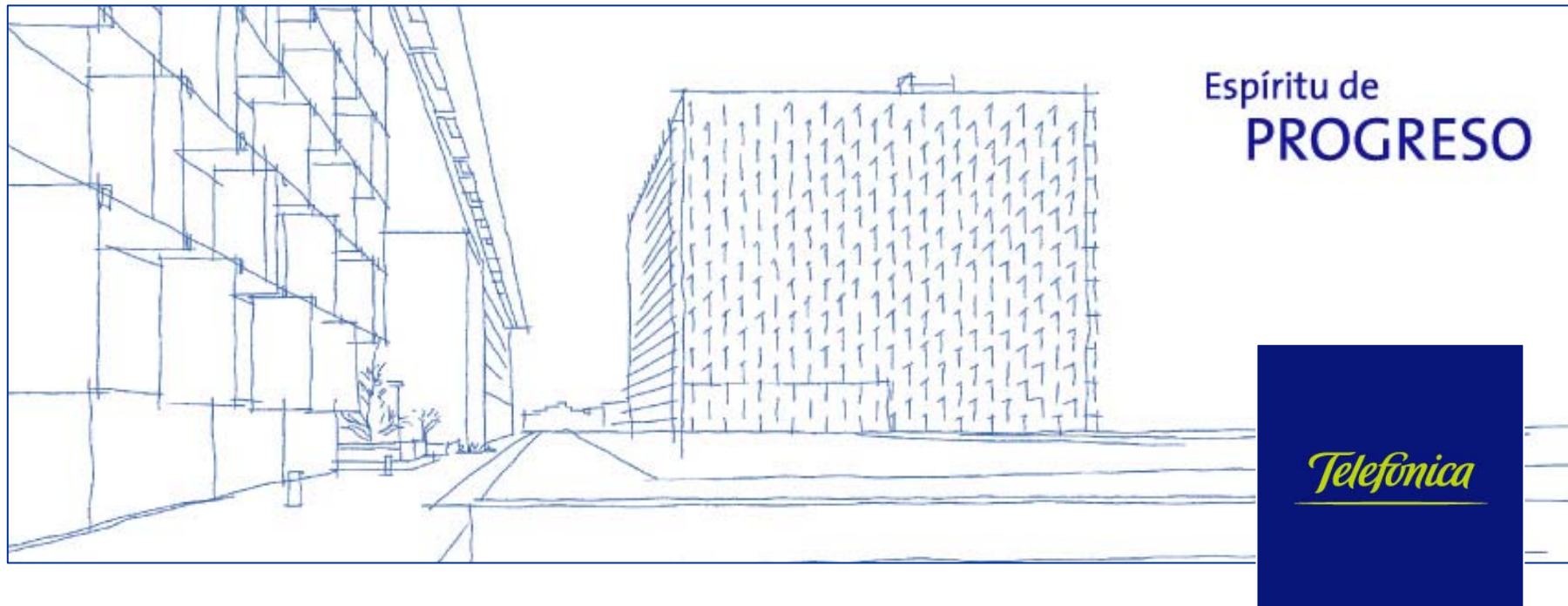


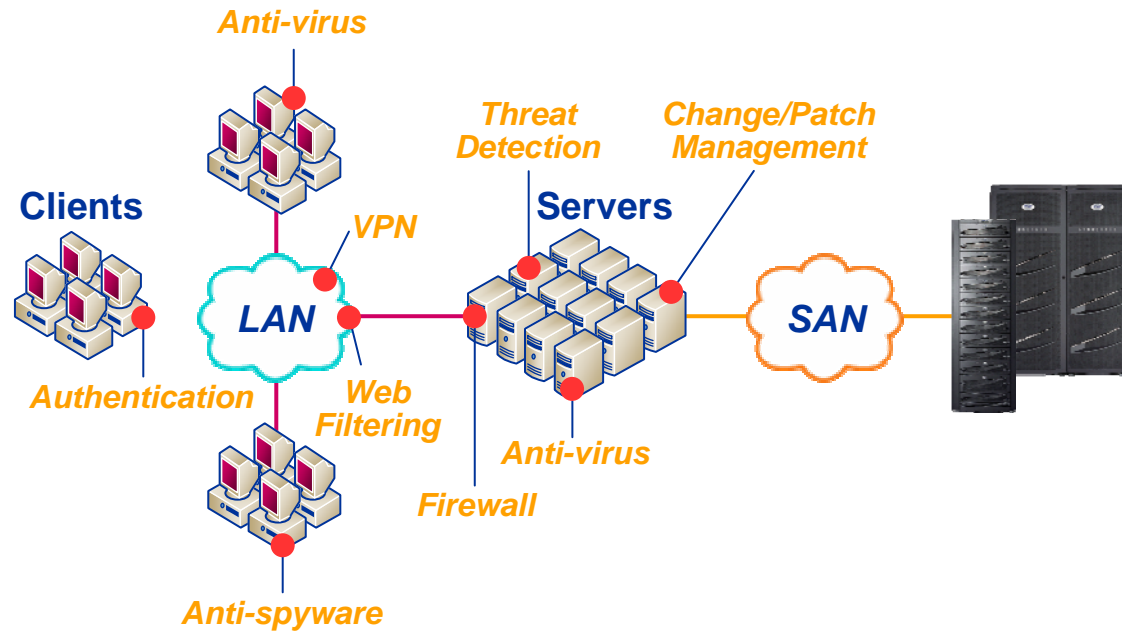
La Gestión Segura de la Información Y la Protección de los Datos *Data Loss Prevention (DLP)*

Telefónica Empresas
Seguridad
Febrero 2009



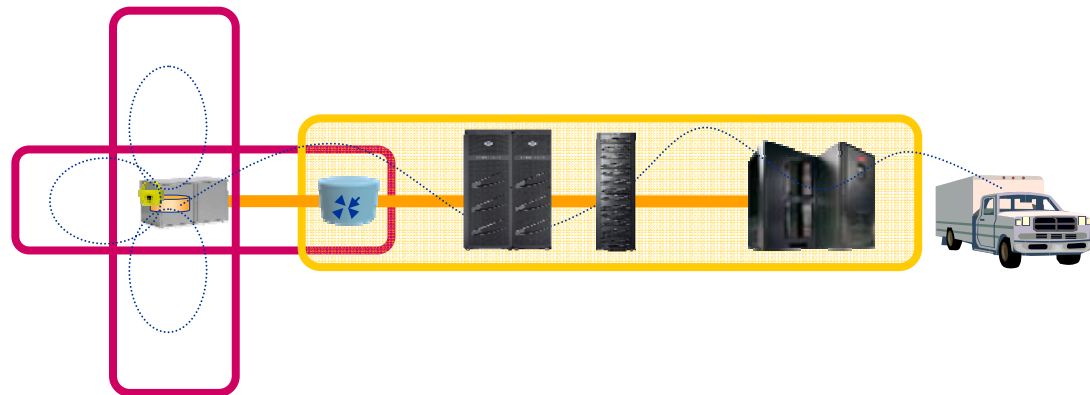
Entendiendo la amenaza

La mayoría de los productos de seguridad no protegen la información



La información está constantemente moviéndose siguiendo su ciclo de vida.

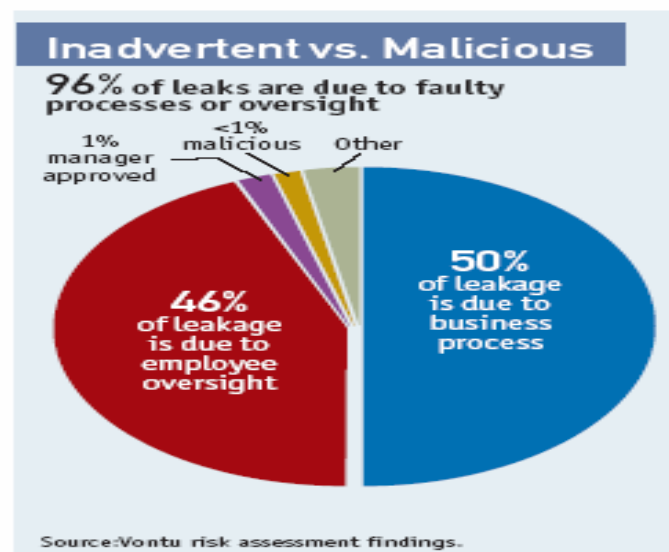
- La seguridad aplicable cambia con el tiempo



La amenaza interna

Más del 80% de fallos de seguridad se deben a incidentes internos

Bases Datos, servidores archivos, y aplicaciones de gran uso son particularmente vulnerables

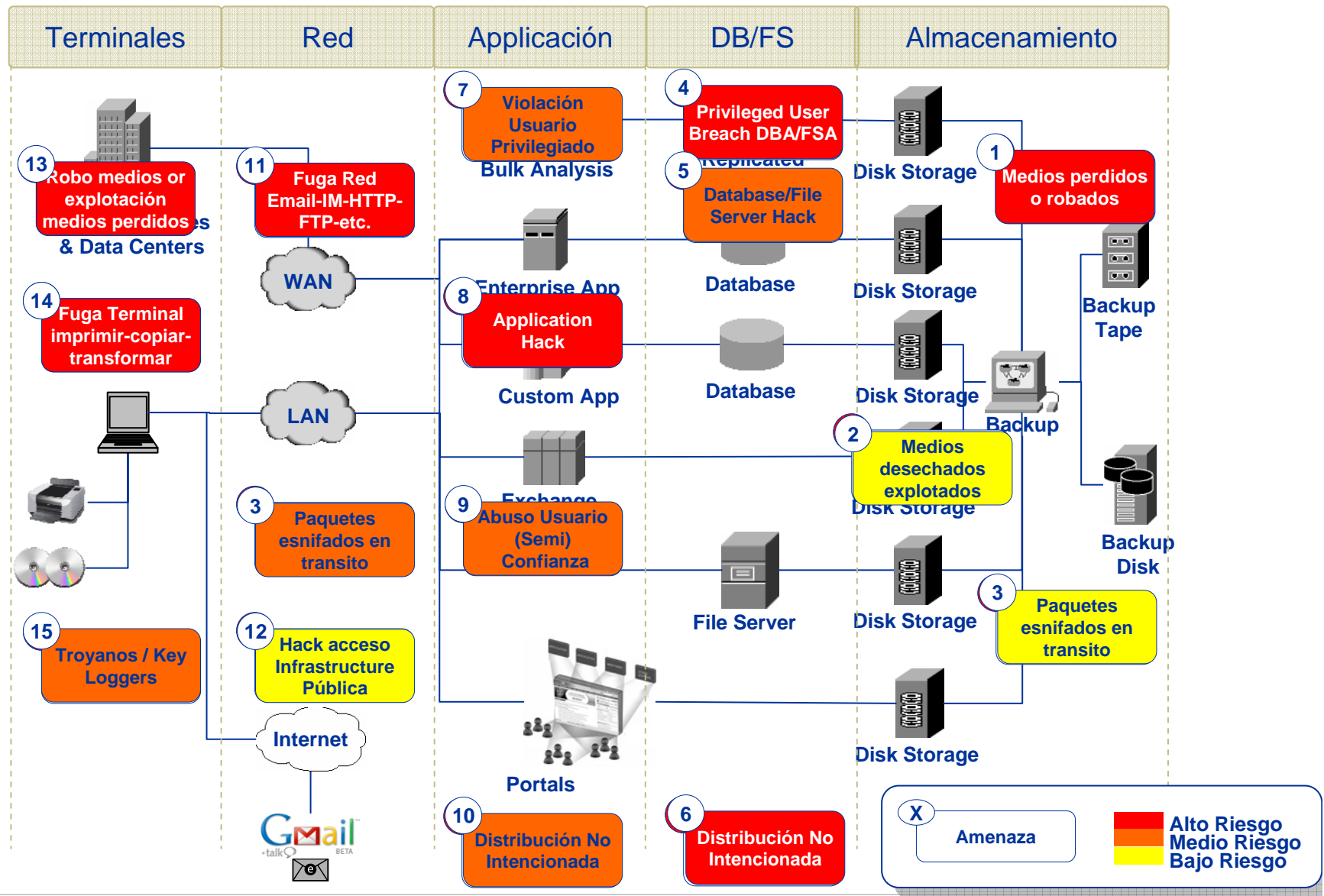


El Robo de Información es uno de los crímenes que más crece en el mundo, y a la vez uno de los más baratos de cometer

Hackear por "Fuerza bruta" un sistema desde el exterior es demasiado caro y consume demasiado tiempo

En lugar de ello, los criminales se valen de explotar **incidentes internos** para obtener la información que necesitan

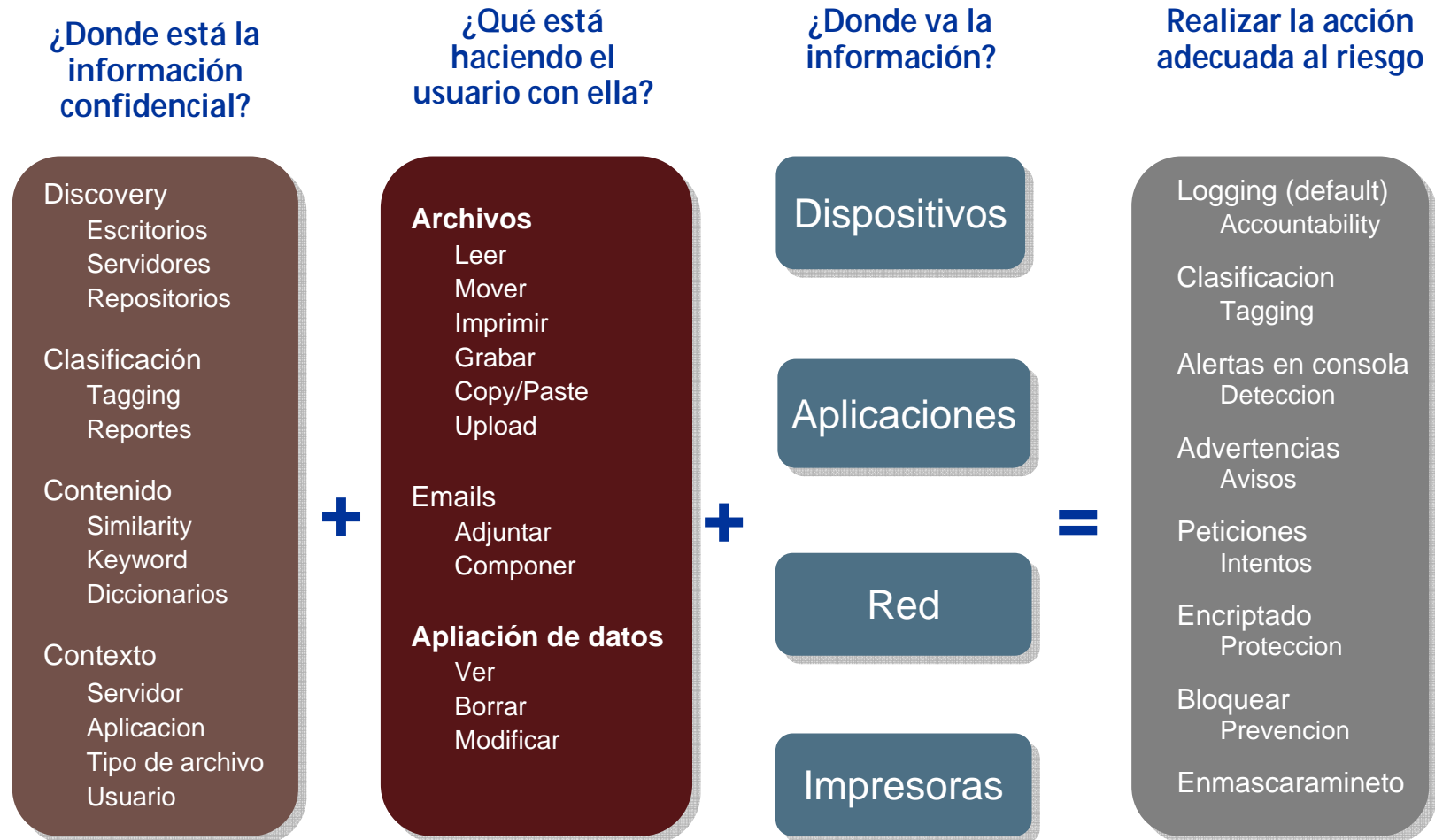
Riesgos asociados a la dispersión



El problema de la fuga de información



¿Qué es Data Loss Prevention?



¿Por qué es necesaria?

— Cumplimiento Regulatorio

Sanción a una clínica de Bilbao por la pérdida de datos de 11.300 pacientes en redes P2P

27/04/2008

TIEMPO PROMEDIO DE LECTURA 0'47 MINUTOS

La **Agencia Española de Protección de Datos (AEPD)** ha sancionado con una multa de 150.000 euros a una clínica ginecológica de Bilbao por considerar que no "ha custodiado con el debido sigilo" los datos de 11.300 pacientes que acabaron circulando por Internet.

El problema se debió a que uno de los empleados de la clínica utilizaba un programa de intercambio de archivos (P2P) lo que permitió que los archivos que incluían información ginecológica de los pacientes circulase por la Red.

En la inspección realizada por la AEPD, se comprobó que el centro médico Lasaitasuna de Bilbao, "no existían ni las garantías mínimas ya que carecía de la redacción de un documento de seguridad con las reglas mínimas, lo que resulta una negligencia inexcusable por la que se impuso una sanción relevante de 150.000 euros por vulnerar el principio de seguridad y haber posibilitado que terceros tengan acceso a su información", explicó el director de AEPD.

¿Por qué es necesaria?

- Prevención de pérdidas de imagen / valor marca / reputación

EL PAÍS edición impresa | INTERNACIONAL

Lunes, 24/11/2008

ELPAÍS.com > Tecnología

El gobierno británico pierde un ordenador a la semana

Una investigación evidencia que la pérdida de equipos informáticos es habitual en la administración inglesa

ELPAÍS.com - Madrid - 23/11/2008

ELPAÍS.com > Tecnología

Una memoria USB con datos confidenciales del Gobierno británico acaba en el aparcamiento de un bar

El 'pen drive' contenía datos relativos a las devoluciones de Hacienda o multas de tráfico

EFE - Londres - 03/11/2008

Vota

Resultado ★★★★★ 25 votos



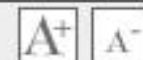
Las autoridades británicas han lanzado una investigación sobre cómo un dispositivo de memoria USB con nombres y claves de entrada en un importante banco de datos del Gobierno ha podido acabar en el aparcamiento de un *pub* inglés.

¿Por qué es necesaria?

- Asegurar la Propiedad intelectual

EEUU: Morgan Stanley, UBS y Bear Sterns, denunciados por uso de información privilegiada

AGENCIAS | 11:43 - 2/03/2007

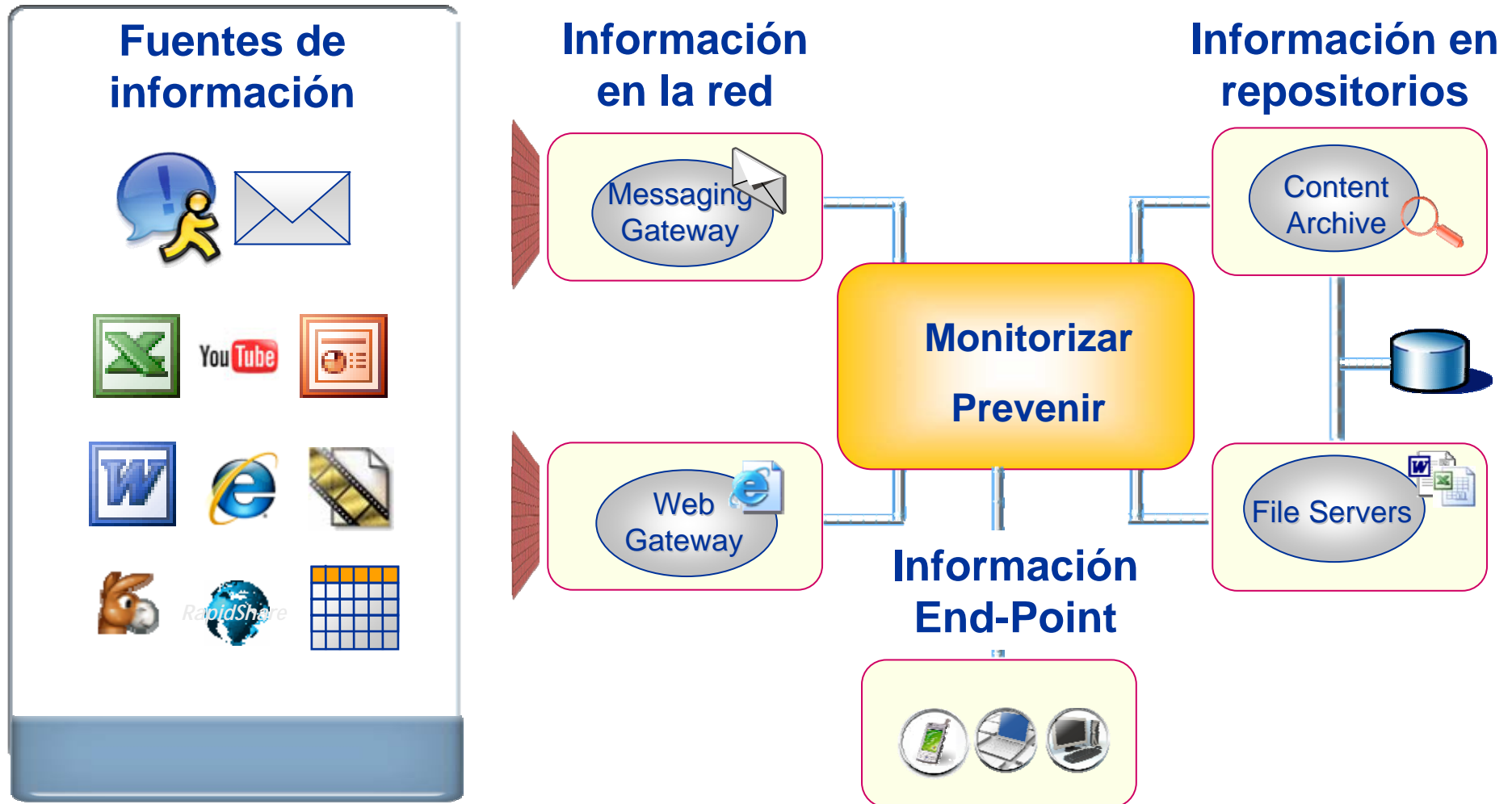


Los fiscales de Nueva York y Washington han presentado cargos criminales **contra 13 personas vinculadas a Morgan Stanley, UBS y Bear Sterns por uso de información privilegiada**. Dos estudios han confirmado que las acciones y los derivados de TXU e Hyperion se elevaron mucho las semanas anteriores a anunciar que habían llegado a un acuerdo para ser compradas. Estos casos han vuelto a incrementar las **sospechas en las relaciones de Wall Street con los hedge funds**, y algunos senadores y congresistas empiezan a exigir al regulador de los mercados que tome cartas en el asunto ante las abundantes evidencias de uso de información privilegiada.

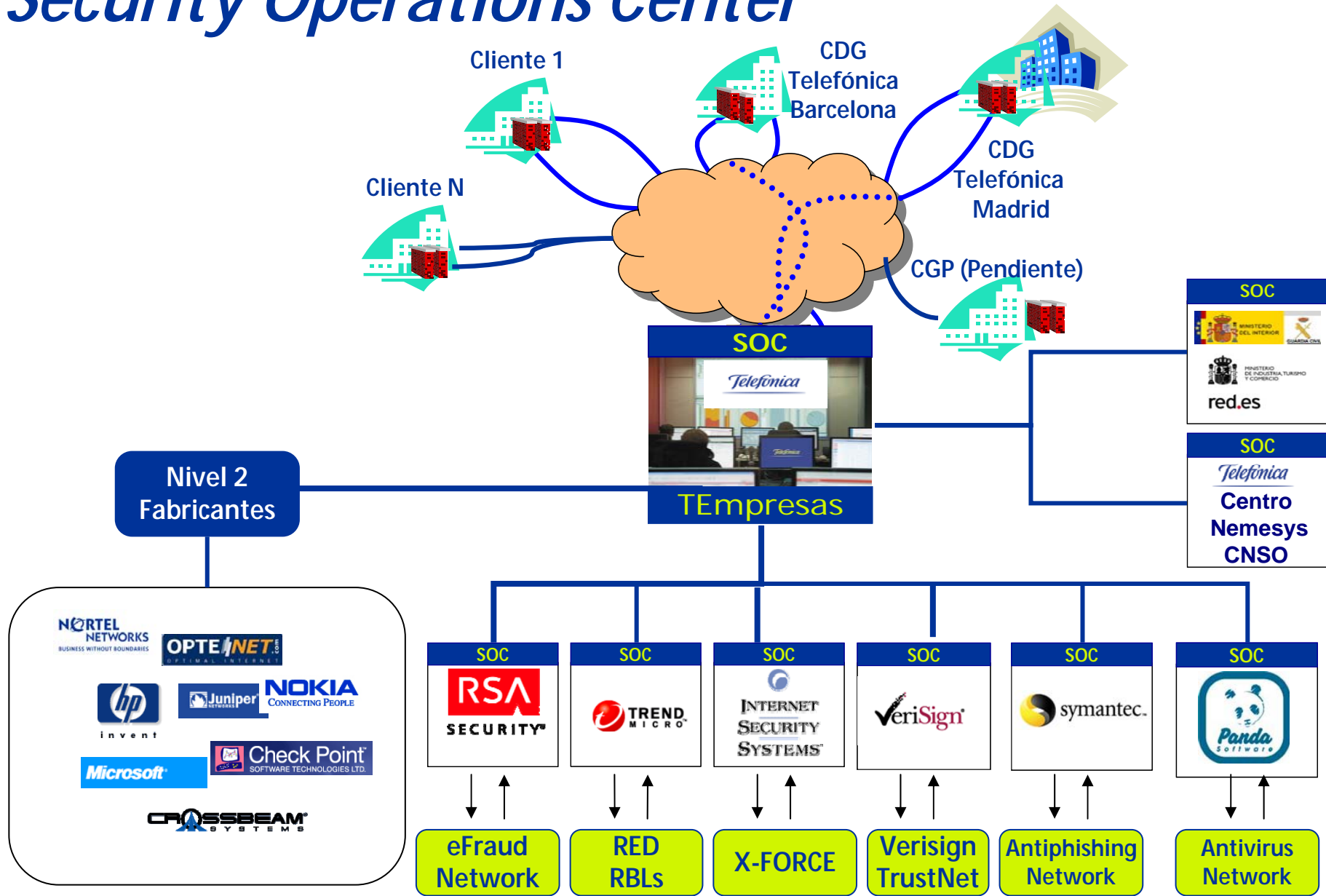
El proyecto DLP



Implantación MultiPunto



Security Operations Center



Centro de Gestión de Seguridad (SOC)



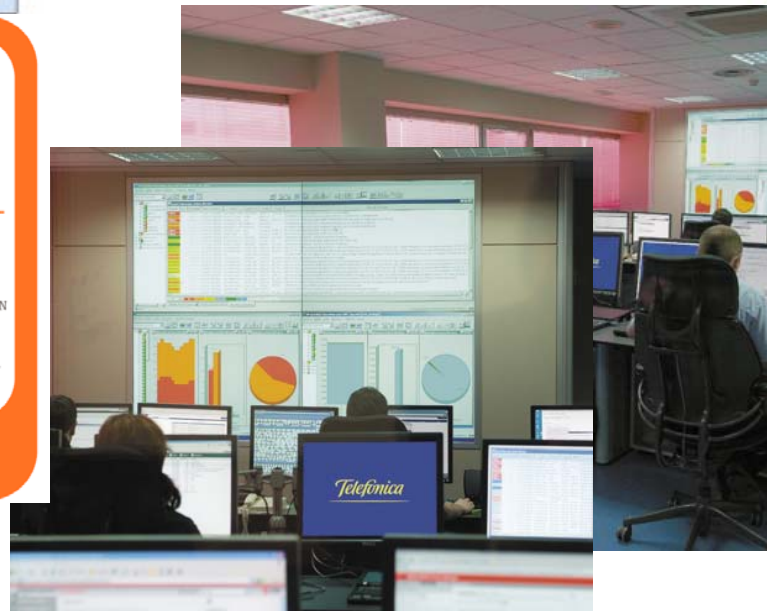
Portales de Servicios de Seguridad

- SOC – Módulo de Gestión de Seguridad del CeGAS (Centro de Gestión y Administración DataCenters)

- Centro de Alta Seguridad física 24x7

Equipo de personal certificado en Seguridad y Comunicaciones en las principales tecnologías

Infraestructuras Certificadas ISO 27001 y WebTrust e ISO 20000



Productos: DLP



Telefonica
