



eFraude: ganar gestionando la derrota

Madrid, Octubre 2013

Somos un nuevo banco

- Banco
 - Resultado de numerosas fusiones e integraciones
 - Diferentes marcas, mercados especializados
- Números
 - Activo 72 Mill €
 - Clientes 2,6 Millones
 - Cuota de mercado superiores al 40% en territorio origen
 - Empleados 5.600, oficinas 1,000
- Presencia
 - Todo el territorio nacional
 - Argentina, Estados Unidos, Francia, México, Portugal, Reino Unido, Alemania, Suiza y Venezuela

NCG Banco



Fraude

Acción contraria a la verdad y la rectitud que perjudica a un tercero, suponiendo la obtención de un beneficio.

e-Fraude

Tipo de delito informático:

Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el proceso automático y/o transmisiones de datos

que suponga un beneficio al que lo ejecuta

- Banking Malware
 - Keyloggers
 - Troyanos
- Fake Websites
 - Phishing
 - Pharming
 - SMiShing
 - Scam

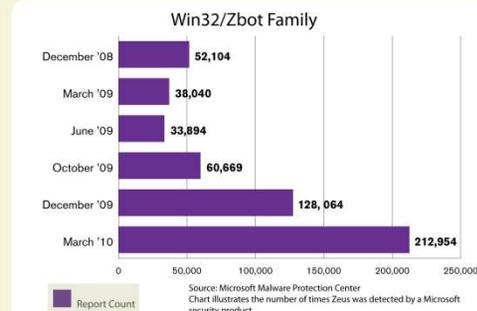
- Otros
 - Cartas Nigerianas
 - Estafa piramidal
 - Mulas
 - Hoax
 - Vishing



STATISTICS

Zeus Infections Skyrocket

Microsoft data shows the number of reported Zeus (also called Zbot) infections shot up early this year.

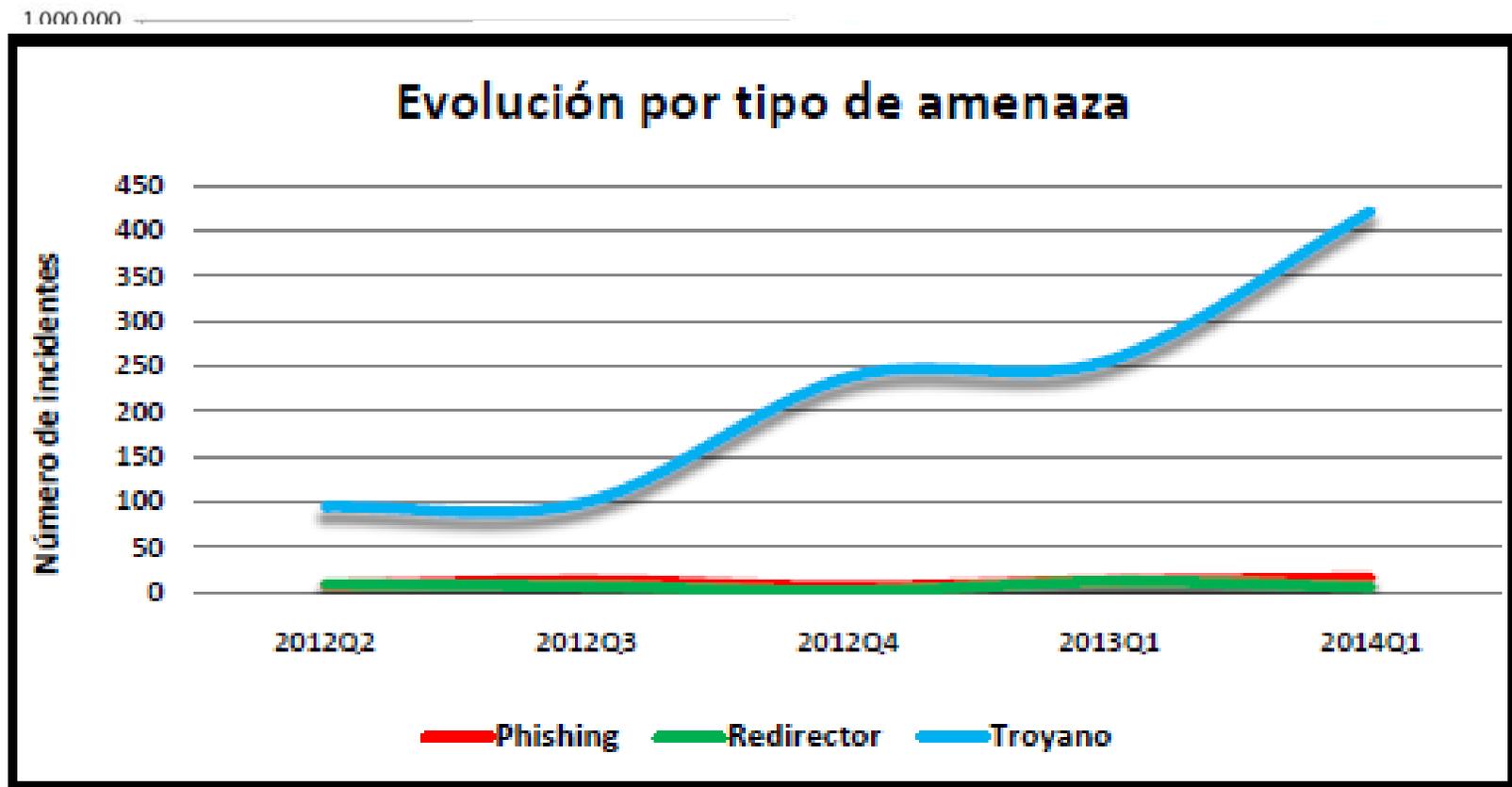


The verification code



The message changes according to the user's language

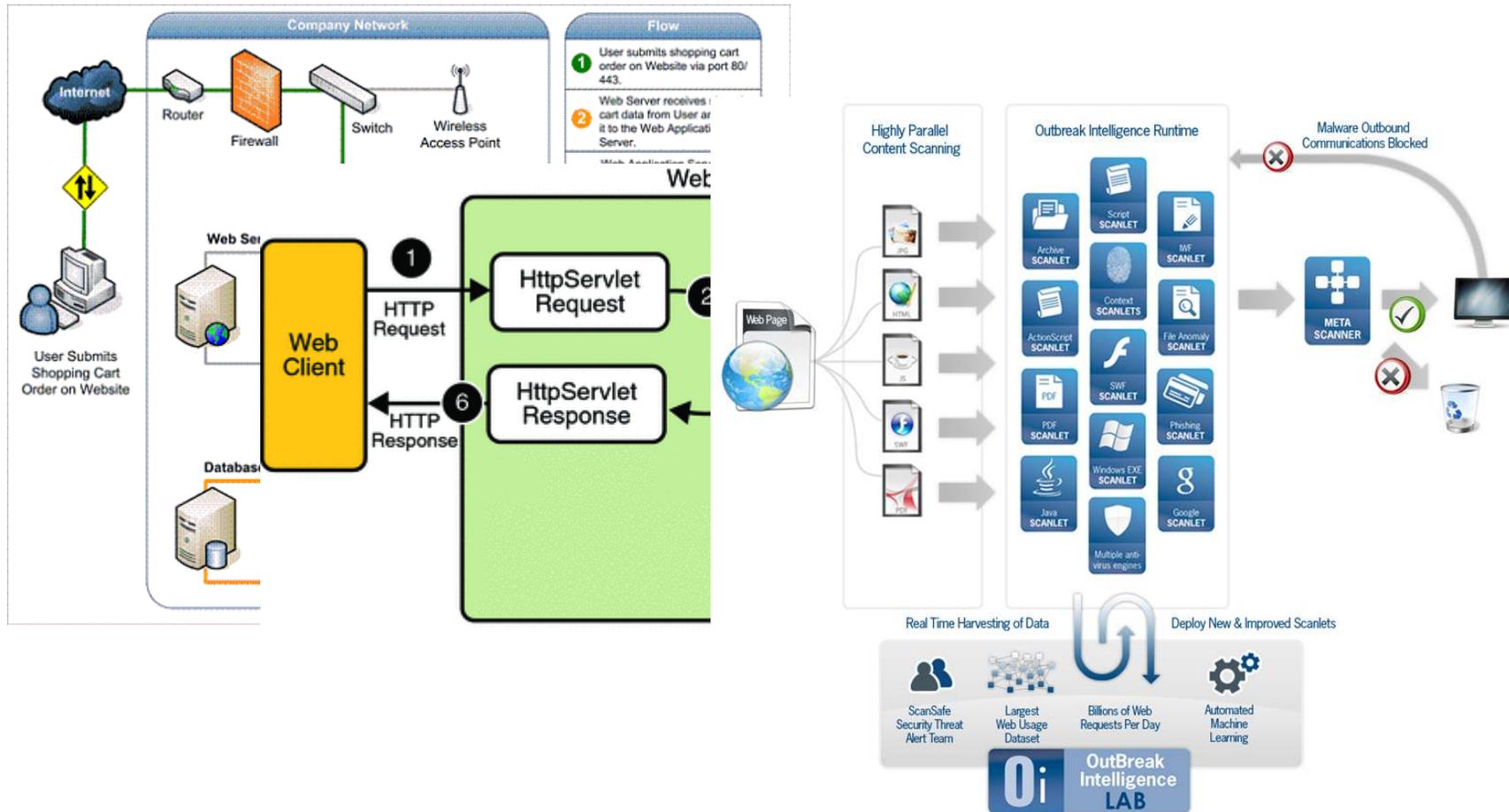
Estadísticamente...



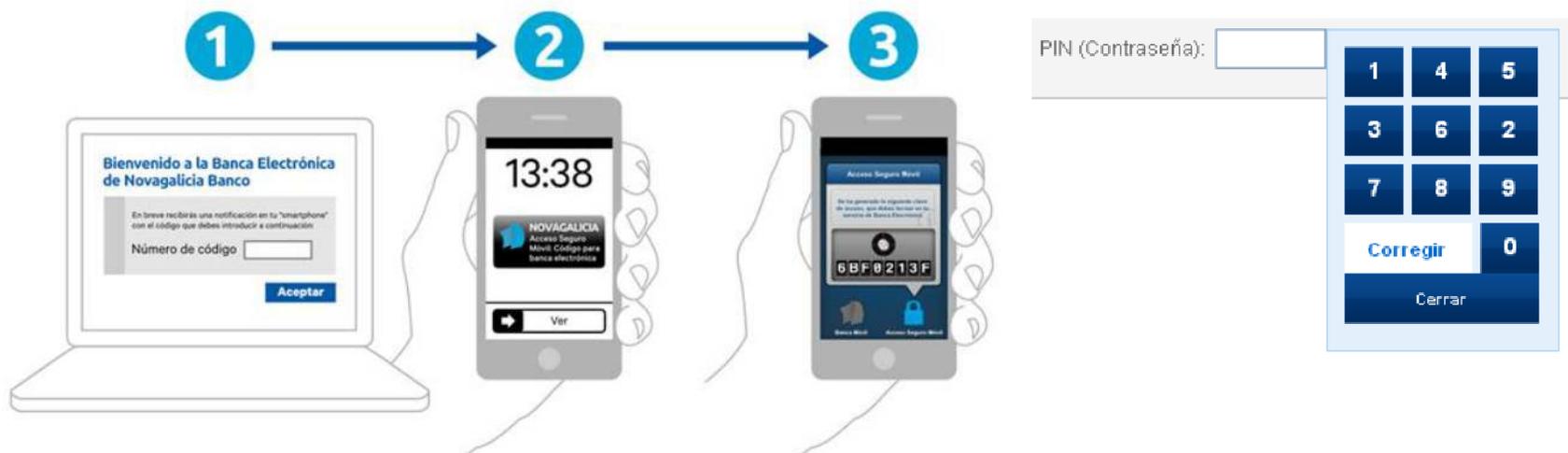
*Captura de pantalla 3: troyano
MMarketpay oculto en la aplicación
meteorológica GO Weather*

*Captura de pantalla 4: troyano
FakeDoc oculto en una aplicación para
mejorar la duración de la batería*

¿Medios técnicos suficientes?



Recuerda la usabilidad!!!



BANCA ELECTRÓNICA

0498****
6531****
5107****

Una nueva generación de Banca electrónica basada en la **seguridad**

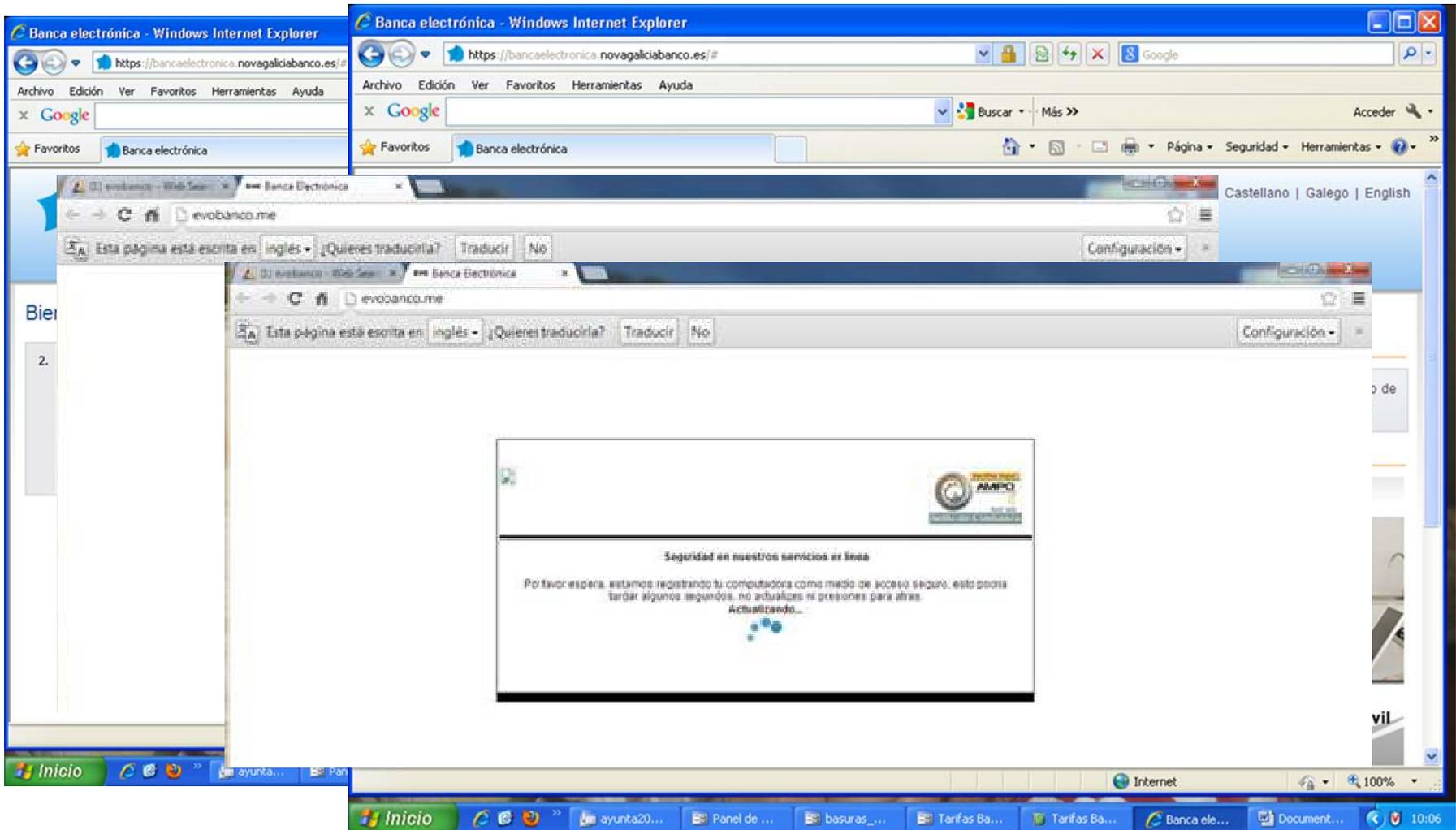
Siéntese a la Banca Electrónica más Segura

Seguridad

Para evitar posibles fraudes, te recomendamos que tomes estas sencillas medidas:

- » No accedas nunca a la banca electrónica de Novagalicia Banco desde enlaces incluidos en correos electrónicos o páginas web de terceros. Teclea directamente la URL en tu navegador o utiliza la opción "Marcadores" o "Favoritos".
- » Verifica que la página pertenece realmente a Novagalicia Banco comprobando la validez del certificado digital.
- » Evita en lo posible acceder a la banca electrónica desde localizaciones públicas como bibliotecas, cibercafés, aeropuertos, etc.
- » Cierra la sesión cuando termines de operar con la banca electrónica, **pulsando el botón "Salir"** y bloquea o apaga tu ordenador siempre que permanezca desatendido.
- » Actualiza periódicamente el software de tu navegador para incorporar las últimas mejoras y correcciones de seguridad.
- » También es recomendable que instales software antivirus, así como un programa o dispositivo "cortafuegos" y que los actualices regularmente.
- » En caso de que tengas alguna duda sobre la autenticidad de cualquier correo electrónico o sitio web que parezca proceder de Novagalicia Banco, ponte en contacto con nosotros de forma inmediata.

...pues no parece suficiente...



--Que accede a la página web de su entidad, a los efectos de consulta y realizar

PREGUNTADA la persona compareciente **DECLARA**.

Que via INTERNET, el denunciante recibió una oferta de trabajo de la empresa UNITED TECHNOLOGICS, de representante de ventas, en la cual dicha empresa se comprometía a ingresar [REDACTED] euros en la cuenta corriente del denunciante, siendo procedente dicho dinero del [REDACTED]

Que la citada empresa le comunico a la vez, que tenía que retirar el dinero antes citado y enviarlo a un tal OLEG SKORYK, natural de Ucrania.

Que el denunciante retiro los [REDACTED] euros de su cuenta corriente perteneciente del Banco NOVA GALICIA para enviarlos al citado OLEG, pensando que la citada empresa ya los había ingresado.

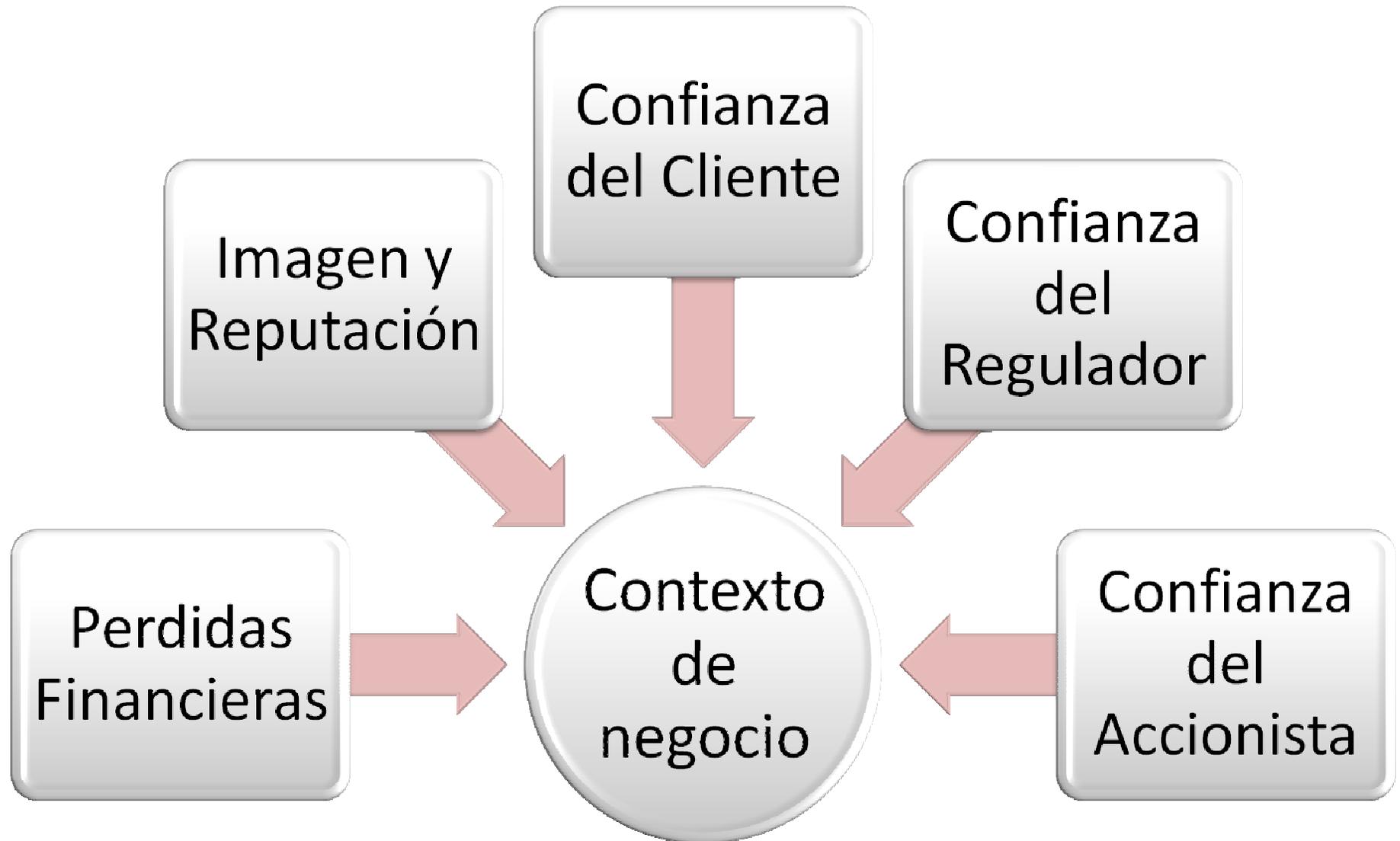
Que el problema viene de que dicho dinero nunca estuvo ingresado en la cuenta corriente del denunciante, aunque así conste en un extracto de la cuenta corriente de este, por lo que el denunciante ha perdido [REDACTED] euros de su cuenta corriente.

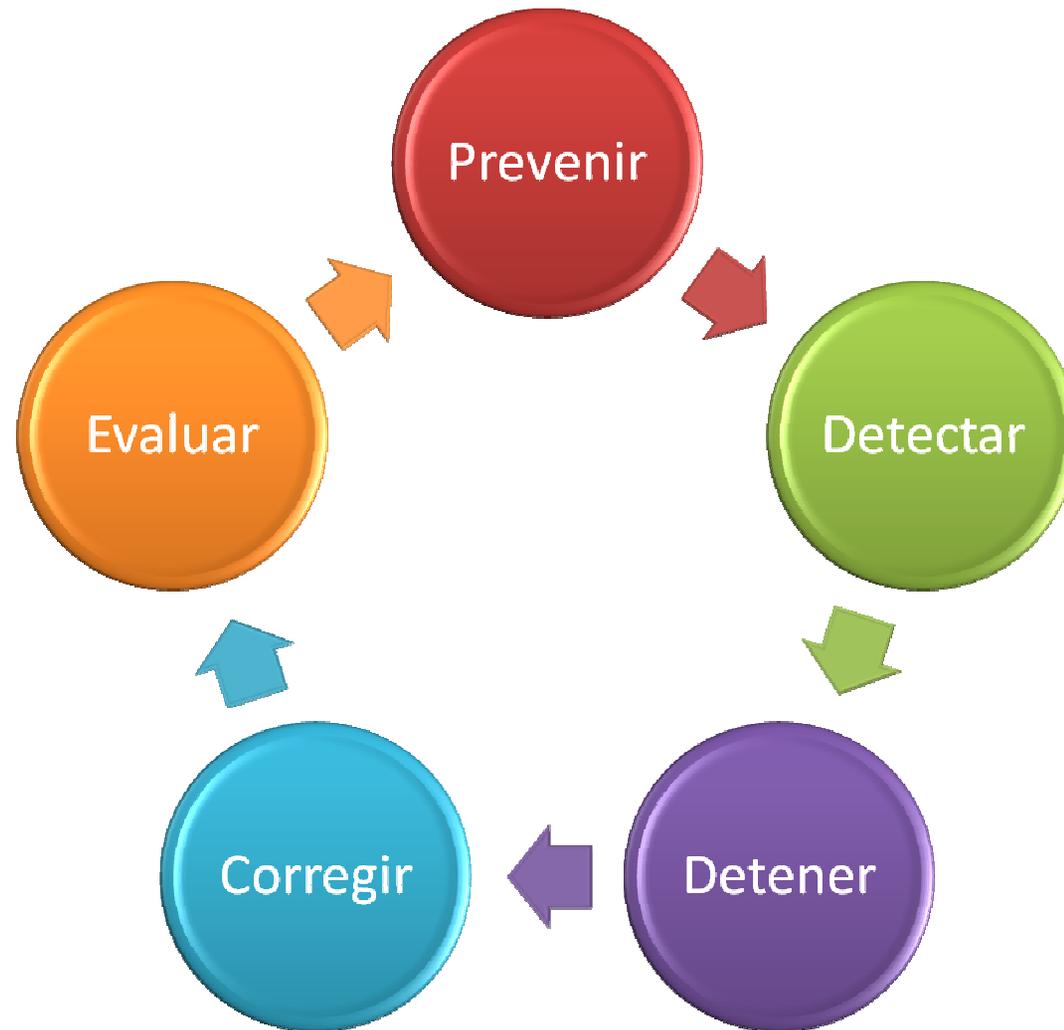
Que el denunciante quiere que se le reintegre en su cuenta corriente la cantidad de [REDACTED] euros.

atendida por la tarjeta número [REDACTED], si bien la dicente no había autorizado dicha solicitud, siendo informada por la encargada de la tienda de que tendría que denunciar lo sucedido, que seguramente alguien sin su consentimiento había efectuado dicho duplicado de su tarjeta y que ella no podía facilitar mas información.

- Procedimientos
 - **Normativa**: qué podemos hacer
 - **Negocio**: qué nos dejan hacer
 - **Uso**: qué se suele hacer







Prevenir

- Gestion de vulnerabilidades y configuraciones
- Seguridad código y aplicaciones
- Concienciación

Detectar

- Monitor de operaciones
- Correlación e histórico
- Alertas

Detener

- ERI – Equipo Respuesta a Incidentes
- Limites operativos
- Sentido común

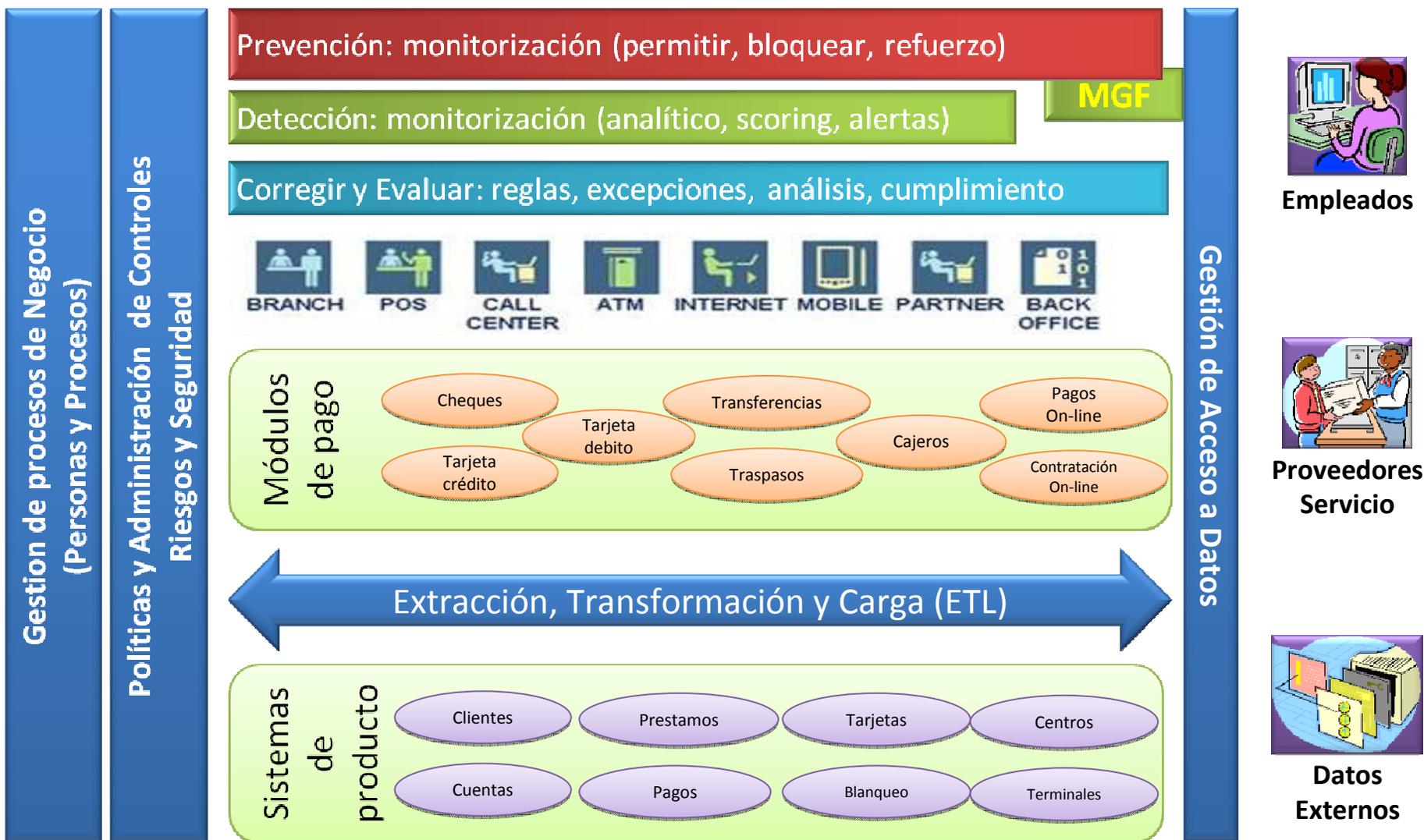
Corregir

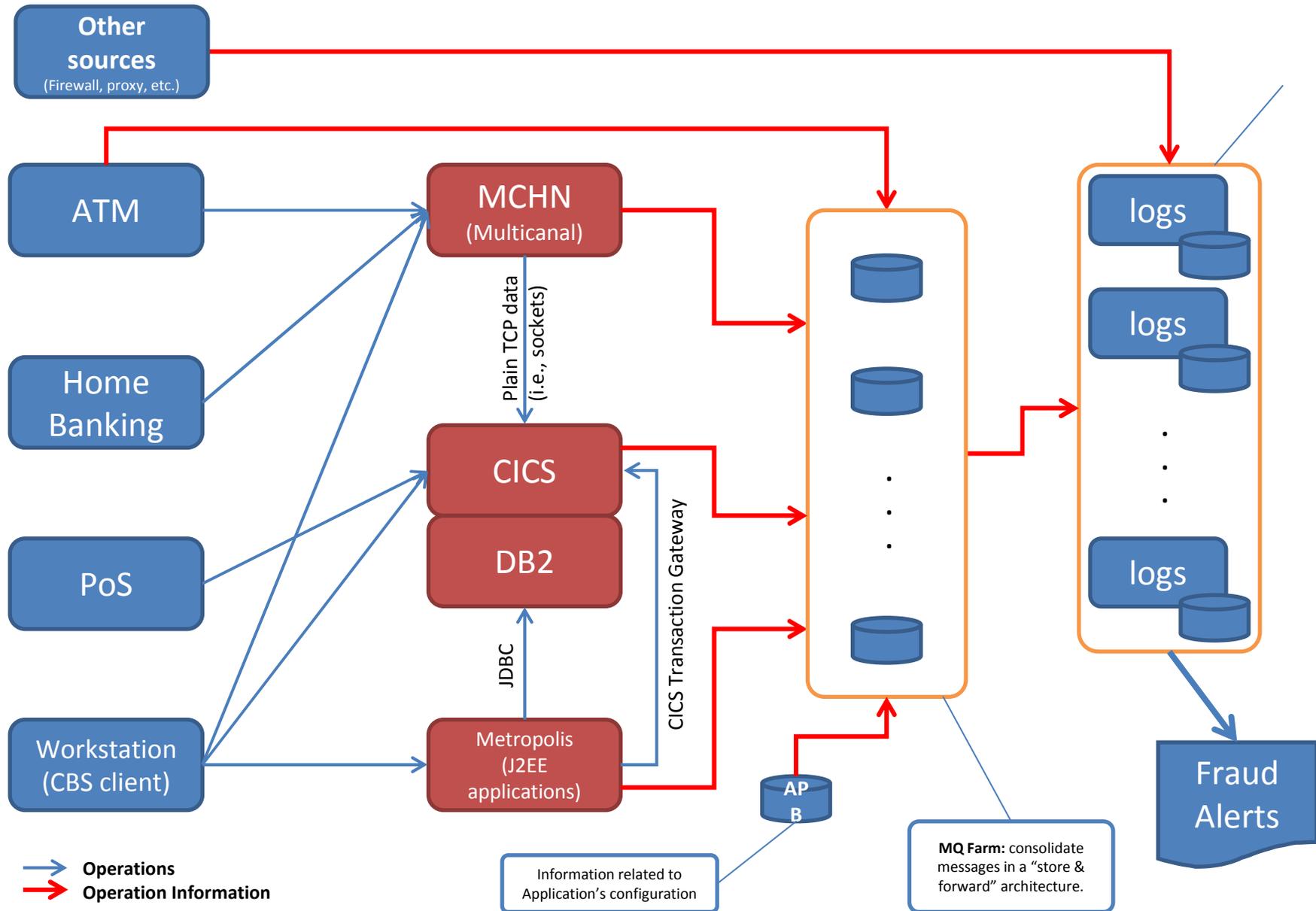
- Colaboración entre entidades
- FFSS
- Denuncia y seguros

Evaluar

- Gestion de riesgos especifica
- Revisión de casos y comunicación
- COLABORACION

eFraude arquitectura BPM







Gracias

Roberto Baratta Martínez
CISO. Gerente Seguridad TI
robertobaratta@novagalicia.es
@RoberBaratta