Telefónica: Seguridad en las Comunicaciones

Marzo 2011

Telefónica España – Grandes Clientes

Juan Miguel Velasco

Gerente de Desarrollo de Negocio

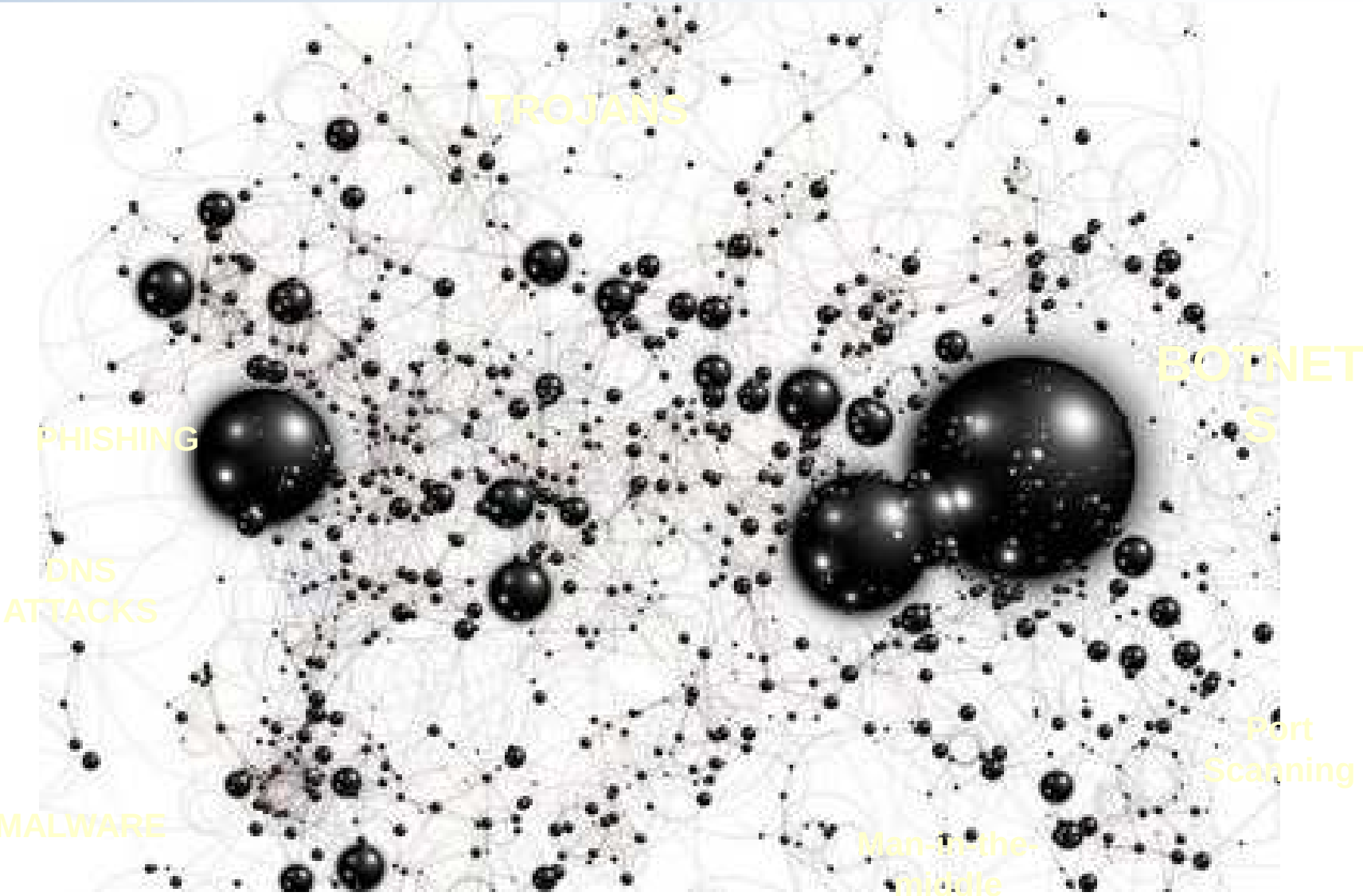
Telefónica

Índice

01

Que hay en la red?

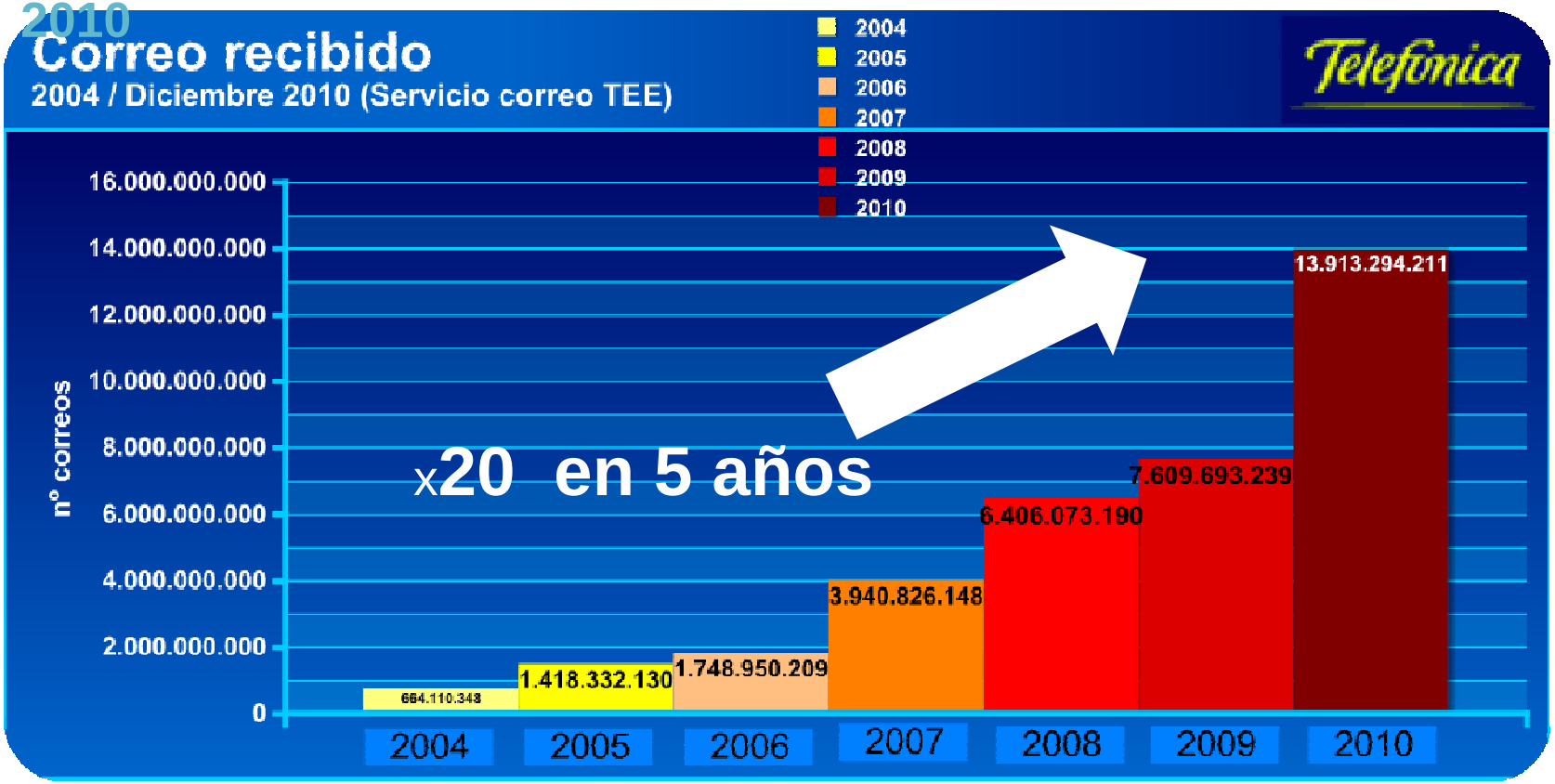
Están nuestras redes repletas de basura?




Más del 18% del tráfico en las redes IP está relacionado con los ataques, malware o tráfico no deseado ... **y más del 80%** de los ordenadores están infectados con algún tipo de malware

Servicio de Correo Limpio

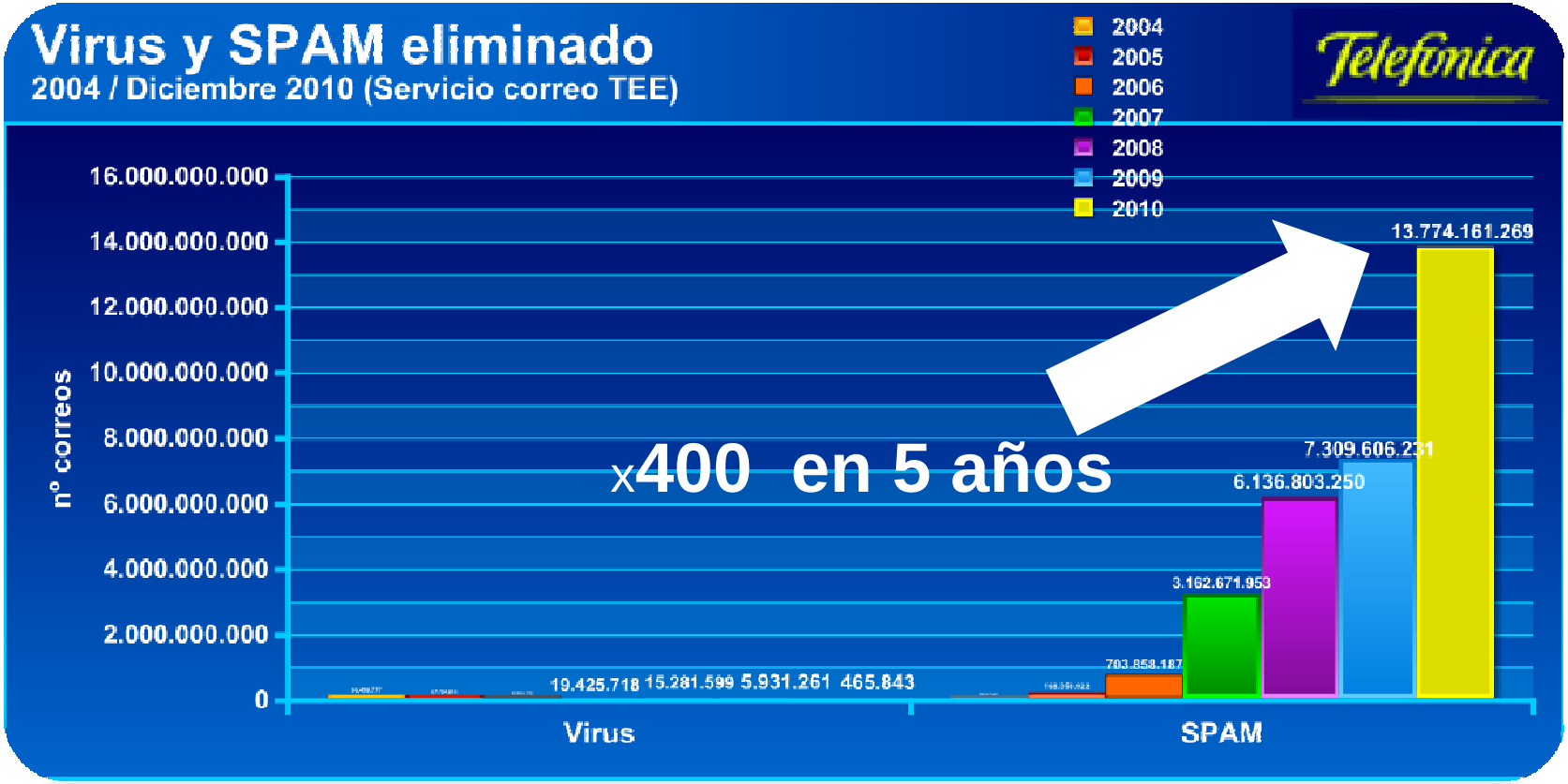
Evolución correos procesados 2004 – Diciembre 2010



A lo largo del año 2010 se confirma el ascenso en el volumen de correo procesados. Se ha pasado de 600 Mill en 2004 a casi 14.000 Mill en 2010

Servicio de Correo Limpio

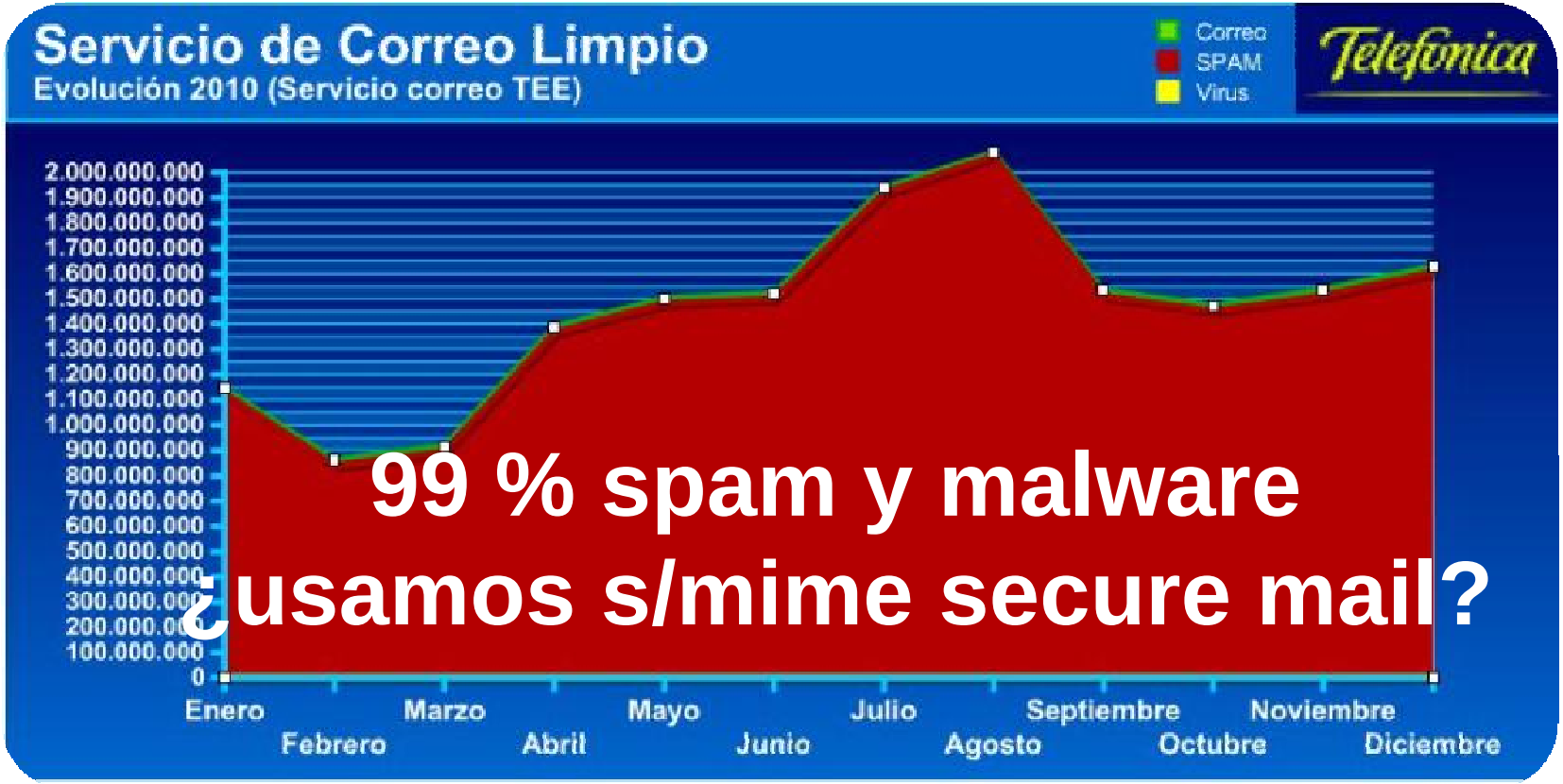
Virus y SPAM eliminado 2004 – Diciembre 2010



A mediados del 2010 el SPAM ya había superado el total del año 2009.

Servicio de correo limpio

Evolución 2010

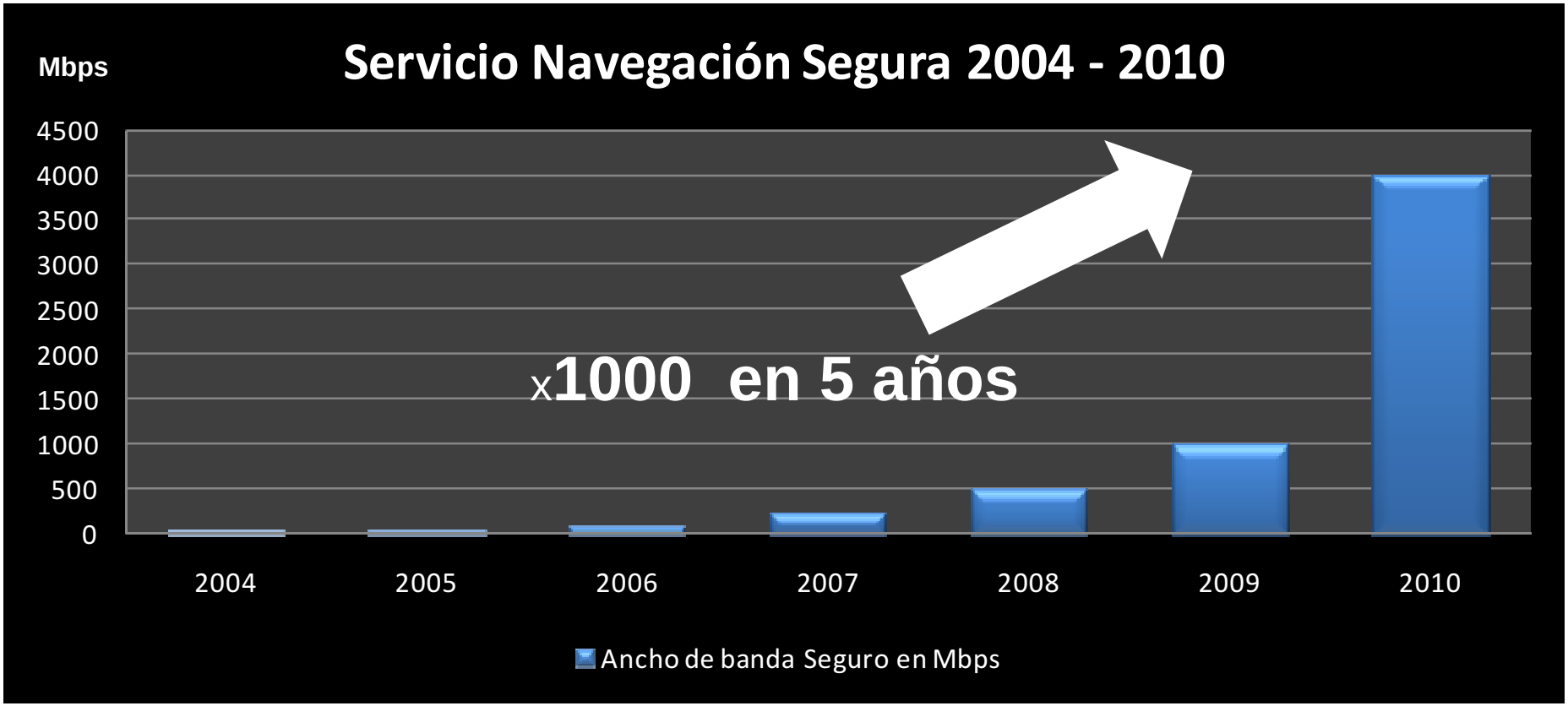


Durante el 2010 el nivel de SPAM sigue en el 99% de todo el correo recibido, aproximadamente 1 email válido por cada 100 procesados.

Sin contar reputacional IP .....

Servicio Navegación Segura

Ancho de banda gestionado 2004 – Diciembre 2010

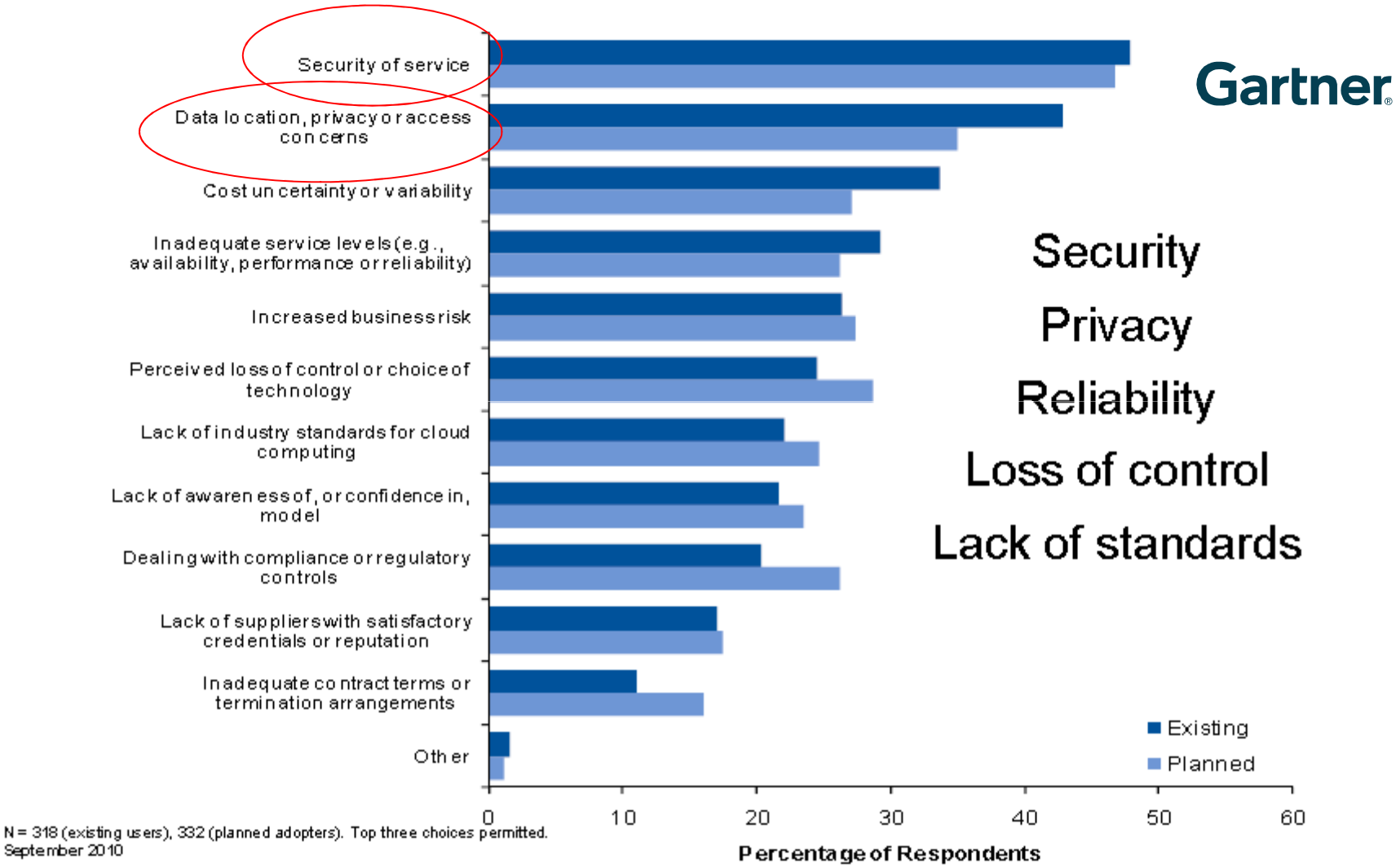


En Diciembre 2010 se alcanzó la capacidad de 4 Gbps de caudal de capacidad agregada para todos nuestros clientes de Redes Limpias o Servicio de Navegación Segura, que es más de 1000 veces la capacidad inicial del servicio en 2004

02

Objetivos y Retos de Telefónica para el 2011

Key Concerns When Adopting Cloud Computing



N = 318 (existing users), 332 (planned adopters). Top three choices permitted.
September 2010

What Control Mechanisms Does the Vendor Provide?

- Identity and access management
  - Federation, strong authentication, access and roles
  - How to verify who has access to what and who has done what?
- Data confidentiality protection
  - Encryption of data at rest and in transit
  - How do you manage encryption keys?
- Monitoring and alerting
  - DLP, IPS, SoD, DAM
  - How do you perform an audit?
- Discovery and investigation
  - How do you do forensics in multiple jurisdictions?
  - What is a business record?
  - Don't forget law enforcement access

If they don't build it in, you can't use it.

Gartner

Los retos del CLOUD Seguridad en 2011…

Proteger el Cloud y su uso seguro

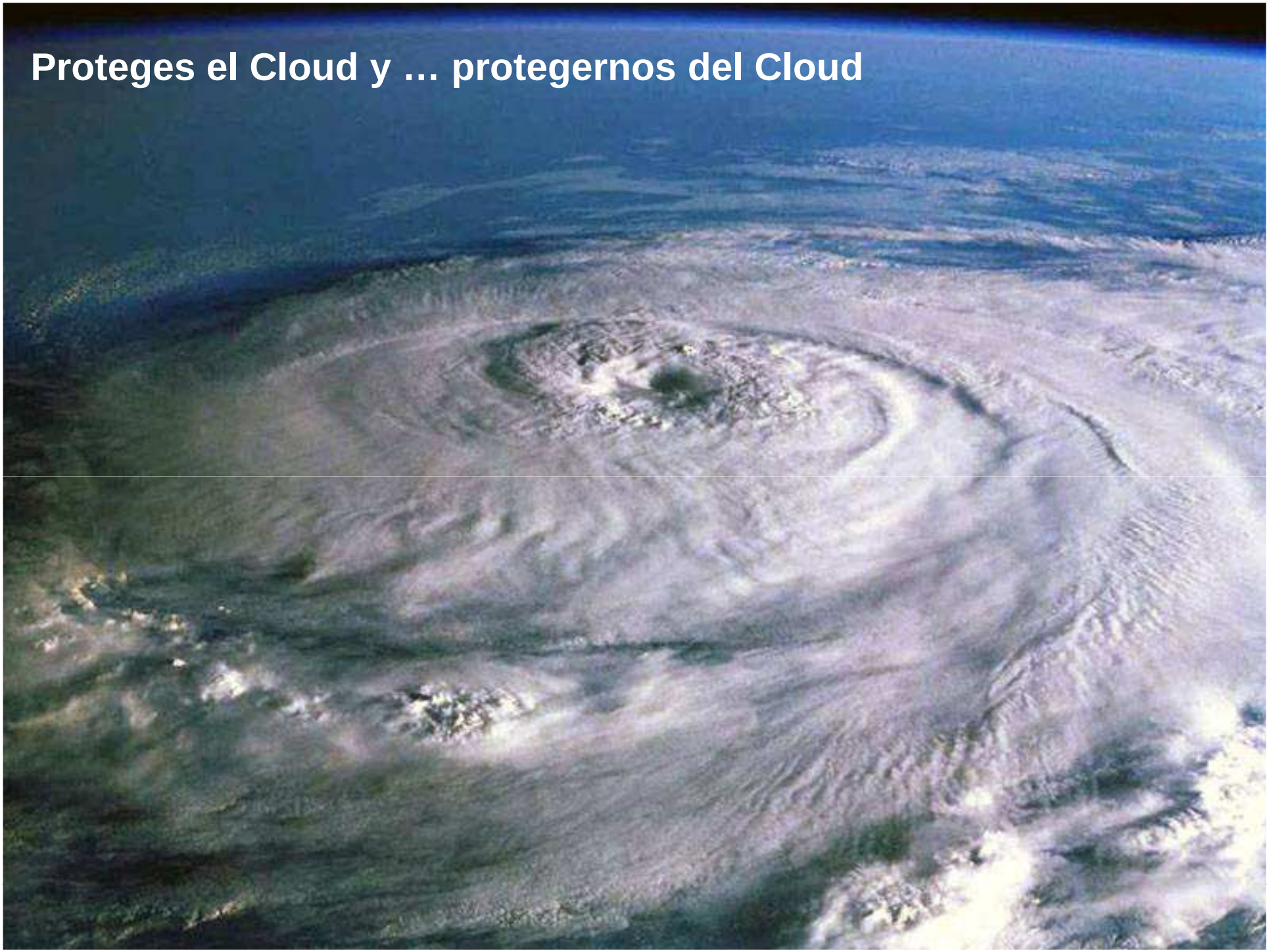
- Proteger el perimetro del Cloud
- Controlar los datos y la información que manejan los proveedores Cloud
- Cumplir con la Legislación local y la multi-regional cuando se usan servicios Cloud
- Inversión o gasto en el Cloud, cambio del modelo de gestión
- Control, administración, reporting , provisionning y billing en Cloud
- Gestionar los SLAs del Cloud

…usar el Cloud para nuestra protección ...

El Cloud Seguridad y protegernos del Cloud

- Servicios de Redes Limpias maduros multidispositivo, ubicuos, rápido despliegue, poca inversión y pago por uso
- Inteligencia en RED, utilizar la compartición anónima de información de fraude, ataques y correlación -> Correlación en Cloud.
- Servicios Seguridad virtual dentro del perímetro de servicios Cloud de infraestructuras
- Protección de ataques en Cloud -> sólo con Servicios de Seguridad
- El uso del “bad cloud” , botnets, DDoS, hacking, phishing, smishing, etc.

Proteges el Cloud y … protegernos del Cloud



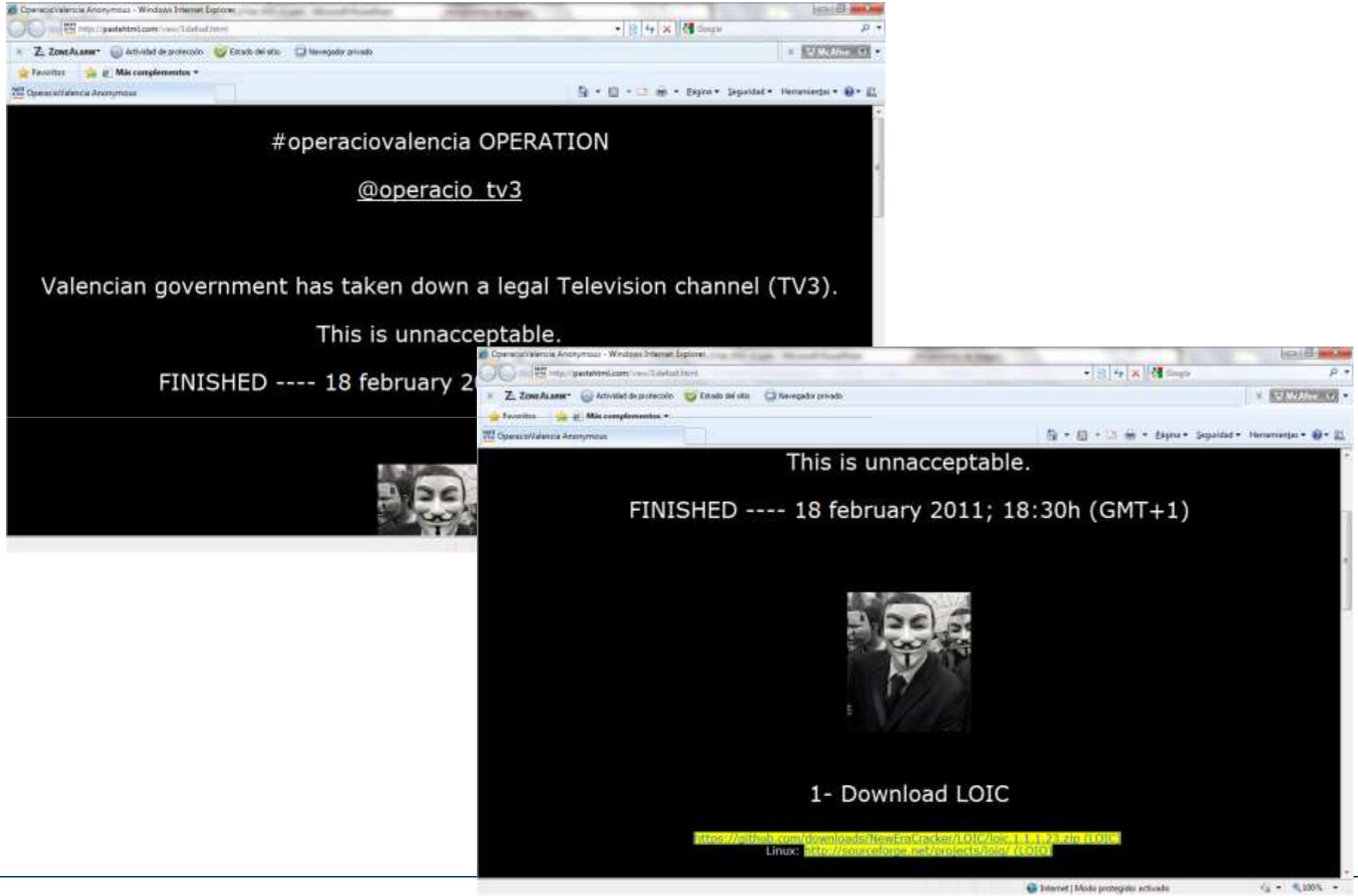
Seguridad en los servicios CLOUD

Proteger el Cloud y su uso seguro

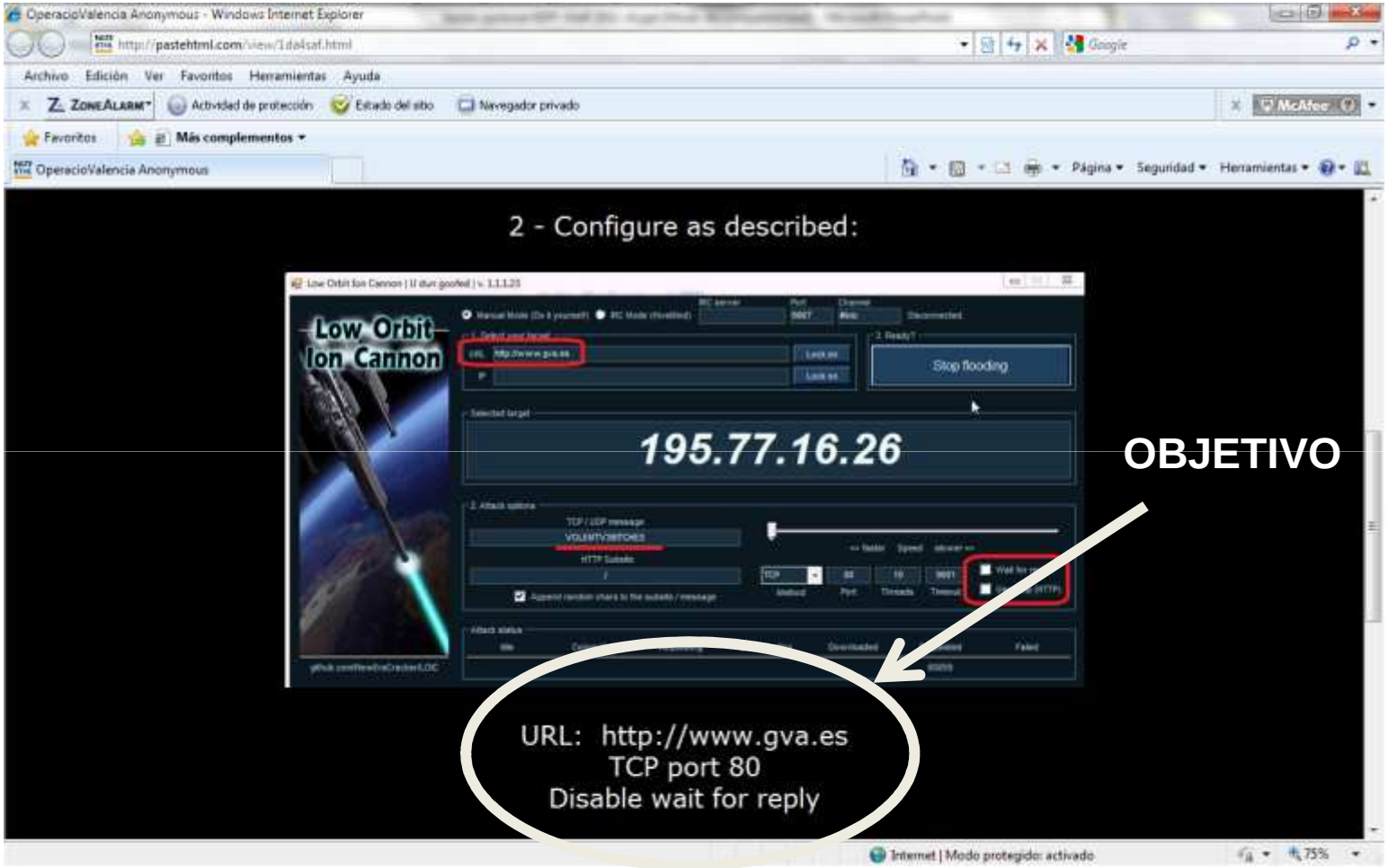
- Autenticación fuerte Cliente - Servidor
- Cifrado de datos almacenados en el Cloud
- Garantía de integridad de datos
- Procesos de firma para autenticación y contratación de servicios en linea
- Autenticación fuerte multidispositivo sobre X.509v3
- Cifrado de dispositivos móviles
- Cifrado de aplicaciones
- Sistemas de doble factor de autenticación

¿es la seguridad un inhibidor de servicios cloud?

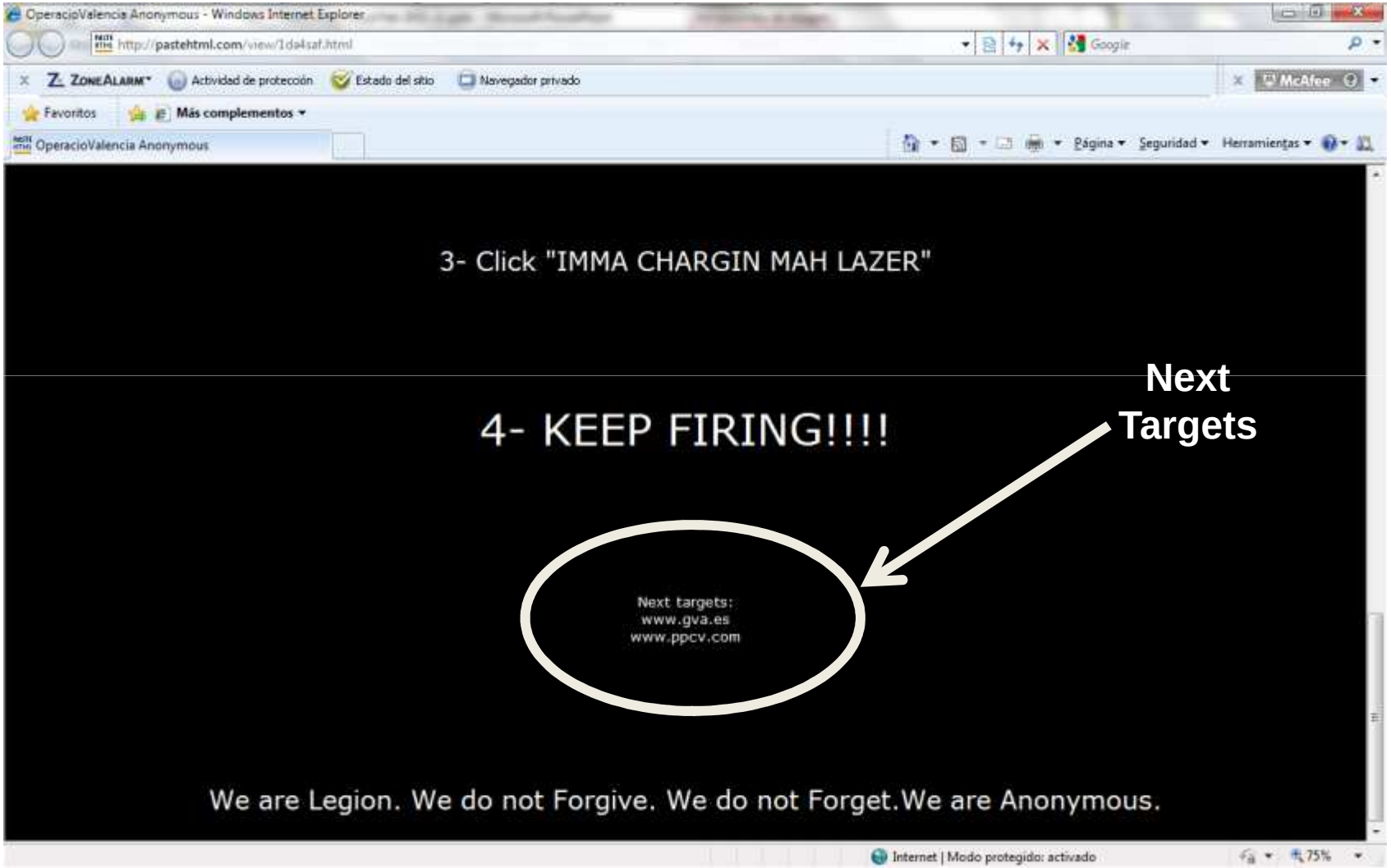
Estamos en medio…. Queramos ….



..... O no queramos y lo siguiente....



…… next steps….. Cualquier! Cualquiera! TODOS!



Ataque DDoS Ideológicos

En el mundo físico:

En Internet:

- Herramientas donde sólo tienes que elegir un objetivo y hacer “click”
  - LOIC, LOIQ, JS LOIC
  - HOIC
  - GOIC

ANONYMOUS

Comunicado de Anonymous para la Operación Hipoteca

Desde An… a de los continuos abusos a… ganizan en movi- …rg/ o …dos YA!.

Asistimos … e reparten lo poco

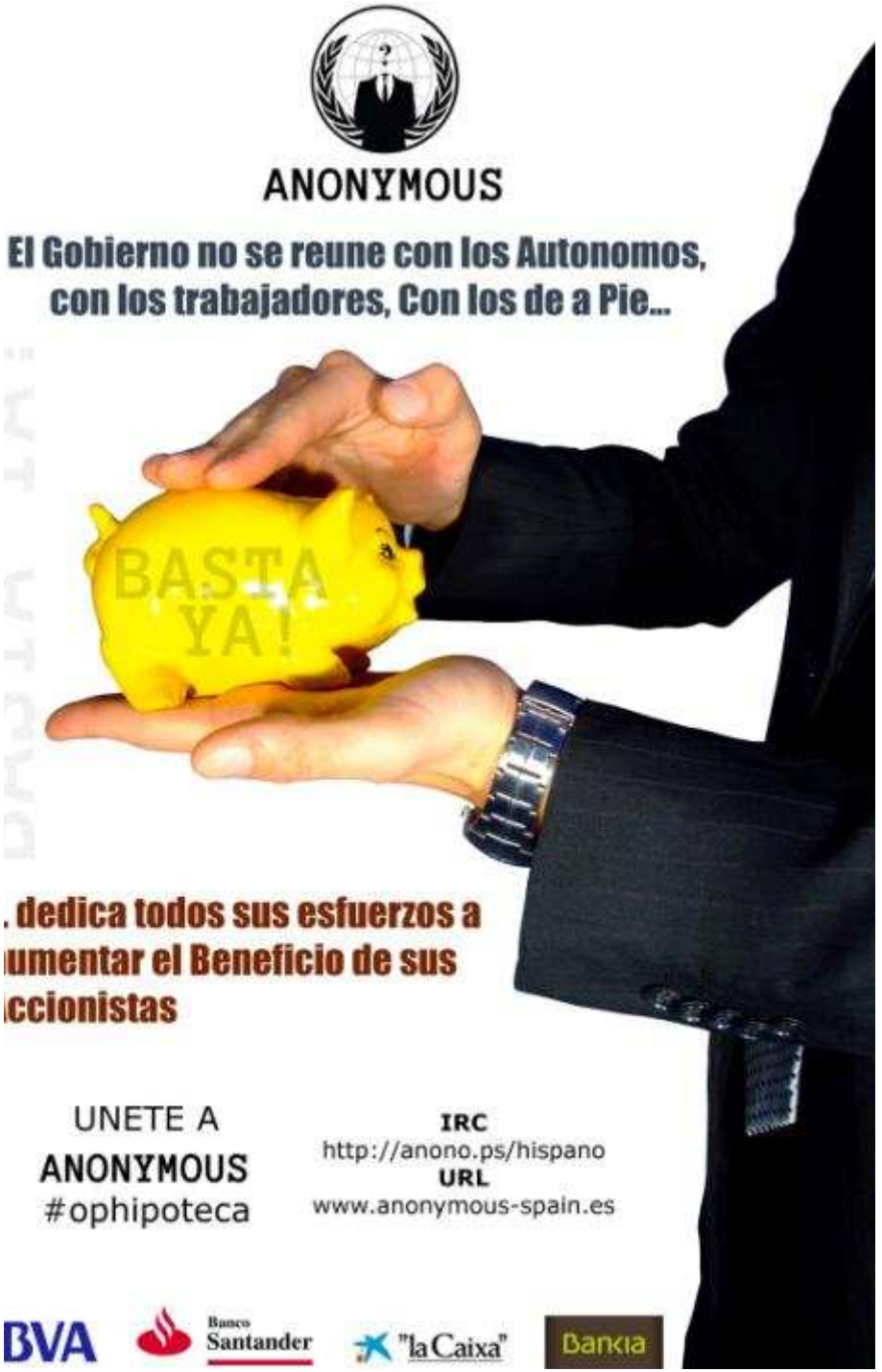
El gobier… con gente que se sienta e… …ccionistas, pero

Casos cor… er que ellos siem- pre gana… legalmente para que se… ar el importe del

Propuesta… azadas por el PP y el PSOE, l… s del pais gracias a las dac… por el dinero pú- blico en ca… a, bonito nombre.

Mientras… za la tragedia del gran núme… fono, transportes, etc., y se… ario", es decir, que para qu… que pretenden

Aún así, … dos, los politicos cuidan s… cos o privados, Aznar co… la banca respira tranquila … tengan que repar- tir el paste… tander registró un beneficio … nes y no fueron los únicos).



Y a SONY-playstation qué le ha pasado?

- Caída en bolsa por el ataque

-3,82%

- **Valor**

-1.130 Mill

Servicios y RED caídos 1 semana

VIDEOJUEGOS | PlayStation Network

Sony admite que un intruso accedió a datos de millones de usuarios de PlayStation

- Sony asegura que no hay indicios de que hayan usado las tarjetas de créd
- No obstante, ya se han dado las primeras denuncias de cargos fraudulent
- En España hay 3.000.000 de cuentas de PSN y 330.000 con tarjeta de crédi

Detalle del tráfico

Tamaño de los ataques de denegación de Servicio

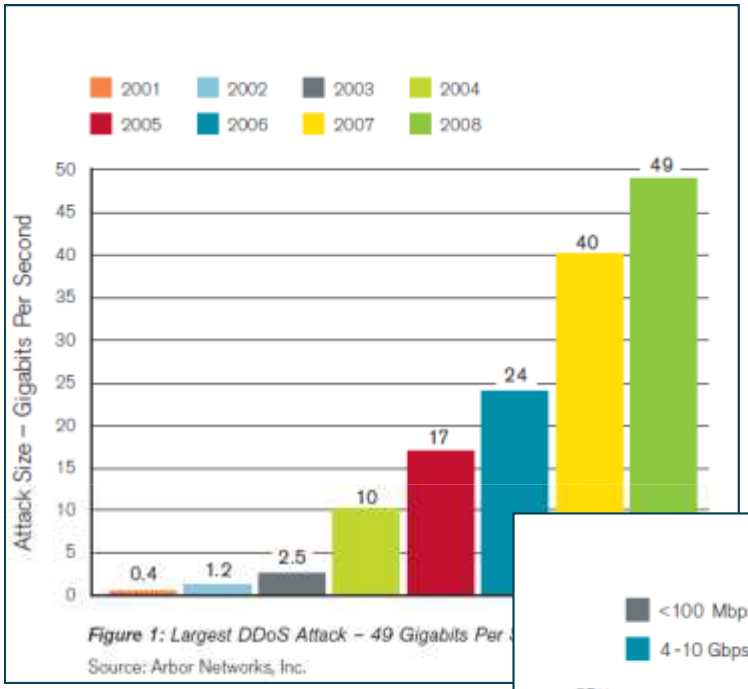


Figure 1: Largest DDoS Attack – 49 Gigabits Per

Source: Arbor Networks, Inc.

Capacidad media actual de ataque
Ataque pequeño < 25 Mbps
Ataque mediano < 100 Mbps
Ataque grande > 100 Mbps

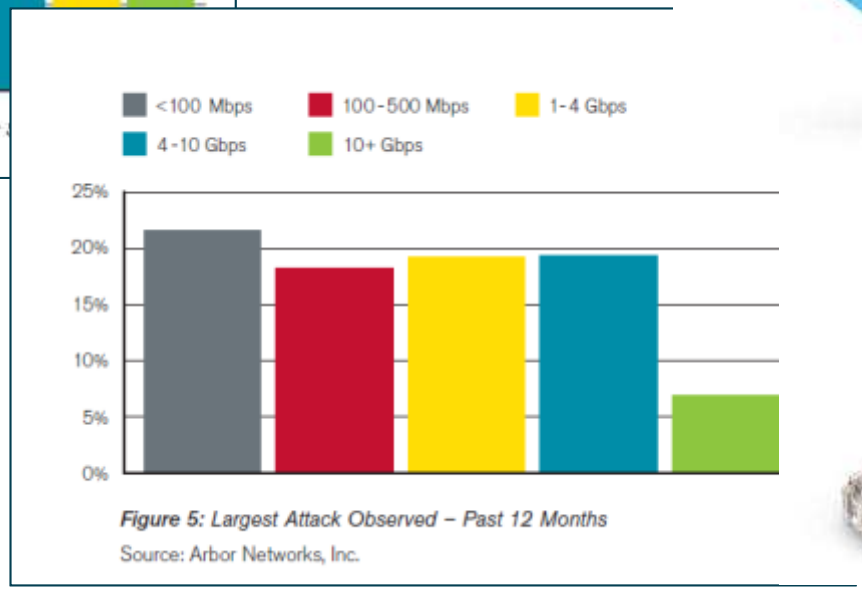


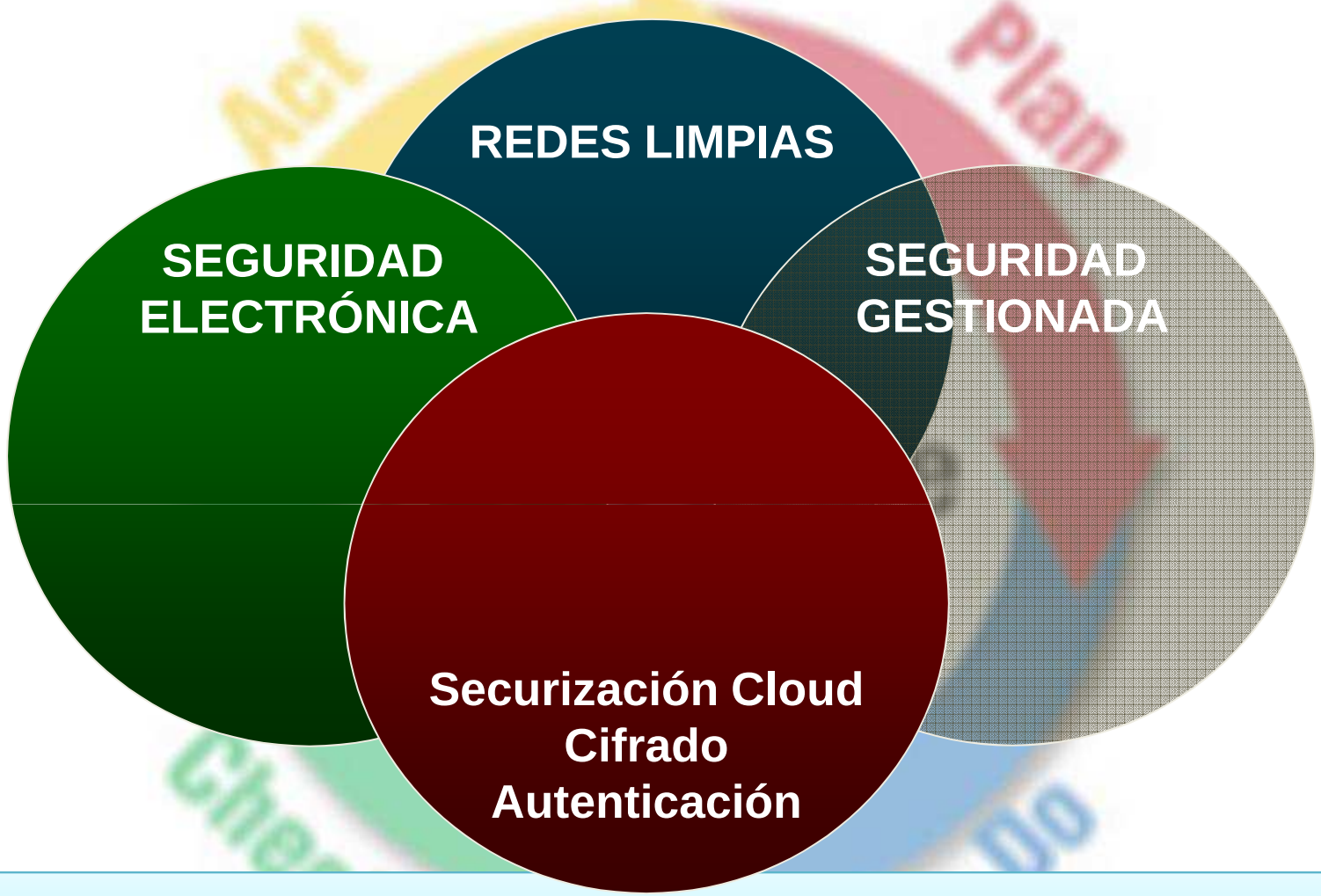
Figure 5: Largest Attack Observed – Past 12 Months

Source: Arbor Networks, Inc.

03

Conclusión

En resumen…



MIX de Servicios Remotos e INSITU / con ahorro de Costes por Gestión Integral / Integración con CGPs ORO / Apalancamiento en Comunicaciones / Apoyándonos en el CLOUD


Telefónica