INVESTIGACIONES Y FORENSIA EN LA ERA DIGITAL

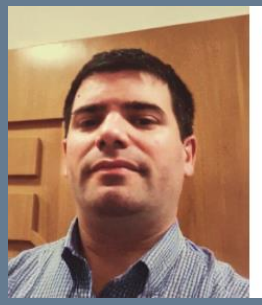
El rol de la tecnología en las investigaciones

01
NUESTROS NÚMEROS

	Global	Argentina
	Presente en más de 166 países y territorios	Presente en Buenos Aires, Córdoba, Santa Fe y Mendoza
OFICINAS	1.776	5
STAFF	+115.661	+900
INGRESO ANUAL	U$S14 Mil Millones	U$S35 Millones

Fabián Descalzo
Socio, Ciberseguridad y Gobierno Tecnológico, BDO en Argentina

Magali Occhiuzzi
Directora de GRC, BDO en Argentina



Leonardo Masip
Supervisor de Ciberseguridad y Tecnología de la Infromación, BDO en Argentina

Agenda


Introducción

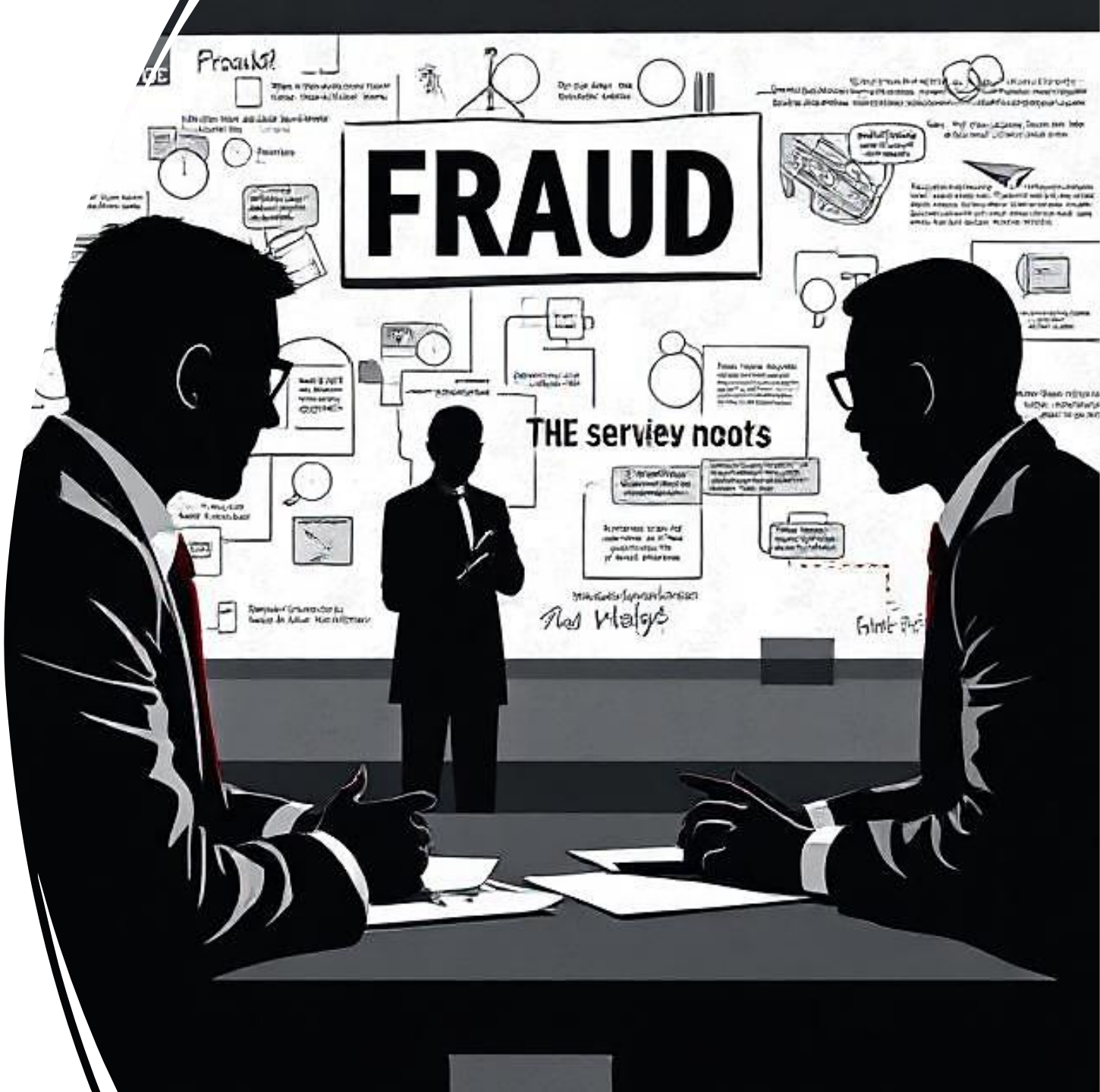

Como la tecnología favoreció al fraude


La tecnología en la Investigación


Caso

INTRODUCCIÓN

Introducción: “Como la tecnología favoreció al fraude”



Evolución de la tecnología para el fraude

Pre Internet

Fraudes manuales y físicos. Antes de la masificación digital, el fraude se centraba en falsificación de documentos, cheques, firmas o suplantaciones físicas. Requería presencia física, contactos y logística limitada.

Años 90

Digitalización inicial: Inicio del uso de correo electrónico y primeras bases de datos digitales. Aparición de fraudes básicos: phishing simple (correos fraudulentos), manipulación de datos contables, skimming en cajeros automáticos.

2000 -2010

Mayor acceso a Internet y comercio electrónico. Crecen ataques como: Phishing masivo y spear phishing (dirigido), Malware básico (keyloggers para robar credenciales), Fraudes en sitios web y e-commerce (tarjetas robadas)

2010 - 2020

Consolidación móvil y redes sociales. Proliferación de smartphones y apps financieras. Explotación de: Apps falsas y marketplaces fraudulentos; Ingeniería social avanzada a través de redes sociales; Smishing (fraude por SMS) y vishing (llamadas falsas); Empleo de botnets y automatización para fraudes masivos.

2020 +

Inteligencia artificial y automatización. Uso de IA y deepfake para suplantación de identidad avanzada. Automatización de ataques a credenciales; Fraudes en criptoactivos y billeteras virtuales; Explotación de grandes volúmenes de datos filtrados en dark web; Fraudes basados en QR y aplicaciones de pago instantáneo.

Tendencias actuales y futuras

Deepfakes para llamadas o videos falsos; Robo y manipulación de identidad digital completa (por ejemplo, clones de voz o imagen); Ataques a infraestructuras críticas y cadenas de suministro; Uso de IA generativa para mejorar la persuasión en estafas.

Cómo la tecnología facilitó el fraude

💻 **1. Digitalización masiva de servicios:** **Cada vez más procesos se realizan online** (pagos, préstamos, contratos).Esto ha abierto más “superficies de ataque” para los delincuentes.

📲 **2. Automatización y escala:** Los estafadores pueden enviar miles de mensajes fraudulentos (phishing) o realizar ataques automatizados con bots. Antes, el fraude requería contacto personal; **hoy se puede hacer de forma masiva y global**.

🔍 **3. Facilidad para falsificar identidades:** Se usan herramientas para crear documentos falsos (fotos, videos deepfake, identidades sintéticas).**Redes sociales y bases de datos filtradas permiten obtener datos personales** para suplantaciones.

💳 **4. Nuevos métodos de pago y transferencias rápidas:** Criptomonedas y billeteras digitales permiten mover dinero sin rastreo claro. **Los pagos inmediatos reducen el tiempo para detectar y frenar transacciones sospechosas.**

🌐 **5. Acceso a herramientas y conocimiento:** En la darkweb se venden kits completos para fraude (por ejemplo, clones de sitios bancarios, malware listo para usar). **Tutoriales y foros permiten a personas sin conocimientos técnicos empezar a defraudar.**

🧩 **6. Ingeniería social más sofisticada:** La tecnología permite personalizar estafas usando información real (por ejemplo, correos o llamadas que parecen legítimos). **La inteligencia artificial puede generar textos y voces creíbles.**

Hacks biométricos “vintage”

“EN LA ACTUALIDAD, LOS NEGOCIOS TIENEN 15 VECES MÁS PROBABILIDADES DE TENER UN CIBERATAQUE QUE DE SUFRIR UN INCENDIO O UN ROBO.“

En 2002 Matsumoto sacó las impresiones de un cristal utilizando las mismas técnicas que las fuerzas del orden, y luego usó las impresiones para hacer un dedo con los materiales gomosos.

En 2012, los investigadores compartieron cómo podrían pasar por alto los lectores de iris con imágenes duplicadas de iris

En 2011, un blogger e investigador engaño a los escáneres faciales de Android con una imagen fija, y las verificaciones de «vida»con un parpadeo con Photoshop para omitir ese nuevo control

Impresoras 3-D violan escáneres faciales 3-D, pero en 2017, Apple lanzó una nueva función de escaneo facial llamada FaceID y mejora esta característica con el aprendizaje automático

En 2013, el Chaos Computer Club derrotó al lector TouchID del iPhone poco después de su lanzamiento. Incluso más recientemente, los investigadores piratearon los lectores de huellas dactilares con papel y pegamento

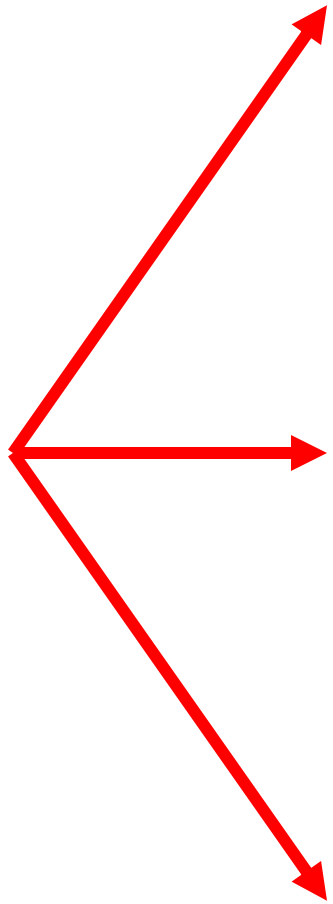
BDO

Ejemplos de fraude informático interno

1. Manipulación de datos contables o financieros
2. Transferencias no autorizadas
3. Robo de información confidencial
4. Creación de usuarios fantasma
5. Abuso de privilegios de administrador
6. Venta de datos personales
7. Fraude en los sistemas de nómina
8. Desviación de productos o servicios digitales

⚠️ Factores que facilitan el fraude interno

- Falta de segregación de funciones.
- Exceso de confianza en personal clave.
- Control deficiente de accesos y logs.
- Cultura organizacional débil (poca ética o supervisión)
- Acceso privilegiado no controlado
- Monitoreo de logs insuficiente.
- Falta de segregación de funciones.
- Cultura débil en ética y control interno.



🔴 **1. Caso Société Générale (Francia)**

•**Empleado**: Operador bursátil.
•**Qué hizo**: Usó su acceso privilegiado para realizar operaciones no autorizadas por miles de millones de euros, ocultando las posiciones mediante manipulaciones en el sistema.
•**Impacto**: Pérdidas de alrededor de **4.900 millones de euros**.
•**Cómo lo hizo**: Aprovechó lagunas en los controles internos y la confianza excesiva de la gerencia para crear transacciones ficticias y ocultar riesgos.

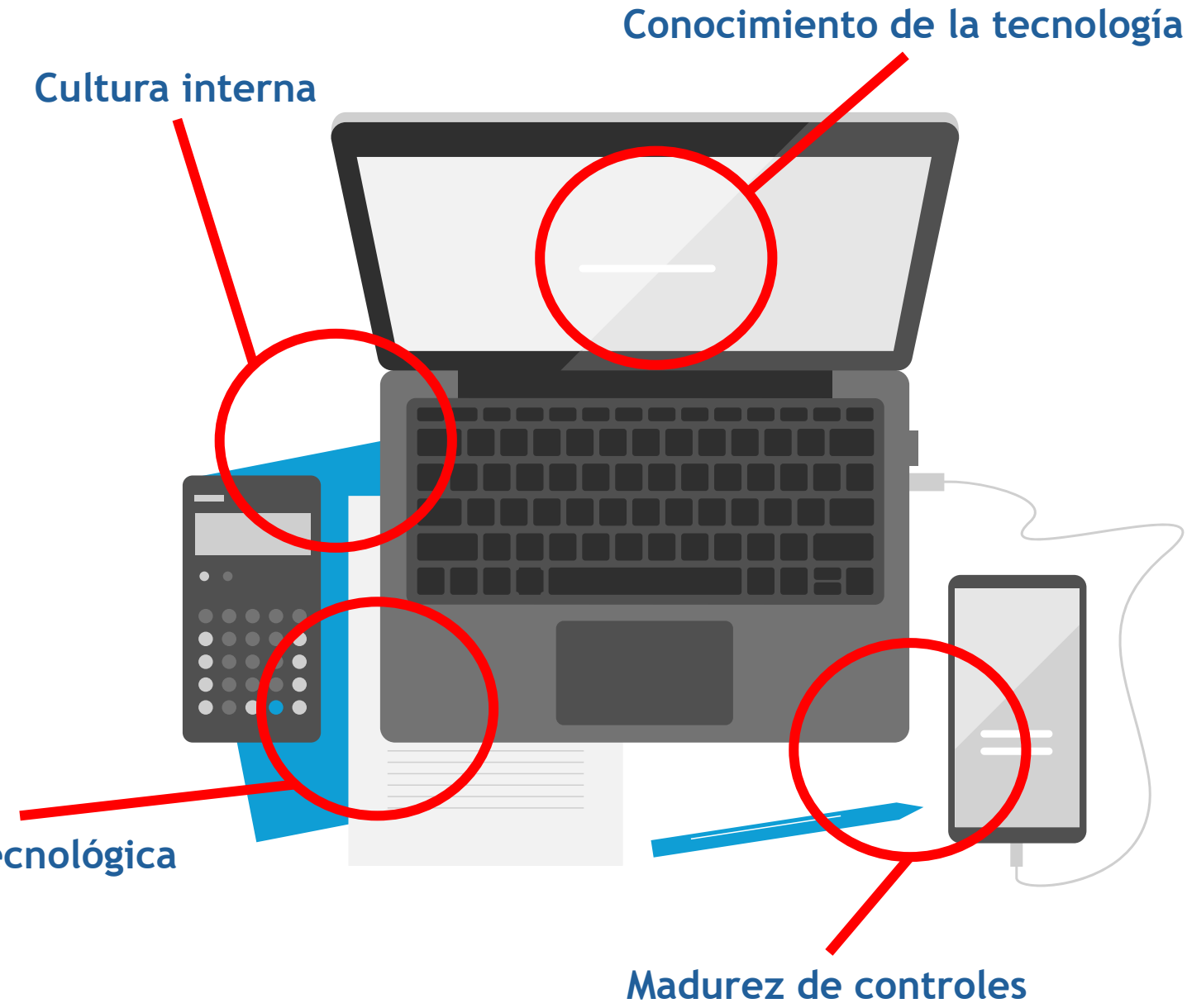
🔴 **2. Caso Edward Snowden (EE. UU.)**

•**Empleado**: Contratista de la NSA (Agencia de Seguridad Nacional).
•**Qué hizo**: Robó y filtró documentos clasificados.
•**Impacto**: Exposición global de programas de vigilancia masiva, gran daño reputacional y político.
•**Cómo lo hizo**: Aprovechó su acceso como administrador de sistemas y sus conocimientos técnicos para copiar y extraer grandes volúmenes de datos sin ser detectado inicialmente.

🔴 **4. Caso Morgan Stanley (EE. UU.)**

•**Empleado**: Asesor financiero.
•**Qué hizo**: Accedió y descargó información de 350.000 clientes sin autorización.
•**Impacto**: Filtración parcial en la dark web; daño reputacional y multas regulatorias.
•**Cómo lo hizo**: Usó accesos internos para crear copias no autorizadas de datos de clientes.

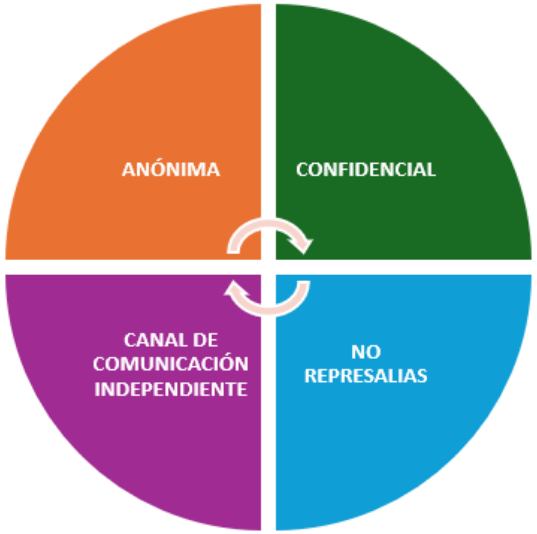
¿La tecnología favoreció al fraude?



CASO INVESTIGACIONES

BDO

DESCRIPCIÓN DEL CASO – Nuevas denuncias...



Comité de Recepción de denuncias

Ingresan 2 denuncias por separado

El Comité o su equivalente, toma conocimiento de las denuncias y define el curso de acción. En caso de considerarlo procedente se llevará a cabo la investigación.

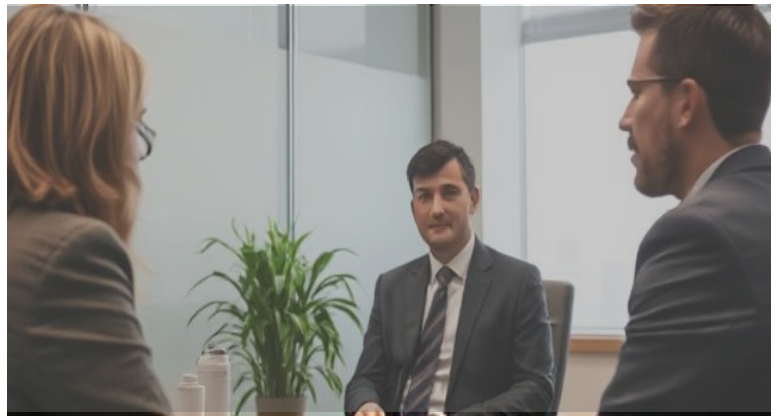
Denuncia 1

1) Posiblemente un potencial proveedor
2) Denuncia al área de Compras, Gerente y Supervisor.
   - Pliegos dirigidos, las compulsas son cerradas.
   - Poca probabilidad de aceptar nuevos competidores, Filtración de tarifas.
   - Pedido de coima para ingresar.

Denuncia 2

1) Un posible colaborador denuncia.
2) Existen área usuarias que por estar en connivencia con Compras contratan proveedores menos convenientes, con incumplimientos recurrentes, baja calidad y demora en la presentación de la documentación requerida.
3) Realizan compras descentralizada, pasando por altos los procesos internos y seleccionando proveedores sin control.
4) Compras innecesarias en connivencia con los terceros.

DIFERENTES TÉCNICAS DE INVESTIGACIÓN



El Rol de la Tecnología en las Investigaciones

- Recolección y preservación de datos (discos, redes, nube)
- Análisis automatizado con software especializado.
- Tecnologías emergentes: blockchain, IA, IoT.
- IA como catalizador para detectar patrones y reducir tiempos.

Introducción de la IA en Forensia

La IA es la evolución natural de las tecnologías forenses

De la automatización simple al aprendizaje inteligente

Machine Learning, Deep Learning, NLP.

LA EVOLUCIÓN EN LAS INVESTIGACIONES

Algunas pocas de las tantas herramientas para la prevención, detección de fraude e investigaciones

Software de análisis de datos:

Herramientas utilizadas para realizar análisis estadísticos complejos, incluyendo modelos predictivos, pruebas de hipótesis y análisis multivariados para investigadores.

Software de gestión de bases de datos:

MySQL es fundamental para la gestión de grandes conjuntos de datos, filtrar y manipular datos almacenados en bases de datos.

Software de análisis de Big Data:

Herramientas como Apache Hadoop, Apache Spark y Druid son utilizadas para analizar grandes volúmenes de datos.

Software de visualización de datos:

crear visualizaciones interactivas y dashboards que facilitan la comprensión de los datos

Software de detección de fraudes

Emailage, ThreatMetrix Sift - Digital Trust & Safety Suite, ArkOwl, Trustfull;

Combinar diversas tecnologías (IA, RPA, NLP) potencia la eficacia en la detección de fraudes.

Lenguajes de programación:

Herramientas para análisis de datos, flexibles con amplia gama de bibliotecas y paquetes para el análisis estadístico y el aprendizaje automático. Ideal para investigadores.

LA EVOLUCIÓN EN LAS INVESTIGACIONES

Background Check, recopilación de antecedentes

Algunas pocas de las tantas herramientas para la prevención, detección de fraude e investigaciones

Google

NotebookLM

Plataformas de encuestas:

Microsoft Forms

Typeform

Gestores de referencias

Mendeley

Zotero

Fidelitas

vlex

INPI INSTITUTO NACIONAL DE LA PROPIEDAD INDUSTRIAL ARGENTINA

ANSES

WORLD-CHECK REDUCING RISK THROUGH INTELLIGENCE

COMPR.AR

Fiscales.gob.ar

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN

opencorporates

AGIP Administración Gubernamental de Ingresos Públicos

VERAZ

Poder Judicial de la Nación

ICIJ

AUTOPSY DIGITAL FORENSICS

LexisNexis

Intella

REPSAL Registro de Empleadores con Sanciones Laborales

INTERNET ARCHIVE

CIJ

ARCA | AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO

Newspaper Map

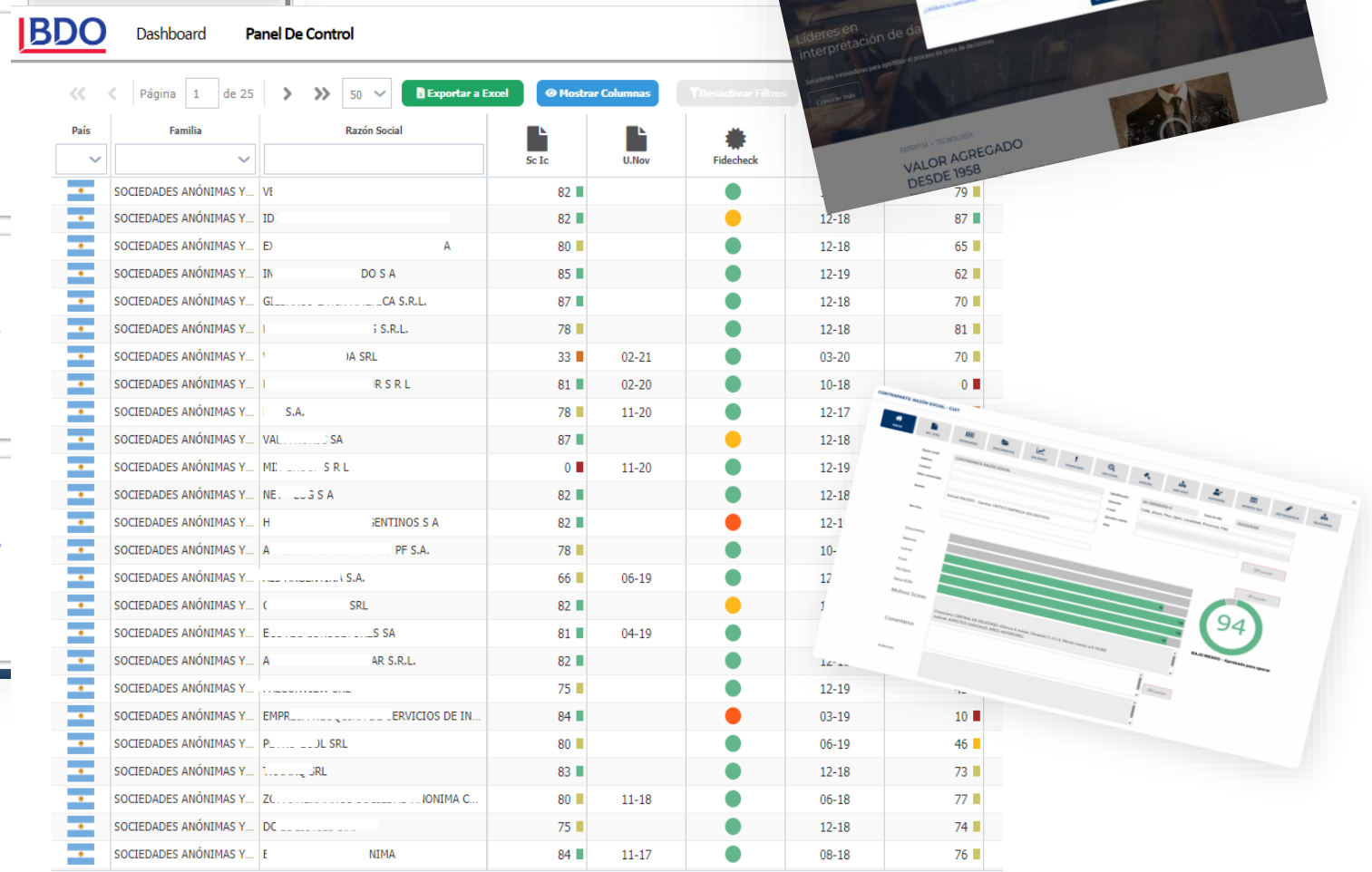
Namech_k

Talkwalker by Hootsuite

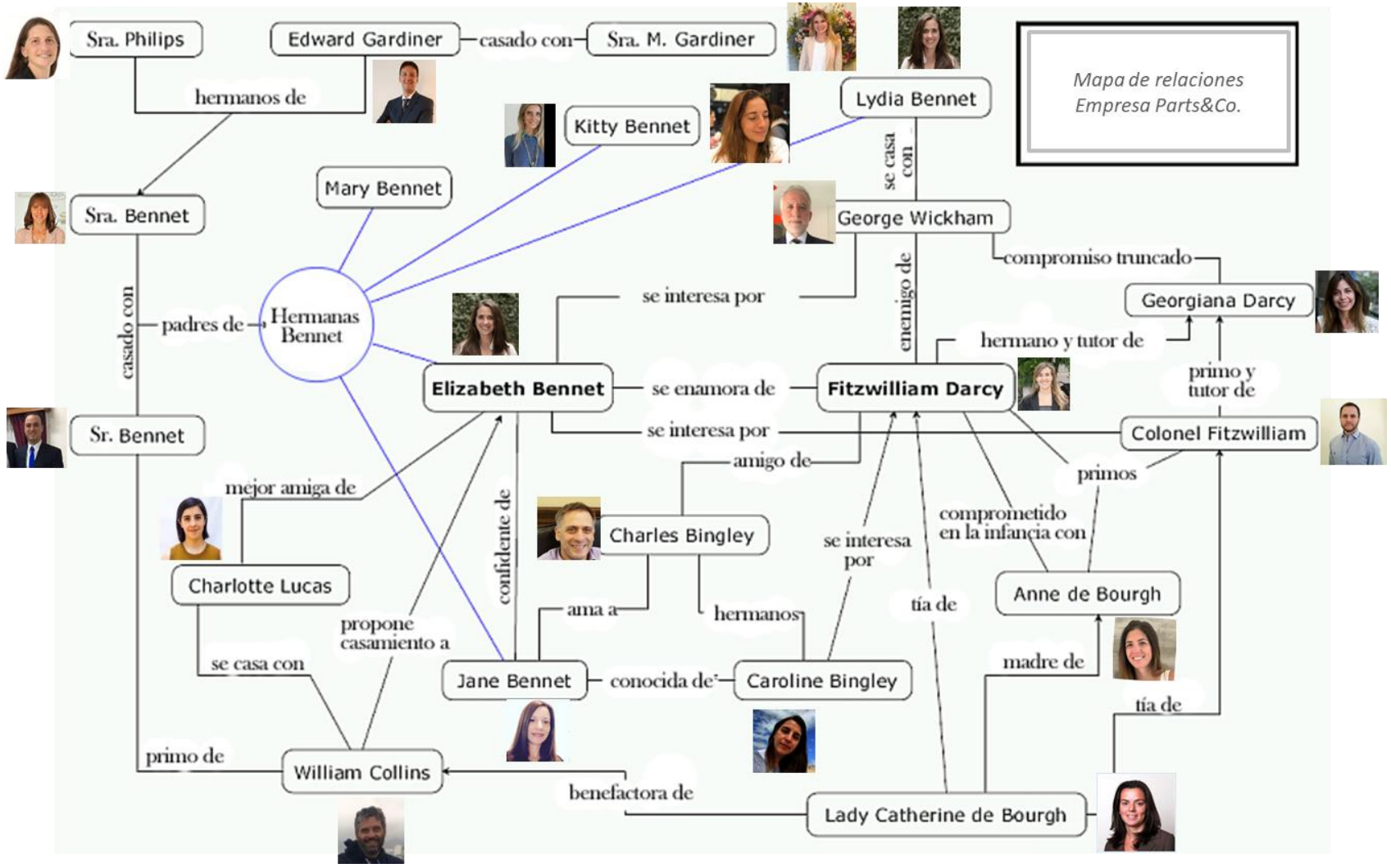
MOODY'S | Orbis

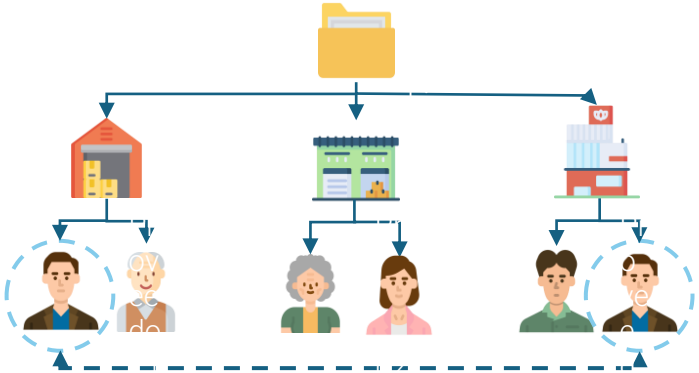
LA EVOLUCIÓN EN LAS INVESTIGACIONES

Avaldigital



MAPA DE RELACIONES

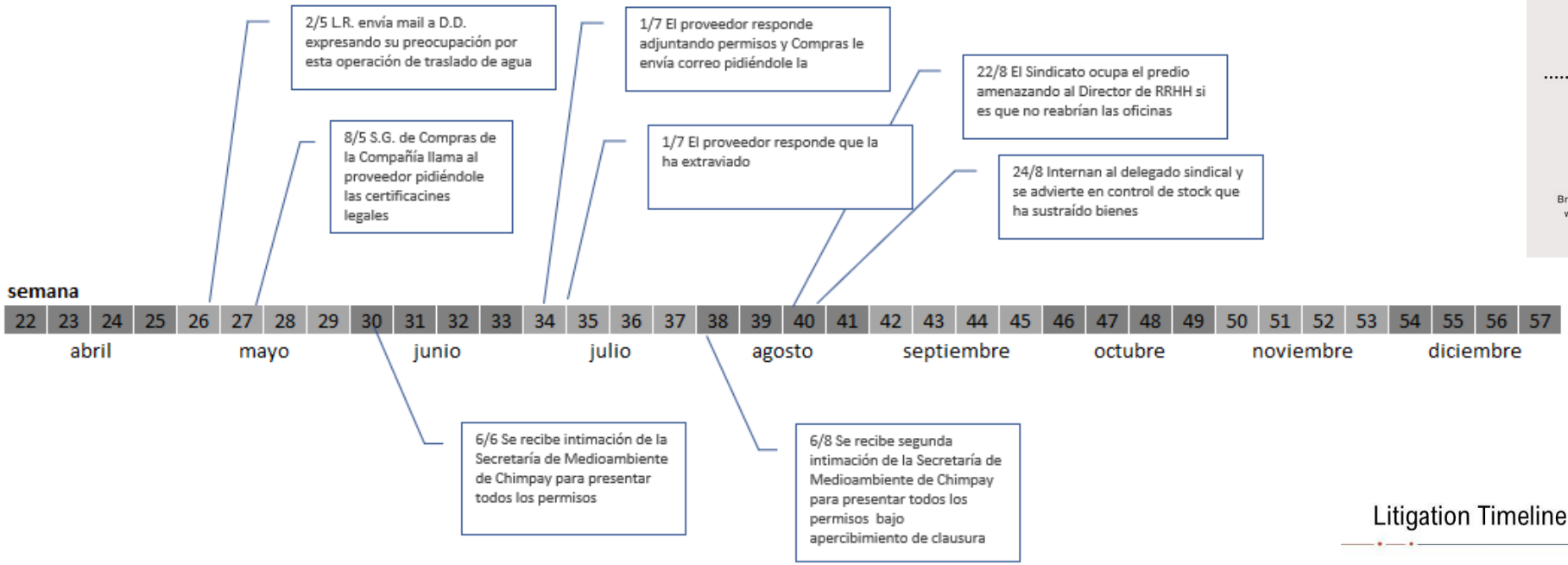


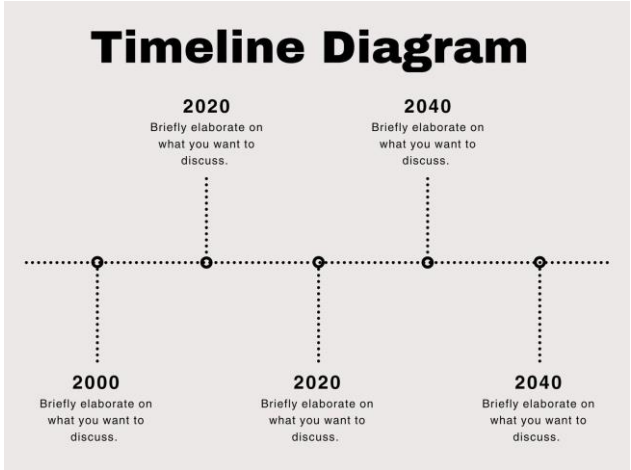


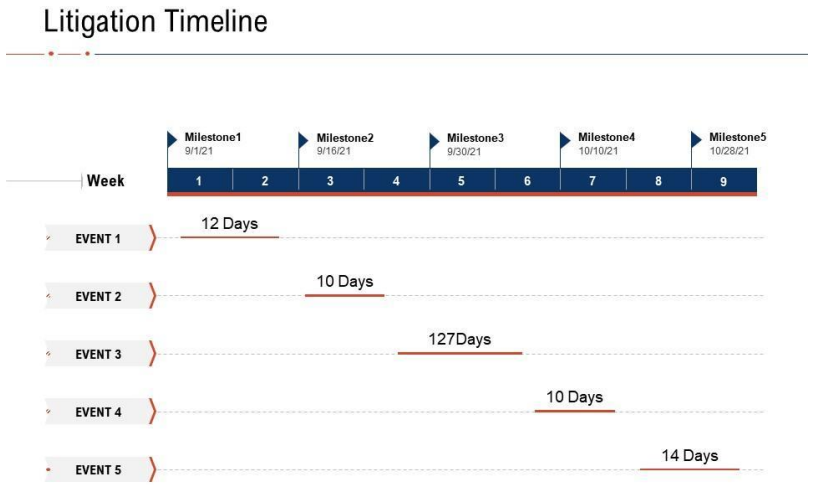
Ejemplo de relacionamientos

La inteligencia de fuentes abiertas aplicada a los participantes de un proceso licitatorio permite identificar la existencia de competidores ficticios / administrados por las mismas autoridades.

LÍNEA DE TIEMPO



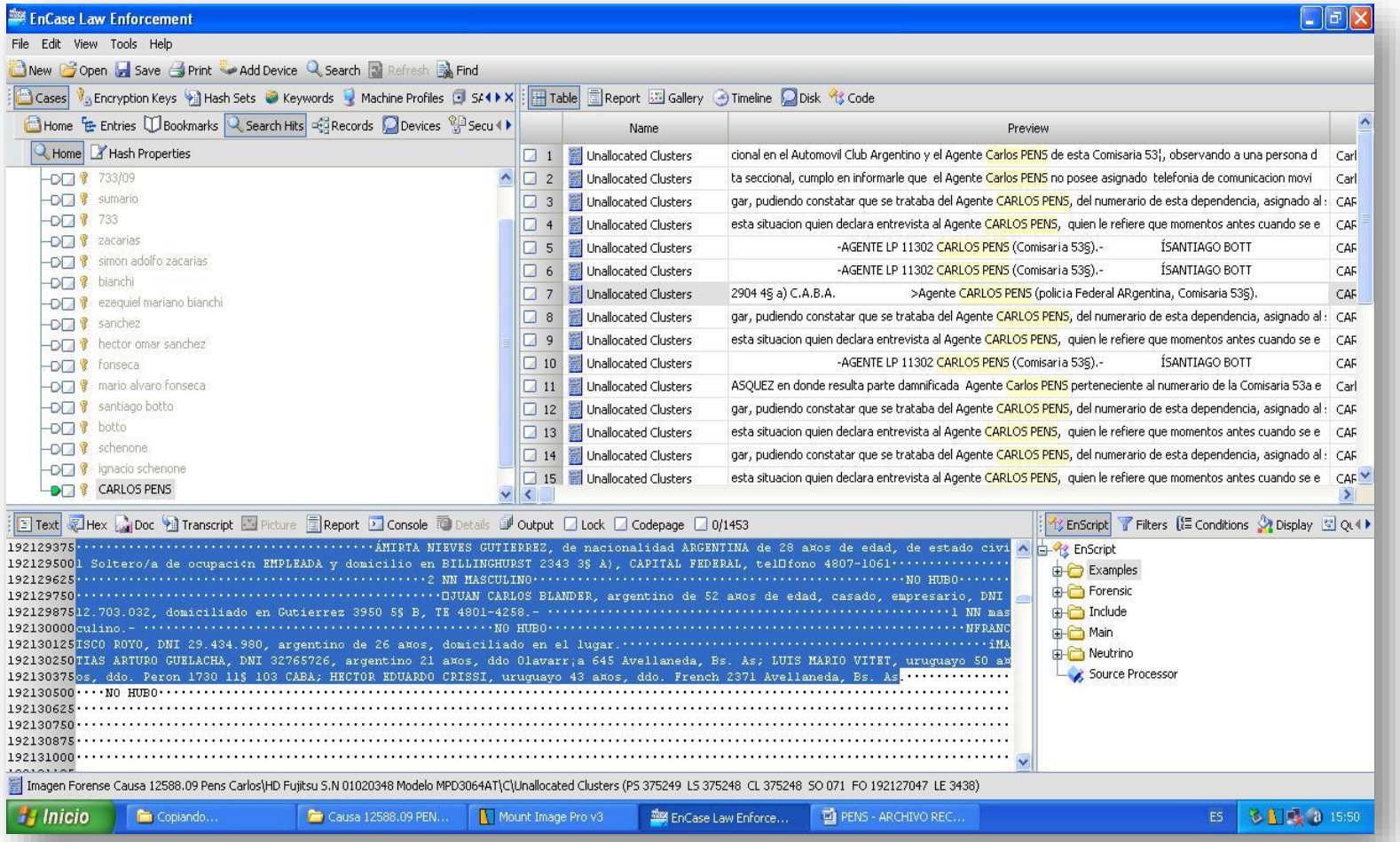




ACCESO INFORMÁTICO FORENSE

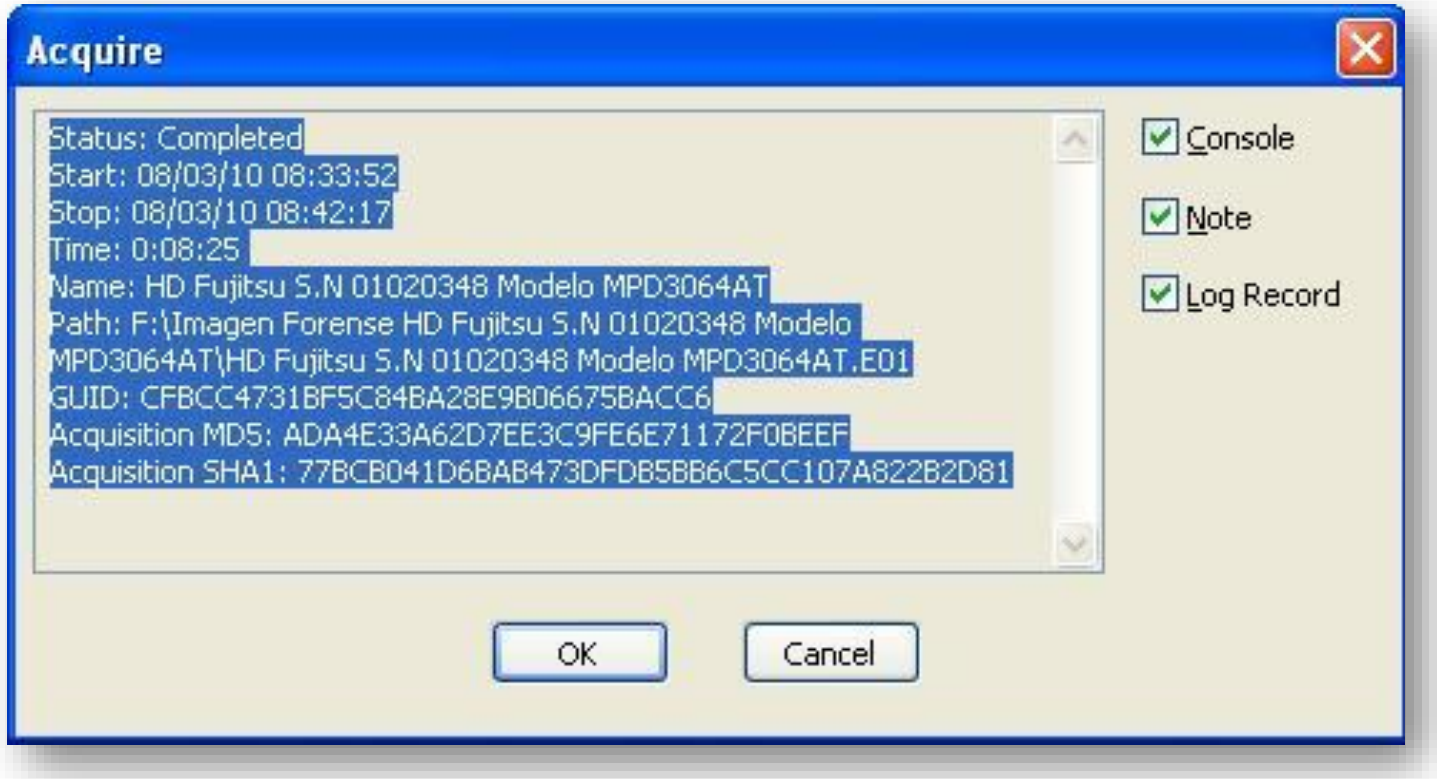
- Extraer el disco a analizar del equipo informático cuestionado
- Se utilizan dispositivos especiales de conexionado para ingresar al HD.
- Se usa la herramienta especializada para analizar el HD (Ej. ENCASE).
- Realizar la Imagen o copia espejo forense.
- Comprobar que el procedimiento haya resultado efectivo.

IDENTIFICACIÓN DE LA EVIDENCIA



- **Identificar un conjunto de pruebas para ser tomadas como evidencia.**
- **Recuperar los atributos del archivo**
- **Relevar la mayor cantidad de evidencia digital (sin alterarla)**

AUTENTICACIÓN DE LA EVIDENCIA



- **Cálculo de firmas digitales.**
- **Obtención de un HASH (MD5 y SHA1).**
- **Garantizar: integridad de evidencias digitales recolectadas y permitir identificar univocamente a tales archivos.**

Aplicaciones de IA en Forensia Digital

- Detección de anomalías en logs
- Clasificación de malware.
- Análisis de imágenes y vídeos (reconocimiento facial, deepfakes)
- Procesamiento de lenguaje natural (NLP) para analizar emails/chats.
- Automatización de informes forenses.

Ventajas de la IA en Forensia

Rapidez: análisis masivo en minutos.

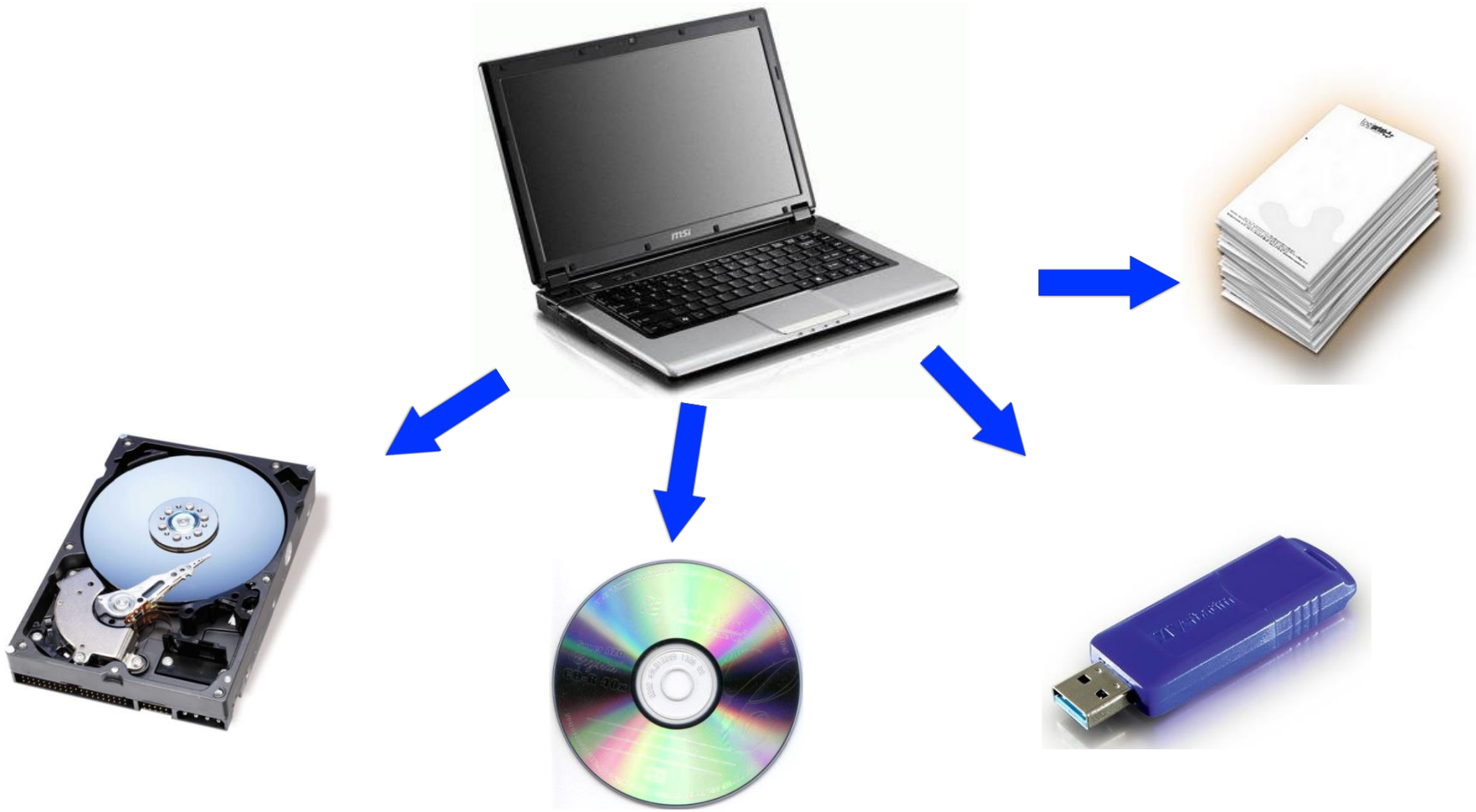
Capacidad predictiva frente a ciberamenazas.

Escalabilidad en entornos complejos (cloud, IoT)

Desafíos y Riesgos

- Necesidad de datasets amplios y fiables
- Explicabilidad limitada de algunos algoritmos.
- Falsos positivos/negativos.
- Aspectos legales: aceptación como prueba en juicio.

PRESERVACIÓN DE LA EVIDENCIA



CADENA DE CUSTODIA

DOCUMENTACIÓN (EN PAPEL) DE:

- **Confiscación o Secuestro**
- **Custodia**
- **Control**
- **Transferencia**
- **Análisis**
- **Remisión de evidencia digital**

MANIPULAR LA EVIDENCIA CUIDADOSAMENTE PARA EVITAR ALEGATOS DE ADULTERACIÓN Y/O FALSIFICACIÓN DE LA EVIDENCIA DIGITAL

CADENA DE CUSTODIA

DOCUMENTAR:

- **Qué es la evidencia?**
- **Cómo se la obtuvo?**
- **Cuándo fue obtenida?**
- **Quién la obtuvo?**
- **Dónde viajó?**
- **Dónde fue guardada?**

ANÁLISIS DE INFORMACIÓN EN DISCOS

BDO

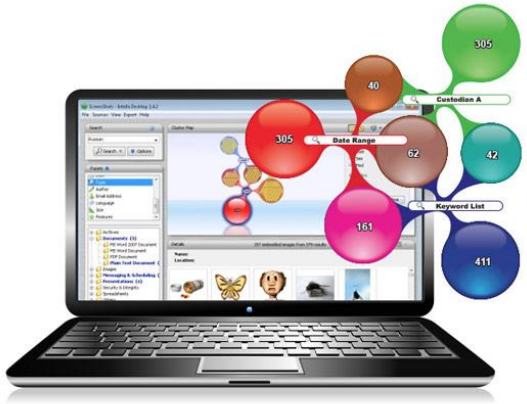
Vound

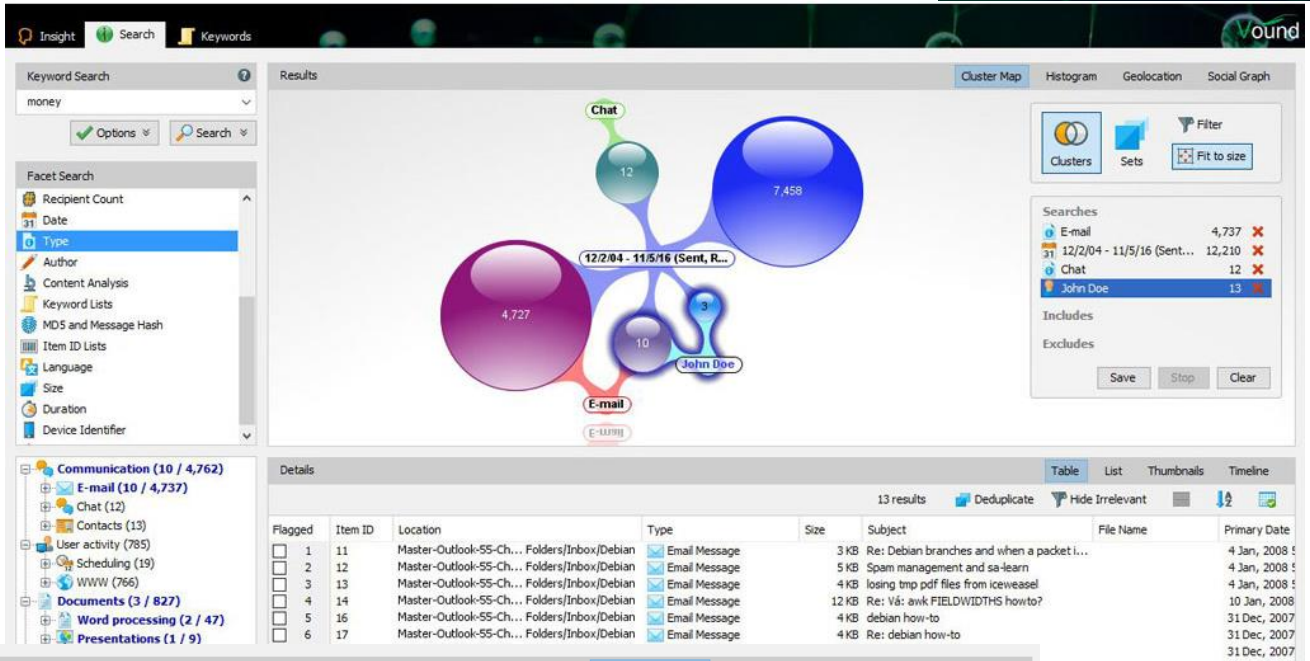
Forum | Intella | Discover Intella | About Us | Support & Training | Buy Online | DOWNLOAD FREE TRIAL

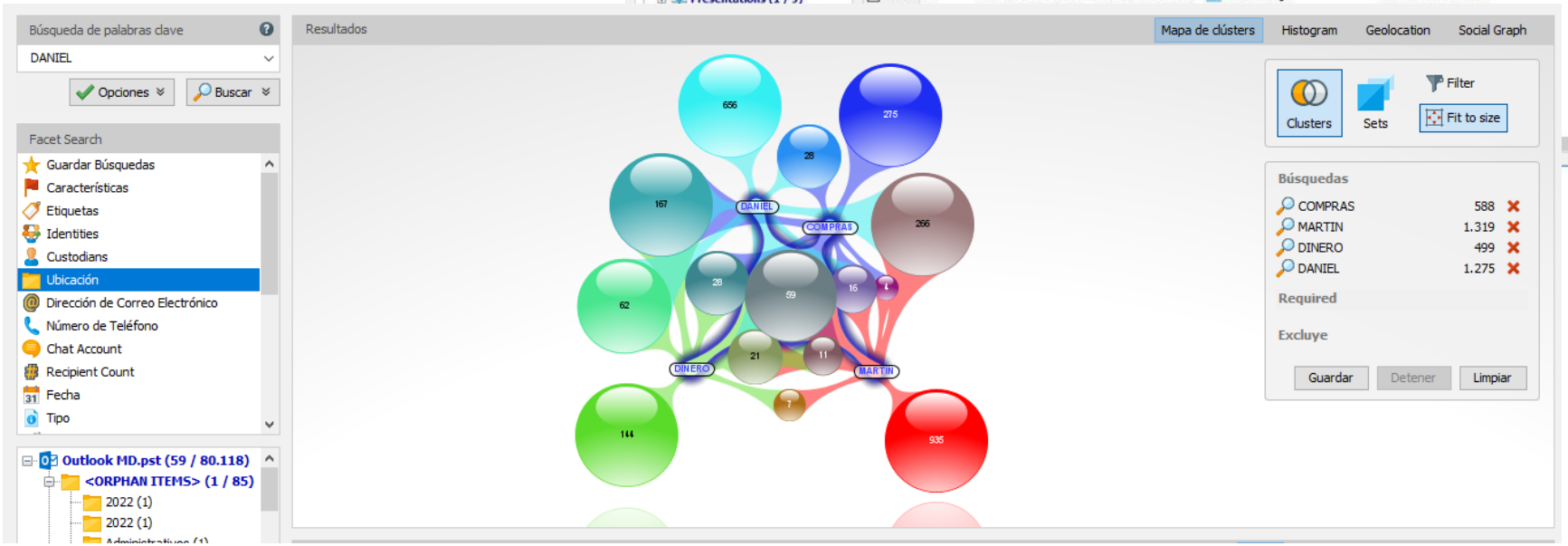
Intella®

Electronically Stored Information (ESI) – Simple

Intella® is a powerful process, search and analysis tool that makes it easy to find critical information. With our unique cluster-map technology, relationships and timelines between custodians and ESI are instantly visualized. That way you can quickly drill down through terabytes of data to find and export the most pertinent of results.





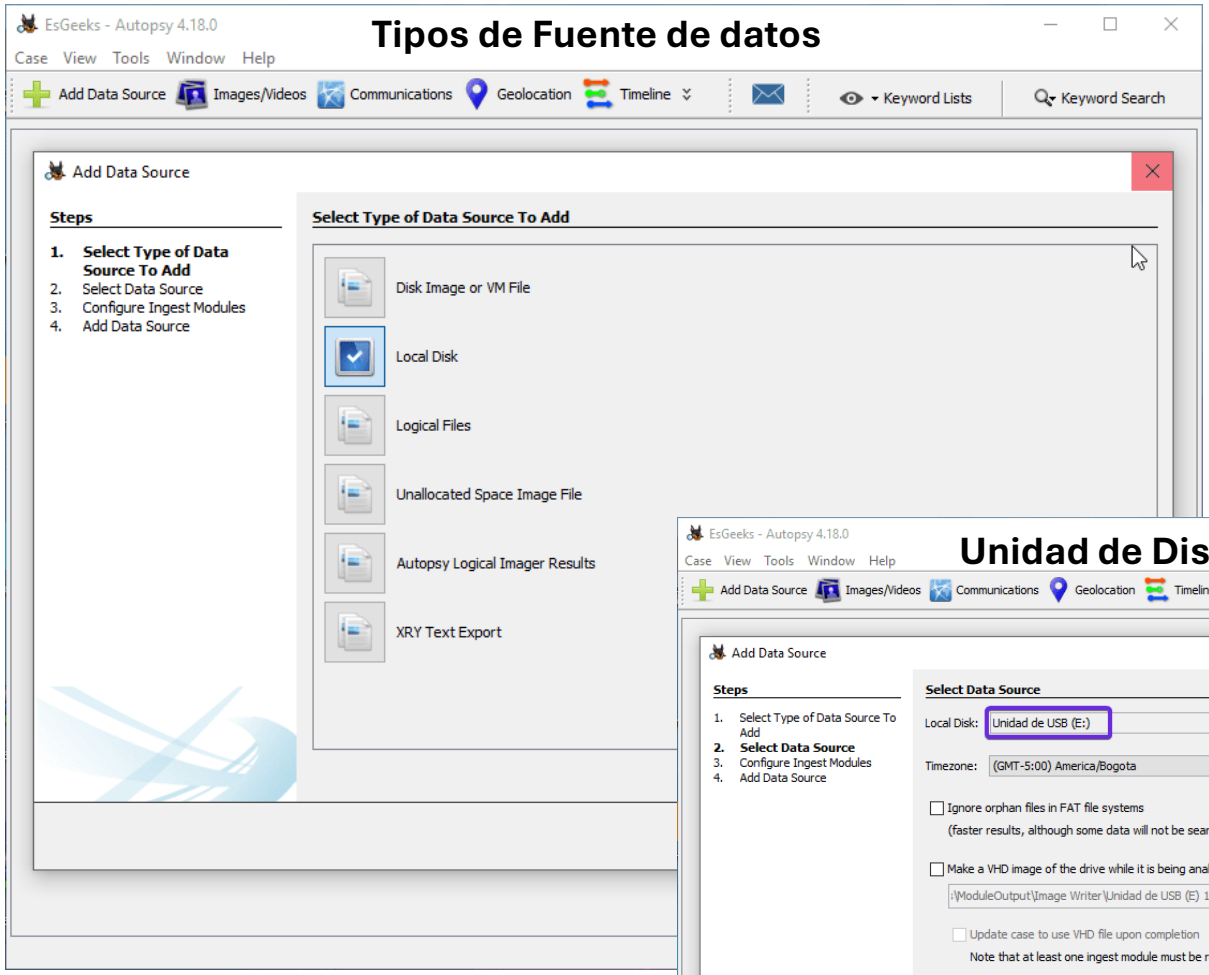


BDO

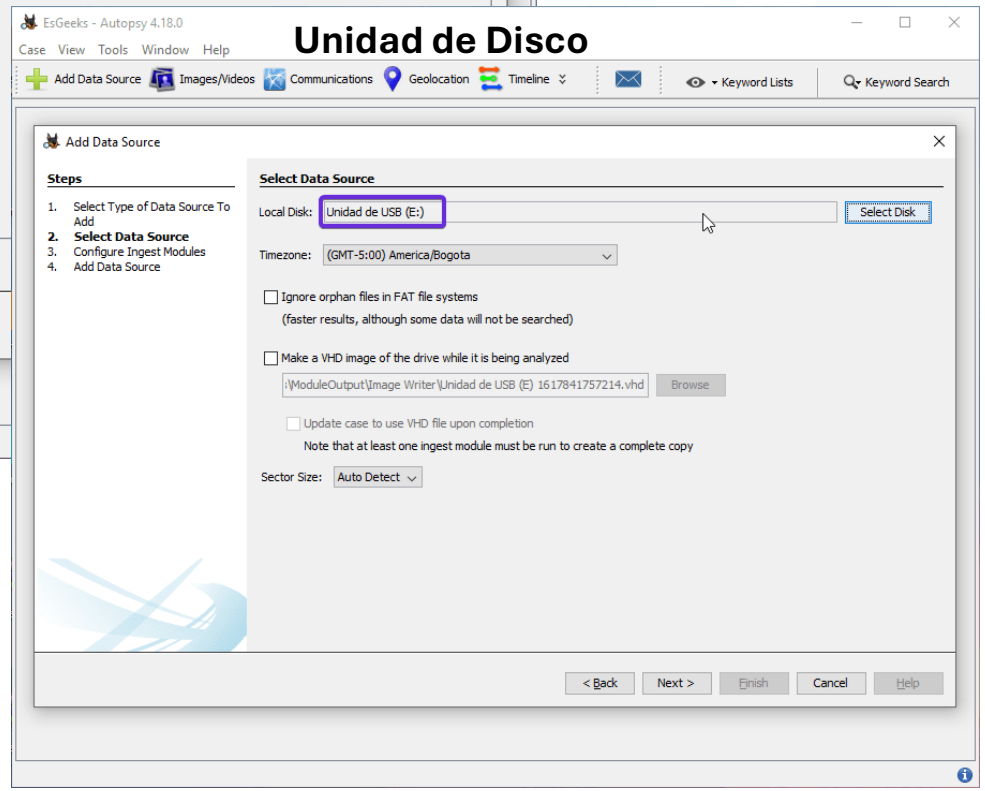
AUTOPSY
DIGITAL FORENSICS

BDO

Tipos de Fuente de datos



Unidad de Disco



Estructura de informe de investigación

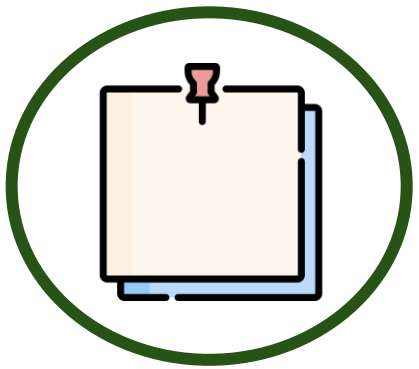
1. Objetivo y alcance de la investigación
2. Restricciones relacionadas con el uso y la distribución del informe.
3. Informe ejecutivo: principales hallazgos
4. Resumen de la denuncia y proceso de investigación
5. Detalle del proceso: entrevistas y documentación
6. Detalle de los hallazgos
7. Conclusiones con recomendaciones y acciones de mitigación
8. Anexos con elementos recabados

También es recomendable incluir...

Mapa de relaciones y/o vínculos detectados durante la investigación

Líneas de investigación definidas

Cuadros o tablas confeccionadas en Excel o PowerBI con la información recabada



Notas al pie de página con aclaraciones o información complementaria

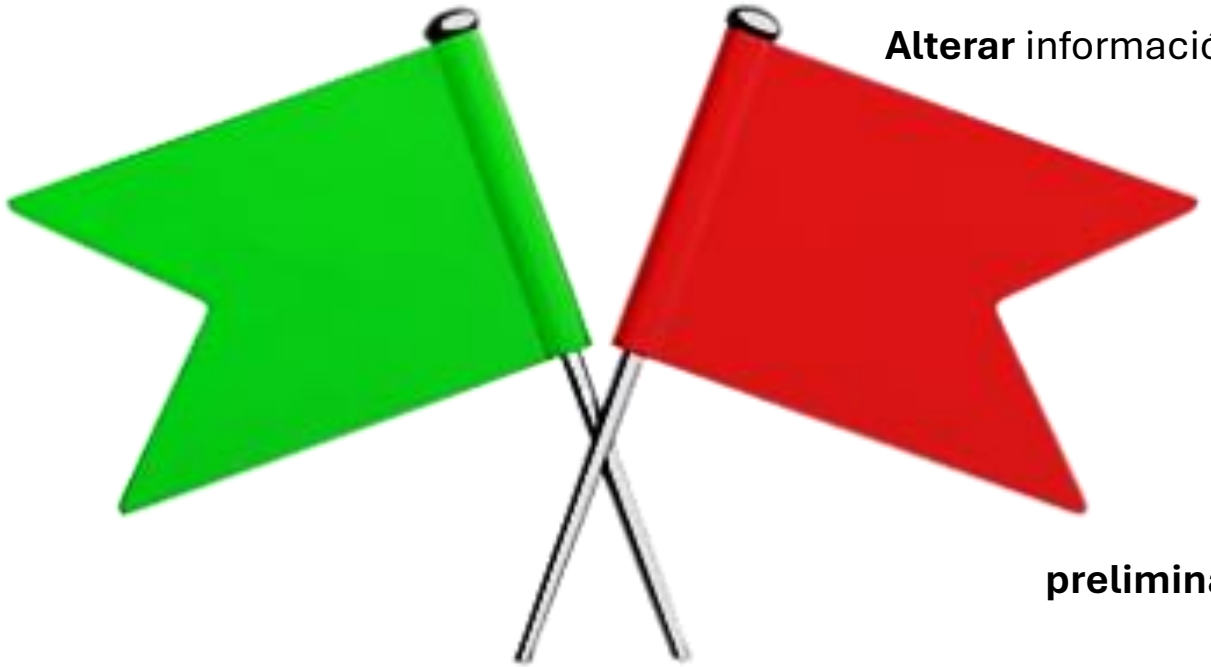
Banderas rojas y verdes en investigaciones

Ampliar el rango de búsquedas e interrelaciones cuando se realizan investigaciones sobre las vinculaciones de las personas a investigar

Documentar y mantener registro de todas las acciones tomadas durante la investigación

Designar a profesionales que **no tengan conflicto de intereses** con el objeto de la denuncia ni las personas involucradas

Proteger a los denunciantes de buena fe de cualquier forma de represalia



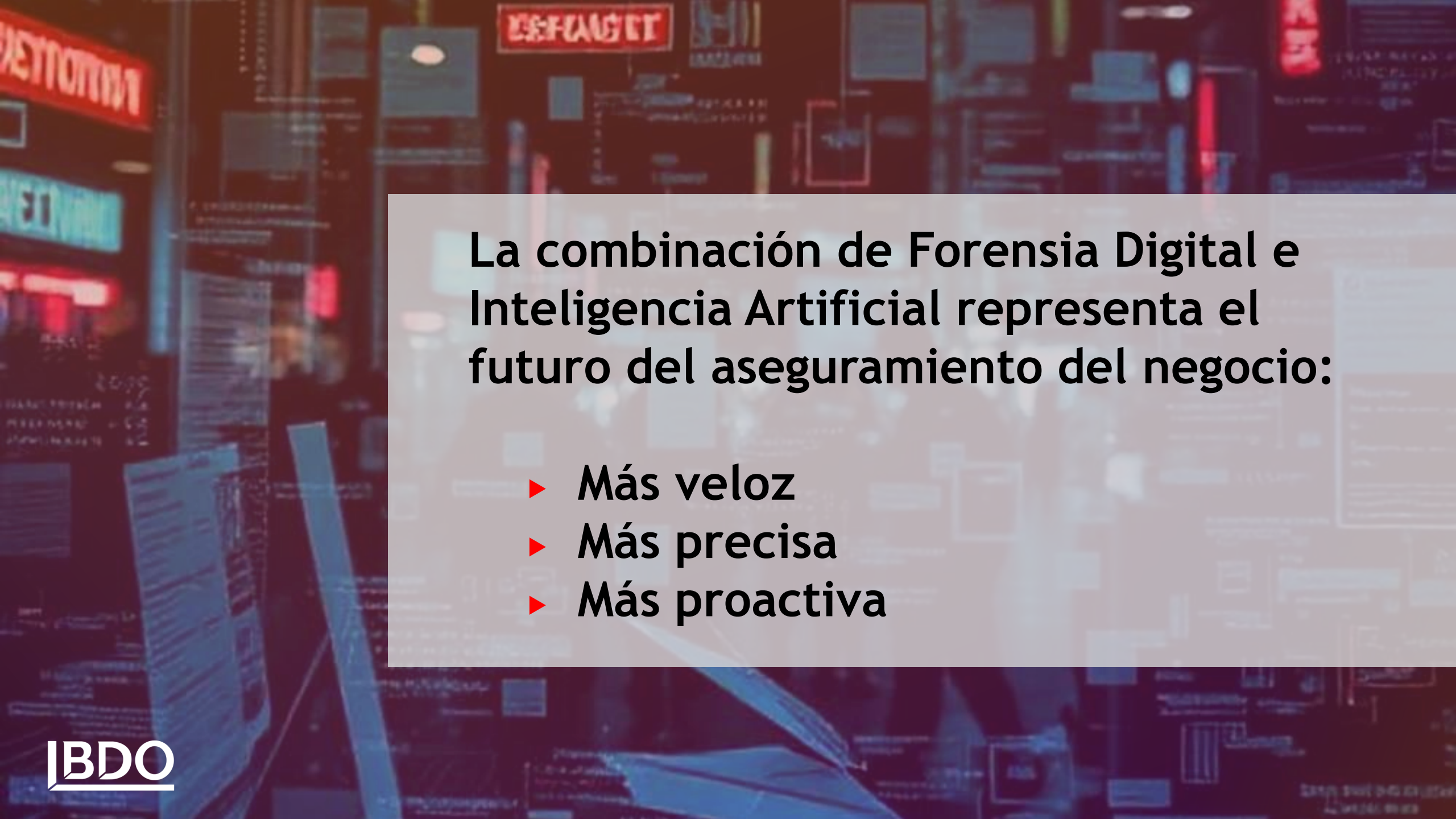
Romper la confidencialidad y exponer a la persona denunciante con la o las personas denunciadas

Alterar información, documentos o sistemas

Poca o nula comunicación con la persona denunciante sobre el progreso de la investigación

Finalizar o desestimar preliminarmente la investigación sin efectuar un análisis

Efectuar una análisis preliminar y desestimar el contenido de la denuncia. Catalogar de “falsa denuncia” inmediatamente



La combinación de Forensia Digital e Inteligencia Artificial representa el futuro del aseguramiento del negocio:

- Más veloz
- Más precisa
- Más proactiva

www.bdoargentina.com

¡Gracias!

Fabián Descalzo
Socio de Ciberseguridad y Gobierno Tecnológico
Mail: fdescalzo@bdoargentina.com

Magalí Occhiuzzi
Directora Compliance & Forensics
Mail: mocchiuzzi@bdoargentina.com

Leonardo Masip
CIT - Ciberseguridad y Gobierno Tecnológico
DRAS | Digital Assurance, Audit & Compliance Services
Mail: lmasip@bdoargentina.com