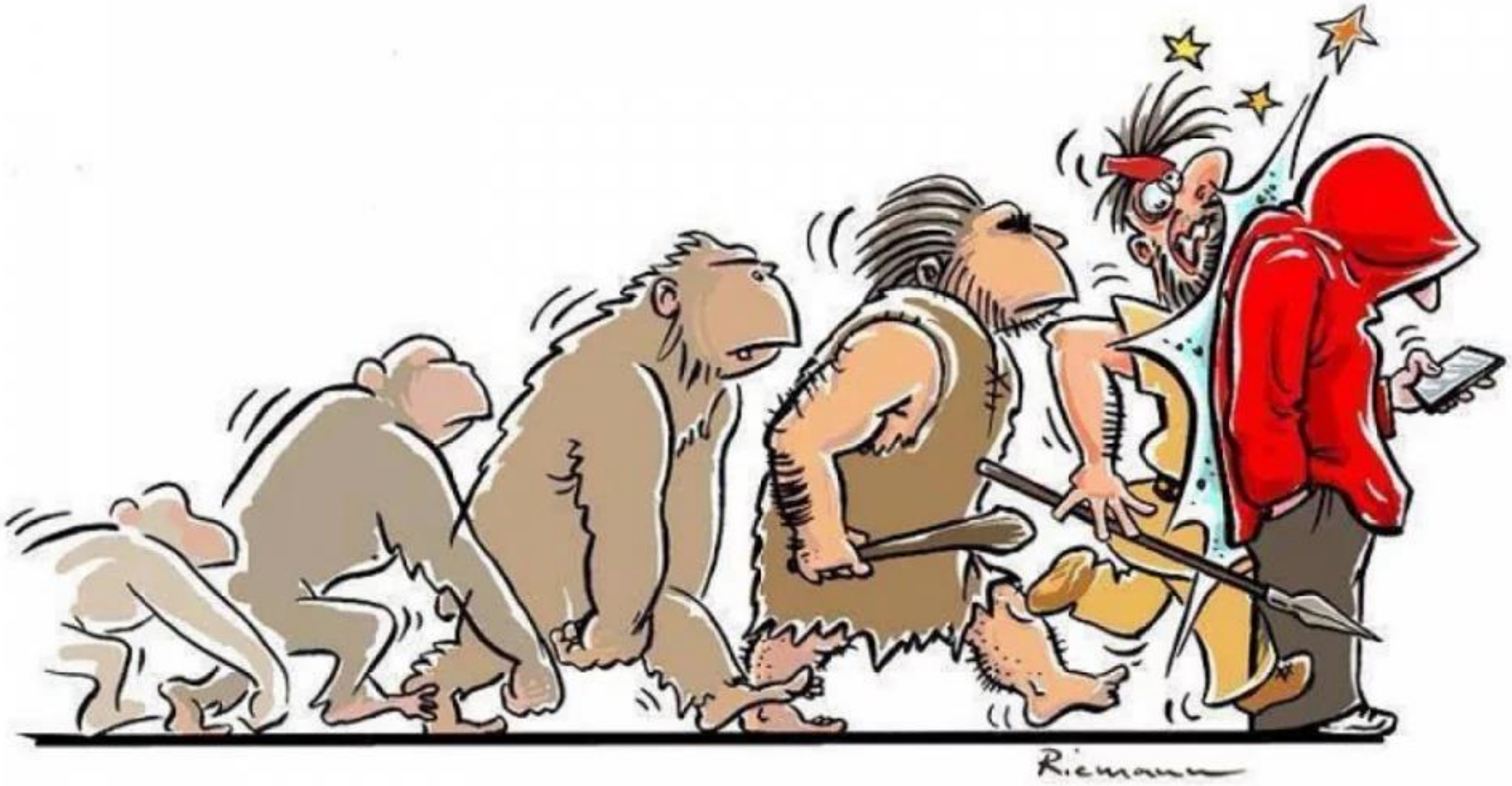
Deloitte.

Gestionar la incertidumbre en un mundo híperconectado

Rubén Frieiro

23 de noviembre 2018



© 2018 Deloitte Advisory S.L.

Un mundo hiperconectado…

… del que no es ajeno el mundo de Securities Services

5.000
Millones de usuarios con móvil en el mundo

4.000
Millones de usuarios con acceso a internet

8.400
Millones de dispositivos conectados IoT

7.800
Millones de usuarios en redes sociales

125
Millones de wearables conectados

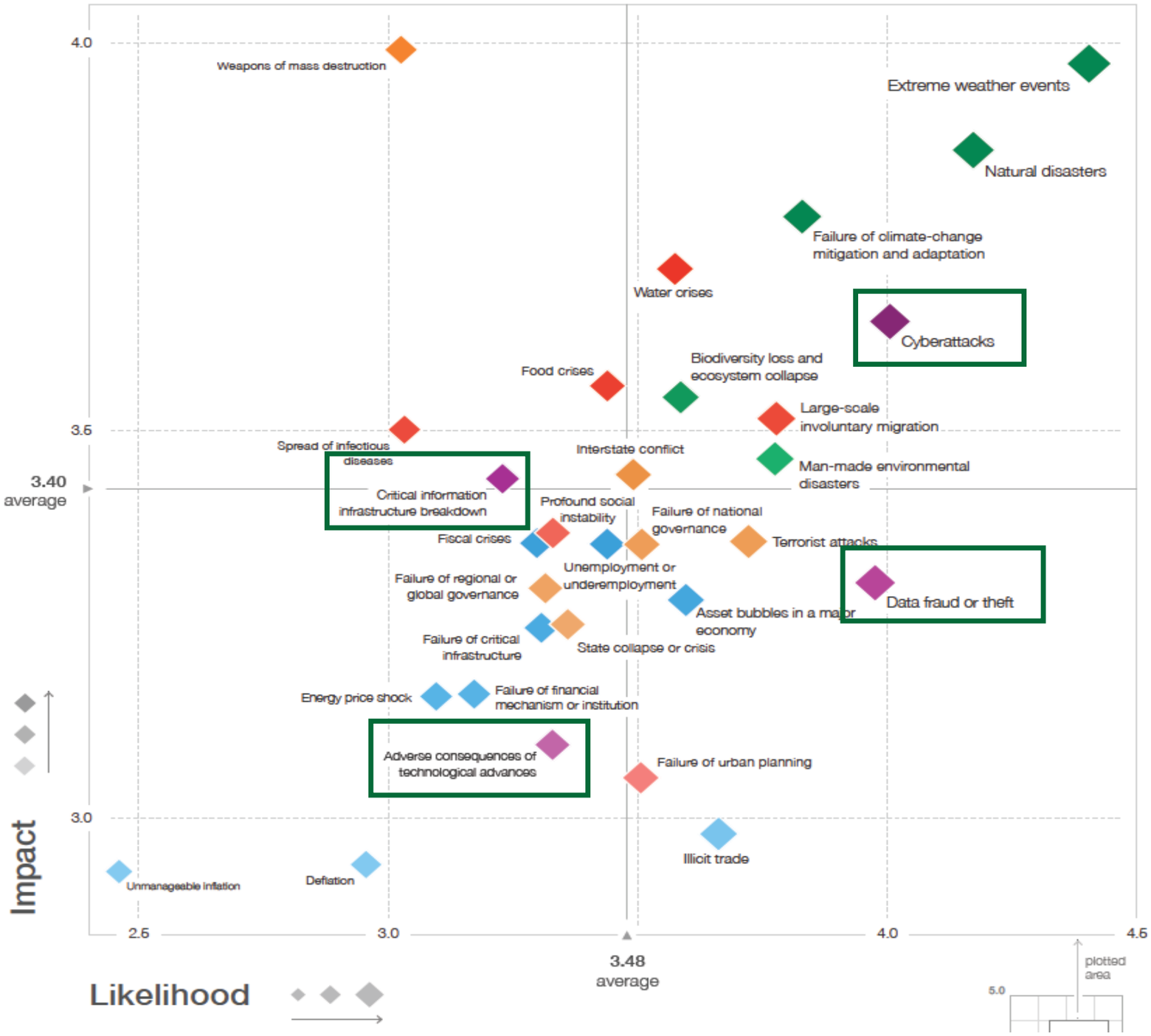
560.000
Operaciones diarias de Target-2 Securities

700.000
Millones de euros diarios

© 2018 Deloitte Advisory S.L.

Importancia del ciberriesgo en el mundo globalizado

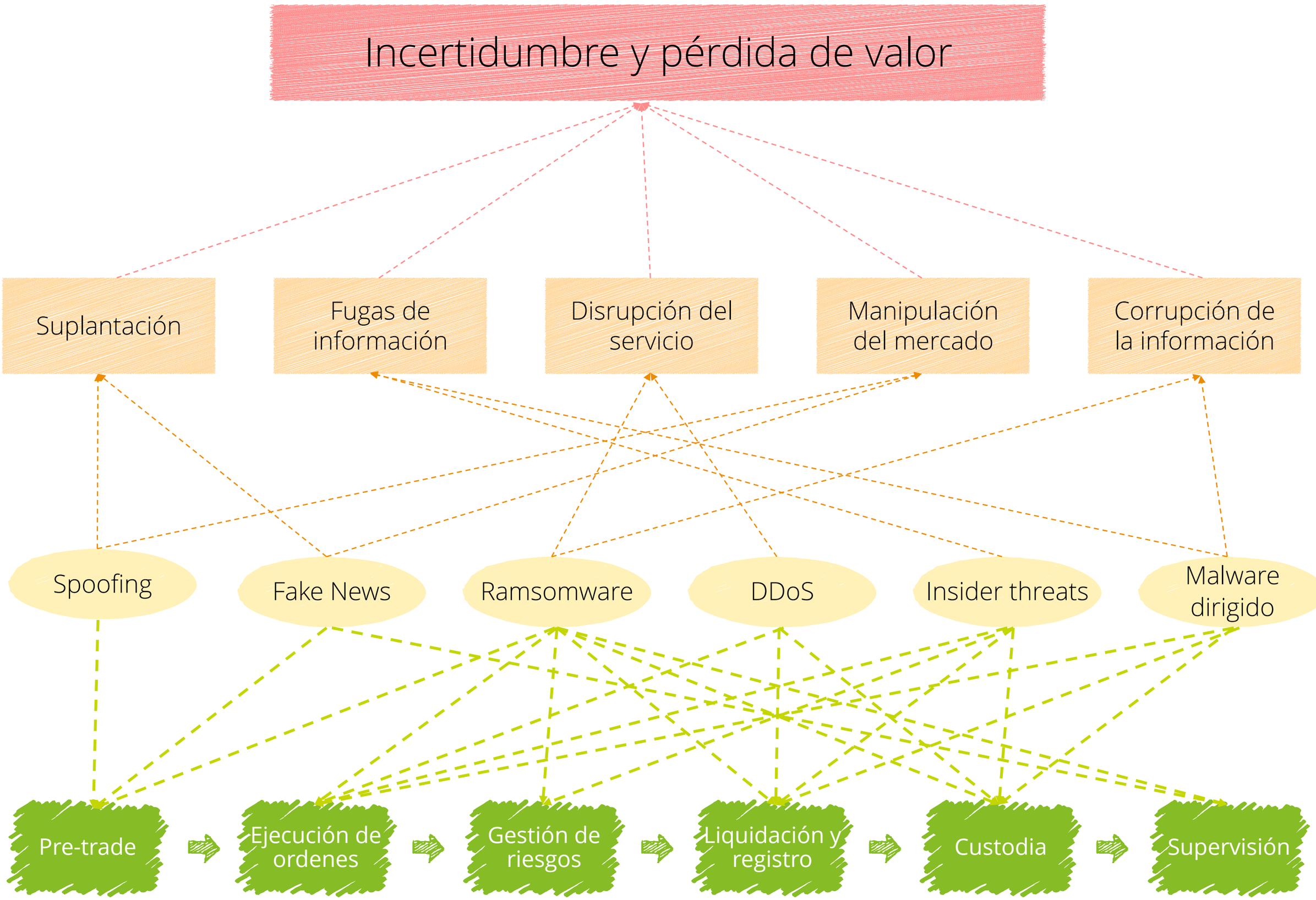
El Foro Económico Mundial (WEF) ha definido el Ciberataque como el 3º riesgo más preocupante para el sector financiero en 2018.



Fuente: World Economic Forum. Enero 2018

© 2018 Deloitte Advisory S.L.

Potenciales vulnerabilidades en el ciclo de los instrumentos financieros



© 2018 Deloitte Advisory S.L.

El grupo de hackers APT38 responsable del robo de más de 100 millones de dólares a entidades financieras – 5 ataques entre el 2015 y el 2018

01

RECOPILACIÓN DE INFORMACIÓN

tanto de la estructura interna de la organización objetivo, como de la manera en que manejan las transacciones SWIFT.

02

COMPROMISO DE LOS SISTEMAS

a través de “watering holes” y explotando una vulnerabilidad de Apache Struts2 en los servidores Linux.

03

EXPLORACIÓN

Los atacantes obtienen las credenciales de la víctima y con ellas, haciendo uso de las herramientas ya presentes en el equipo, escanean el entorno.

04

PIVOTACIÓN A LOS SERVIDORES SWIFT

Con el objetivo de extraer más información acerca de la organización, implantan herramientas de monitorización de red en los sistemas utilizados para SWIFT.

05

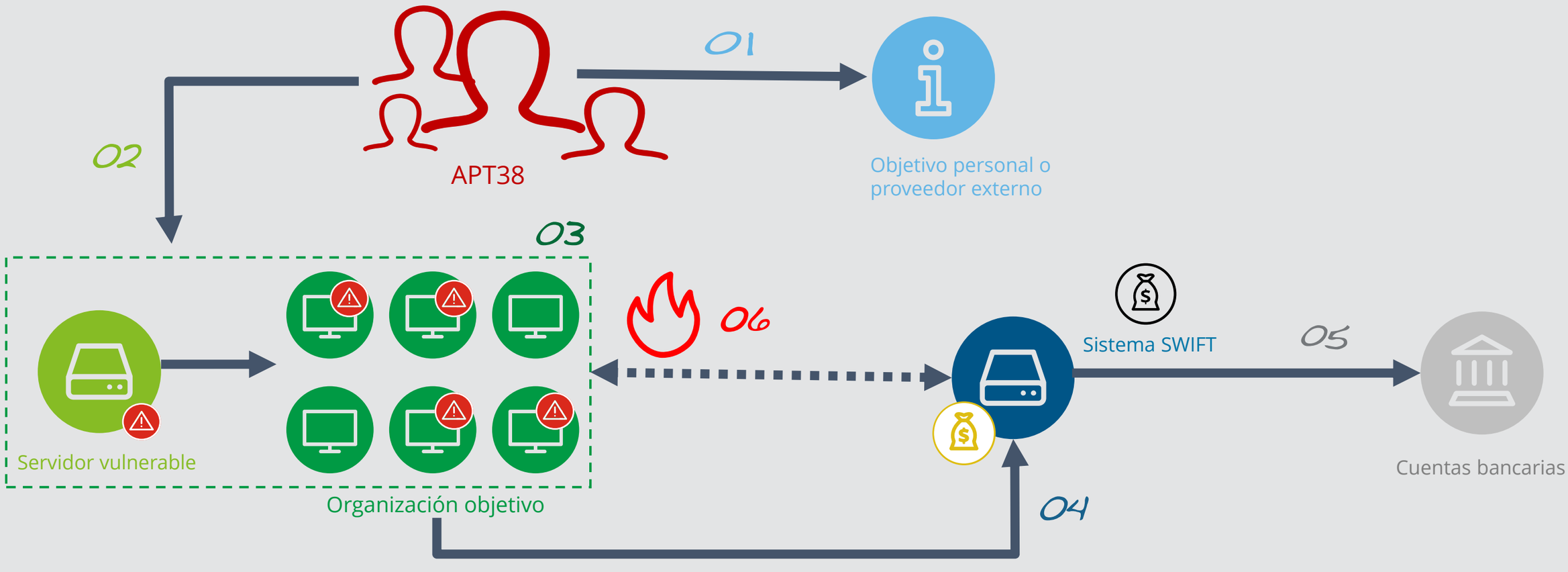
TRANFERENCIA DE FONDOS

Una vez los sistemas de SWIFT están comprometidos, ejecutan el malware DYEPACK que les permite procesar transacciones fraudulentas y alterar el historial.

06

DESTRUCCIÓN DE EVIDENCIAS

El dinero obtenido es transferido a múltiples cuentas distribuidas por todo el mundo, y los registros y todo rastro de la infección es eliminado.



© 2018 Deloitte Advisory S.L.

La respuesta de legisladores y supervisores

EBA

- Opinion of the European Banking Authoroty on the implementation of the RTS on SCA and CSC
- Guidelines on ICT Risk Assesment under the Supervisory Review and Evaluation process (SREP)

CPMI – IOSCO

- Guidance on Cyber resilience for financial market infraestructures

ECB

- TIBER-EU Framework
- Cyber resilience oversight expectations (CROE) for financial market infrastructures

Unión Europea

- Reglamento General de Protección de Datos
- Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

SEC

- Guidance on Public Company Cybersecurity Disclosures

© 2018 Deloitte Advisory S.L.

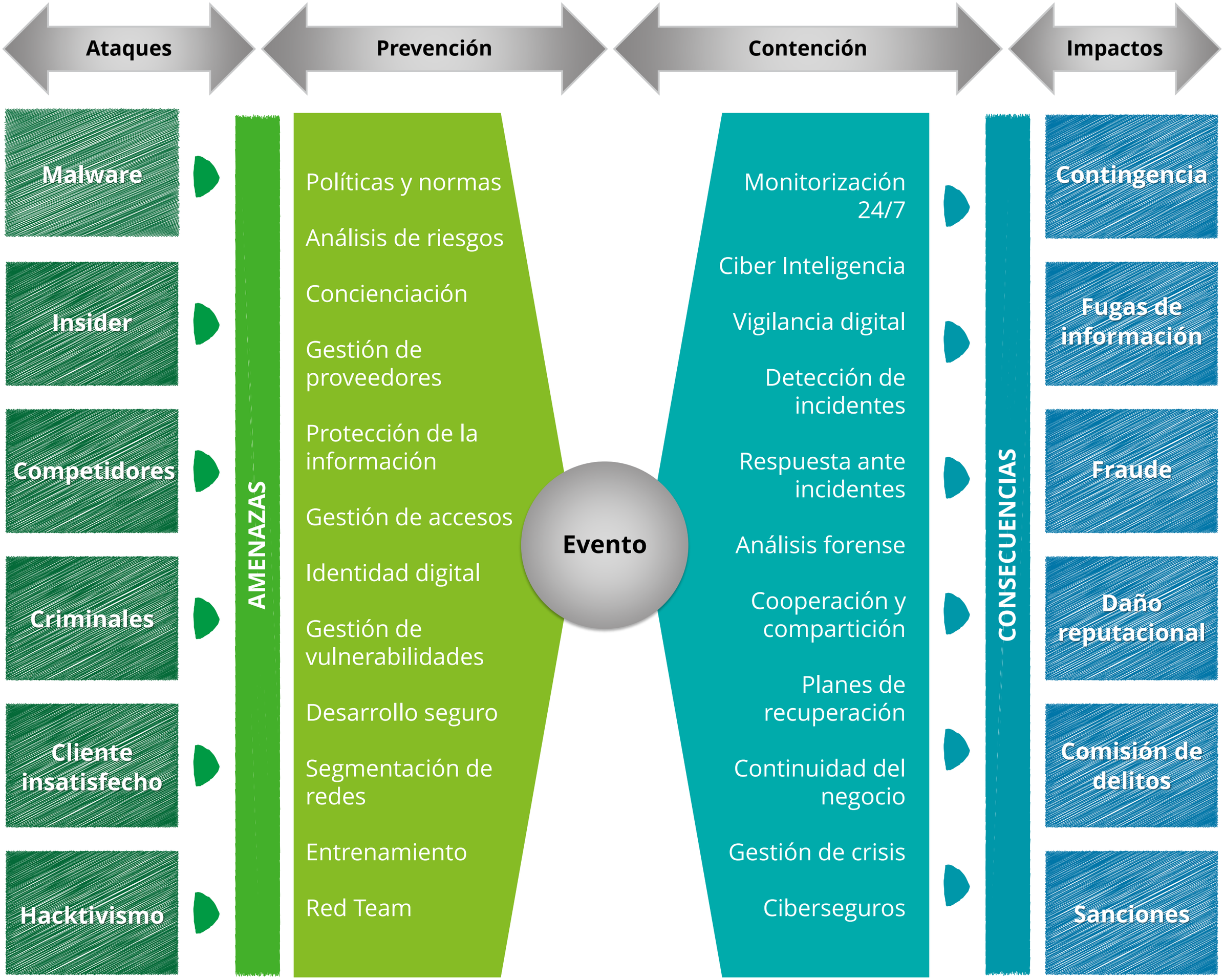
Enfoque tradicional

Cambio de paradigma

Proteger un mundo híperconectado es como defender una gran ciudad, donde no es posible prevenir los incidentes de seguridad en su totalidad. Por ello, las organizaciones deben desarrollar nueva habilidades y capacidades basadas en la inteligencia, la vigilancia, la respuesta y la resiliencia.

© 2018 Deloitte Advisory S.L.

¿Cómo se responde al ciberriesgo?



© 2018 Deloitte Advisory S.L.

Conclusión: La preparación es la base de la resiliencia

La diferencia está en **reaccionar a tiempo**. En minutos, no en días

Información sensible **se continúa transmitiendo** y publicando varios días

El **rumor** del ataque y de una brecha mayor de seguridad en los sistemas **se extiende rápidamente a través de redes.** El equipo de auditoría comienza una investigación

Se informa al CEO de la **fuga de información sensible sin saber a dónde y sin posibilidad** de recuperación de la misma

El **departamento de Comunicación no puede negar ni confirmar el tamaño de la fuga** cuando llega a los medios de comunicación

Un código malware hecho a medida de su compañía **se salta la solución** antivirus corporativa

El código malware **empieza a funcionar** transmitiendo documentos sensibles por Internet

Se daña la reputación y es necesario buscar culpables

El sistema monitor de Seguridad **alerta de patrones** anómalos

Los **equipos afectados se aíslan y se reemplazan** por otros nuevos conteniendo la brecha de seguridad

Se **identifica el método de ataque, se capturan evidencias** forenses y se prepara la denuncia contra los hackers

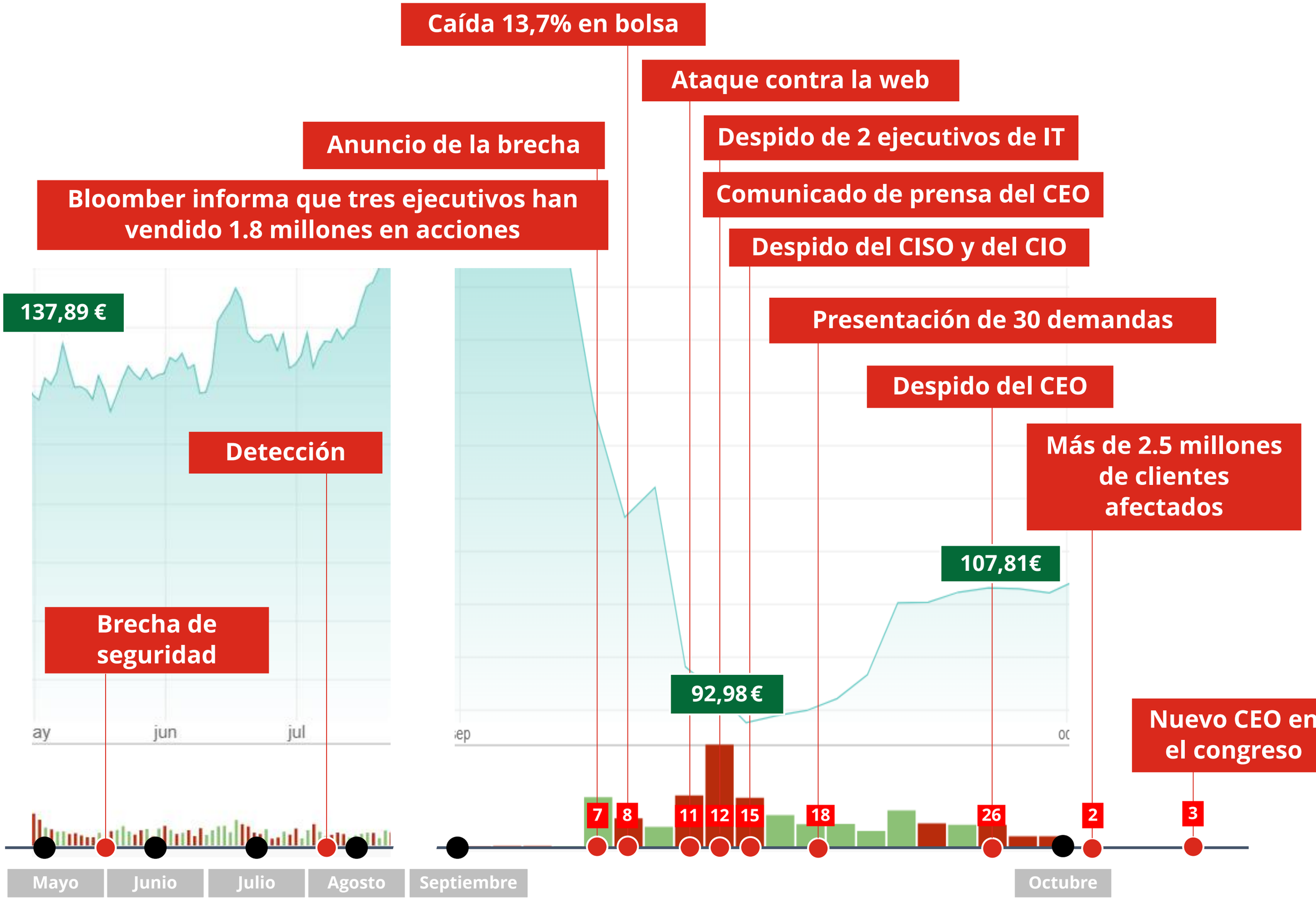
Se **informa al departamento de Comunicación** para que actúe el caso de que los medios den cobertura y se comparte lo detectado con las fuentes de inteligencia

El negocio continúa sin incidentes

© 2018 Deloitte Advisory S.L.

Ejemplo de pérdida de valor en la gestión de la crisis

EQUIFAX - 2017



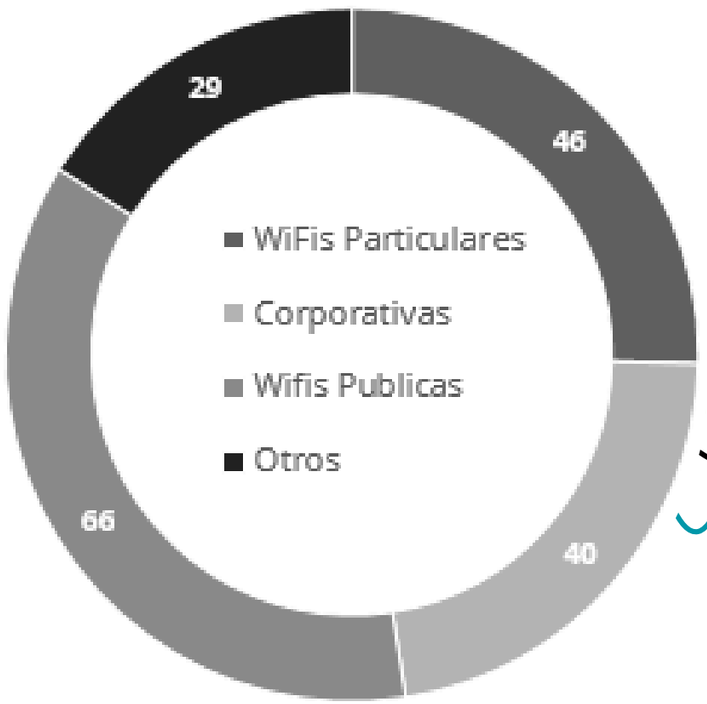
© 2018 Deloitte Advisory S.L.

¿Quién ha visto y/o utilizado algo como esto?

Ingeniería social

Resultado obtenidos

Recopilación de redes Wi-Fi



Se han descubierto **181 redes** Wi-Fi almacenadas en los dispositivos de los asistentes al evento.

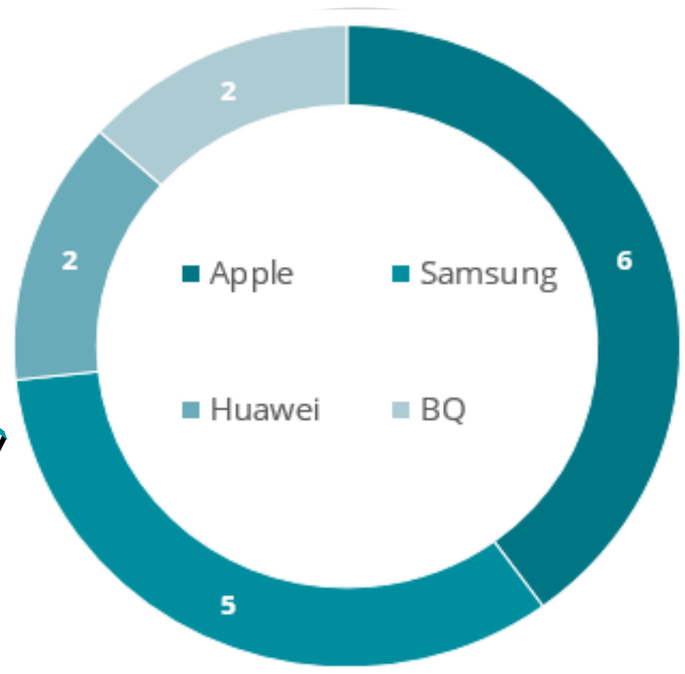
Posible ataque: Se podría publicar una red falsa con el nombre de alguna de las redes descubiertas para que los dispositivos se conectasen automáticamente, teniendo además visibilidad completa sobre la red.

Tráfico en red Wi-Fi gratuita

Se han accedido a **378 páginas web** a través la red Wi-Fi que se ha publicado y a la que **han accedido 27 asistentes**.

Posible ataque: Al tratarse de una red publicada por un atacante, se podría controlar la redirección a webs fraudulentas que imitan ser lícitas (bancos, correos corporativos…).

Estación de carga



15 dispositivos se han conectado a la estación de carga, de las que **2 han permitido el acceso** a los datos del dispositivo.

Posible ataque: Al haber aceptado el acceso a los datos del dispositivo, se podría obtener toda la información almacenada (contacto, fotos, documentos…) y hacer uso de cualquier funcionalidad del dispositivo (cámara, micrófono…).

© 2018 Deloitte Advisory S.L.

Deloitte.

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited (“DTTL”) (private company limited by guarantee, de acuerdo con la legislación del Reino Unido), y a su red de firmas miembro y sus entidades asociadas. DTTL y cada una de sus firmas miembro son entidades con personalidad jurídica propia e independiente. DTTL (también denominada "Deloitte Global") no presta servicios a clientes. Consulte la página http://www.deloitte.com/about si desea obtener una descripción detallada de DTTL y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, legal, asesoramiento financiero, gestión del riesgo, tributación y otros servicios relacionados, a clientes públicos y privados en un amplio número de sectores. Con una red de firmas miembro interconectadas a escala global que se extiende por más de 150 países y territorios, Deloitte aporta las mejores capacidades y un servicio de máxima calidad a sus clientes, ofreciéndoles la ayuda que necesitan para abordar los complejos desafíos a los que se enfrentan. Los más de 244.000 profesionales de Deloitte han asumido el compromiso de crear un verdadero impacto.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o entidades asociadas (conjuntamente, la “Red Deloitte”), pretenden, por medio de esta publicación, prestar un servicio o asesoramiento profesional. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado. Ninguna entidad de la Red Deloitte será responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.

© 2018 Para más información, póngase en contacto con Deloitte Advisory, S.L.