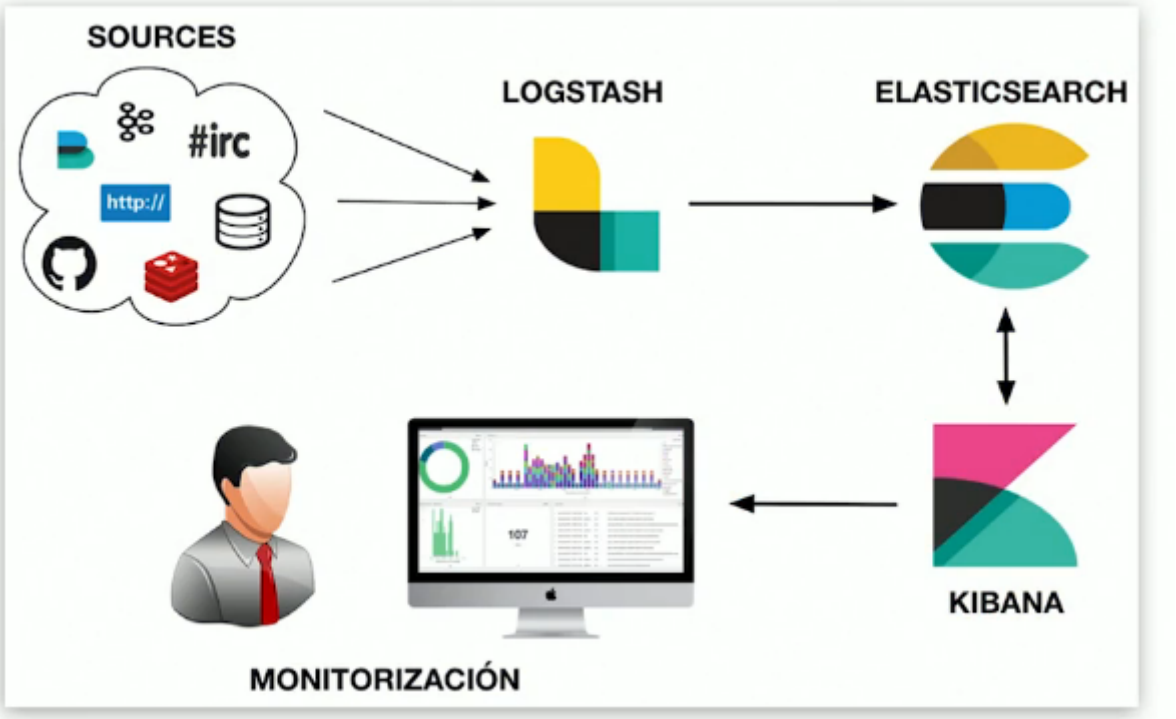
ELK: Logstash



- preprocesamiento (antes de elasticsearch)
- servicio para procesar/transformar información recolectada de diferentes fuentes y enviarla a múltiples tipos de salidas.
- múltiples plugins (de entrada y salida)
  - +200 plugins y posibilidad de desarrollarlos
- permite usar cola de almacenamiento ante errores
  - kafka, redis como alterntivas más profesionales
- monitorización: visibilidad de recursos de los nodos y estadísticas de servicio
- seguridad: información cifrada en la comunicación con los servicios
- 3 etapas claramente diferenciadas: entrada, filtrado, salida

entrada

- limpieza de datos
  - gran cantidad de campos ¿todos necesarios?
  - campos mal formados
- enriquecimiento de datos
  - añadir información a campos existentes
  - crear campos nuevos
  - geolocalización
  - (ejemplo) convertir puertos a protocolos
  - (ejemplo) IP → latitud, longitud
- ingesta de datos:
  - formas, tamaños, fuentes variados

filtrado

- transformaciones al vuelo
- estructura de datos
- trabaja con fingerprints
- reconocmiento de fechas

salida

- varias opciones

- ELK: Logstask(instalación y configuración)
- ELK: Logstask(procesamiento)