Ciberseguridad en la empresa digital:

mitos y realidades

Ignacio Santillana

Javier Miyares

Mitos y realidades de la ciberseguridad

✗ Las páginas falsas son **fácilmente identificables**	**Son idénticas a las originales** y se apropian de tu identidad ✓
✗ Los **dispositivos Apple** no son susceptibles de ataques	Son más seguros, pero solo en abril de 2017 **600.000 Macs fueron atacados** ✓
✗ Los ataques no ocurren dentro de las **redes sociales**	**Gran número de ataques en las redes**, 56% a través de tarjetas regalo ✓

AUSAPE

Mitos y realidades de la ciberseguridad

✗ Los **antivirus gratuitos** son suficientes para un uso personal	✓ Las protecciones básicas no son suficientes **en casos de ransomware**
✗ Virus y Malware **solo afectan a ordenadores**	✓ Cada vez más ataques a **móviles y tablets**. Aumentaron un 58% en 2017
✗ Es un asunto que impacta **principalmente a IT**	✓ El **daño reputacional** es el que más impacta a las compañías y al valor de la acción

AUSAPE

Mitos y realidades de la ciberseguridad

✗ Los ataques van dirigidos a empleados con **pocos conocimientos de IT**	El 64% va **dirigido a Directores y Managers**, seguidos por empleados de IT ✓
✗ Mi riesgo es bajo ya que visito **páginas con riesgo bajo**	El 61% de las páginas infectadas son **páginas legítimas** ✓
✗ Percibo si mi ordenador ha sido infectado. **Entran y salen**	En el caso del botnet es habitual que permanezcan un **largo periodo en tu equipo** (146 días) ✓

AUSAPE

Los 10 riesgos que más preocupan a la Dirección en 2018

Fidelización de clientes

Situación económica

Resistencia al cambio

Cambios regulatorios

Cultura de riesgo

Ciberataques

Volatilidad del mercado

Innovaciones disruptivas

Atracción y retención de talento

Seguridad de la información

¿Por qué es un problema con un impacto transversal, no solo de IT?

Tecnológico

- Robos de datos
- Daños a activos críticos
- Incremento de la inversión en la detección

Regulatorio

- Investigación y auditoría
- Sanciones y compliance

Financiero

- Robo o desvío de fondos
- Pérdida de clientes
- Costes adicionales

Reputacional

- Imagen de marca
- Costes elevados de retención/captación
- Marketing defensa

Operacional

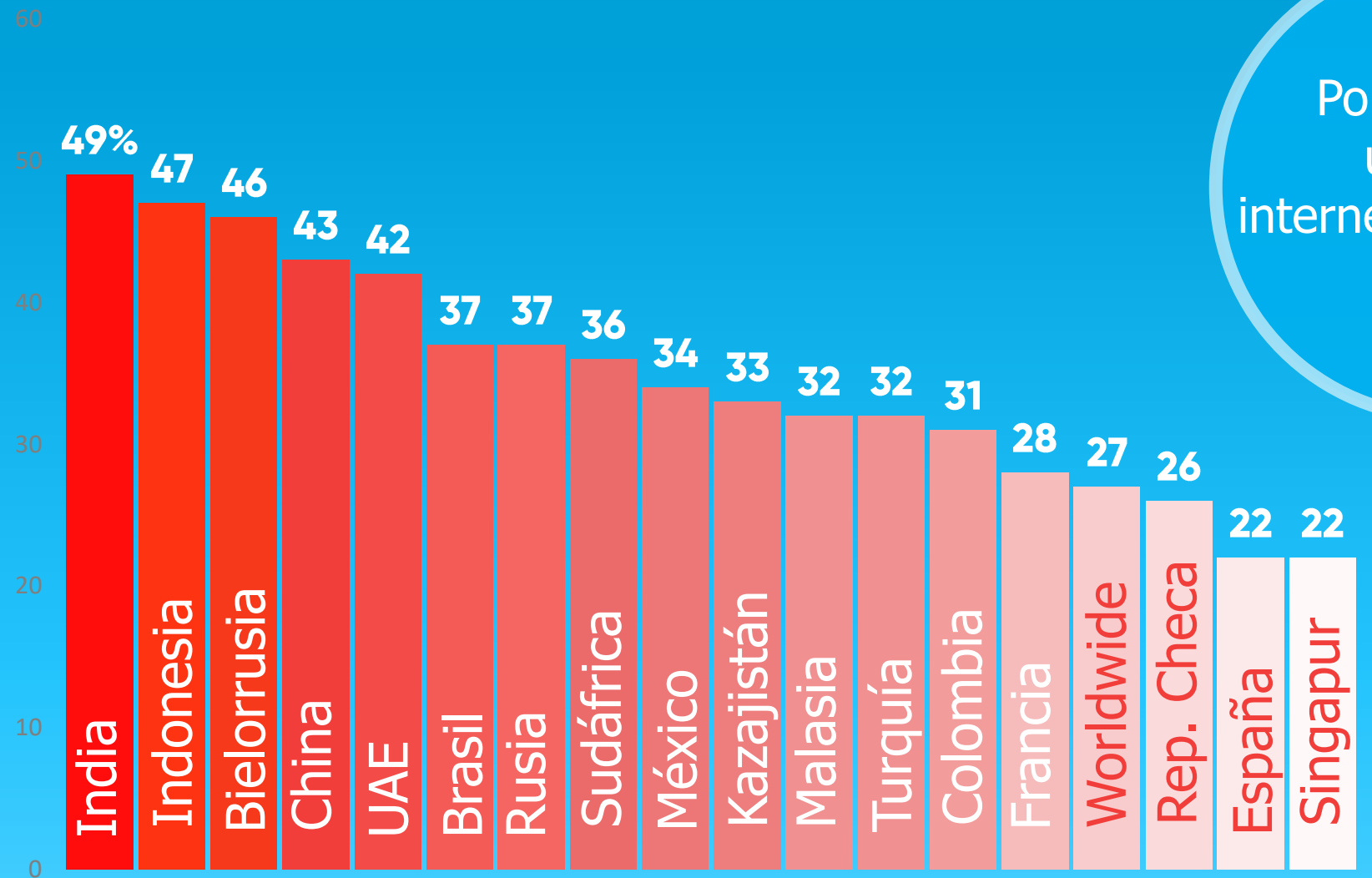
- Disrupción de operaciones
- Pérdida de información crítica
- Costes de recuperación

Estratégico

- Bajada de la acción
- Pérdida de confianza
- Robo o pérdida de información clave

AUSAPE

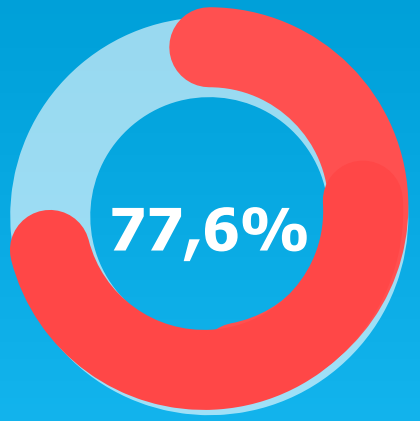
No solo afecta a IT, afecta a gobiernos, corporaciones y personas físicas



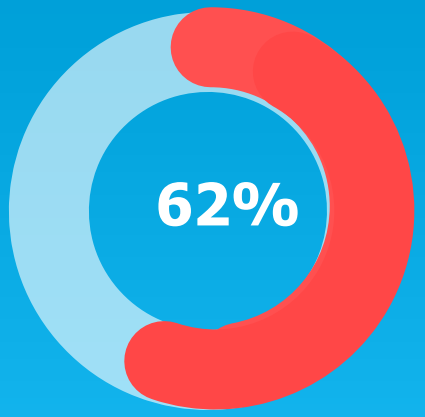
Porcentaje de usuarios de internet atacados en 2017

AUSAPE

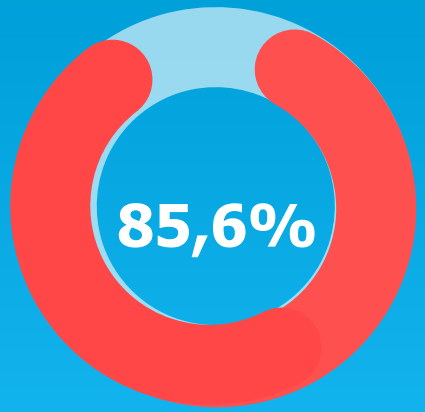
No solo afecta a IT, afecta a gobiernos, corporaciones y personas físicas



De las empresas confirma que **los riesgos han aumentado** a pesar de aumentar la inversión en seguridad



Registró **ataques o deficiencias** de control en los últimos meses



Reportaron un **incremento en las amenazas** de seguridad

$4,38 millones

En 2017 de media en **daños en compañías de la UE** con más de 1.500 empleados

Datos de ataques a nivel mundial

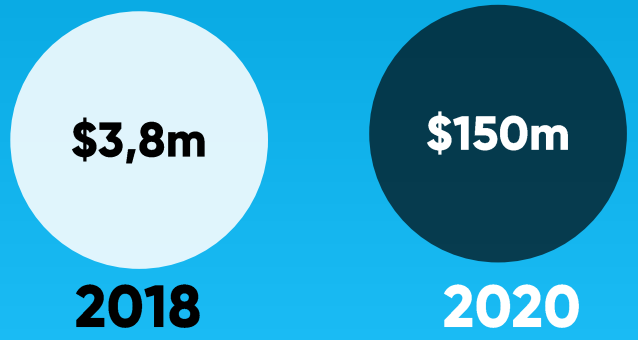
2.500 millones de fugas de información en 2017
(Breach Level Index-BLI)

7.125.940	por día
296.914	por hora
4.949	por minuto
82	por segundo

+88
que en 2016

Coste de las fugas de información en 2017

Coste medio de una sola fuga de información:



Crecimiento de ransomware

Estos ataques van en aumento, se han incrementado un **36% en los últimos 12 meses** y un **266% la cantidad demandada por criminales**

- Estadounidenses dispuestos a pagar un rescate para recuperar sus datos
- A nivel global dispuestos a pagar un rescate para recuperar sus datos

Ataques por día

4.000

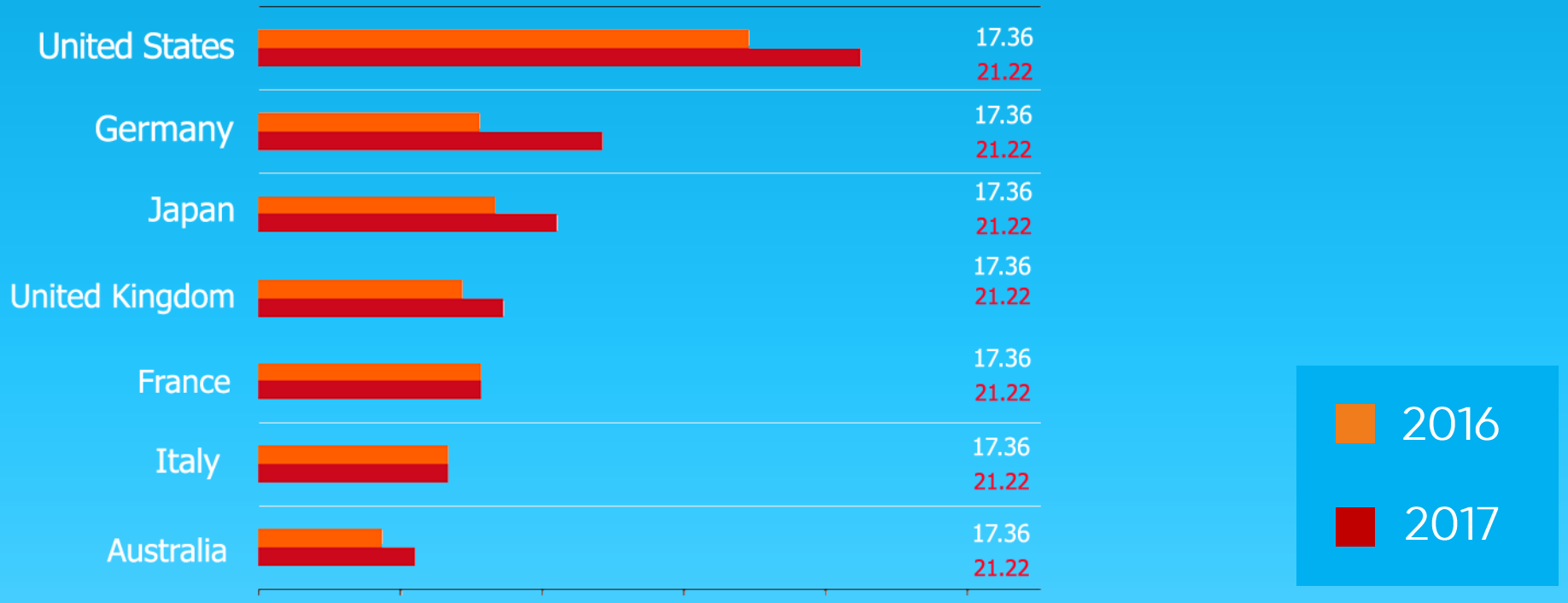
Coste medio ataque

$1.077

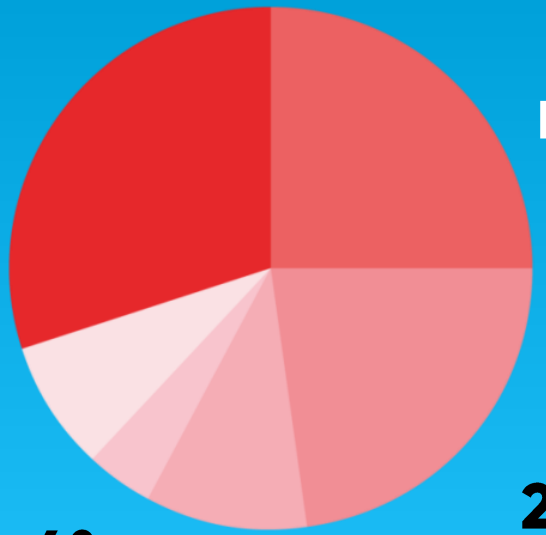
AUSAPE

Coste de ataques a nivel mundial

- **500.000 millones:** Estimación del coste total del cibercrimen en la comunidad global
- **3,8 millones:** Coste medio por compañía de una fuga de información
- **158.000 millones** perdieron los consumidores debido al cibercrimen



Coste de ataques a nivel mundial



30%
Pérdida de productividad
Para el usuario IT y final
$1.503.180

25%
Tiempo de
Inactividad del sistema
$1.252.650

Daño a la reputación
$400.848

8%

Demandas, multas y
acciones regulatorias
$400.848

4%

10%

Daño a la
Infraestructura
$501.060

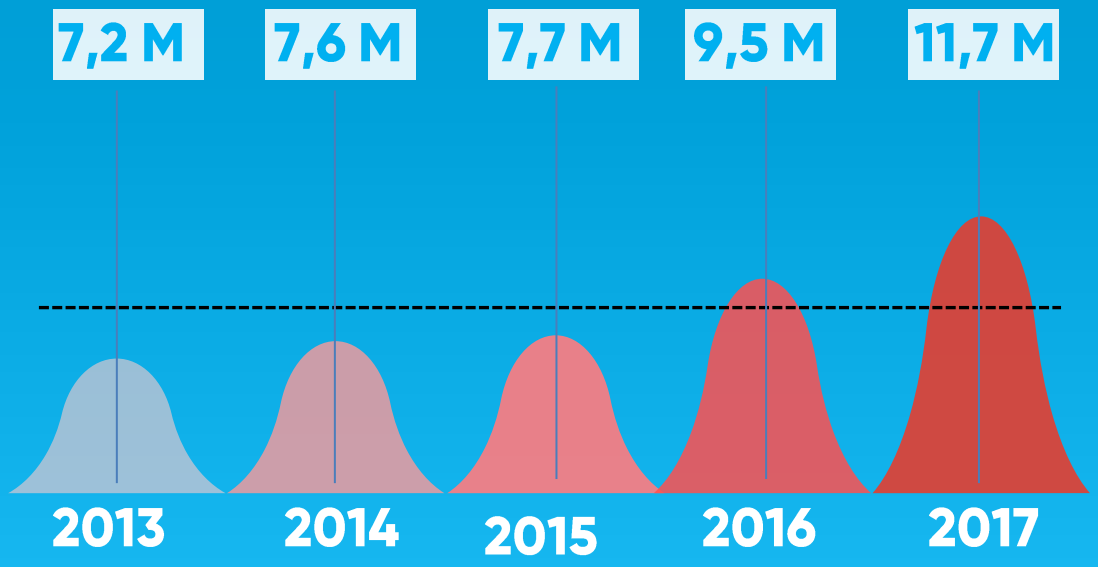
23%
Robo de activos
de información
$1.152.438

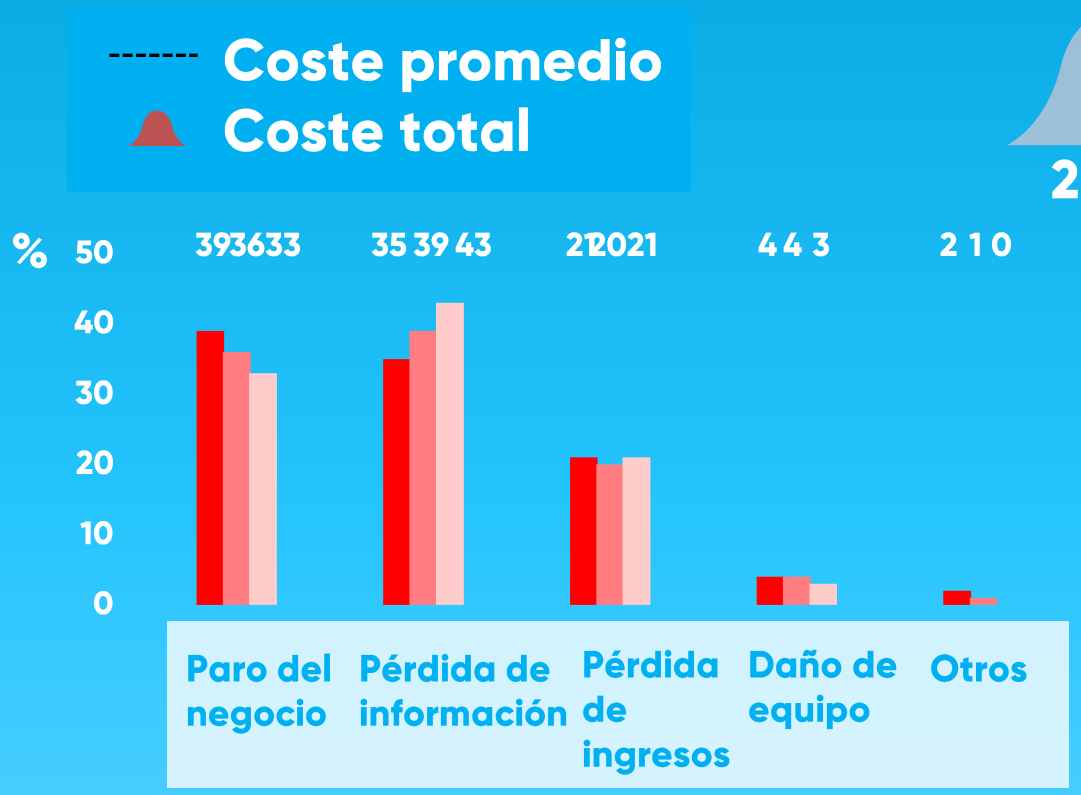
Coste de los ciberataques según el área afectada

AUSAPE

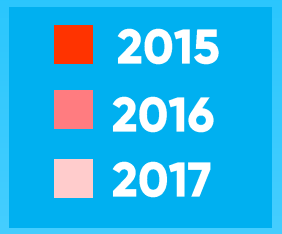
Coste de ataques a nivel mundial

Coste de los ciberataques en los últimos 5 años (US $)



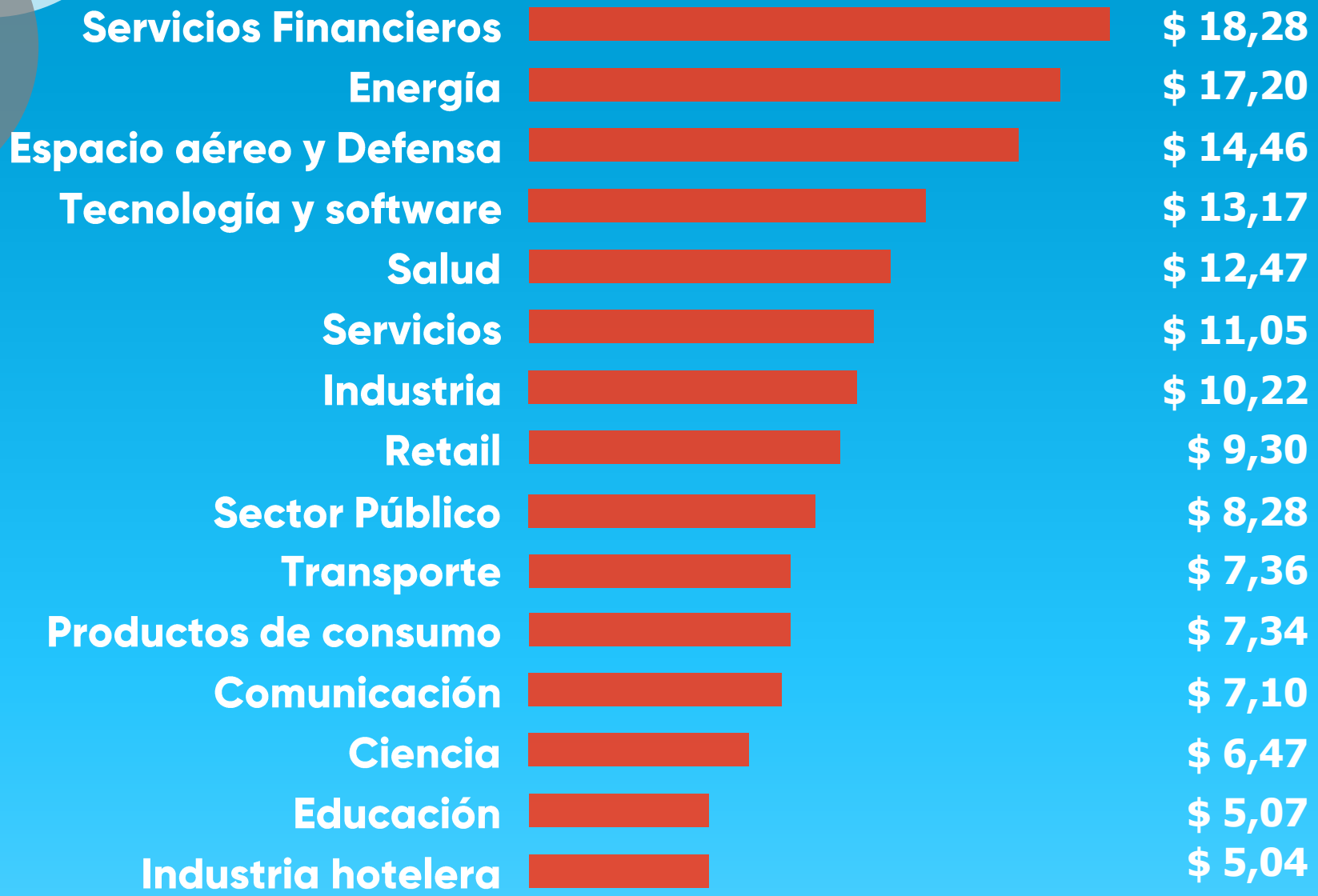


Coste de las consecuencias de los ciberataques en los últimos 3 años



AUSAPE

Datos de ataques a nivel mundial – por sector



Coste total anual $

Basado en 254 compañías.

AUSAPE

Datos de ataques a nivel nacional

18.000	2014
50.000	2016
123.064	2017

Incidentes de seguridad

El incidente más común es la infección del equipo a través de **malware o programa informático malicioso**

2.425	18.111	49.924
Incidentes de **ransomware** resueltos correctamente	**Notificaciones a terceros** para su implicación en investigación y resolución de incidentes	Nuevas **vulnerabilidades**

338	491
Incidentes diarios	**Avisos de seguridad**

AUSAPE

Datos de ataques a nivel nacional con respecto a la UE

Países Bajos cuenta solo con un **6%**, y **Croacia** el mayor % con un **40**

El **25% de los usuarios sufrió un ataque** en España, frente al 21% en la UE

España 25%

UE 21%

España se encuentra, con un 40% de probabilidad, entre los 5 países con **más riesgo de Ciberataques**, junto con Malta, Grecia, Rumanía y Eslovaquia.

AUSAPE

Coste de ataques a nivel nacional

España es el tercer país más atacado del mundo

(Es probable que sea porque otras naciones omiten información)

75.000 €

De **coste para las empresas,** según el Instituto Nacional de Ciberseguridad

14.000.000 €

Coste medio de un ciberataque

480

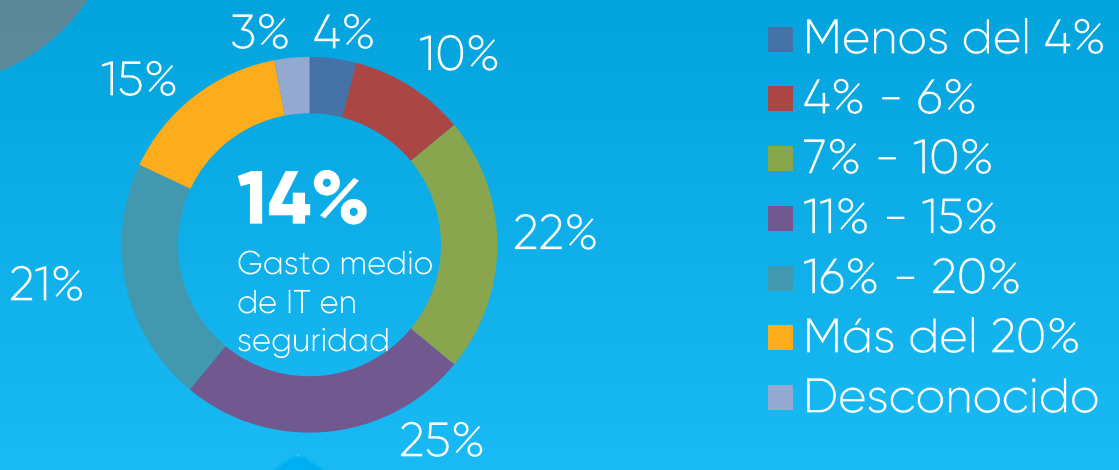
Ataques a infraestructuras críticas (aeropuertos, hospitales, centrales eléctricas, etc.) en 2016.

El **INCIBE** estima que cada día son **atacados** entre **100.000 y 120.000 equipos en España**

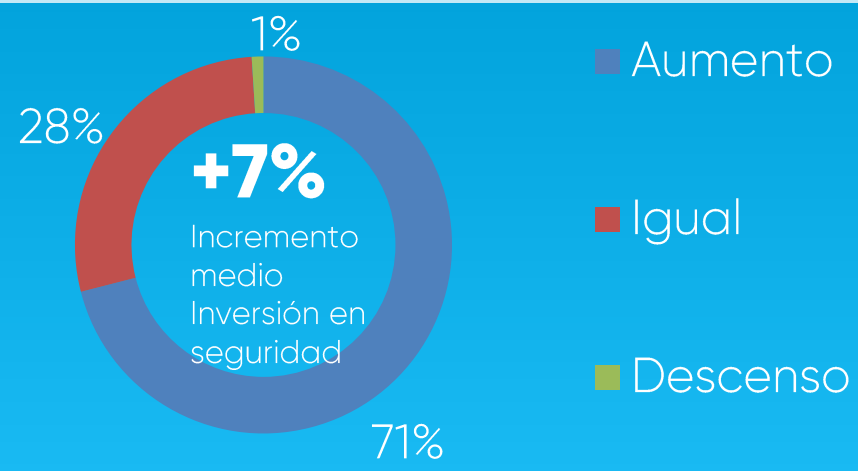
AUSAPE

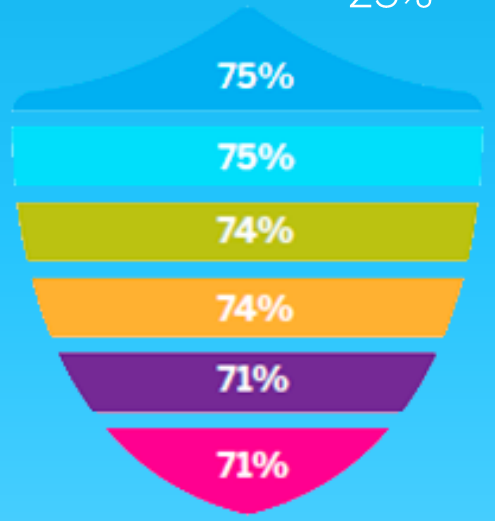
Gasto de IT en seguridad a nivel mundial y a nivel nacional

Cambios en los presupuestos en 2017



Presupuesto gastado en seguridad





Servicios de seguridad gestionados
Plataformas de detección de amenazas
Herramientas de ciberriesgo
Analítica avanzada de seguridad
GRC de nueva generación
Herramientas de gestión de incidentes

Áreas de seguridad que despiertan un mayor interés

AUSAPE

Gasto de IT en seguridad a nivel mundial y a nivel nacional

En **España** IDC prevé que en el año 2019 **el 50%** de la operativa de **seguridad** se gestione con servicios **en la nube**

Seguridad

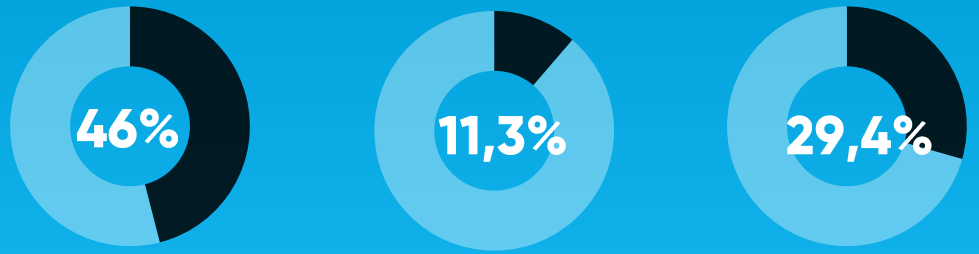
Regulación

En 2019 el **50%** de las empresas españolas habrá adaptado su **infraestructura** de cara a cumplir con las **regulaciones de seguridad** y protección de datos

AUSAPE

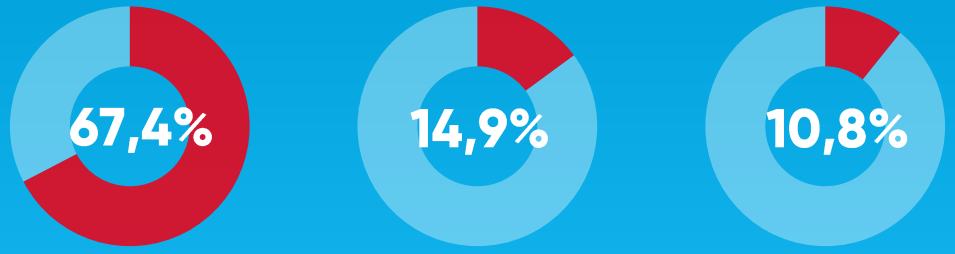
Dónde o qué se ataca – Por tipología de ataque

Orquestados por:



Cibercriminales | Organizaciones gubernamentales | Empleados

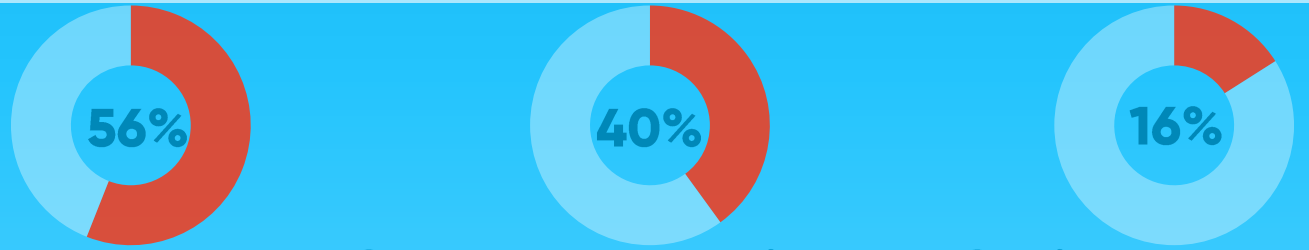
Tipología de ataques:
(De acuerdo con INCIBE)



Malware | Accesos no autorizados | Fraudes

El **spam malicioso** que sigue con vida en la Red gracias a la ingeniería social, las denegaciones de servicio, los escaneos de redes y sistemas y los intentos de robo de información

Preocupaciones de las empresas:



Temen por su infraestructura | Creen que su propiedad intelectual es vulnerable | Gobiernos y agencias de inteligencia entre los atacantes

AUSAPE

Dónde o qué se ataca – Por industria

54%

de las compañías sufrieron **ataques a su infraestructura crítica** en 2017

91%

de los ataques empezaron por un correo electrónico (**phishing**)

AUSAPE

Ataques en SAP

- Red
- Base de datos
- Front-end
- Código Z
- Mantenimiento y actualización
- Cambios en configuración
- Comunicaciones
- Seguridad y accesos
- Usuarios y gobierno de accesos
- Accesos de emergencia

70 países

220 subsidiarias

77.000 usuarios finales

95.000 ordenadores

8.500 sistemas SAP

30.000 servidores

Dispositivos móviles

10.000 ataques diarios

AUSAPE

Ataques en SAP

SAP entiende la seguridad como una responsabilidad compartida con sus clientes. SAP incluye los mejores estándares de seguridad en el desarrollo de sus aplicaciones. SAP ayuda a responder la pregunta **¿Qué puedo hacer para asegurar que el sistema sigue siendo seguro?**

AUSAPE

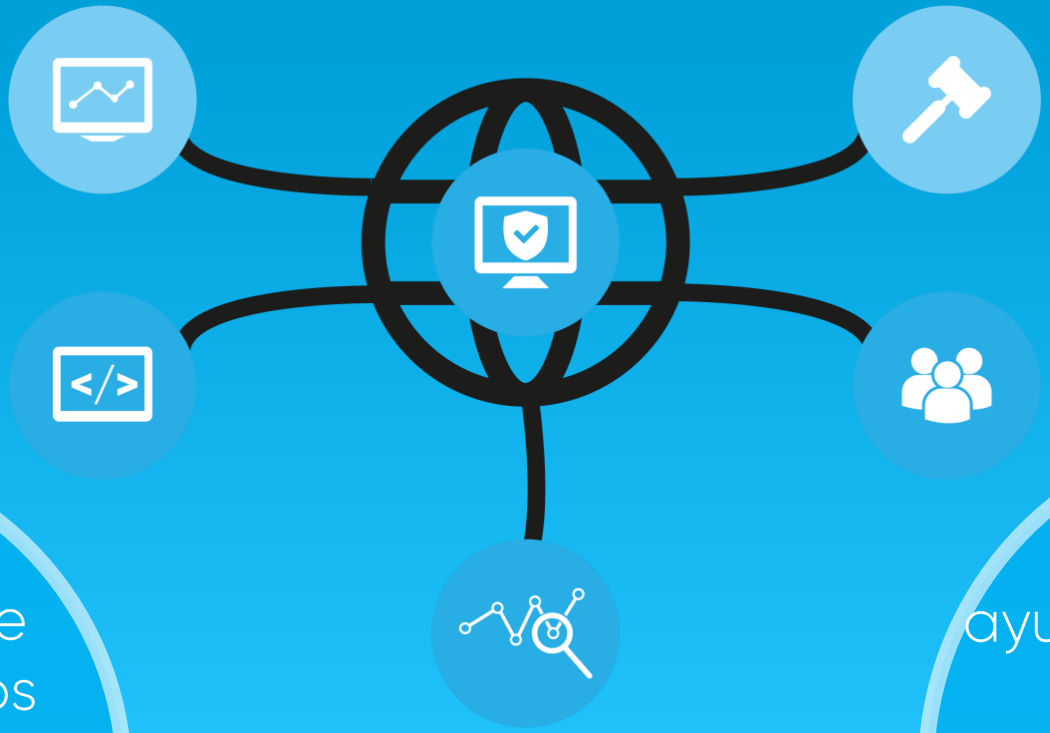
Ataques en SAP

La seguridad es una responsabilidad compartida

Soluciones SAP

Servicios IT

Desarrolladores IT



Cumplimientos y procesos legales

Usuarios

Analytics

Dependiendo de dónde existan los riesgos, SAP dispone de un portfolio de **seguridad IT y de compliance**

Estos productos ayudan a **proteger de ataques** a las compañías, así como los activos de información con soluciones de seguridad

AUSAPE

Recomendaciones generales

1.

Crear una buena base de

CIBERSEGURIDAD

Invertir en básicos como el gobierno y gestión de accesos, analíticas de seguridad, **innovar para detectar vulnerabilidades** y adelantarse a los hackers

2.

Dedicar mucho esfuerzo en el

TESTING

Invertir tiempo y recursos en las **pruebas** (configuraciones, nuevas conexiones, subidas de parche o versión, etc.) y **actualizaciones para identificar vulnerabilidades** y cerrar las puertas de entrada a los hackers

3.

Invertir en innovación y

ÚLTIMAS TECNOLOGÍAS

Incluye **servicios Cloud gestionados** con capacidades analíticas e inteligencia artificial, para asegurar la correcta gestión de la seguridad, y emplea las **últimas tecnologías en identificación de ciber ataques**

AUSAPE

Recomendaciones SAP

1. **Identificar los riesgos** más críticos en tu contexto organizacional
2. **Monitorizar logs** para identificar anomalías y ataques
3. Revisar el **código Z**
4. Aplicar los **parches y actualizaciones** consistentemente
5. Revisar las **conexiones e interfaces**
6. Mover los **procesos a la nube** gestionada de **SAP**

.7 Pasar de controles preventivos a **detectivos**

.8 **Monitorizar** cambios en las configuraciones

.9 Revisar **accesos críticos y transacciones** más relevantes

.10 Gobernar los **accesos** y el ciclo de la **identidad** adecuadamente

.11 Establecer **políticas y formación** de seguridad

AUSAPE

Muchas gracias

Ignacio Santillana

Javier Miyares