



# Guía para la Detección del Fraude Basada en Reglas

# Tabla de Contenidos

<b>¿Qué es una Regla de Detección de Fraude?</b>	<b>2</b>
<b>Sistemas para la Detección de Fraude Basados en Reglas</b>	<b>3</b>
Reglas Estáticas Para la Detección del Fraude	3
Reglas de Puntuación Para la Detección de Fraude	5
Reglas de Velocidad para la Detección del Fraude	6
Reglas de Machine Learning para la Detección del Fraude	7
<b>Los Beneficios de una Solución de Prevención de Fraude Basada en Reglas</b>	<b>8</b>
La capacidad de escalar y automatizar	8
Fricción dinámica	8
Reducir las tasas de fraude con el tiempo	8
<b>Cómo Elegir una Solución de Detección de Fraude Basada en Reglas</b>	<b>9</b>
<b>Cómo Realiza SEON la Detección de Fraude Basada en Reglas</b>	<b>9</b>
<b>Preguntas Frecuentes</b>	<b>10</b>
¿Por qué elegir una solución de prevención basada en reglas?	10
¿Cuál es el método de detección de fraude más común?	10
¿Qué tipo de algoritmo se usa para la detección de fraude?	10



Las reglas de detección de fraude son la piedra angular de una estrategia de gestión de riesgo adecuada, y es igual de importante escalarla conforme crezcas como compañía.

Examinemos esas reglas más a detalle a continuación, incluyendo ejemplos concretos que puedes aprovechar hoy.

## ¿Qué es una Regla de Detección de Fraude?

Una regla de detección de fraude es una condición que te ayuda a decidir si una actividad es fraudulenta o no. La regla se establece para permitirte **revisar, declinar o aprobar** una acción de usuario. Esto puede ser con base en una correlación, estadísticas o comparación lógica.

Una regla de fraude necesita datos activos. Por ejemplo, los datos pueden ser una dirección de IP.

Supongamos que sabes que una dirección IP le pertenece a un estafador y aparece en una lista negra. El tipo de regla más básico con base en la lógica if/then podría ser:

```
if IP address = 192.168.1.1, then block website access.
```

Claro que tener acceso a más datos (particularmente a través del **enriquecimiento de datos**) te permite tener mayor precisión al decidir qué se considera fraude y qué no.

Además, **apilar varias reglas de fraude te permite llevar a cabo una puntuación de fraude**, que los negocios utilizan para mitigar el riesgo como les sea más conveniente.

La detección de fraude basada en reglas abarca tanto las reglas básicas estáticas como las complejas verificaciones de velocidad, en las que observas ciertas acciones en un período de tiempo específico. Esta última está diseñada para analizar el comportamiento del usuario en lugar de observar puntos de datos aislados.

# Sistemas para la Detección de Fraude Basados en Reglas

No todos los fraudes se crean de igual forma. Veamos cinco tipos diferentes de reglas con ejemplos claros con base en la plataforma de SEON.

## Reglas Estáticas Para la Detección del Fraude

Una regla estática es la forma más básica de regla de fraude y tiende a seguir una lógica simple if/then. Se considera estática cuando el resultado de la regla es estricto e inflexible, por ejemplo, bloquear una acción del usuario.

Históricamente, las primeras reglas estáticas tenían que ver con las direcciones IP. Si una IP era hallada en una lista negra, el usuario sería bloqueado.

Sin embargo, **las reglas estáticas pueden ser tan creativas como lo desees** con base en los datos que tienes a la mano.

Digamos, por ejemplo, que tienes acceso a la información de IP y los detalles de tarjeta de crédito. Tu regla estática puede conformarse de hasta dos parámetros.

El primer parámetro marcará los detalles de tarjeta de crédito que apunten a Estados Unidos.

ADD YOUR RULE PARAMETER

Rule parameter type ⓘ \*

Data field ⓘ \*

Operator ⓘ \*

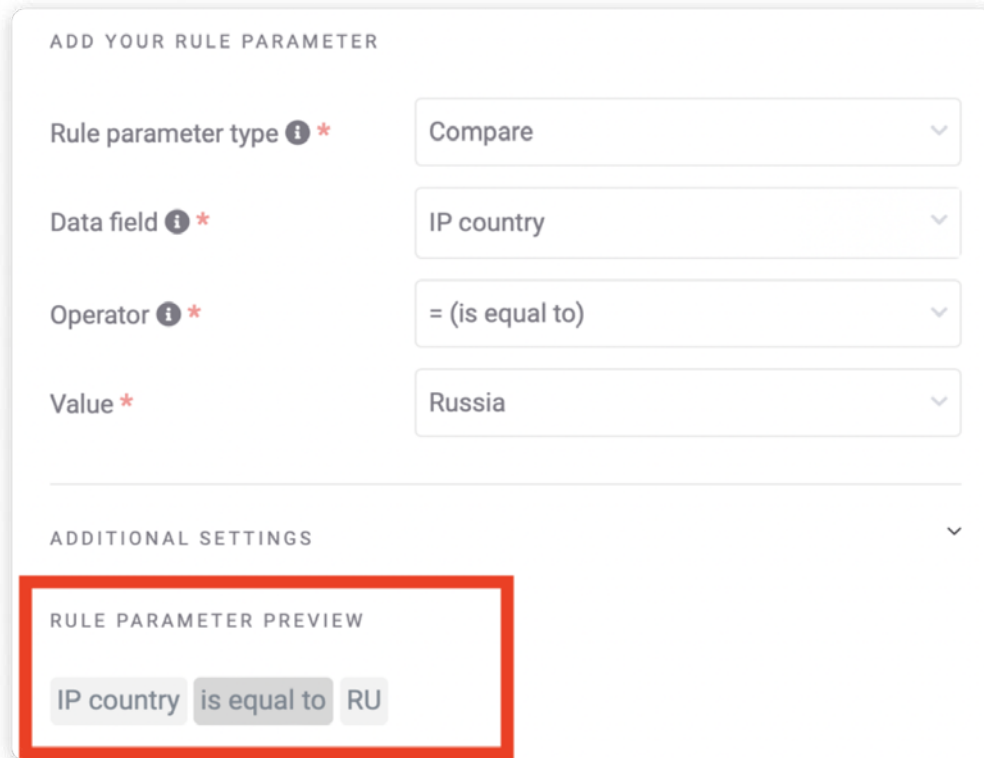
Value \*

ADDITIONAL SETTINGS ▾

RULE PARAMETER PREVIEW

Card country is equal to US

El segundo parámetro observará las direcciones de IP que apuntan a Rusia.



ADD YOUR RULE PARAMETER

Rule parameter type ⓘ \* Compare

Data field ⓘ \* IP country

Operator ⓘ \* = (is equal to)

Value \* Russia

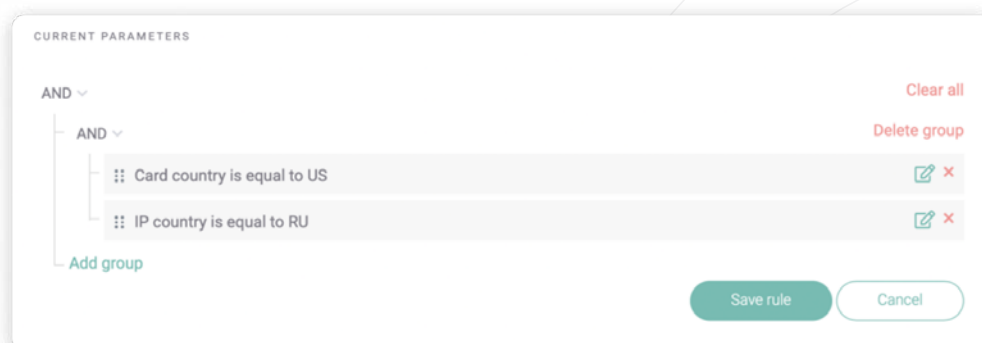
ADDITIONAL SETTINGS

RULE PARAMETER PREVIEW

IP country is equal to RU

Entonces nuestra regla puede ser la siguiente:

Si(If) el país de la tarjeta de crédito del usuario apunta a Estados Unidos pero su IP apunta a Rusia, entonces (then) la transacción debería ser bloqueada.



CURRENT PARAMETERS

AND

AND

Card country is equal to US

IP country is equal to RU

Add group

Clear all

Delete group

Save rule

Cancel

Aunque las reglas estáticas pueden ser extremadamente sofisticadas, una clara desventaja es su falta de flexibilidad. En el mundo de la **prevención del fraude**, esto se refleja en un gran número de **falsos positivos**.

Los falsos positivos son perjudiciales para cumplir tus objetivos (ya que bloqueas a clientes legítimos), y terribles para tu reputación de negocio. Los buenos usuarios cuyas acciones

son bloqueadas automáticamente estarán comprensiblemente frustrados y potencialmente buscarán otras opciones. Incluso pueden correr la voz a sus amigos y conocidos.

Es por ello que a menudo es mejor utilizar las reglas de fraude como indicadores. Aquí es donde entran las reglas de puntuación de fraude...

## Reglas de Puntuación Para la Detección de Fraude

Las reglas de fraude no siempre tienen que bloquear acciones. Algunas veces, querrás que te informen sobre tu estrategia de riesgo, y esto se logra gracias a las puntuaciones de riesgo.

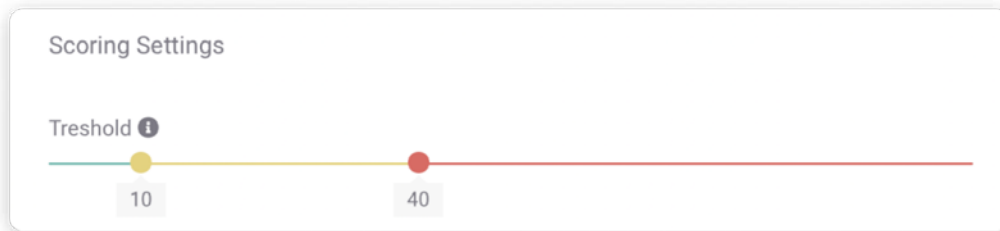
A continuación hay ejemplos de reglas de puntuación de fraude. Observa la columna "score": cada una añade un número de puntos para calcular en última instancia lo riesgosa que es esta acción de usuario, y por lo tanto lo que debería hacer el sistema al respecto.

OFF/ON	ID	RULE NAME	ACTION	SCORE	CATEGORY
<input checked="" type="checkbox"/>	HC132	Card is corporate or business	+	0	Other Rules
<input checked="" type="checkbox"/>	HC131	Card is virtual or prepaid	+	0	Other Rules
<input checked="" type="checkbox"/>	E130	Customer is using Private Email Relay Service	+	2	Email Rules
<input checked="" type="checkbox"/>	P114	Customer is using a harmful IP address	+	2	IP Rules
<input checked="" type="checkbox"/>	PH105	Phone is disposable	+	10	Phone Rules
<input checked="" type="checkbox"/>	HC125	Suspicious browser profile - Spoofing	+	2	Other Rules
<input checked="" type="checkbox"/>	HC124	Browser version age is greater or equal to 5 years	+	5	Other Rules
<input checked="" type="checkbox"/>	HC123	Browser version age is between 2-5 years	+	3	Other Rules
<input checked="" type="checkbox"/>	HC122	Browser version age is between 1-2 years	+	1	Other Rules
<input checked="" type="checkbox"/>	HC121	Suspicious browser profile - High risk	+	5	Other Rules

Este negocio ha decidido claramente que la evidencia más abrumadora de que alguien es un estafador es un número de teléfono desechable. Le han asignado una puntuación de +10.

Ten en cuenta que las puntuaciones de fraude no están estandarizadas. Por ejemplo, algunas plataformas deciden que entre más baja es un puntaje, más riesgoso es el cliente. Y la puntuación funciona de forma similar.

Sin embargo, la clave está en **adaptar las puntuaciones de riesgo a las necesidades de tu negocio**. También puedes automatizar la prevención de fraude al establecer límites con base en las puntuaciones de fraude.



En el ejemplo anterior, el verde (0-10 puntos) significa **APROBAR**, el amarillo (10-40 puntos) significa **REVISAR** y el rojo (40+ puntos) significa **DECLINAR**. En la plataforma de SEON, esto se puede ajustar a voluntad fácilmente.

## Reglas de Velocidad para la Detección del Fraude

Incrementando un poco la sofisticación, tenemos las verificaciones de velocidad, o [reglas de velocidad](#).

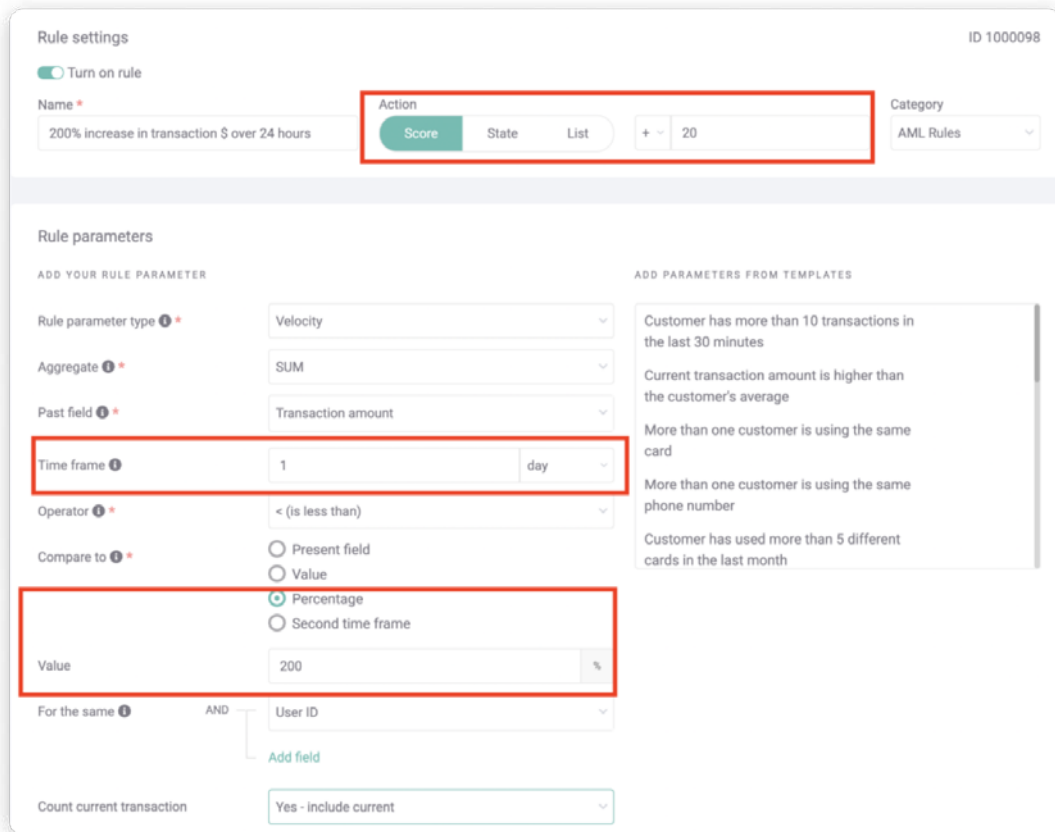
Estas reglas intentan **entender el comportamiento del usuario al observar una serie de acciones durante un periodo de tiempo**.

Un buen ejemplo de una regla de velocidad sería en la fase de inicio de sesión. Una forma para prevenir que un [ataque de robo de identidad \(ATO\)](#) tenga éxito es asegurarse de que los estafadores puedan realizar demasiados intentos de inicio. Si no tienes barreras, pueden utilizar el relleno de credenciales o la fuerza bruta para descifrar los detalles de usuario y contraseña.

Aquí es donde es útil una regla de velocidad. Tu regla podría simplemente observar el número de intentos fallidos dentro de, supongamos, 5 minutos.

Otro ejemplo sería monitorear los movimientos monetarios sospechosos. Esto puede ser útil en el contexto del AML (anti lavado de dinero).

Puede lucir intimidante, pero en esencia es sumamente simple. Aquí estamos observando un incremento en el gasto (más del 200%) en un período de 24 horas, Si eso sucede, se disparará esta regla.



Rule settings ID 1000098

Turn on rule

Name \* 200% increase in transaction \$ over 24 hours

Action: Score State List + - 20

Category: AML Rules

Rule parameters

ADD YOUR RULE PARAMETER

Rule parameter type \* Velocity

Aggregate \* SUM

Past field \* Transaction amount

Time frame \* 1 day

Operator \* < (is less than)

Compare to \*  Present field  Value  Percentage  Second time frame

Value: 200 %

For the same \* AND User ID

Count current transaction: Yes - include current

ADD PARAMETERS FROM TEMPLATES

- Customer has more than 10 transactions in the last 30 minutes
- Current transaction amount is higher than the customer's average
- More than one customer is using the same card
- More than one customer is using the same phone number
- Customer has used more than 5 different cards in the last month

En el ejemplo anterior, configuramos el sistema de tal modo que la regla arroja una puntuación de +10, pero eso depende de ti. Una opción realista podría ser también pausar automáticamente la transacción mientras se envía a una revisión manual.

## Reglas de Machine Learning para la Detección del Fraude

Por último, podemos ver lo que pasa cuando tienes un sistema diseñado para aprender programáticamente de tus casos de fraude anteriores.

Tal sistema se desarrolla con base en inteligencia artificial, y la idea es simplemente que pueda analizar grandes cantidades de datos para detectar patrones sospechosos conforme aparezcan. El sistema entonces hará sugerencias que son relevantes únicamente para ti.

Está claro que la IA (o machine learning en nuestro caso) no sabrá si las reglas son buenas o no. Necesitarás revisarlas y probarlas manualmente tú mismo, ya sea sobre datos históricos o en un ambiente sandbox.



En la plataforma de SEON, el motor de machine learning corre en tiempo real y recolecta datos de las transacciones y la puntuación conforme sucede.

Como resultado, entre más lo uses, más precisas serán las sugerencias, al tiempo que estás continúan siendo fácilmente **explicables** gracias a la naturaleza **whitebox** del módulo.

## Los Beneficios de una Solución de Prevención de Fraude Basada en Reglas

Como puedes ver por los ejemplos anteriores, la prevención de fraude basada en reglas varía dependiendo del tipo de reglas que despliegues. Sin embargo, existen varios beneficios innegables, como por ejemplo:

### La capacidad de escalar y automatizar

Aunque es posible para los pequeños negocios hacer la revisión manual de cada acción de usuario, únicamente puedes escalar tu estrategia de prevención de fraude automatizando las verificaciones con base en reglas de fraude.

### Fricción dinámica

Un gran beneficio de la detección de fraude basada en reglas es que aún puedes revisar casos manualmente si caen dentro de un área gris. Esto significa que los defraudadores obvios son bloqueados y a los usuarios legítimos se les permite el acceso sin fricción. Para asegurar que no pierdes ningún cliente legítimo, puedes introducir verificaciones adicionales para aquellos que requieran mayor comprobación en lugar de bloquearlos de inmediato.

### Reducir las tasas de fraude con el tiempo

La prevención de fraude basada en reglas está enfocada en los datos. Esto significa que puedes monitorear resultados, establecer KPIs y afinar las reglas para que se alineen con tu estrategia. Gracias al machine learning, incluso puedes obtener sugerencias que sean relevantes con base en el uso de caso de tu negocio en específico.

# Cómo Elegir una Solución de Detección de Fraude Basada en Reglas

Hay tantas estrategias de prevención de fraude como empresas en el mercado. Sin embargo, algunos fundamentos clave deben aplicar para tu solución de detección de fraude basada en reglas:

- | **¿Es efectiva?** ¿Estás obteniendo los resultados que esperabas? Algunos proveedores favorecen un enfoque con base en listas negras compartidas, mientras que otros prefieren confiar en el poder de los datos en tiempo real.
- | **¿Es flexible?** While rule-based systems sound inflexible, it doesn't have to be the case. Finding a solution that lets you stack rules, use fraud scoring, custom fields, or even machine learning suggestions will reap better rewards in the long run. And more importantly, consider whether you can deploy the right rules based on your vertical. An iGaming company has very different needs from, say, a neobank.
- | **¿Es escalable?** ¿Cuántas reglas puede soportar tu sistema? ¿Puedes ejecutar **miles de llamadas API al día**? Y, si está alojado en línea, ¿cuál es el tiempo de funcionamiento que tiene?
- | **¿Es costosa?** ¿Pagarás por cada llamada API o en conjunto por un contrato de varios años? ¿Micro cargos vs garantía de contracargos?
- | **¿Es fácil de integrar?** ¿Podrías empezar hoy mismo? ¿Cuánto esfuerzo tomaría integrarla completamente con tu plataforma?

# Cómo Realiza SEON la Detección de Fraude Basada en Reglas

En SEON antepone la flexibilidad y la personalización en todas nuestras características de prevención de fraude. Esto significa que puedes hacer todo lo que se detalla a continuación:

- | **Desplegar la solución rápidamente, sin ninguna interrupción.**
- | **Iniciar con reglas de riesgo basadas en casos de fraudes similares dentro de tu industria.**

- | **Personalizarlas completamente según las necesidades de tu negocio.**
- | **Recibir sugerencias de un poderoso motor de machine learning whitebox.**
- | **Aprovechar los beneficios de la EA black box para detectar nuevos patrones.**
- | **Añadir y editar reglas fácilmente, así como activar o desactivarlas.**

Todo está diseñado para puntuar, entender y monitorear el riesgo en tu compañía como te sea más conveniente, y con el mismo grado de flexibilidad con respecto a la integración y el pago.

## Preguntas Frecuentes

### ¿Por qué elegir una solución de prevención basada en reglas?

Todas las buenas soluciones de prevención deberían ofrecer configuraciones basadas en reglas. Estas están diseñadas para permitirte aprobar, revisar o bloquear las acciones de los usuarios automáticamente. La ventaja sobre las revisiones manuales es que puedes automatizar la prevención de fraude y escalar conforme tu negocio procese más solicitudes, transacciones e inicios de sesión.

### ¿Cuál es el método de detección de fraude más común?

El método de **detección de fraude** más común son las reglas estáticas que siguen una lógica if/then. Por ejemplo, si (if) la dirección IP aparece en una lista negra, entonces (then) deberías bloquear al usuario para que no acceda a tu sitio.

### ¿Qué tipo de algoritmo se usa para la detección de fraude?

Los algoritmos de prevención de fraude le permiten a las compañías recomendar si deberías bloquear o permitir una acción de usuario con base en un sistema de puntuaciones. Los algoritmos tienden a ser propios. Sin embargo, puedes ajustar manualmente los límites de tus reglas de riesgo para tomar el control de los algoritmos de forma manual.

