



Comprometidos con la seguridad

## ¿Qué pueden hacer las TIC en la Lucha contra el Fraude?

Mariano Largo

Director

S21sec FRM



## Cuando y como empezamos.

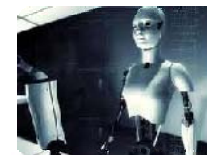
- En el año 2004 gestionamos los primeros casos de fraude sobre las Bancas Internet de nuestros clientes.
- En ese momento vimos que las tecnologías que habíamos ido desarrollando e implantado en el entorno de seguridad eran extremadamente útiles para atacar esta nueva problemática.
- En el año 2005 creamos la unidad de e-crime para focalizar otro tipos de fraude que se daban en Internet y que iban mas allá de las web de Banca Electrónica.
- En el año 2007 comenzamos el desarrollo de Herramientas específicas de monitorización de Internet.
- Durante los últimos años hemos gestionado miles de incidentes de fraude por Internet al año y reducido enormemente las perdidas por fraude de nuestros clientes.

## ¿Por qué S21sec FRM?

- Desarrollar, Implementar y Gestionar soluciones enfocadas en la prevención de fraude.
- Entendimos que cada € ahorrado por control de fraude va en positivo en la cuenta de resultados.
- Los malos en este caso no buscan notoriedad.
- Hoy somos mas de 100 profesionales en la lucha contra el fraude
- Y estos no tienen exactamente el mismo perfil que los profesionales de la seguridad.



## Algunos de Nuestros Servicios



- Fraude en Medios de Pagos.
- Fraude en Portales Internet.
- Fraude en Cajeros.
- Fraude en Telecomunicaciones.
- Fraude interno en control de accesos a la información.
- Fraude por abuso de marca.
- Fraude en canales de venta.
- Fraude por Robo de propiedad Industrial o Intelectual.
- Fraude en contadores de Tele gestión.
- etc.

## ¿ Que tecnologías utilizamos?



- **BITACORA.**

- Herramienta de Recolección Online, Almacenamiento y Búsqueda de información, que nos permite identificar los patrones de fraude y programar las alertas necesarias para poder monitorizar la actividad del negocio.

- **IRATI (Vigilancia Digital).**

- Sistema de monitorización e indexación de información tanto interna como externa que nos permite monitorizar internet en búsqueda tanto de informaciones validas para analistas o incumplimientos por terceros de los derechos de nuestros clientes, entre otros.

- **FDS.**

- Sistema experto basado en sistemas de clustering que nos permite monitorizar la actividad de accesos en una red en búsqueda de accesos sospechosos combinando varias técnicas, clustering, arboles de decisión y un motor de reglas, que aportan información a un sistema final de scoring.

- **SDA (Sistema de detección de anomalías).**

- Sistema desarrollado para detectar anomalías en la actividad habitual del negocio de manera que nos indique que se debe de mirar que es anómalo y que no esta identificado en ninguno de los patrones existentes.



# No solo con Tecnología, Metodología del Proceso



- ✓ No sabemos del negocio mas que nuestros clientes.
- ✓ Identificamos los patrones de fraude conocido.
- ✓ Identificamos las fuentes de información.
- ✓ Creamos las alertas necesarias y el procedimiento de actuación.
- ✓ Medimos el impacto y proponemos medidas si se justifican.

- ✓ Detección de incidentes.
- ✓ Monitorización de actividad.
- ✓ Ejecución de los procedimientos asociados.
- ✓ Comunicaciones a terceros.
- ✓ Solicitud de cierres de sites.
- ✓ Notificación a clientes

- ✓ Investigación del Incidente.
- ✓ Recopilación de Información Adicional.
- ✓ Análisis detallado del Incidente y obtención de conclusiones.
- ✓ Investigaciones asociadas.
- ✓ Informes de daños / impacto.

- ✓ Comunicación del incidente con las evidencias asociadas.
- ✓ Comunicación de las medidas adoptadas.
- ✓ Comunicación de informes adicionales obtenidos de otras fuentes
- ✓ Comunicación a terceros que se puedan ver afectados.

- ✓ Resumen de incidentes gestionados.
- ✓ Métricas de servicio.
- ✓ Informe de tendencias
- ✓ Recomendaciones de cambio o implantación de otras medidas.
- ✓ Etc.

## Algunas conclusiones



- **El fraude es un suceso cambiante en cada momento y las técnicas son diferentes en cada negocio / sector / país.**
- **La razón del fraude siempre es económica aunque el medio no sea siempre dinero.**
- **No solo necesitamos monitorizar la información que tenemos, hemos de poder llegar a otras informaciones publicadas.**
- **Si no luchamos contra el y tomamos medidas seguro que crecerá.**
- **El espíritu de colaboración entre los implicados es necesario.**
- **No solo lo resolveremos con tecnología, el “olfato” y las “capacidades” de los analistas es muy importante.**

# GRACIAS

SPAIN • MEXICO • BRASIL • UK • USA

[www.s21sec.com](http://www.s21sec.com)

