

Retención y rotación de datos

The Fraud Explorer establece políticas para la retención de todos sus datos. Una de ella es la política de retención de datos para la información que llega desde los agentes y otra es para los eventos o alertas que se generan en la plataforma en nube o local.

Por defecto, la retención de los datos que llega de los agentes es cero; esto significa que, una vez procesada esa información, no se guarda. Para los eventos, recomendamos que se mantenga una retención de 30 días, es decir, las alertas por comportamientos antiéticos solo tendrán una vida de 30 días en la plataforma y pasados esos 30 días se eliminarán de forma segura.

Maintenance & Health

Retention Policy (source data, alerts)

12

180

Set words age now !

You don't have any data yet

Excel Reports Retention

Preserve all

7 reports older than 90 days

Purge old endpoint events

Preserve all

You have 75 regs in 0.5 MB

Delete old endpoint sessions

Preserve all

0 sessions in dead status (30 days)

Elasticsearch Snapshots Retention

Preserve all

229 elasticsearch snapshots

Delete old events status records

Preserve all

You have 5 regs in 0.1 MB

Check The Fraud Explorer health system status

Cancel

Purge data now

Los únicos datos que se retienen son las alertas, nosotros no retenemos los datos que se usaron para generar las alertas. Esto es importante resaltarlo para que no se entienda que **The Fraud Explorer** es un software que guarda conversaciones, sino que guarda alertas y éstas al final son solamente una porción muy pequeña de una conversación.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones. Este software está siendo desarrollado por [NOFRAUD.la](#). Por favor lea la [licencia de uso](#) y el [descargo de responsabilidad](#) antes de usar nuestra metodología antifraude.

