

# 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.",
  "IlmEngine" : "yes"
}
```

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

The screenshot shows a Postman interface for a POST request to `https://demo.thefraudexplorer.com/rest/fraudTriangle`. The request body is a JSON object with the following fields:

```
1 "businessUnit" : "TECHNOLOGY",
2 "application" : "Microsoft Word - My letter.docx",
3 "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate
4 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 intereses. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo
quise eliminar, saludos.",
5 "llmEngine" : "yes"
6
```

The response body is a JSON object with the following fields:

```
1 "pressureEvents": 1,
2 "opportunityEvents": 3,
3 "rationalizationEvents": 1,
4 "suspiciousProbability": "91%",
5 "messageTone": "neutral",
6 "1stPersonPronouns": "yes",
7 "criticalityFlag": "yes",
8 "IntimityFlag": "no",
9 "eventTopics": "information, suppliers",
10 "eventClassification": "conocimiento, renuncia, negociaciones, ocultamiento, estres",
11 "eventRisks": "concealment, psicosocial, suppliers",
12 "llmResult": "suspicious",
13 "phrasesMatched": {
14   "pressureTerms": "estamos algo estresados",
15   "opportunityTerms": "propuesta de trabajo, conflictos de intereses, cerremos la boca",
16   "rationalizationTerms": "quise eliminar"
17 }
18
19
```

Status: 200 OK, Time: 7.52 s, Size: 1.29 KB

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",
    "IlmEngine" : "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",
    "IlmEngine" : "yes"
  }
}
```

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

Home Workspaces Explore Search Postman Sign In Create Account

POST https://demo.thefraudexplorer.com/rest/fraudTriangleBulk

POST https://demo.thefraudexplorer.com/rest/fraudTriangleBulk

Params Authorization Headers (12) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary JSON

```
1 {
2   "1":
3   {
4     "businessUnit" : "TECHNOLOGY",
5     "application" : "Microsoft Word - My letter.docx",
6     "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 intereses. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos",
7     "llmEngine" : "yes"
8   },
9   "2":
10  {
11    "businessUnit" : "TREASURY",
12    "application" : "Microsoft Teams",
13    "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",
14    "llmEngine" : "yes"
15  }
16 }
```

Body Cookies (1) Headers (14) Test Results Status: 200 OK Time: 11.96 s Size: 2.03 KB Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "id": 1,
3   "pressureEvents": 1,
4   "opportunityEvents": 3,
5   "rationalizationEvents": 1,
6   "suspiciousProbability": "91%",
7   "messageTone": "neutral",
8   "firstPersonPronouns": "yes",
9   "criticalityFlag": "yes",
10  "intimidityFlag": "no",
```

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 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",
    "IlmEngine": "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",
    "IlmEngine": "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:

The screenshot shows a Postman interface with a REST client request and response. The request is a POST to `https://demo.thefraudexplorer.com/rest/fraudTriangleMailBulk` with a JSON body containing two mail items. The response is a 200 OK status with a JSON body containing the first mail item's details.

```
1 POST https://demo.thefraudexplorer.com/rest/fraudTriangleMailBulk
2
3 {
4   "ownerName": "John Doe",
5   "mailDate": "2-28-2023 3:07:38 PM",
6   "businessUnit": "BASELINE",
7   "llmEngine": "yes",
8   "mailFrom": "John Doe",
9   "mailTo": "Jason Emerald",
10  "mailSubject": "Problemas en puerto",
11  "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"
12 }
13 "2":
14 {
15   "ownerName": "John Doe",
16   "mailDate": "2-28-2023 11:39:20 AM",
17   "businessUnit": "BASELINE",
18   "llmEngine": "yes",
19   "mailFrom": "John Doe",
20   "mailTo": "Mary Stewart",
21   "mailSubject": "Devolución de mercancia",
22   "phrases": "Hola Mary, vende la mercancia, luego devuélvela 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."
23 }
24 }
```

```
1 {
2   "id": 1,
3   "mailOwner": "John Doe",
4   "mailDate": "2-28-2023 3:07:38 PM",
```

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.