XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Seguridad y prevención del fraude en bankinter.

Organizado por

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

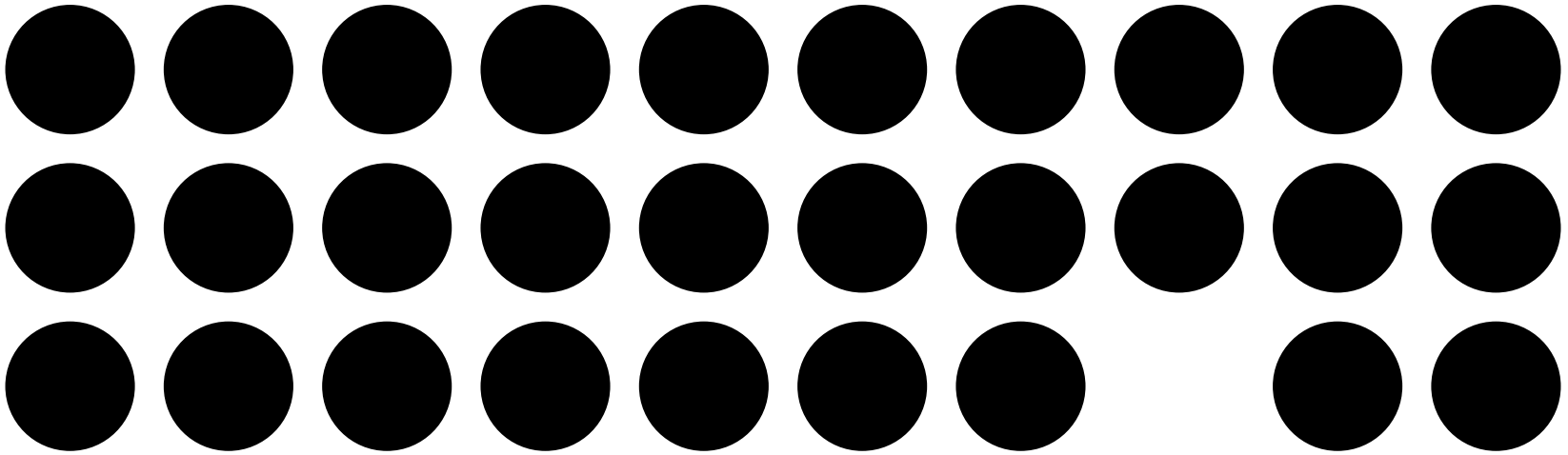
20 años de convivencia con la multicanalidad

bankinter

gneis.
Una idea Bankinter

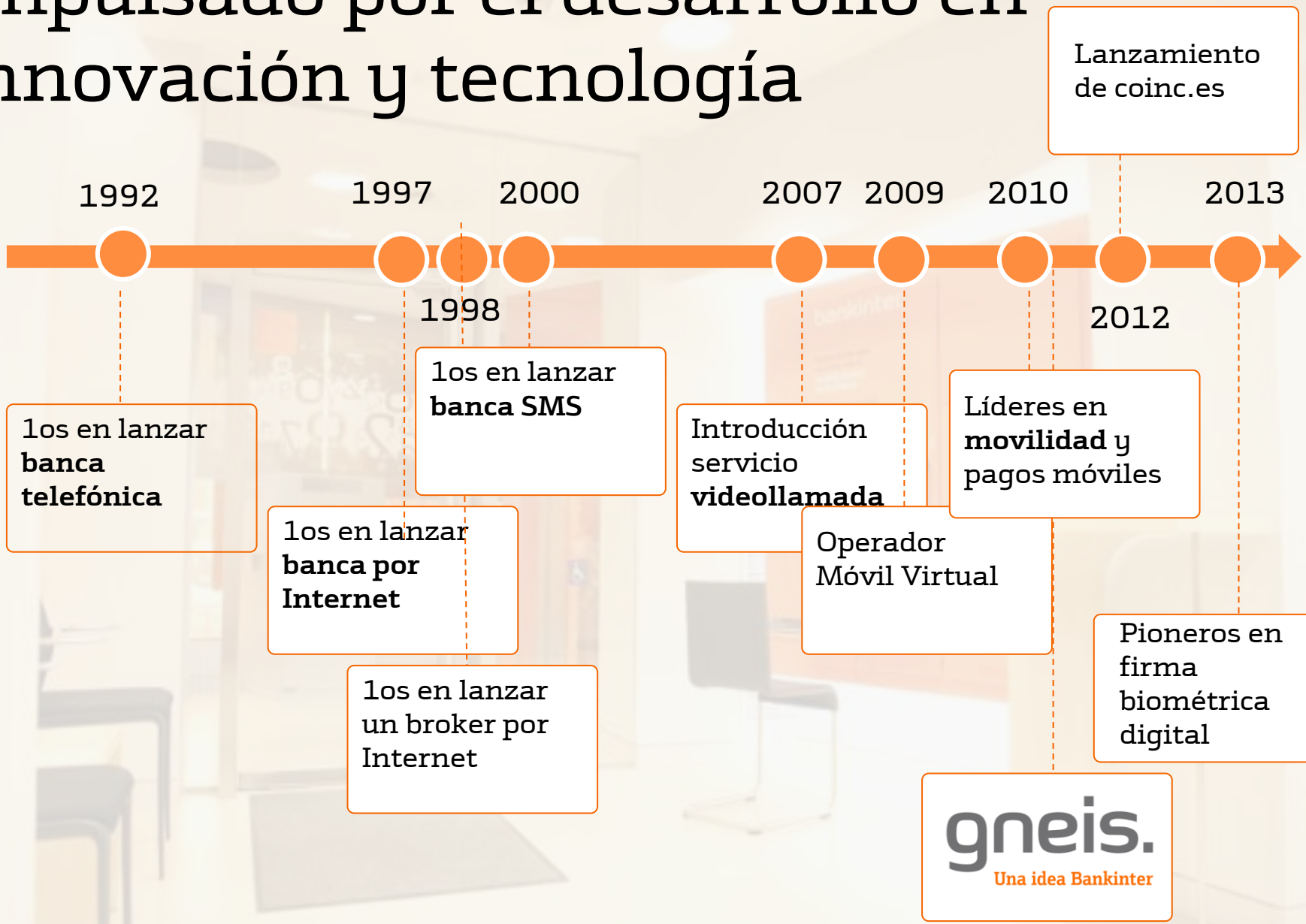
- IBEX 35
- 47 años de experiencia en la industria española
- Crecimiento orgánico y eficiencia
- Enfoque en clientes de perfil alto

Una historia de éxito, crecimiento y creación de valor a través de la diferenciación



bankinter.

Impulsado por el desarrollo en innovación y tecnología



bankinter

Que nos permiten aproximarnos al mercado con una estrategia multicanal

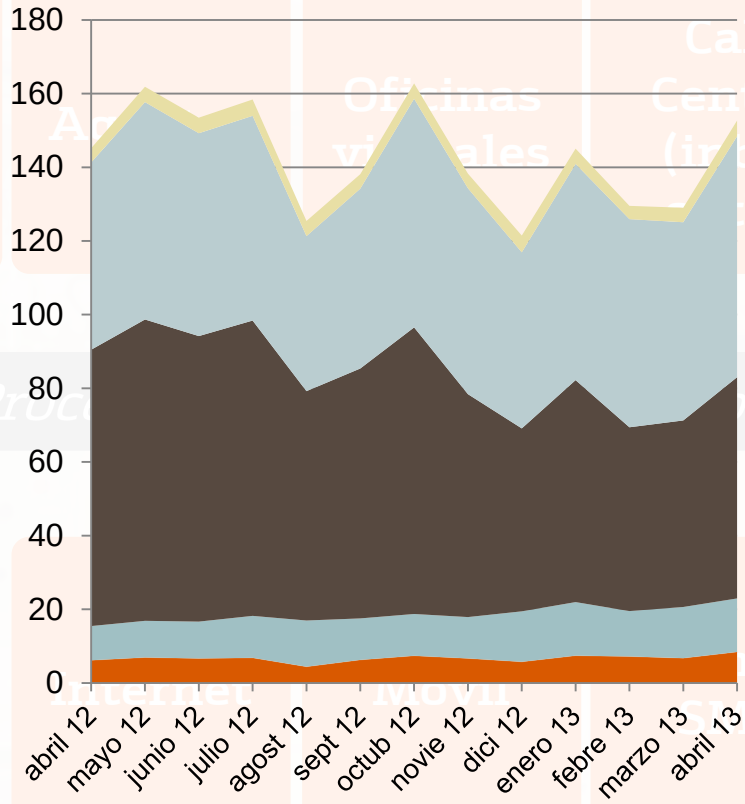
Oficinas | Agentes | Oficinas virtuales | Call Center (inb + outb) | Videocall

*Proceso comercial **multicanal** orquestado por CRM*

Internet | Móvil | Banca SMS | ATM

bankinter

Que nos permiten aproximarnos al mercado con una estrategia multicanal



Seguridad y prevención del fraude

bankinter. gneis.
Una idea Bankinter

Equipo dedicado

- Claro **liderazgo** de Seguridad Informática en el Sector Financiero Español
- 15 años de **experiencia** como equipo gestor de la Seguridad en sector financiero
- Entorno Tecnológico caracterizado por la **Innovación**
- **Mejora continua** avalada por la renovación periódica de certificaciones
- Reconocimiento y Participación en **foros especializados y publicaciones** a nivel mundial

Certificaciones

ISMS ISO/IEC 27001:2005 Certificado IS 508474

2006. 1er banco certificado en España ISO/IEC 27001 – Seguridad de la Información

2008. Primera compañía certificada en España BS 25999 – Continuidad de negocio

2012. Primera compañía certificada a nivel mundial ISO/IEC 22301 – Continuidad de Negocio

The Banker innovation in banking technology awards 2012

FINANCIAL WORLD INNOVATION AWARDS 2012

gneis.
Una idea Bankinter

1995

"**Dicen que** hay una cosa que se llama Internet y que es el futuro y que está muy bien y que se pueden hacer muchas cosas …. hasta comprar"

1996

"**Yo conozco a un fulano** que me ha dicho que ha comprado por Internet y que patatín y que patatán…."

1997

"Pues **yo, ¡ya he comprado** por Internet!"

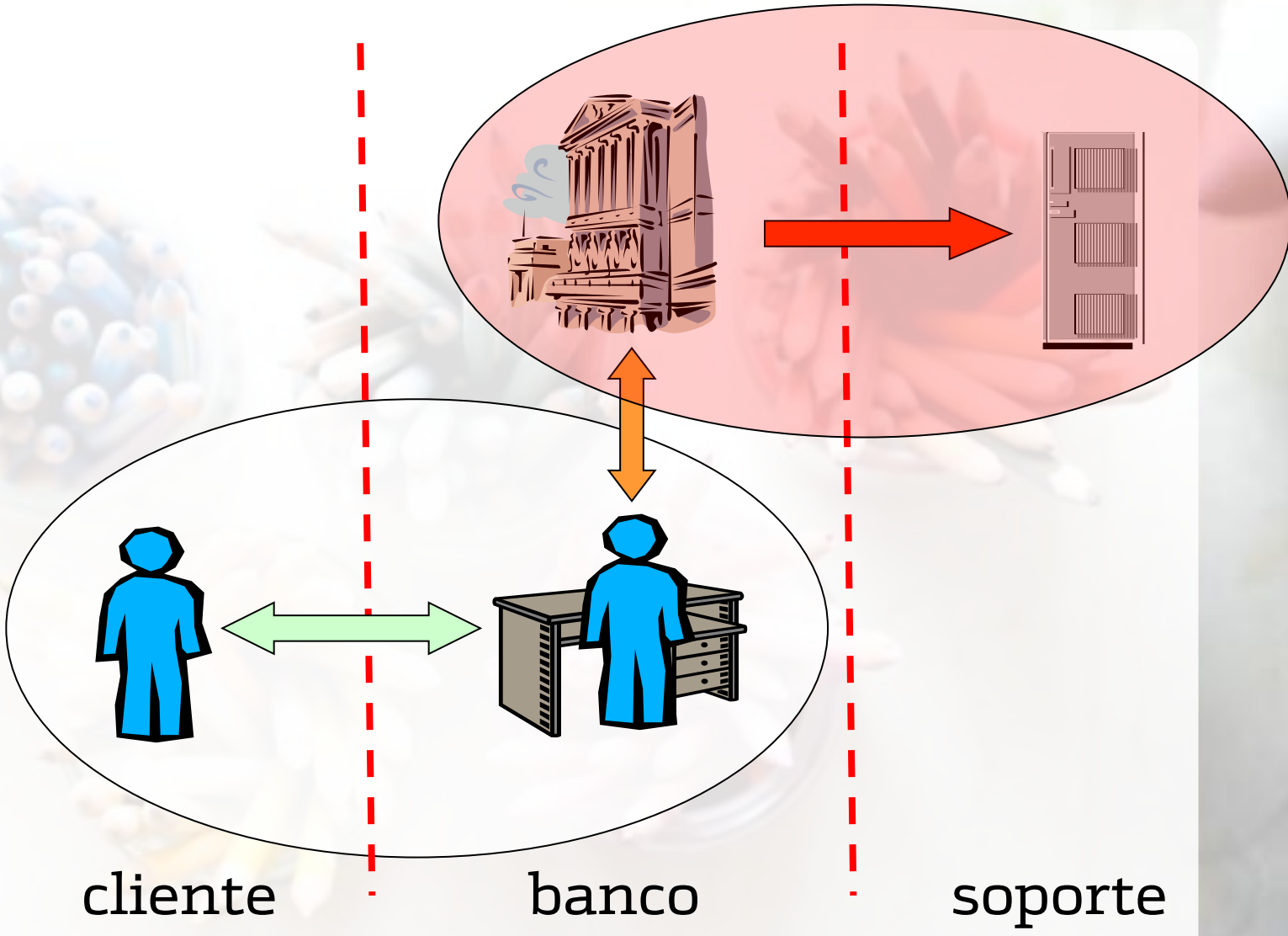
1998

"Mira, aquel de allí, **aún no ha comprado** por Internet"

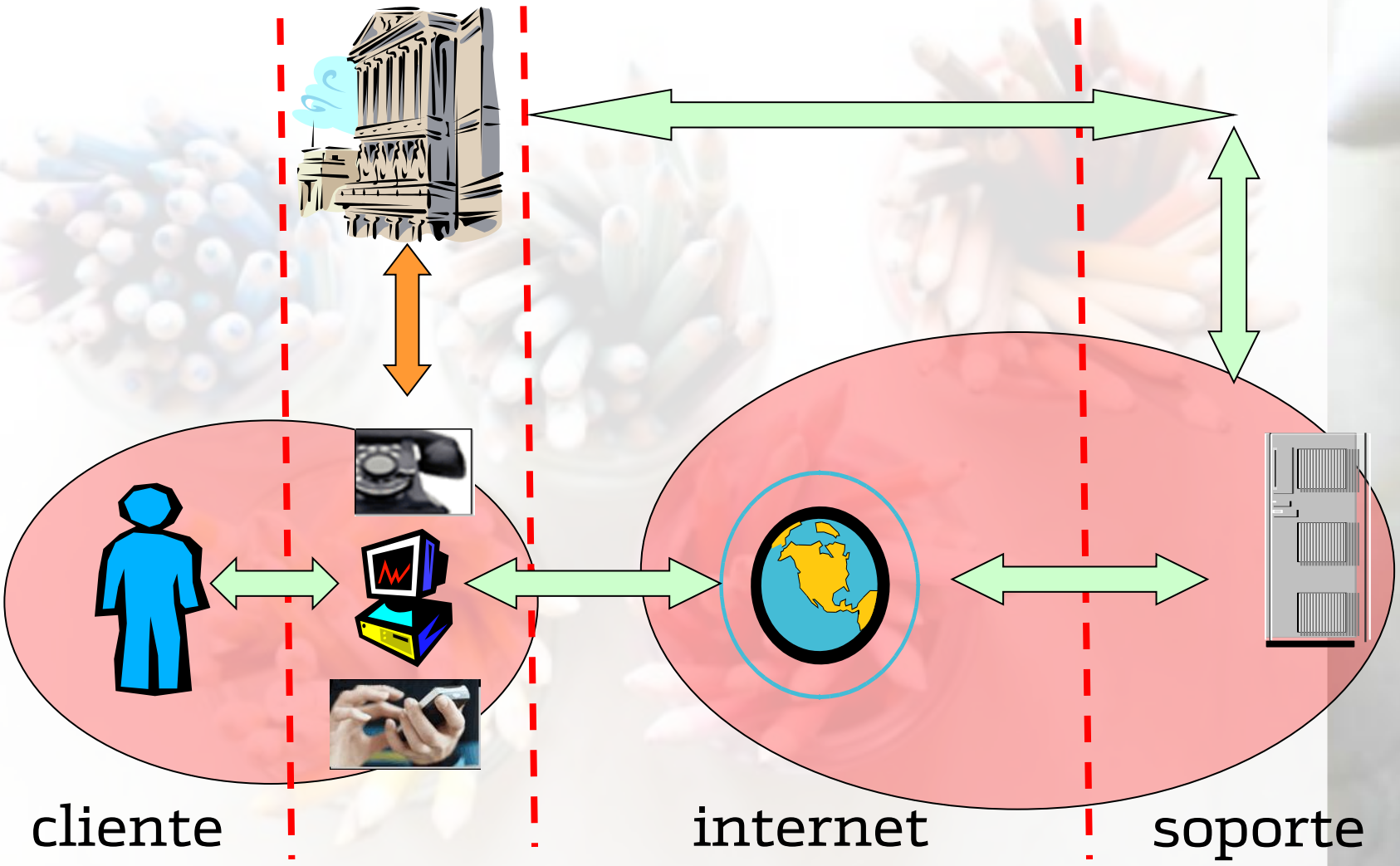
Estrategia del banco

- **Posicionamiento *on-line* multicanal**
  - Nos expone a riesgos con un impacto muy severo en imagen y negocio
- **Fuerte contenido tecnológico y de innovación**
  - Tecnologías inmaduras
    - Poco testadas
    - Poco legisladas/regladas
    - Los nuevos canales nos traen nuevos riesgos
    - Hay que combinar el *time-to-market*

Modelo de relación tradicional



Modelo de relación a distancia



El primer banco en España en permitir a sus clientes la compra-venta de valores en el mercado continuo fue Bankinter a través de BKnet en 1997

SEGURIDAD

Un 'web' falso intenta capturar las claves de los usuarios de Bankinter

Un usuario alertó sobre una página alojada en Come.to que podría estar intentando aprovechar un fallo de los antiguos navegadores - Los expertos consultados niegan la existencia de cualquier riesgo para la seguridad de los datos de acceso

JUAN GONZALO

MADRID.- Fuentes de Bankinter han negado categóricamente que la seguridad de su web de banca electrónica haya podido quedar comprometida en ningún momento, y han restado importancia a la denuncia de un usuario sobre la existencia de una página que, en opinión de éste, supone un intento de interceptar los datos de los clientes.

La página en cuestión, come.to/copiadeseguridad, está alojada en un sitio de redireccionamiento de páginas web, Come.to, y consiste en un burdo conjunto de dos marcos (*frameset*) o subventanas que incluye la página original de Bankinter (*www.bankinter.es*).

Estrategia de la seguridad

Evolución de los FOCOS DE LA SEGURIDAD en Bankinter (Selección de categorías significativas)

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

Evolución de los FOCOS DE LA SEGURIDAD en Bankinter (Selección de categorías significativas)

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

Premisas de seguridad y riesgos

Seguridad

- La **prevención** es necesaria, pero la **detección** es una obligación
- Si **un canal** se ve comprometido, **el resto de canales** no han de ser contaminados
- Nuestros clientes son **parte de nuestro entorno** de seguridad

Gestión del riesgo

- Medir y comunicar nuestra exposición al riesgo **en términos de negocio**
- Mejora continua orientada a la **eficacia**, la **seguridad** efectiva y a la gestión por **procesos**
- Preparar y entrenar **personas** en la gestión de procesos y un ambiente de control

Premisas de seguridad y riesgos

Seguridad

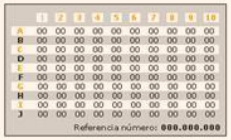
Gestión del riesgo

- La **prevención**
  pero la **detecc**
  obligación
- Si **un canal** se
  comprometid
  canales no ha
  contaminados
- Nuestros clien
  parte de nues
  de seguridad

Banca Telefónica voz

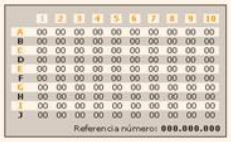
C.A.P. + Clave aleatoria

Internet

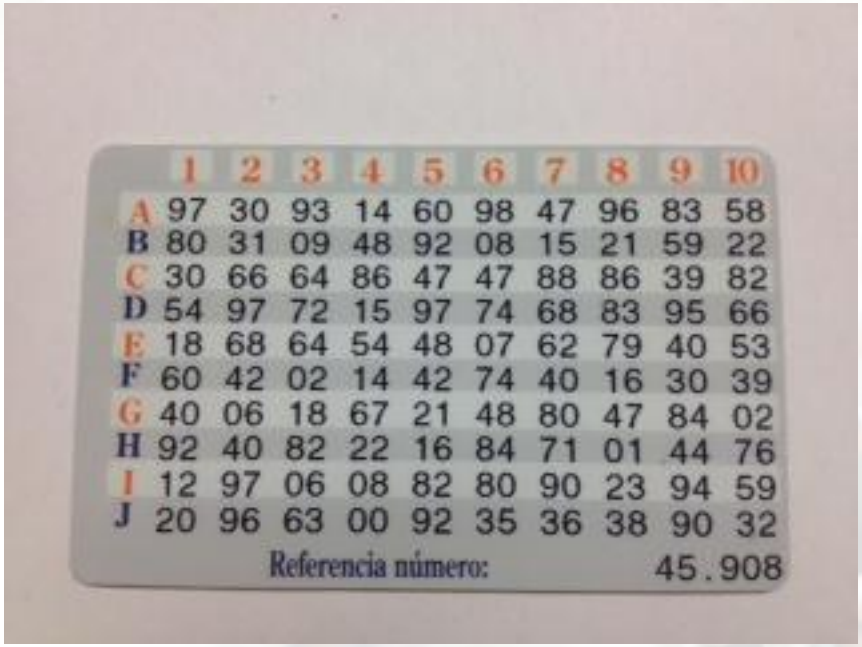


usuario contraseña + Clave aleatoria

Móvil



usuario contraseña + Suma claves aleatorias



Evolución de los FOCOS DE LA SEGURIDAD en Bankinter (Selección de categorías significativas)

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

1. Hackers de ayer… Máfias de hoy…

2. Los clientes son el eslabón más débil

3. Ataques basados en el "engaño"

Los clientes forman parte de nuestro perímetro de control de seguridad

Seguridad en ebankinter

- Nuestro sistema de seguridad está basado en unas claves de acceso y una tarjeta de coordenadas. **Por eso, le recomendamos que:**

- **mantenga sus claves en secreto** y cámbielas regularmente.
- **no entregue su tarjeta de coordenadas** a otras personas.
- **no proporcione por correo electrónico u otro canal sus claves de acceso**.
- **no olvide pulsar desconectar** al terminar su sesión en ebankinter.

- Además, añadimos una serie de **medidas de seguridad excepcionales**.
  Consúltelas en nuestro apartado sobre operar en ebankinter.

Ir a Operar en ebankinter

Seguridad en Internet

- Le proporcionamos una serie de consejos sobre **cómo navegar en Internet con seguridad**. Vea, entre otros, cómo borrar sus archivos temporales, eliminar cookies y consultar el certificado Verisign.
  Consulte nuestro apartado sobre seguridad en Internet.

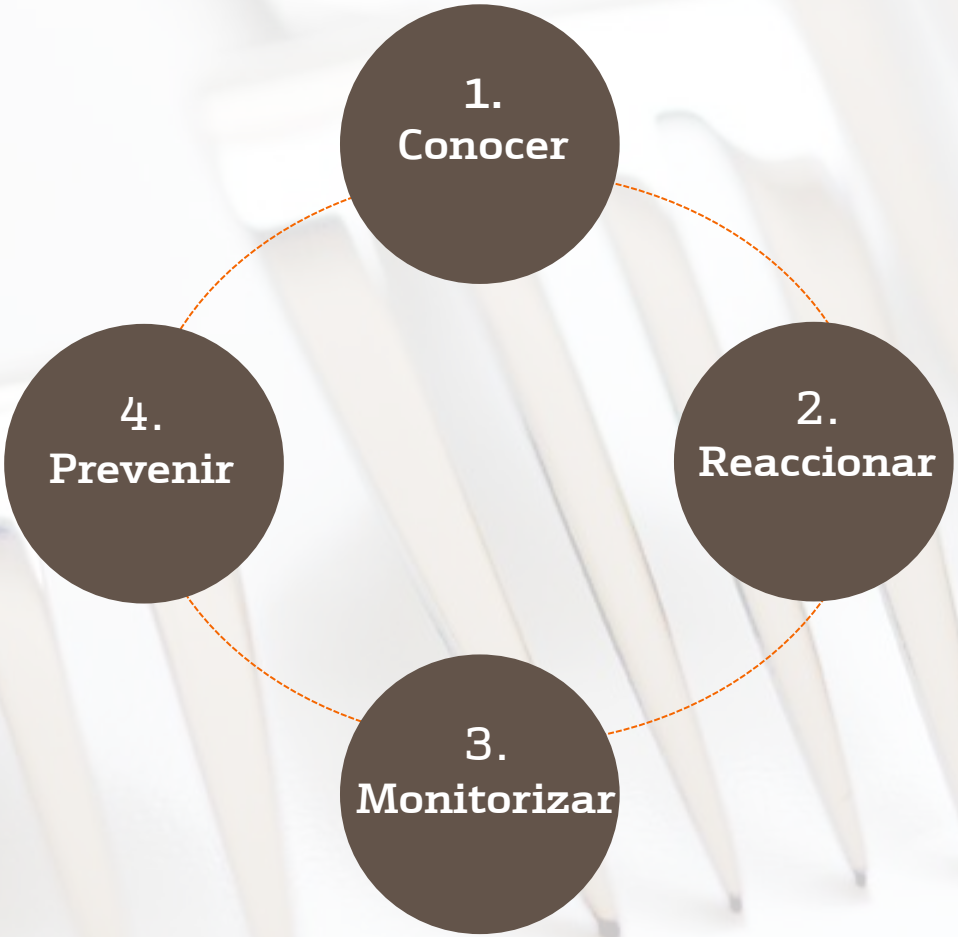
Ir a Seguridad en Internet

Seguridad en su equipo

- Conozca las herramientas gratuitas que tiene a su disposición para que su ordenador esté protegido.

Ir a Seguridad en su equipo

Modelo de seguridad

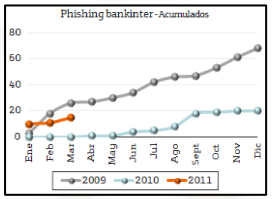


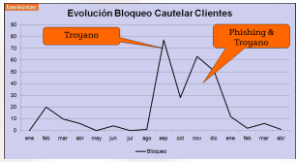
gneis.
Una idea Bankinter

Modelo de seguridad

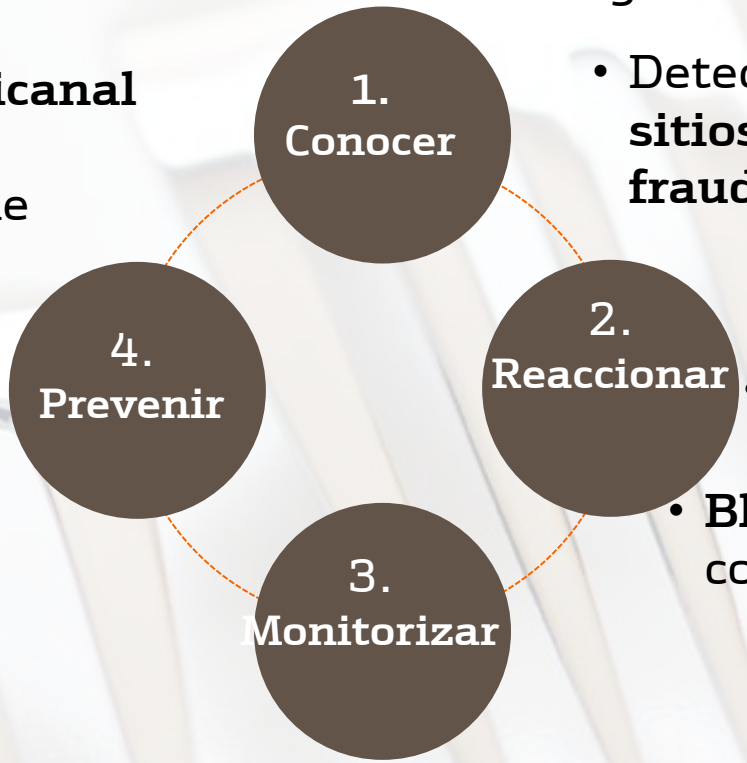
- **Validación** on line de cifrado
- Integración **multicanal**
- **Ofuscación** de contenido sensible

- **Detección activa** del código **malware** "in memory"





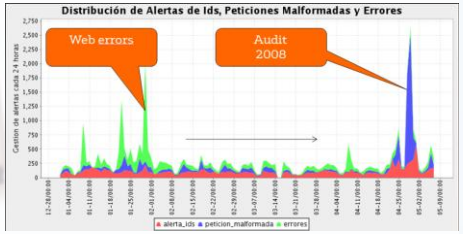
- Detección de **sitios web fraudulentos**



- **Prohibición** de sites fraudulentos
- **Inyección de ruido**

- **Bloqueo** de usuarios comprometidos

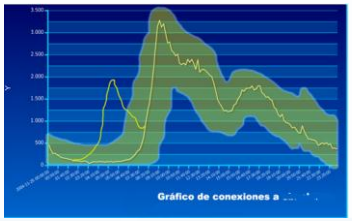
- **Evolución** de los sistemas de identificación, autenticación y firma



- Gestión de **alertas**

- **Correlación** de anormalidades

- CRM de seguridad. **Scoring** transaccional vs patrón de cliente



gneis.
Una idea Bankinter

¿Cómo nos/los protegemos?

gneis.
Una idea Bankinter

Evolución de los FOCOS DE LA SEGURIDAD en Bankinter (Selección de categorías significativas)

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

CRM Seguridad. Imagina… que

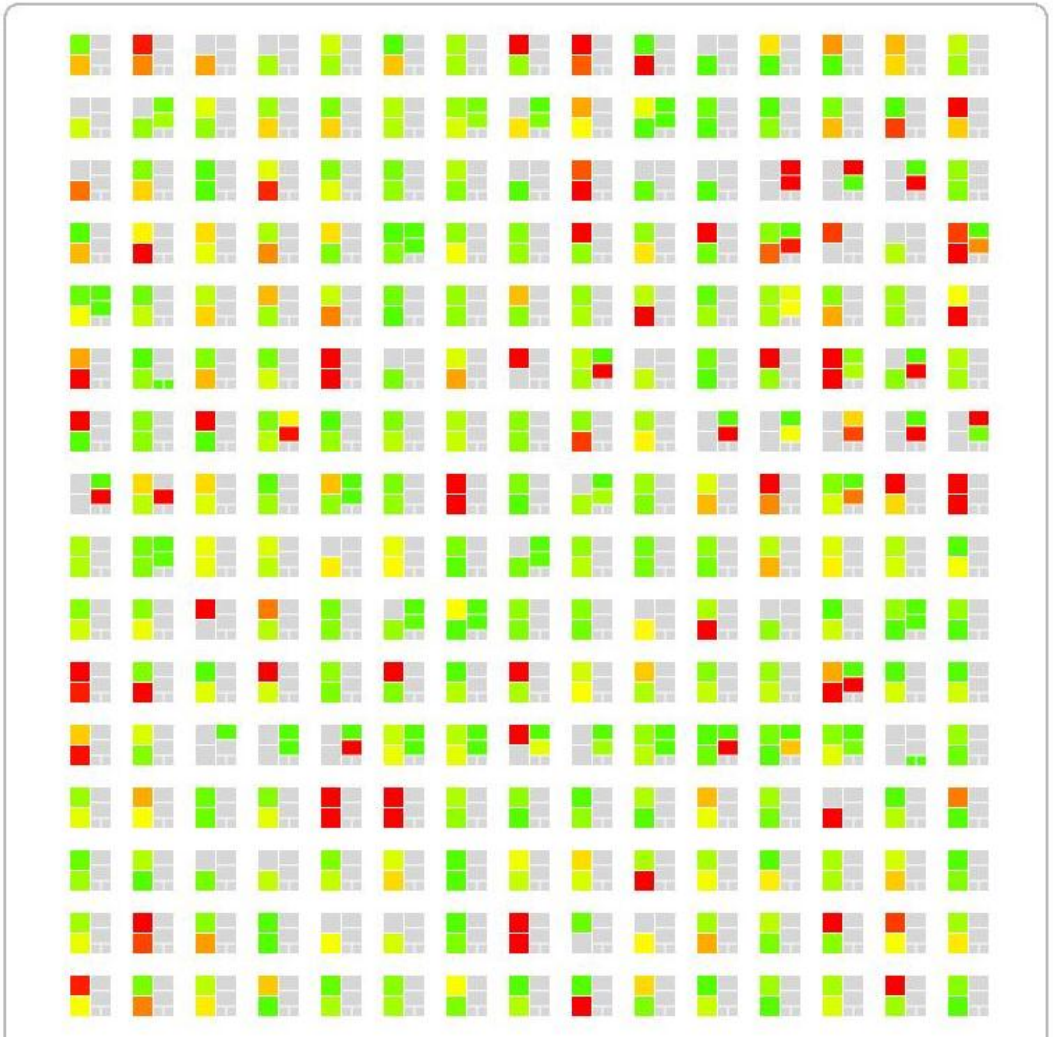
1. Los sistemas **reportan en tiempo real** la actividad en un repositorio único centralizado

2. La información es **accesible** de manera transparente e independiente a su formato y contenido

3. **Aplicamos** "inteligencia" de negocio y seguridad mediante reglas de correlación y patrones de comportamiento

gneis.
Una idea Bankinter

CRM Seguridad



Scoring de Sesión: Normal

IDXXXXX - Nombre y apellidos

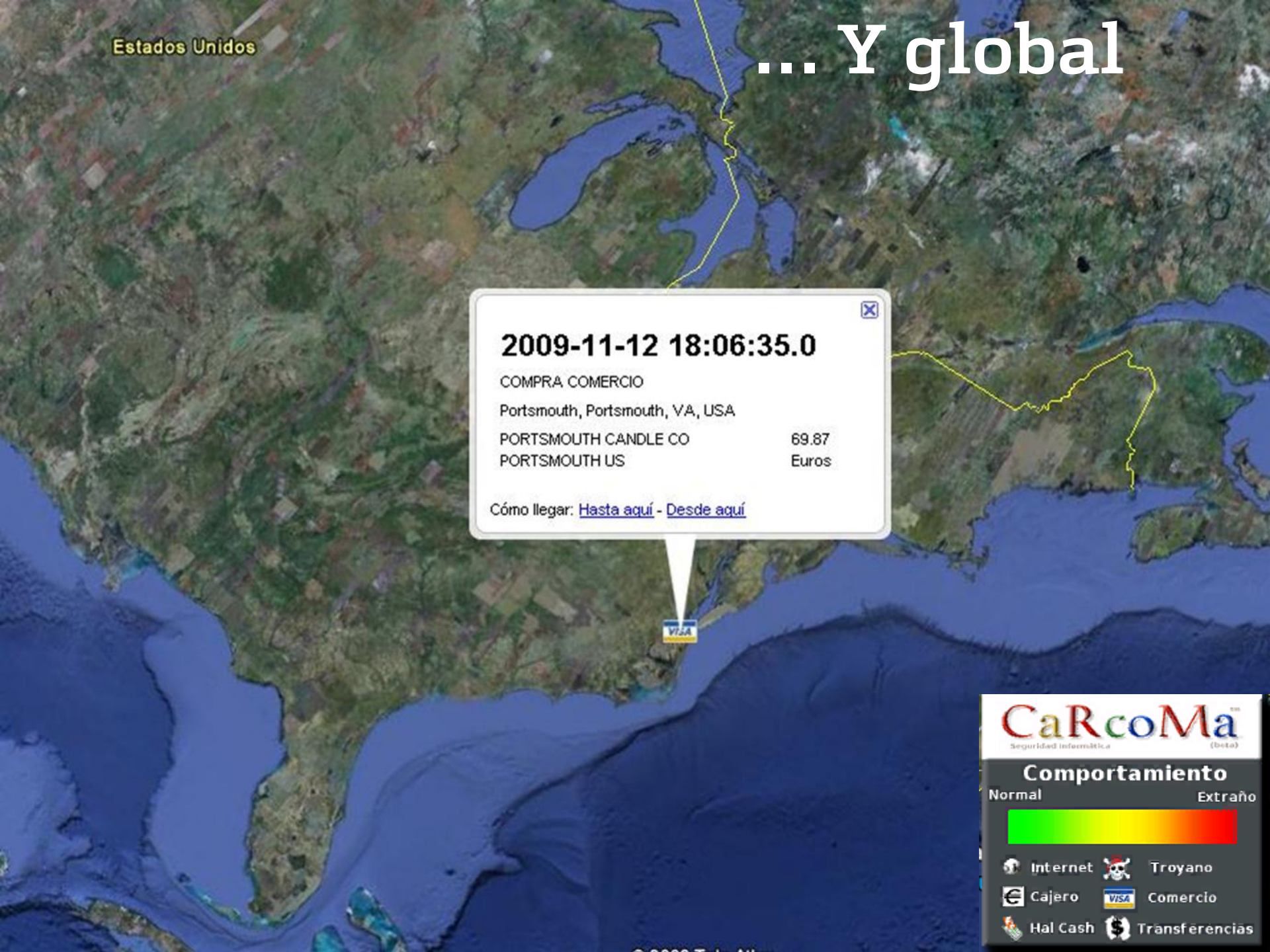
Login: 2008-12-05 11:05:04
Puntuaciones:

- Geolocalización: 0,1 - Normal
- Patrón de tecleo: 0,2 + 0,3 - Normal
- Rango dia/hora: 0,6 - Sospechoso
- Intervalo conexión: 0,8 - Vigilar
- Distancia conexión: 0,0 - Normal
- Equipo conexión: 0,2 - Normal
- Cuenta destino: 0,1 - Normal
- Importe operación: 0,6 - Vigilar

Local...


Golfo de Vizcaya
Castro Terrace
Mónaco
Mar de
Stoechades Cany
(Oporto)
Porto
España
Madrid
Portugal
Lisboa
Eivissa (Ibiza)
Cádiz
Gibraltar
Estrecho de Gibraltar
© 2010 Europa Technologies
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2010 Tele Atlas
© 2010 Google
CaRcoMa
Seguridad Informática
(beta)
Comportamiento
Normal
Extraño
Internet
Troyano
Cajero
Comercio
Hal Cash
Transferencias

... Y global


Estados Unidos
2009-11-12 18:06:35.0
COMPRA COMERCIO
Portsmouth, Portsmouth, VA, USA
PORTSMOUTH CANDLE CO 69.87
PORTSMOUTH US Euros
Cómo llegar: Hasta aquí - Desde aquí
CaRcoMa
Seguridad Informática
(beta)
Comportamiento
Normal
Extraño
Internet
Troyano
Cajero
Comercio
Hal Cash
Transferencias

CaRcoMa broker (beta)

Usuario

Búsqueda avanzada

Buscar | Voy a tener suerte | ¿suerte?

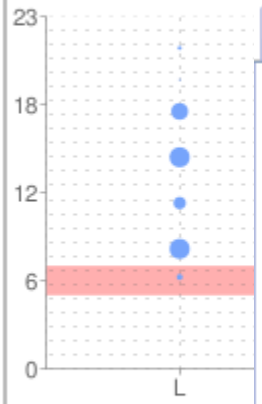
Resumen | Horario | Epifanis | Flash | Navegadores | Usuario | Contraseña | Geolocalización | Comentarios

online | perfil | última conexión | cómo funciona?

broker

Online

2009-11-16 06:59:35 GMT+1



Resumen | Horario | Epifanis | Flash | Navegadores | Usuario | Contraseña | Geolocalización | Comentarios

cómo funciona? | mapa

Online

2009-11-16 06:59:35 GMT+1

perfil | actual | ultima

Conexiones entre: 2009-08-17 13:05:00 GMT+1
y 2009-11-13 17:15:29 GMT+1
Muestras: 164

gneis.
Una idea Bankinter

Evolución de los FOCOS DE LA SEGURIDAD en Bankinter (Selección de categorías significativas)

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

Expertos advierten que uno de los principales riesgos que se enfrentará durante este 2013 es la propagación de información falsa a escala masiva

Global Risks 2013

Cat.	Risk	Likelihood	Impact
	Critical systems failure	2.96	3.62
	Cyber attacks	3.82	3.52
	Failure of intellectual property regime	3.00	2.99
	Massive digital misinformation	3.36	3.24
	Massive incident of data fraud/theft	3.51	3.27
	Mineral resource supply vulnerability	3.42	3.45
	Proliferation of orbital debris	2.87	2.80
	Unforeseen consequences of climate change mitigation	3.23	3.35
	Unforeseen consequences of nanotechnology	2.79	2.99
	Unforeseen consequences of new life science technologies	3.11	3.36

Pero, ¿cómo luchar contra un tuitero anónimo que puede provocar el pánico en el parqué? Eso fue lo que pasó hace cuatro meses, cuando alguien difundió el rumor de que, tras el paso del huracán Sandy, se había inundado la bolsa de Nueva York, que supuestamente parecía una piscina con tres metros de profundidad.

Donde los incendios digitales se propagan de forma

vertiginosa

gneis.
Una idea Bankinter

¿Y qué podemos hacer nosotros?

¿**Nada**, pensando que con algo de suerte, no nos ocurrirá a nosotros?

¿Seguir esperando los ataques y **defendernos en nuestras trincheras**?

Tenemos que tomar permanentemente la temperatura

Tarjetas y fraude

Ataques 'socializados' y Abuso Marca

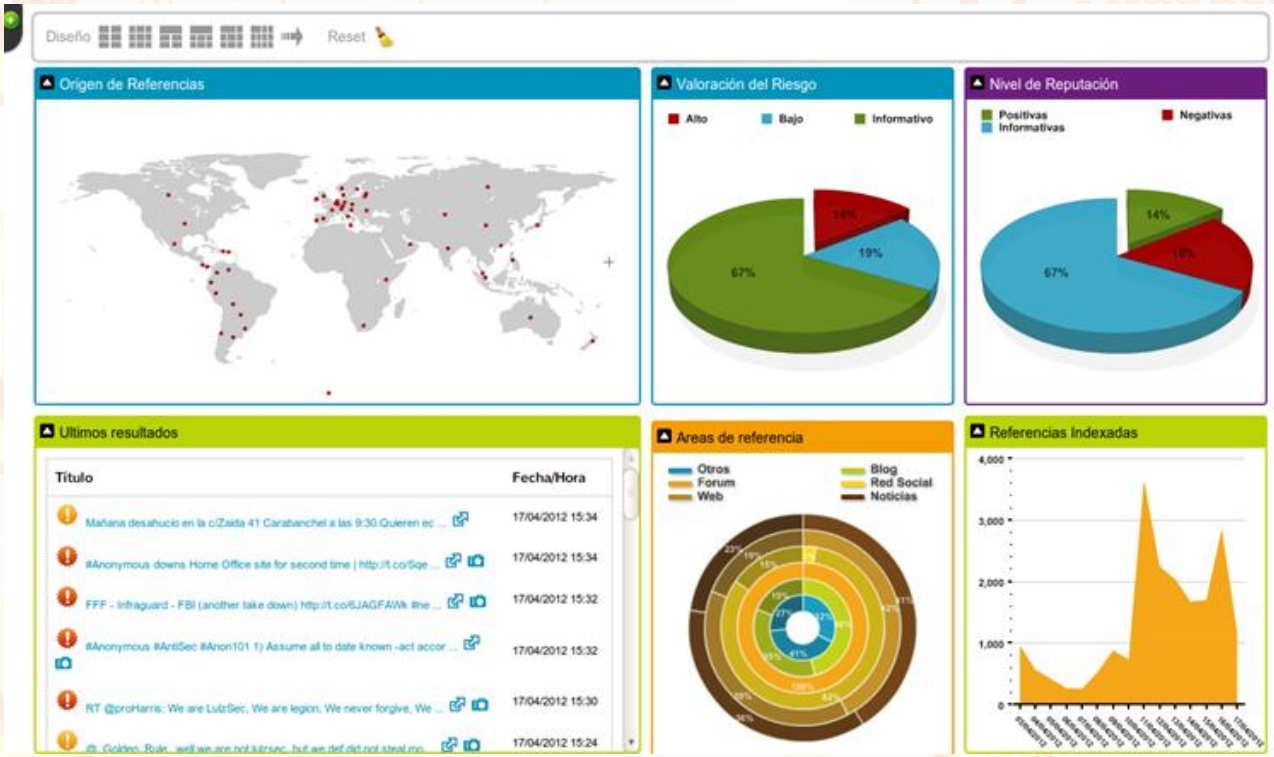
Malware 'Móvil'

Malware

Botnets & APTs

Origen y causa raíz

Tenemos que tomar permanentemente la temperatura



Resumiendo…

1997 - Premisas de seguridad

2005 - Defensa del puesto del cliente y no del puesto del banco

2007 - Sistemas de detección no intrusivos

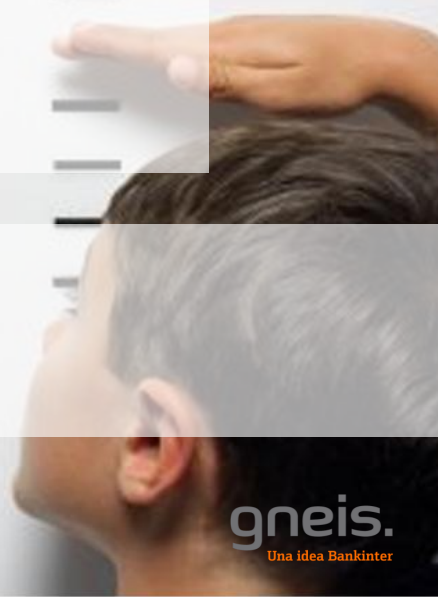
2008 - Análisis del comportamiento de la actividad del cliente

2011 - Cibervigilancia y Social Security Networks

gneis.
Una idea Bankinter

Y el futuro… (1/2)

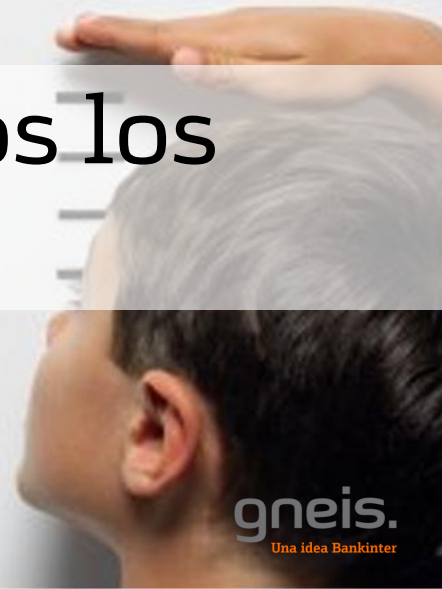
- Mayor regulación
- Compromiso con clientes
- Productividad
- Rentabilidad



gneis.
Una idea Bankinter

Y el futuro… (2/2)

- Miremos fuera del perímetro
  - Sepamos que los malos van por delante
    - Vigilemos y detectemos los fuegos



La tecnología es la misma para todos…
… hasta que alguien la utiliza de manera
diferente

Gracias

julio_sanjose

jsanjose@bankinter.es

http://www.linkedin.com/in/juliosanjose

gneis.
Una idea Bankinter