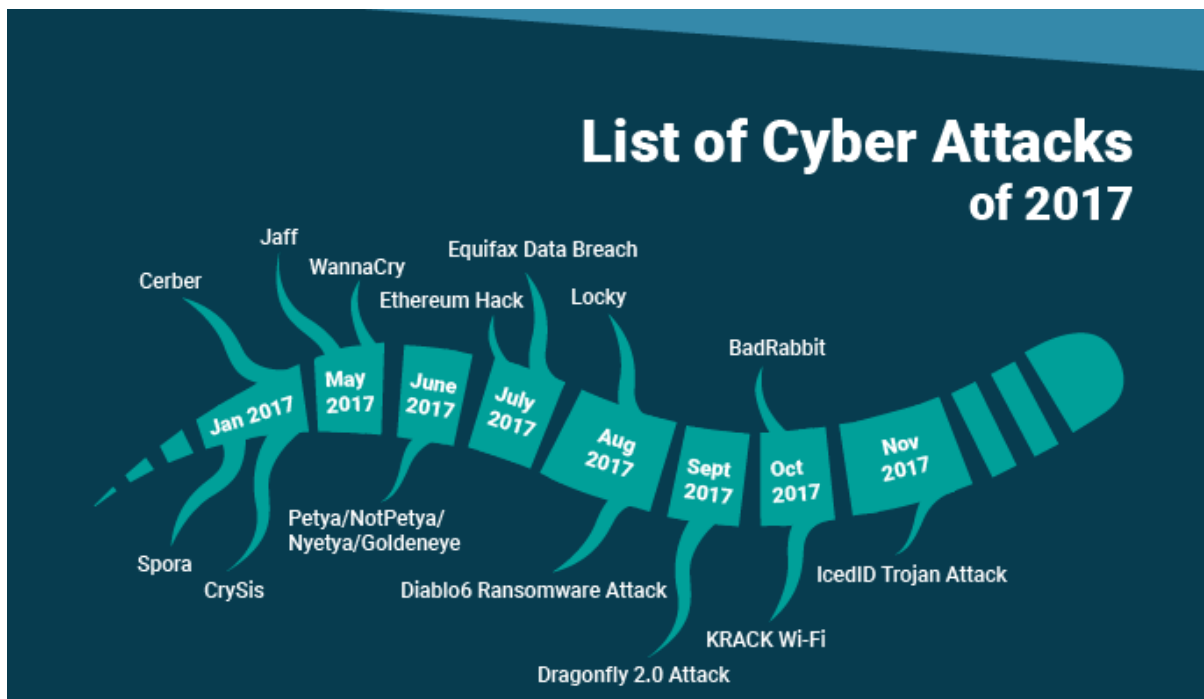
Computer Crooks Steal \$100,000 from Ill. Town

FBI Investigating Theft of \$500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

Casos recientes de ciberataques

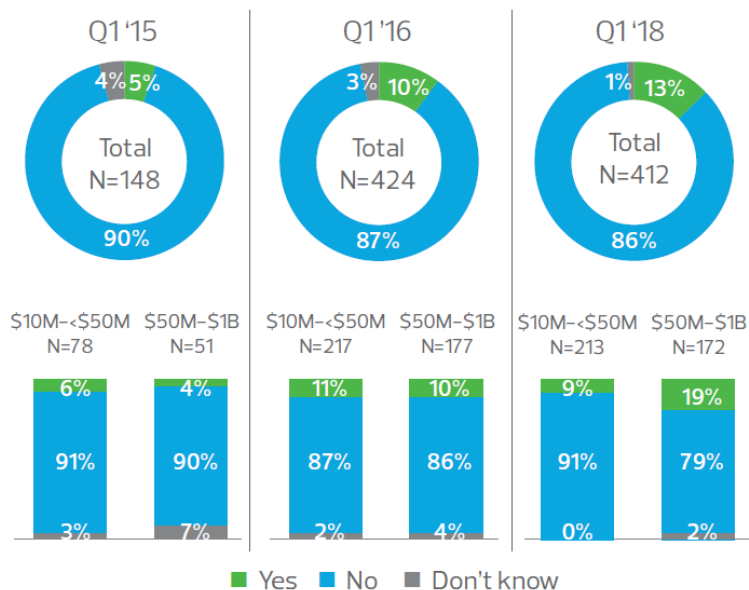
Incidentes de ciberseguridad más grandes del 2017



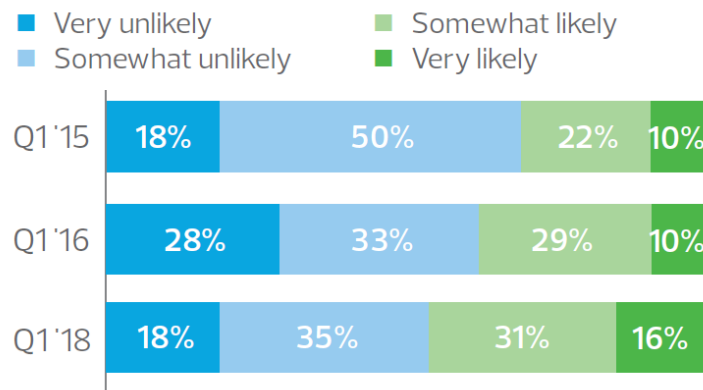
Ciberataques sobre el sector empresarial

Los ataques dirigidos son cada vez más comunes ...

Empresas que han sufrido ciber ataques
en los últimos 12 meses



Probabilidad de que usuarios no autorizados
intenten acceder a los datos / sistemas



Cibercrimen

Según Forbes, para el 2019 la ola del cibercrimen en el mundo alcanzará los 2.1 trillones de dólares.

En Latinoamérica, las pérdidas económicas producto de este tipo de ataques ascienden a **USD 76 mil 766 millones de dólares**.

País	Pérdidas
Brasil	USD 19 mil 291 millones
México	USD 11 mil 921 millones
Venezuela	USD 9 mil 142 millones
Argentina	USD 7 mil 400 millones

Perú se encuentra entre los países más afectados por el cibercrimen en la región, registrando pérdidas que alcanzarían los **USD 4 mil 782 millones de dólares**.

Tipos de ciberataques

Los 4 tipos de ciberataques más frecuentes

Los ciberdelincuentes a menudo utilizan correos electrónicos masivos, mensajes emergentes que aparecen en sus computadoras y el uso de redes sociales y sitios web para engañar a los usuarios.

1. **Malwares**
2. **Adwares**
3. **Phishing**
4. **Ciberbullying**



Tipos de infección

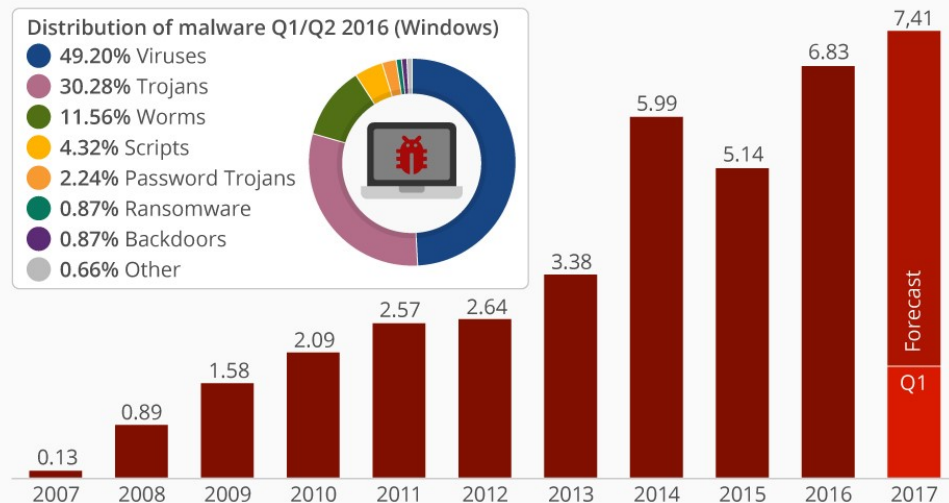
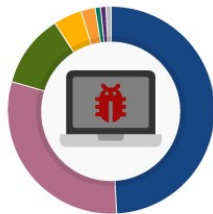
Mapa de infección global

Viruses, Worms and Trojan Horses

Number of new malware specimen (in millions)

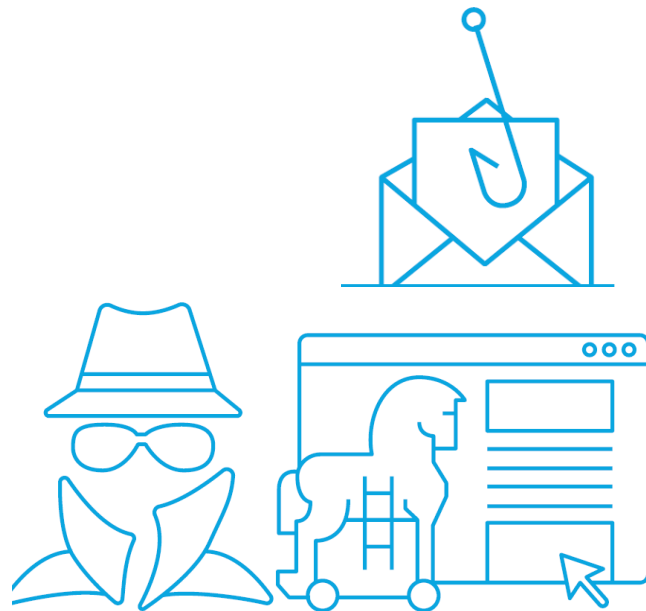
Distribution of malware Q1/Q2 2016 (Windows)

- 49.20% Viruses
- 30.28% Trojans
- 11.56% Worms
- 4.32% Scripts
- 2.24% Password Trojans
- 0.87% Ransomware
- 0.87% Backdoors
- 0.66% Other



@StatistaCharts Source: G DATA, AV-TEST

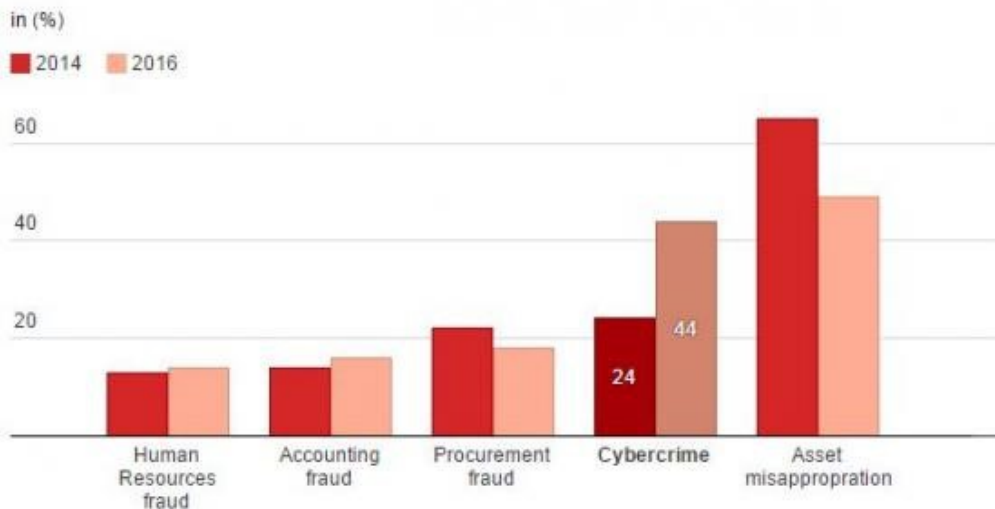
statista



Tipos de fraudes

Los cibercrimen entre los fraudes más reportados en 2016

Cybercrime climbs to 2nd most reported fraud in 2016



Global Economic Crime Survey 2016

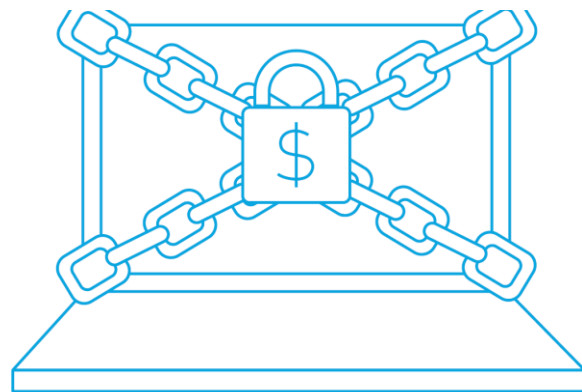
Source: PwC [Get the data](#)

Created with [Datavrapper](#)

Costos

El delito cibernético impone una serie de costos directos a las empresas globales:

- Robo de activos financieros
- Pérdida de propiedad intelectual
- Violación de información confidencial
- Costos de recuperación / restauración de datos violados
- Daño a la reputación de la compañía



Recomendaciones para reducir ciber ataques

Tu mejor defensa es entender los métodos utilizados por los ciberdelincuentes

1. Comprender no solo cómo acceder a sus datos críticos, sino también cómo se usan los datos puede ayudarlo a identificar sus activos más vulnerables.
2. Entender las tecnologías y metodologías que puede implementar para protegerse.
3. El monitoreo de intrusos en tiempo real.
4. Tener acceso a expertos en seguridad certificados.

Recomendaciones para reducir ciberataques

Proteger

1. Eduque a todos, sobre tipos y fuentes de fraude
2. Mejore la seguridad dentro de los sistemas de red para proteger contra el fraude
3. Mejore la seguridad en torno a los procesos y controles bancarios
4. Comprender responsabilidades

Detectar

1. Tenga en cuenta cualquier cambio en el rendimiento
2. Presta atención a las advertencias
3. Manténgase alerta de los correos electrónicos fraudulentos
4. Ejecuta escaneos regulares del sistema en busca de virus y malware

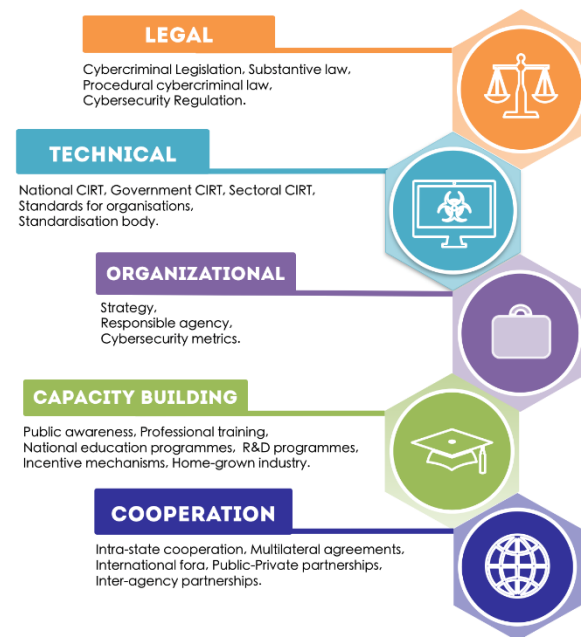
Responder

1. Desarrollar un sistema de respuesta
2. Asegúrese de que los empleados sepan quiénes son los contactos clave
3. Mantener la cronología escrita de los eventos
4. Archivo de informe policial
5. Tener un plan de contingencia para sistemas comprometidos

Indice de Ciber seguridad en América

Resumen de puntuación por países

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80



Inversión en ciberseguridad

Inversión de Perú en ciberseguridad

Perú invirtió aproximadamente USD 22 millones de dólares en servicios de ciberseguridad, con un crecimiento esperado de USD 28 millones al cierre del 2017 y unos USD 42 millones para el 2019.

Servicios de ciber seguridad (Perú)	%
Gestión de activos y monitoreo	71%
Inteligencia, investigación, detección y remediación de amenazas	18%
Gestión de riesgos y cumplimiento	8%

5% del presupuesto anual en ciberseguridad

Recomendaciones para reducir ciber ataques

Recursos que pueden evitar un ataque

- Si no cuenta con los recursos internos adecuados para ayudar con la protección, detección y respuesta al fraude, asegúrese de encontrar un proveedor que comprenda los riesgos asociados con el delito cibernético.

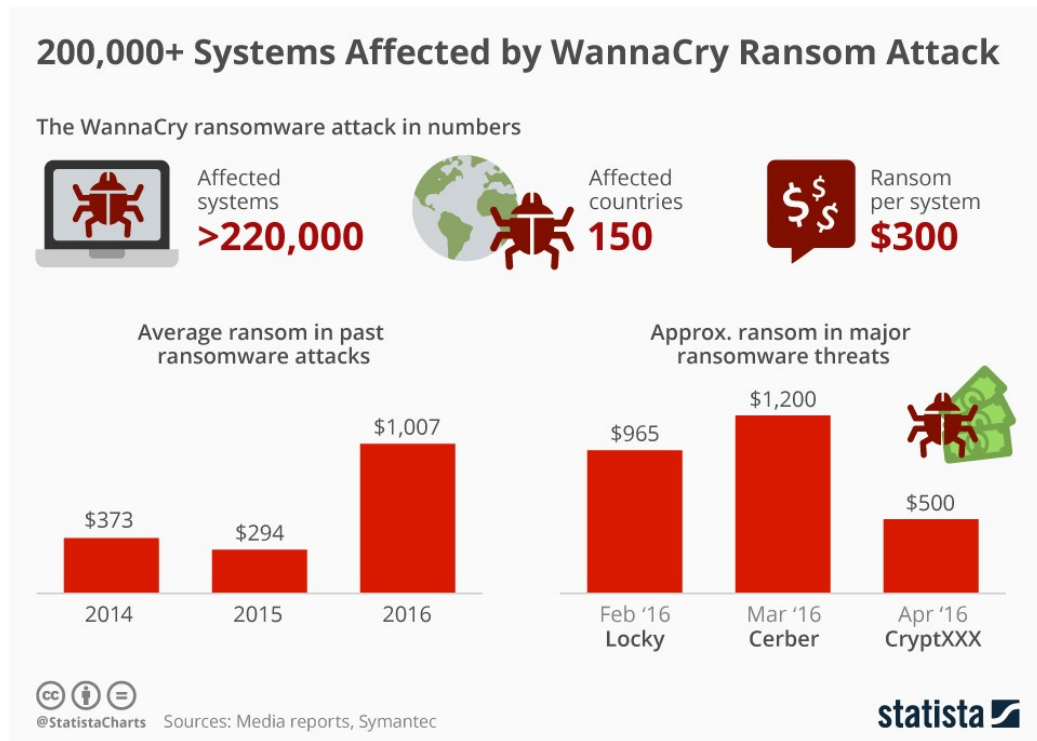


WannaCrypt epidemic

Ransomware Attack

WannaCrypt epidemic

Sistemas afectados por el ataque



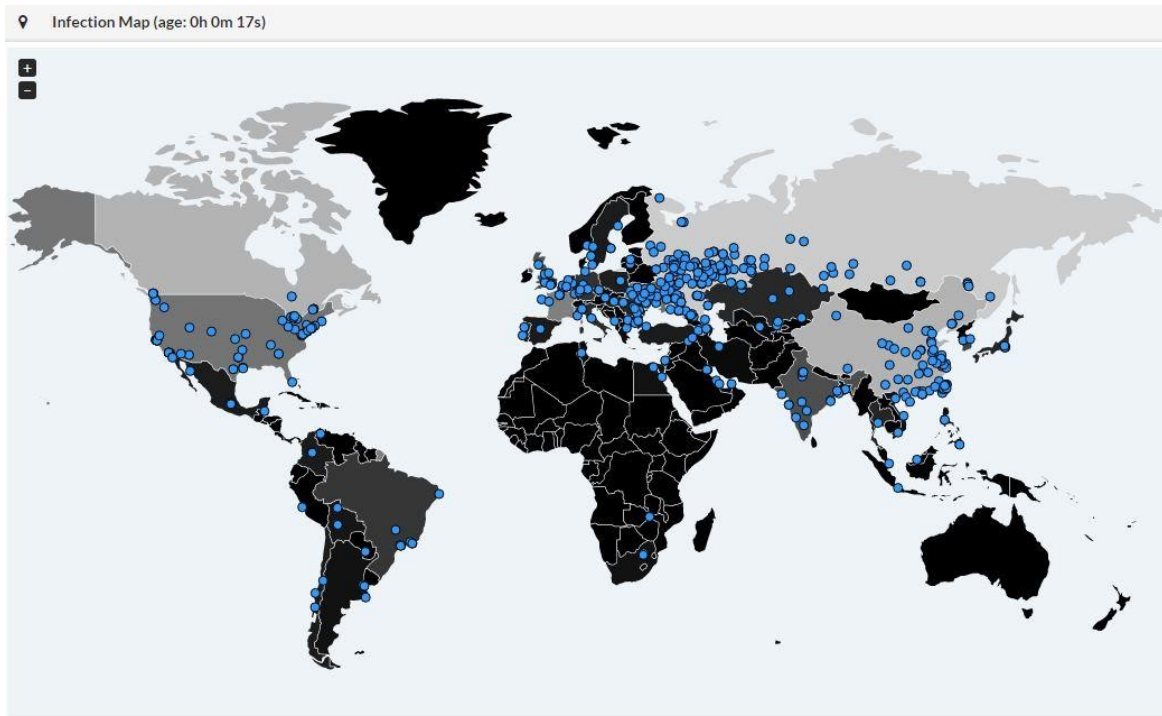
WannaCrypt epidemic

Recuperar archivos



WannaCrypt epidemic

Mapa de infección global



Sanciones para empresas que no prevengan

Reglamento General de Protección de Datos (GDPR)

- El GDPR supondrá que las empresas informen de la filtración de datos a las autoridades reguladoras y pongan a sus clientes al corriente del robo de su información en las 72 horas posteriores al descubrimiento del ataque.
- El incumplimiento de esta ley puede conllevar multas de hasta 20 millones de euros o del 4% de los ingresos mundiales de la empresa, dependiendo de qué cantidad sea mayor.



Sanciones para empresas que no prevengan

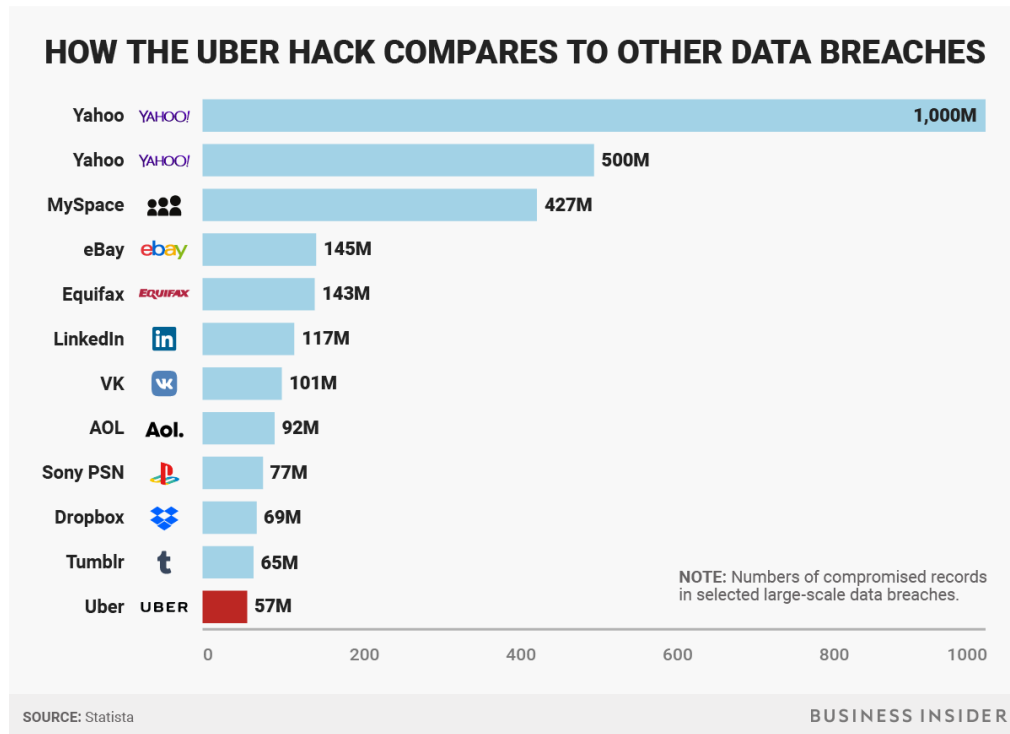
Caso UBER

- Uber escondió un gran ciberataque a sus servidores en 2016 lo que ha suscitado nuevos llamamientos para que las normas sobre este tipo de infracciones sean más estrictas, también en Estados Unidos.
- Bloomberg informó que Uber había pagado a los piratas informáticos \$ 100,000 para ocultar una violación de datos en octubre de 2016 que expuso la información personal de 57 millones de usuarios.



Sanciones para empresas que no prevengan

Otros casos (Cantidad de información comprometida)



- Está claro que tanto los piratas informáticos como los abogados van a estar muy ocupados en el 2018.

Riesgos que nos rodean para próximos años

Nuevos objetivos de los piratas informáticos

- Filtraciones de datos cada vez mayores
- Ransomware en la nube
- La inteligencia artificial se convierte en arma
- Ataques *ciberfísicos*
- La minería de las criptomonedas
- Los ciberataques protagonizan las elecciones (¡otra vez!)



• RSM

6ta red más grande del mundo

AUDIT | TAX | CONSULTING

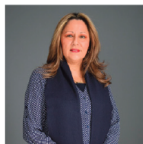
+ 50 años de experiencia

+ 800 oficinas

+ 120 países

+ 41,400 profesionales

Contactos:



Marisa Panez
Managing Partner
marisa.panez@rsm.pe



Carlos Quintero
IT Manager
carlos.quintero@rsm.pe

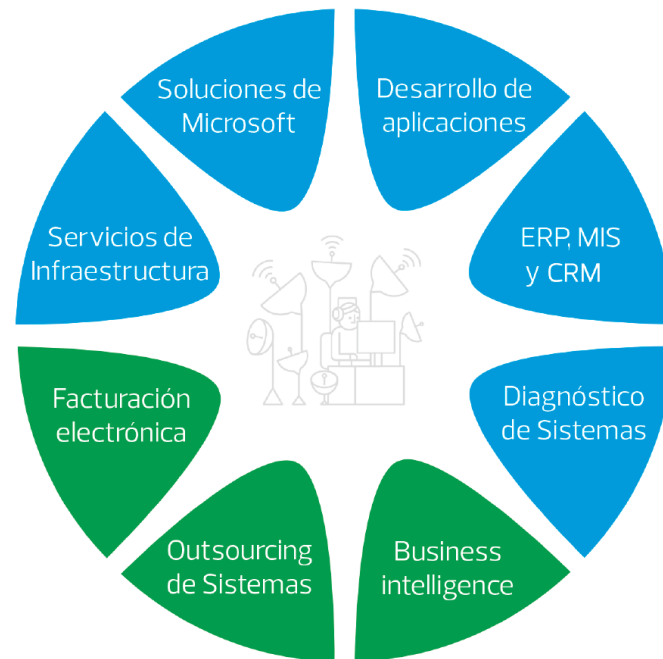


Daniel Montezuma
Commercial Manager
daniel.montezuma@rsm.pe

Consultoría en Tecnología de la Información

MAXIMICE SU INVERSIÓN EN TECNOLOGÍA Y REDUZCA COSTOS

En RSM le ayudamos a interactuar de manera eficaz en los objetivos estratégicos de su organización siendo un soporte tecnológico de infraestructura, metodologías, innovación y desarrollo mediante la combinación de conocimientos técnicos y experiencia de negocios con nuestra gama completa de servicios de TI, estamos en condiciones de evaluar las situaciones complejas, idear soluciones eficaces, y ponerlas en práctica de forma rápida y rentable.



Gracias por su tiempo y
su atención