Tecnologías Emergentes en la AGE: La Plataforma de Análisis Forense de la Agencia Tributaria

Diciembre de 2019

Índice

- eDiscovery vs análisis forense
- Inspecciones de la AEAT
- Plataforma de análisis forense
- Posible interés para otras AAPP

eDiscovery vs análisis forense

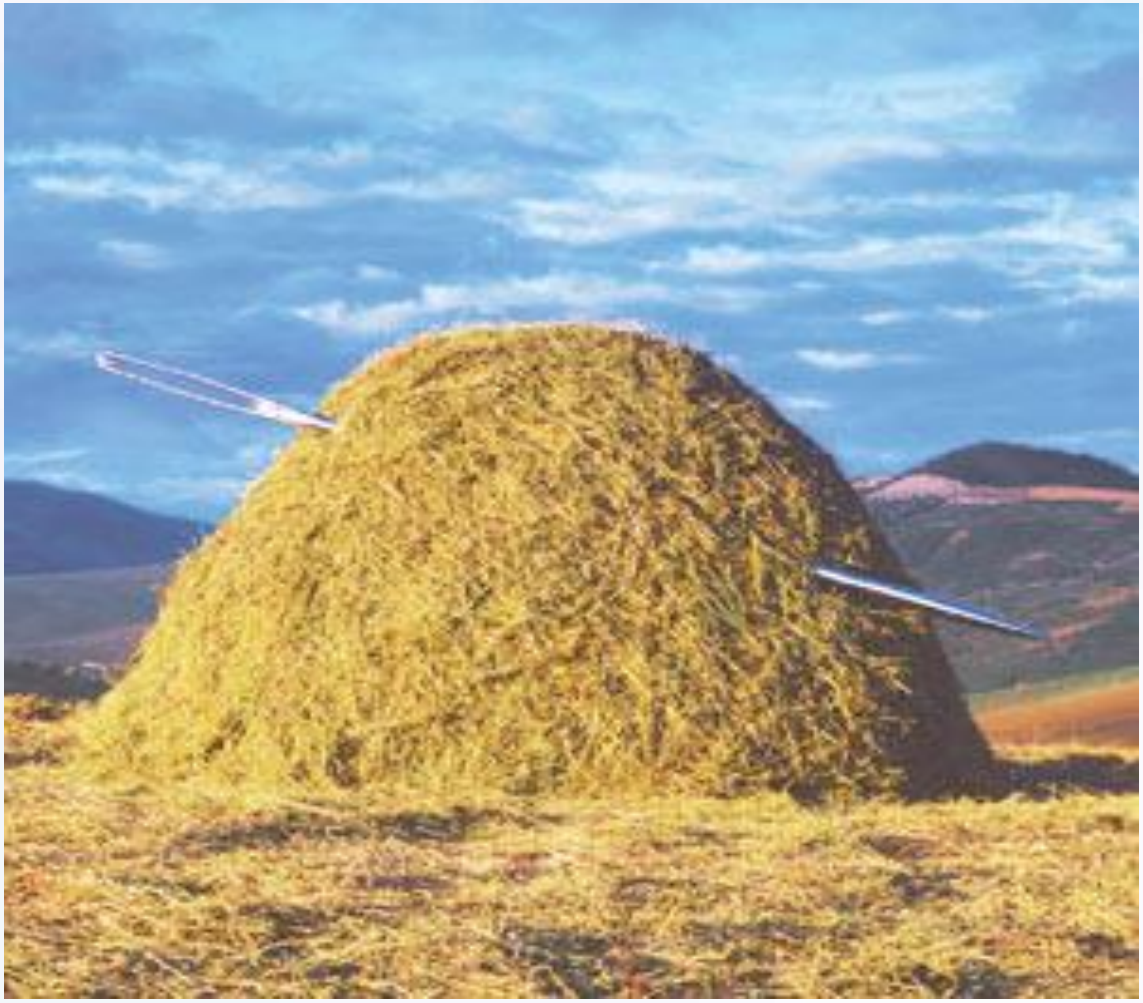
eDiscovery vs análisis forense

- Tecnologías emergentes
  - Inteligencia artificial
  - Big data
  - Blockchain
  - …
- eDiscovery y análisis forense (digital)
  - Hacer investigaciones sobre medios y contenidos digitales
  - Ejemplo clásico: discos duros

eDiscovery vs análisis forense

- Análisis forense digital
  - Lo aplican las FFCC de Seguridad
  - Investigar delitos o crímenes
  - Investigaciones muy detalladas
- eDiscovery
  - Lo aplican las corporaciones privadas
  - Investigaciones internas o litigios privados
  - Tienen un enfoque más documental (ofimática, correo, …)
- Análisis de grandes volúmenes de información no estructurada

eDiscovery vs análisis forense



Inspecciones de la AEAT

Inspecciones de la AEAT

- La AEAT, entre otras competencias, inspecciona a contribuyentes
- Podemos ir a la casa de un contribuyente o a la sede de una empresa y obtener información
- Esa información luego hay que analizarla para identificar pruebas de fraude fiscal
- Es en este terreno en el que estamos aplicando las técnicas y herramientas de eDiscovery

Inspecciones de la AEAT

- Unas 2000 investigaciones al año
- Judiciales y administrativas
  - Judiciales → auxilio de la Justicia
  - Administrativas → ejercicio de sus competencias
  - Las administrativas pueden convertirse en judiciales

Inspecciones de la AEAT

- Judiciales
  - Pocas al año (unas 20)
  - Mucha información (algunos TB)
  - Pueden durar muchos años
- Administrativas
  - Muchas al año (unas 2000)
  - Menos información (cientos de GB)
  - Duran 1 año

Inspecciones de la AEAT

- Proceso en 3 fases
  - Captura de la información → equipos mixtos
  - Procesamiento técnico → unidades de auditoría informática
  - Análisis fiscal → inspectores
- Campos de mejora
  - Uso de herramientas corporativas
  - Uso de métodos de trabajo comunes
  - Agilizar la interacción entre procesamiento y análisis
  - …
- Proyecto → Plataforma de análisis forense

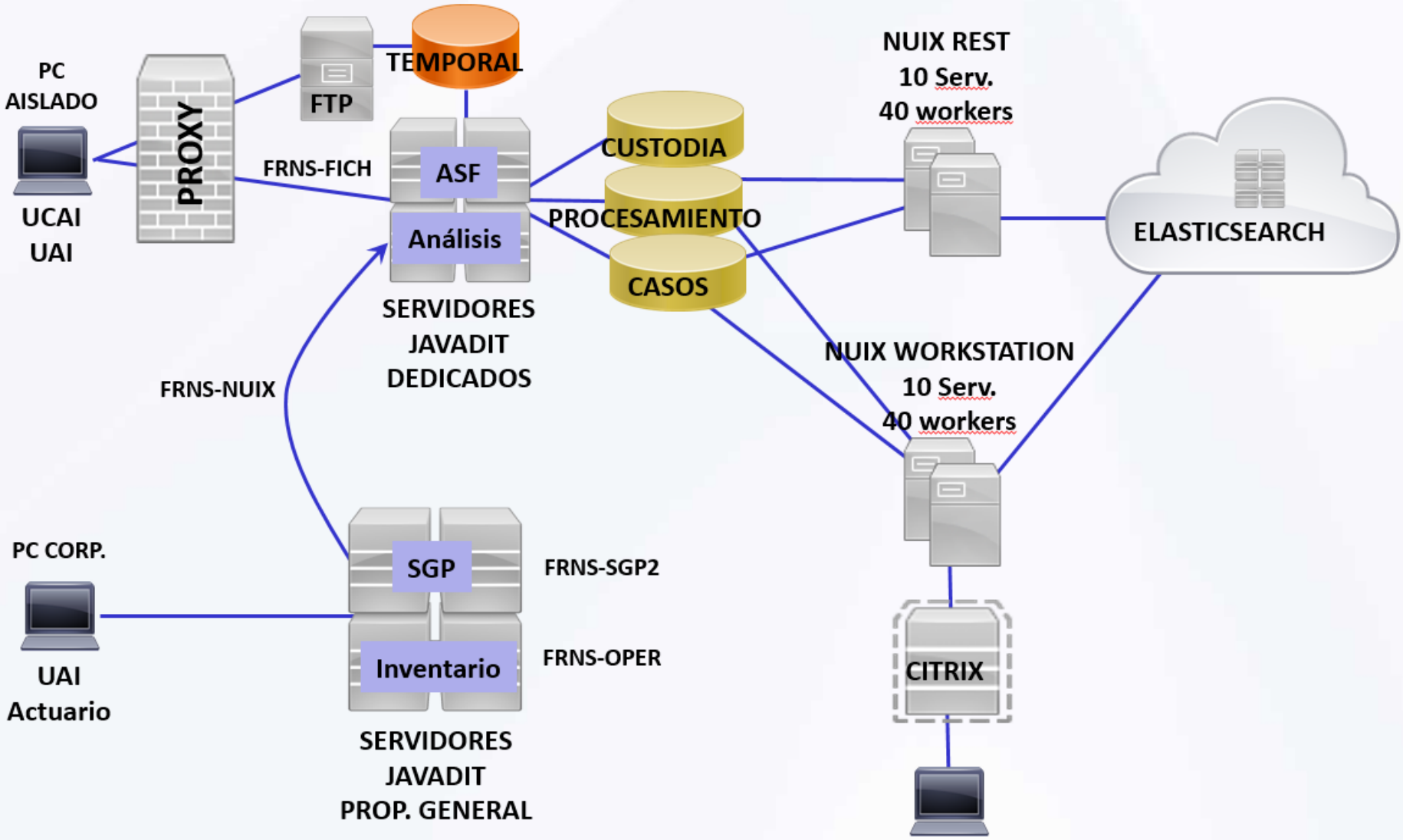
Plataforma de Análisis Forense

Plataforma de Análisis Forense

- Objetivo del proyecto
  - Desarrollar una plataforma corporativa
  - Que sirva para analizar la documentación capturada
  - Tanto en procedimientos judiciales como administrativos
  - Tanto en la fase de procesamiento técnico con en la de análisis fiscal
- Muy importante el carácter corporativo
  - Herramientas comunes
  - Procedimientos y métodos comunes

Plataforma de Análisis Forense

- Análisis de mercado
  - Nuix FTK
  - Encase Cellebrite (herramienta de análisis)
  - Relativity
- Optamos por Nuix por
  - Enfoque documental (eDiscovery), no tan forense
  - APIs abiertas (REST)
  - Basado en Elasticsearch (indexador / buscador en cluster)
  - Ya conocido y usado en la AEAT


PC
AISLADO
UCAI
UAI
PROXY
FTP
TEMPORAL
FRNS-FICH
ASF
Análisis
SERVIDORES
JAVADIT
DEDICADOS
CUSTODIA
PROCESAMIENTO
CASOS
NUIX REST
10 Serv.
40 workers
ELASTICSEARCH
NUIX WORKSTATION
10 Serv.
40 workers
FRNS-NUIX
PC CORP.
UAI
Actuario
SGP
FRNS-SGP2
Inventario
FRNS-OPER
SERVIDORES
JAVADIT
PROP. GENERAL
CITRIX

Plataforma de Análisis Forense

- Subida de evidencias
  - Subida por FTPS y HTTPS
  - Circuito separado de la red corporativa (seguridad)
  - Además de subida, metadatización (operación, hash, …)
  - Servicios de custodia y procesamiento
- Aplicaciones de análisis
  - Cliente pesado accesible por Citrix
  - Cliente ligero accesible por Intranet (API REST) e integrado con las aplicaciones corporativas de la AEAT
  - Indexación y revisión

Plataforma de Análisis Forense

- Indexación
  - Cientos de formatos soportados (imágenes forenses, máquinas virtuales, backups, ficheros comprimidos, ficheros TAR, etc.)
  - Crea un índice en Elasticsearch
  - Permite pasar OCR
  - Recuperar archivos borrados
  - Identificar entidades (personas, empresas, IBAN, tarjetas, …)
  - Generar miniaturas
  - Etc.

Plataforma de Análisis Forense

- Revisión
  - Buscar (simples, comodines, parecido, frases, exp. regulares, …)
  - Navegar y seleccionar / deseleccionar evidencias
  - Exclusiones, conjuntos y etiquetas
  - Filtrar por tipos de documento y/o extensión
  - Deduplicar
  - Previsualizar texto, líneas, metadatos y PDF
  - Comparar diferencias contra un documento “pivote”
  - Mostrar documentos relacionados con uno dado
  - Descargar PDF y/o documento original
  - Pasar OCR
  - Descifrar
  - Exportar a Expediente Electrónico
  - Exportar a CSV
  - Etc.

Posible interés para otras AAPP

Posible interés para otras AAPP

- El proyecto ha sido complejo, pero está implantado y funcionando
- Otras AAPP con competencias similares pueden beneficiarse de nuestra experiencia
  - Competencia
  - Protección de datos
  - Inspecciones de trabajo
  - Seguridad Social
  - …

¿Preguntas?