Ejemplos

Cómo se usa la API de The Fraud Explorer a través de varios ejemplos

- Insights del triángulo del fraude
- Modo Bulk para los insights
- Modo Mail Bulk

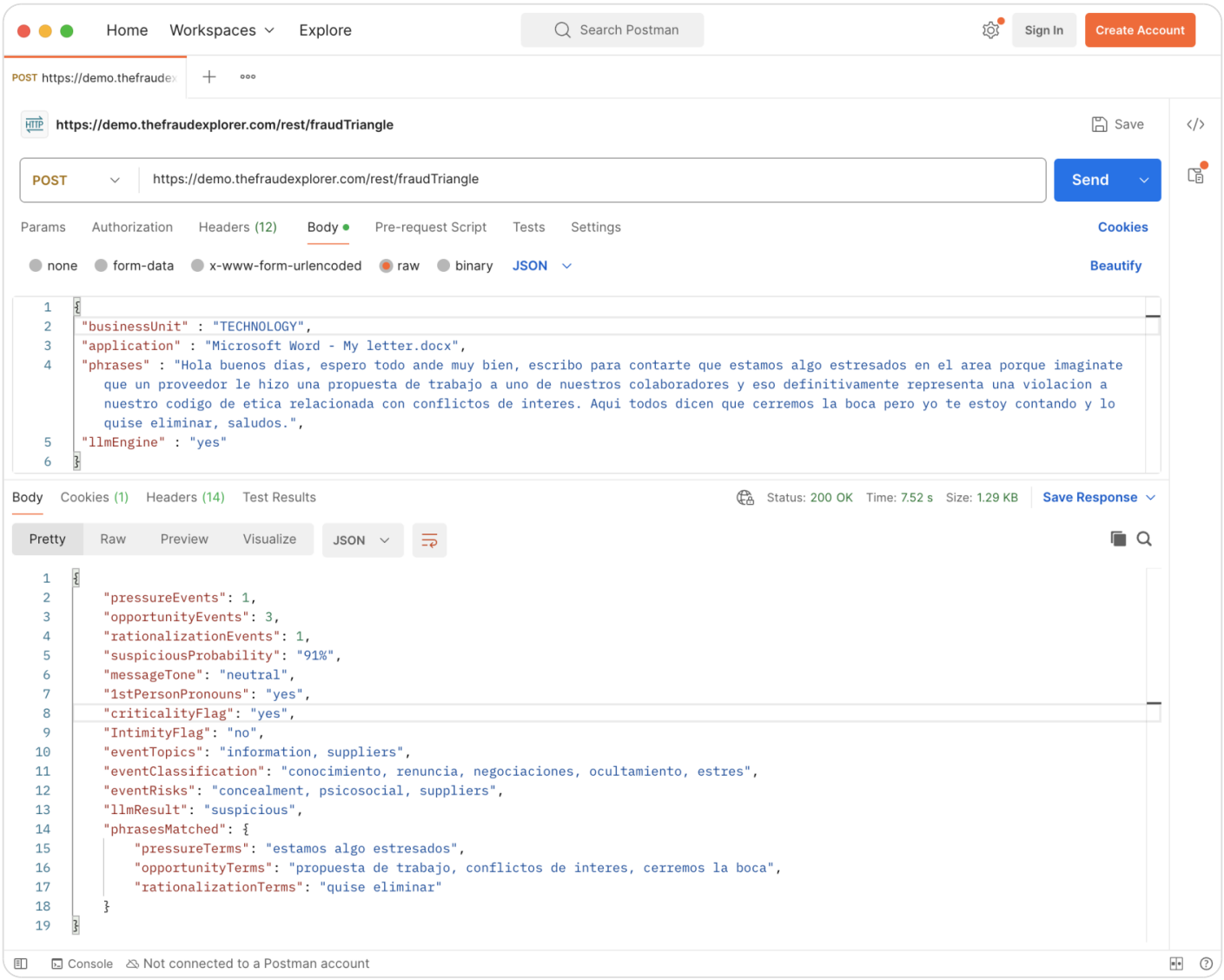
Insights del triángulo del fraude

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangle, seleccione el método **POST** y luego en la pestaña **BODY** escriba:

```
{
 "businessUnit" : "TECHNOLOGY",
 "application" : "Microsoft Word - My letter.docx",
 "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos.",
 "llmEngine" : "yes"
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio entrega información de la cantidad de comportamientos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

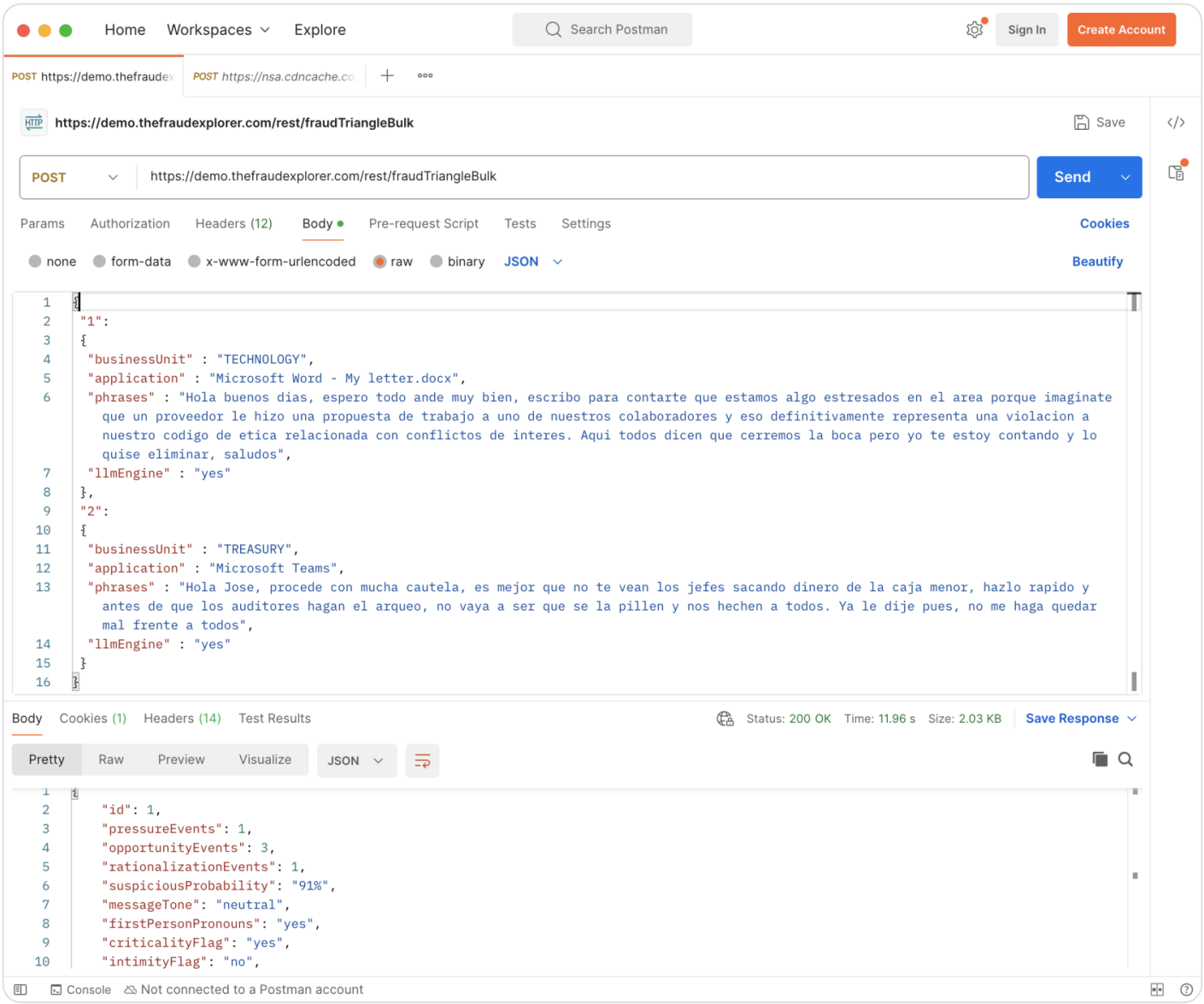
Modo Bulk para los insights

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangleBulk, seleccione el método **POST** y luego en la pestaña **BODY** agregue cada evento de forma numérica así:

```
{
 "1":
 {
  "businessUnit" : "TECHNOLOGY",
  "application" : "Microsoft Word - My letter.docx",
  "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos",
  "llmEngine" : "yes"
 },
 "2":
 {
  "businessUnit" : "TREASURY",
  "application" : "Microsoft Teams",
  "phrases" : "Hola Jose, procede con mucha cautela, es mejor que no te vean los jefes sacando dinero de la caja menor, hazlo rapido y antes de que los auditores hagan el arqueo, no vaya a ser que se la pillen y nos hechen a todos. Ya le dije pues, no me haga quedar mal frente a todos",
  "llmEngine" : "yes"
 }
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio en modo **BULK** entrega información de la cantidad de comportamientos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

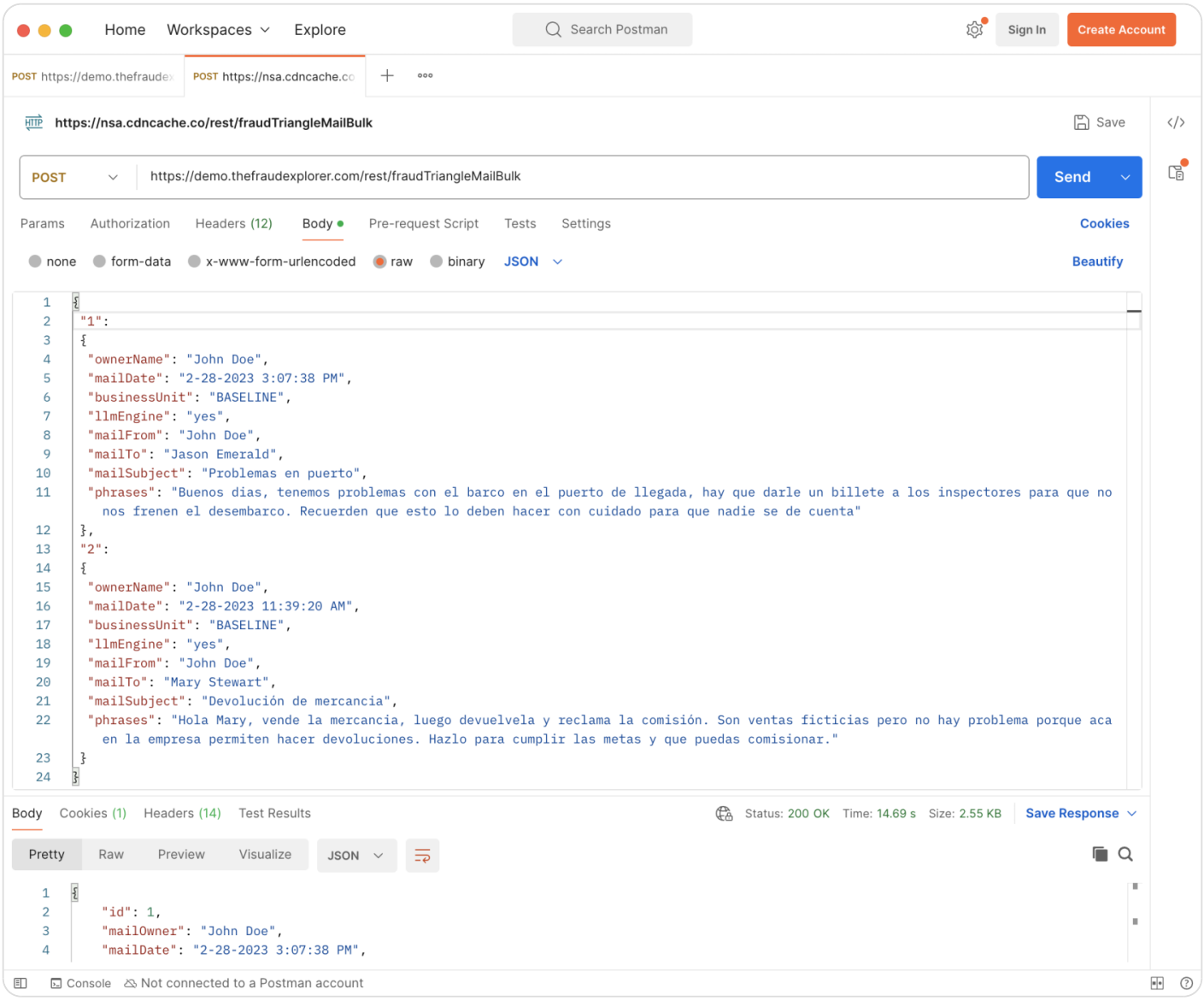
Modo Mail Bulk

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangleMailBulk, seleccione el método **POST** y luego en la pestaña **BODY** agregue cada evento de forma numérica así:

```
{
 "1":
 {
  "ownerName": "John Doe",
  "mailDate": "2-28-2023 3:07:38 PM",
  "businessUnit": "BASELINE",
  "llmEngine": "yes",
  "mailFrom": "John Doe",
  "mailTo": "Jason Emerald",
  "mailSubject": "Problemas en puerto",
  "phrases": "Buenos dias, tenemos problemas con el barco en el puerto de llegada, hay que darle un billete a los inspectores para que no nos frenen el desembarco. Recuerden que esto lo deben hacer con cuidado para que nadie se de cuenta"
 },
 "2":
 {
  "ownerName": "John Doe",
  "mailDate": "2-28-2023 11:39:20 AM",
  "businessUnit": "BASELINE",
  "llmEngine": "yes",
  "mailFrom": "John Doe",
  "mailTo": "Mary Stewart",
  "mailSubject": "Devolución de mercancia",
  "phrases": "Hola Mary, vende la mercancia, luego devuelvela y reclama la comisión. Son ventas ficticias pero no hay problema porque aca en la empresa permiten hacer devoluciones. Hazlo para cumplir las metas y que puedas comisionar."
 }
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio de **Mail** en modo **BULK** entrega información de la cantidad de comportamientos expresados en correos electrónicos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.