Módulo ANTIFRAUDE Procesadora PnP

Introducción

El modulo antifraude de Paynopain es un sistema de puntuaciones dinámicas de riesgo encargado de monitorizar en tiempo real las transacciones de las procesadoras de pago que hagan uso del mismo.

Este sistema se desarrolló a finales del 2011 y desde entonces ha sido usado y perfeccionado de forma continua. La gran aceptación que ha tenido, en especial dentro del sector de los comercios de alto riesgo en concreto las casas de apuestas, ha conseguido que a día de hoy más del 50% de las transacciones de juego online españolas sean evaluadas por este sistema.

En este documento se detalla las características actuales, el funcionamiento del sistema, y futuros desarrollos dentro del *road map* que permitirán mejorar el rendimiento sobre la base de la experiencia acumulada.

Características de la transacción

El primer paso para poder evaluar el riesgo de una transacción financiera es poder caracterizar la misma en base a los parámetros que la definan, es decir, los datos entrada en el sistema antifraude.

Actualmente dadas las necesidades de los clientes habituales de Paynopain el número de características obtenidas por cada transacción serían las siguientes:

- Importe
- Identificador de usuario (por parte del cliente)
- Número de tarjeta (PAN)
    - Banco emisor
    - País de emisión
    - Tipo de tarjeta
- Titular de la tarjeta
- Moneda
- IP
- Referer

Con estos datos el sistema es capaz de realizar una serie de cálculos y asignar una puntuación a cada una de las transacciones.
Actualmente con la entrada de sistemas de pago propios, tales como GlassPay, donde se pueden obtener una colección de datos mucho más rica, se están añadiendo nuevos parámetros:

- Geolocalización de la compra
- Tipos de productos

- Identificadores de comercio

Sistema de puntuación

Una vez recopilados todos esos datos, se carga la configuración de prevención de fraude del cliente indicado, ya que dicha configuración **debe amoldarse a las necesidades de cada tipología de comercio y sus clientes.**

Esta configuración se compone de un conjunto de reglas definidas en el sistema que una transacción puede cumplir o no. A cada una de estas reglas, además, se les asigna una puntuación mayor o menor dependiendo en la importancia que esta tiene para el comercio en cuestión.

El sistema aplica cada una de estas reglas sobre la transacción evaluada, para ello realiza una serie de comprobaciones sobre el histórico de transacciones del cliente: la tarjeta, la IP y las comprobaciones de seguridad del usuario final.

Tras esta operación y teniendo en cuenta las puntuaciones asignadas por el comercio, la transacción obtiene una puntuación de riesgo. Dependiendo de si esta puntuación supera o no los umbrales establecidos la procesadora de pagos que use el sistema puede aplicar sus medidas para mitigar los riesgos de fraude tanto para el comercio como para el usuario final.

Reglas puntuables

Las distintas reglas que se pueden configurar a día de hoy en el sistema, son las que se enumeran a continuación:

- Número de transacciones correctos realizados con la misma tarjeta en 24 horas.
- Número de transacciones correctos realizados a través de la misma IP en 24 horas.
- Número de transacciones incorrectos realizados con la misma tarjeta en 24 horas.
- Número de transacciones incorrectos realizados con la misma tarjeta en 24 horas.
- Frecuencia máxima permitida de pagos a través de una misma IP.
- Frecuencia máxima permitida de pagos con una misma tarjeta.
- Número de pagos semanales superiores a una cantidad determinada siendo esta la habitual para el tipo de comercio.
- Número de pagos mensuales superiores a una cantidad determinada siendo esta la habitual para el tipo de comercio.
- Número máximo de tarjetas distintas que pueden ser usadas a través de una misma dirección IP.
- Número máximo de IPs distintas que pueden usar la misma tarjeta.
- Importe de la transacción superior a una cantidad determinada.
- Tarjetas distintas usadas por un mismo identificador de cliente en los últimos 30 días.

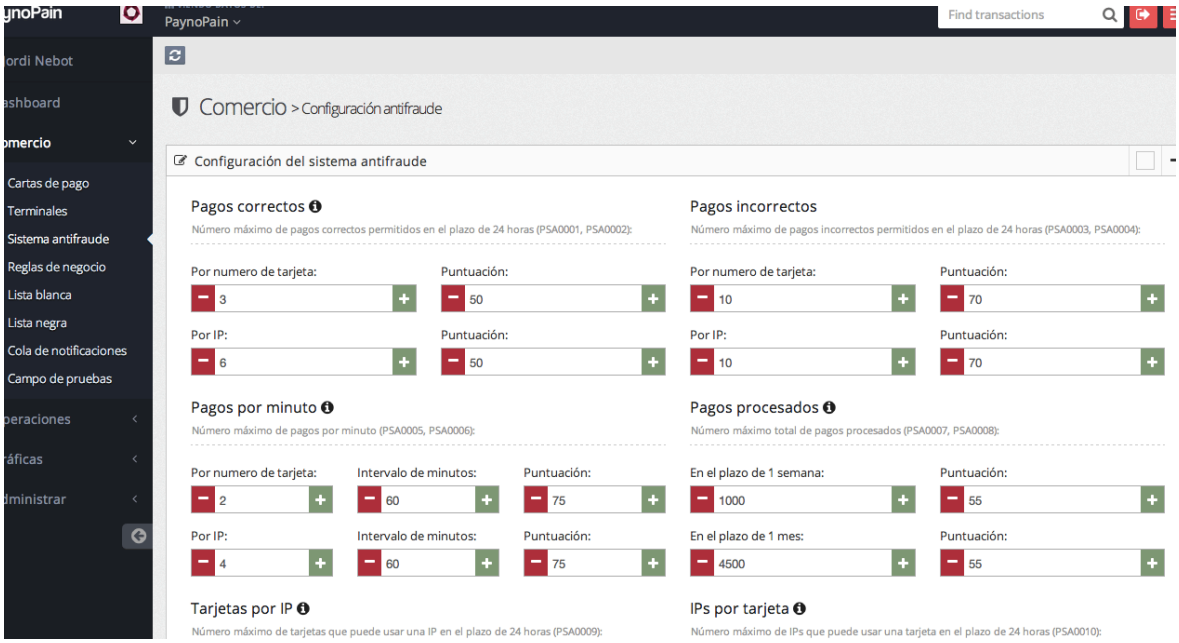
- No coincidencias del país de emisión de tarjeta y el país de origen de la dirección IP.
- Uso de proxy.
- Uso de un nodo de la red TOR.
- Uso sucesivo de tarjetas con numeraciones muy similares o secuenciales.
- Coincidencia de alguno de los campos con las listas negras (Identificador de usuario, número de tarjeta, IP o país)
- Tarjeta usada por distintos identificadores de usuarios en el último mes.

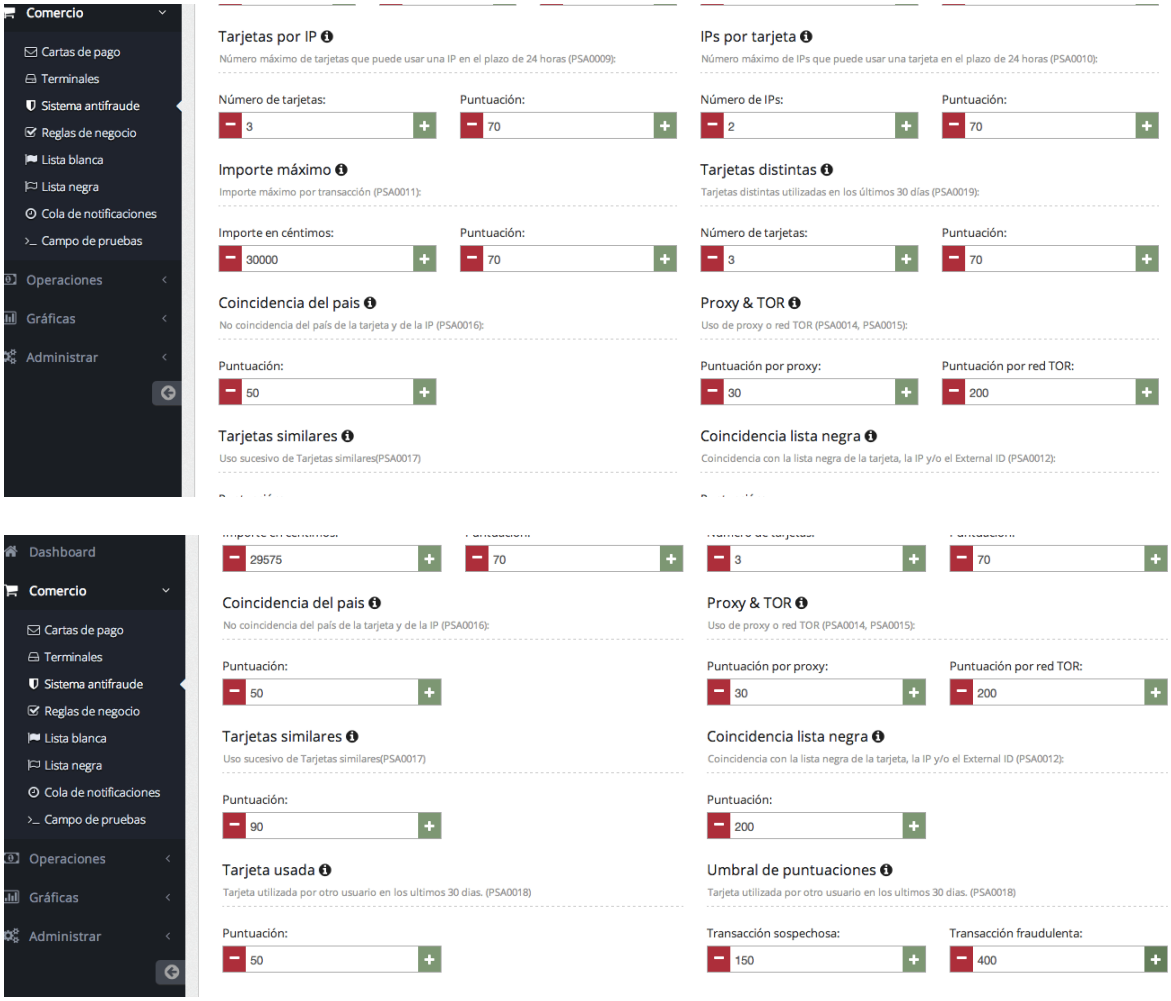
Todas estas reglas son las que al final aportan una puntuación determinada a cada transacción. El sistema permite definir dos umbrales de puntuación para poder aplicar medidas menos restrictivas si sólo se supera el primer nivel y medidas mucho más severas si se superan ambos umbrales:

- Transacción Sospechosa
- Transacción Fraudulenta

Caso de uso: Procesadora Paynopain

A continuación se puede observar la interfaz de usuario desarrollada por Paynopain para usar el sistema antifraude. Se debe recalcar que cada cliente del sistema antifraude podría personalizar esta interfaz acorde a sus necesidades.





En este ejemplo la procesadora ha utilizado la configuración de los umbrales para darle un comportamiento un poco más inteligente al proceso de pago, siempre buscando maximizar los beneficios de nuestros clientes minimizando al máximo el riesgo de fraude.

Cuando una transacción supera el umbral llamado **Transacción Fraudulenta**, Paynopain directamente rechaza el pago. Sin embargo cuando simplemente se supera el primer umbral **Transacción Sospechosa**, se activa un proceso llamado **reglas de negocio**, que en lugar de aplicar una medida tan restrictiva como bloquear una transacción, busca otras opciones que no tengan un impacto tan grande en la facturación, p.e: Pagos seguros, preautorizaciones, uso de otra entidad bancaria, etc. Se aporta más información sobre este sistema de **reglas de negocio** en los anexos.

Futuros desarrollos

Con la incorporación de nuevas características diferenciales en cada transacción financiera, surgen nuevas reglas a aplicar así como nuevos mecanismos más sofisticados a aplicar.

Por un lado, la incorporación del *conocimiento completo del usuario* que realiza las compras, puede permitir desarrollar estadísticas sobre sus hábitos de compra: edad, sexo, raza, país de nacimiento, cantidades habituales, tipología de productos, zonas geográficas donde suele

comprar, etc.

Por el otro lado, el aumento de conocimiento del propio comercio también permite añadir nuevas características tales como: Destinos habituales de sus productos, compras medias de los usuarios de la tienda, etc.

Ambos campos se pueden combatir a través de un sistema de reglas, creando nuevas reglas como serían:

- Ubicación del usuario fuera del destino habitual de las entregas del comercio.
- Tipo de producto poco frecuente dentro del perfil del usuario.
- Importe fuera del hábito de compra del usuario
- Importe fuera del hábito de compra de su rango de edad

Dado que estas reglas son mucho más complejas, la solución en la que estamos trabajando incluye el desarrollo de un sistema de aprendizaje automático o semiautomático, que entrene un sistema de toma de decisiones. El objetivo es probar con todos los algoritmos dentro del state-of-art en el momento del desarrollo, presumiblemente: Redes neuronales con retropropagación, arboles de decisión, discriminantes lineales, bayesianos, SVMs.

Anexo 1: Reglas de negocio

Como se ha comentado previamente la procesadora Paynopain ha diseñado un sistema inteligente para usar el módulo de prevención de fraude minimizando el impacto en la facturación, esto es posible a la implantación de las denominadas **reglas de negocio.**

Las reglas de negocio son una funcionalidad del sistema de pagos de PayNoPain que permite a los clientes fijar unas condiciones a la hora de tramitar un pago que, cuando se cumplen, realizan cambios en el los datos del mismo.

Cuando se define una regla de negocio hay 3 valores básicos:

- ✓ el campo,
- ✓ el operador
- ✓ el valor.

El campo, entre los datos a evaluar de una transacción se encuentran los siguientes (se han obviado el resto para simplificar la explicación):

- Moneda.
- Importe.
- Identificador de usuario.
- Resultado del sistema antifraude.
- País de la IP.
- País de emisión de la tarjeta.

El operador, puede ser cualquiera de los típicos “lógicos” (mayor, menor, igual, etc.)

El valor, puede ser cualquier cosa que tenga sentido para el campo en cuestión.

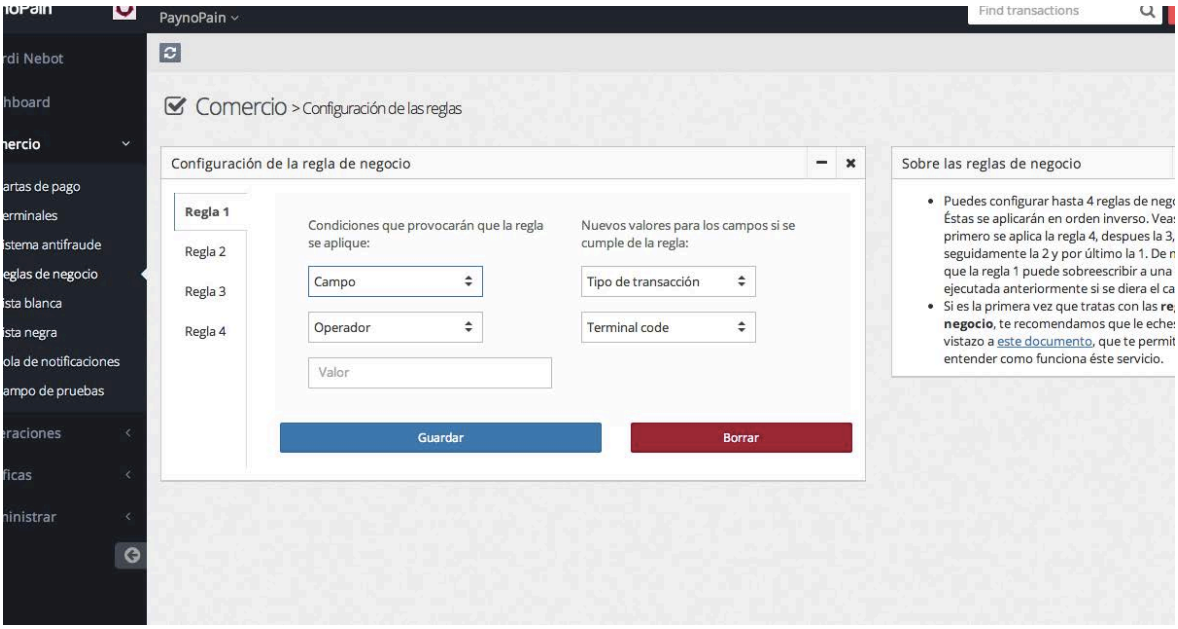
La conclusión de las acciones a realizar cuando se cumple un resultado determinado son:

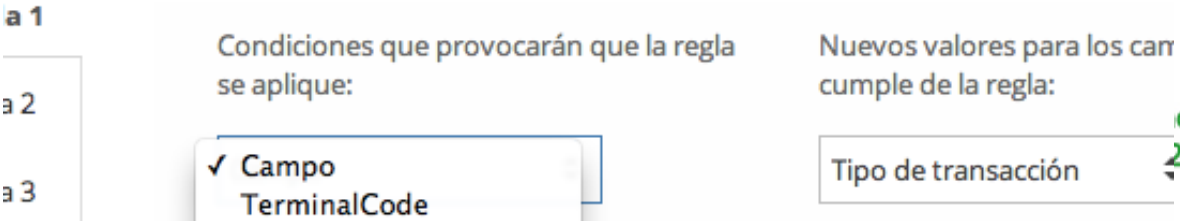
- Cambiar el tipo de transacción (Autorización, autorización en diferido, autorización segura, devolución).
- Cambiar el banco adquiriente.
- Cambiar entre pago seguro y no seguro.

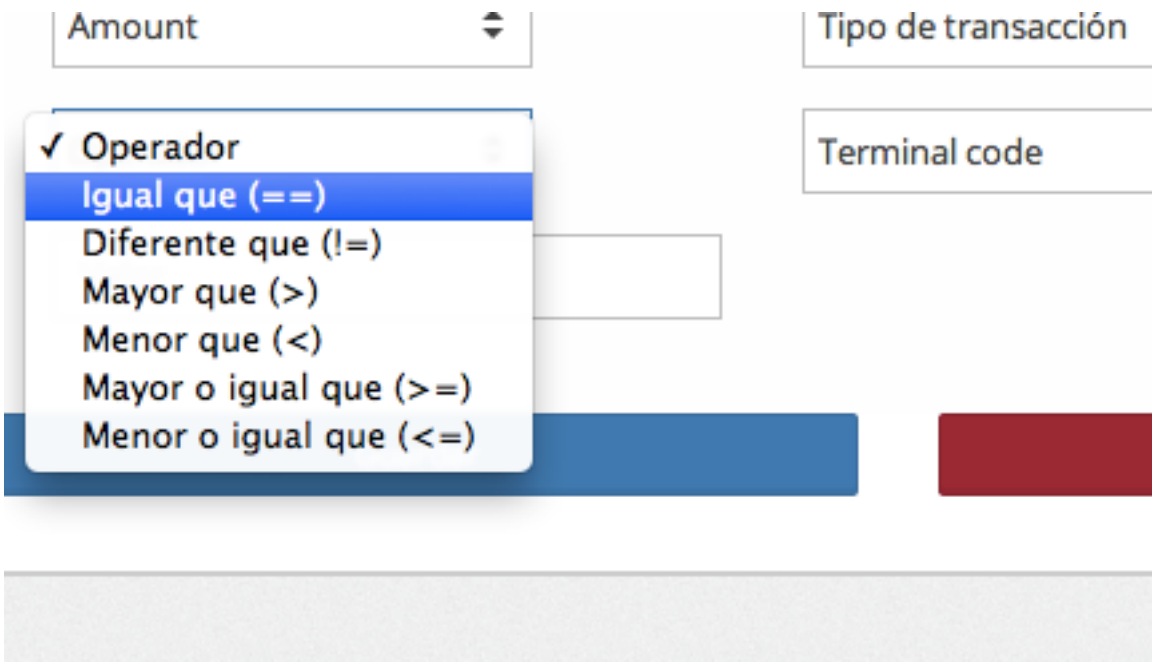
Unos ejemplos prácticos de configuración de estas reglas de negocio son las que se enumeran a continuación :

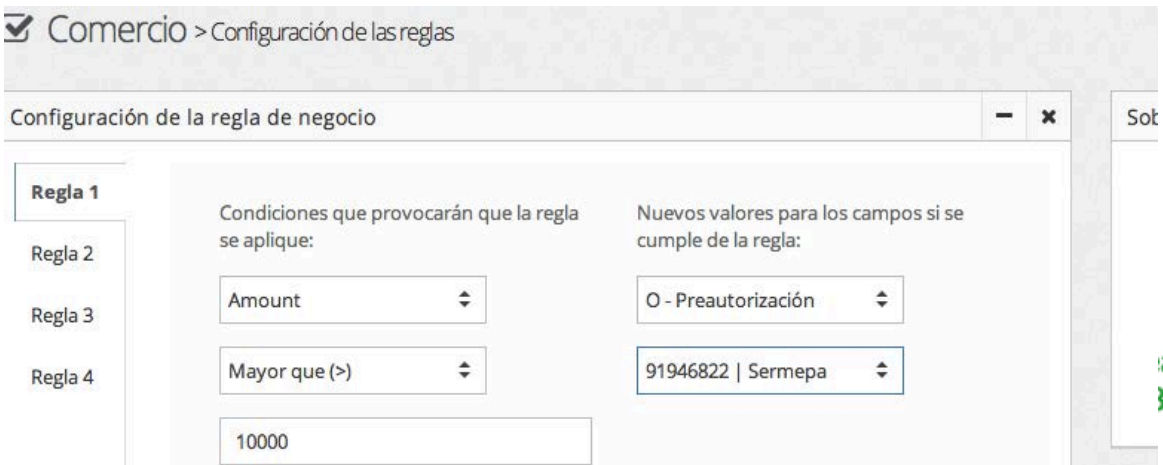
- *Redirigir una transacción que ha superado el **primer umbral de fraude** a una TPV segura (El fraude cometido en este tipo de terminales es asumido por el banco emisor de la tarjeta. Por contrapartida, al ser un proceso de pago un poco más complejo, hay usuarios que no finalizan este proceso)*
- *Cambiar el tipo de transacción de 'Autorización' a 'Autorización en diferido' cuando la operación supera el primer umbral de fraude de forma que esta operación sea estudiada por el departamento de riesgo y validada antes de ser procesada definitivamente.*
- *Cambiar el banco adquiriente cuando un pago no supera una cantidad determinada para minimizar las comisiones.*
- *Cambiar el banco adquiriente cuando los pagos vienen de una serie de países para maximizar el porcentaje de aceptación de las autorizaciones.*
- *Cambiar el banco adquiriente según el tipo de moneda y la cantidad.*

A continuación se muestra un ejemplo real del sistema:






Amount
Tipo de transacción
✓ Operador
Igual que (==)
Diferente que (!=)
Mayor que (>)
Menor que (<)
Mayor o igual que (>=)
Menor o igual que (<=)
Terminal code


Comercio > Configuración de las reglas
Configuración de la regla de negocio
Regla 1
Regla 2
Regla 3
Regla 4
Condiciones que provocarán que la regla se aplique:
Nuevos valores para los campos si se cumple de la regla:
Amount
O - Preautorización
Mayor que (>)
91946822 | Sermepa
10000

Anexo 2: Certificados

El PCI Security Standards Council es un foro mundial abierto, establecido en 2006, que se encarga de la formulación, gestión, educación y conocimiento de las Normas de seguridad de la industria de tarjetas de pago (PCI), entre ellas: La Norma de seguridad de datos (DSS), la Norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de Seguridad de transacciones con PIN (PTS).

Certificaciones estándar de seguridad de primer orden a nivel internacional (PCI e ISO 27001). Los clientes pueden gozar de las ventajas de estar certificados sin tener que cumplir las certificaciones, ya que el servicio que ofrecemos esta diseñado para gestionar todo lo referente a PCI.

El PCI Security Standards Council es un foro mundial abierto, establecido en 2006, que se encarga de la formulación, gestión, educación y conocimiento de las Normas de seguridad de la industria de tarjetas de pago (PCI), entre ellas: La Norma de seguridad de datos (DSS), la Norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de Seguridad de transacciones con PIN (PTS).

Los cinco miembros fundadores han acordado incorporar la PCI DSS como los requisitos técnicos de cada uno de sus programas de cumplimiento en materia de seguridad de datos. Cada miembro fundador también reconoce que los Evaluadores de seguridad certificados (QSA) y los Proveedores aprobados de escaneo (ASV) certificados por el PCI Security Standards Council están habilitados para validar el cumplimiento con la PCI DSS.

La misión del PCI Security Standards Council es aumentar la seguridad de los datos de cuentas de pago mediante la promoción de la educación y el conocimiento sobre las Normas de seguridad de la PCI (Industria de tarjetas de pago). Las empresas fundadoras de esta organización son American Express, Discover Financial Services, JCB International, MasterCard y Visa, Inc.

Las medidas que han sido implantadas pueden verse en:

https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php


PCi
Security
Standards Council
™