POLICÍA NACIONAL

1824 · 2024

Análisis Forense:
El Estado del Fraude.
Ciberdelitos

IV EDICIÓN CONGRESO SEGURIDAD DIGITAL Y CIBERINTELIGENCIA

1. Introducción al **Fraude como Ciberdelito**
   - ➢ Del fraude a la estafa
   - ➢ Tipología e Impacto
2. **Análisis Forense**. Importancia del análisis forense en la lucha contra el fraude y ciberdelitos
3. **Casos Prácticos**
   - ➢ El Fraude Facturas
   - ➢ El fraude del CEO

1. Introducción al Fraude como Ciberdelito

- **<u>Definición de Fraude</u>**
- RAE : **Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete**.
- OLAF (Oficina Europea de la lucha contra el Fraude / European Anti-Fraud Office): **Acción deliberada de engaño con ánimo de lucro personal o de perjudicar a otra parte** (Directiva (UE) 2017/1371 artículo 3, apartado 2 - del Parlamento Europeo y del Consejo, de 5 de julio de 2017, sobre la lucha contra el fraude que afecta a los intereses financieros de la Unión a través del Derecho penal).
  - La OLAF "sólo" investiga:
    - Fraude u otras irregularidades graves con posibles repercusiones negativas para los fondos públicos de la UE
    - Faltas graves de los miembros o el personal de las instituciones y organismos de la UE.

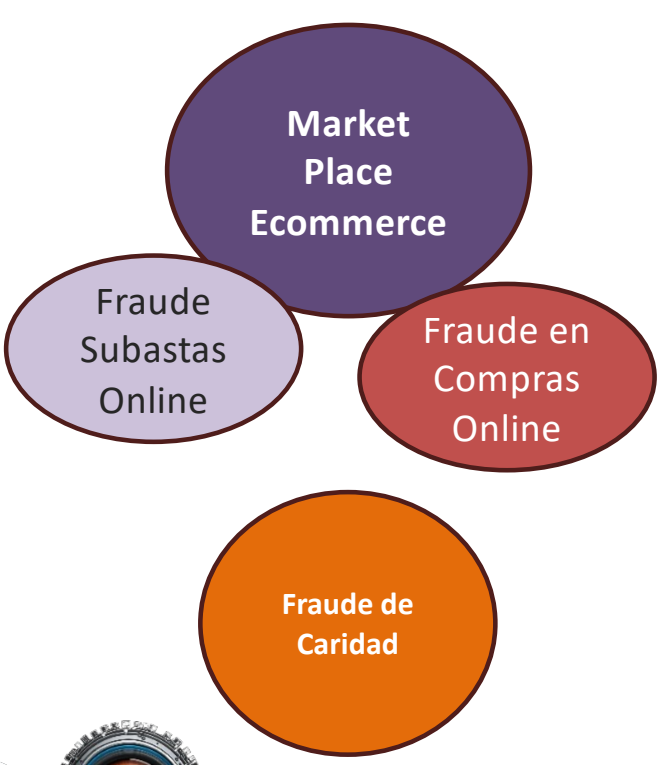
1. Introducción al Fraude como Ciberdelito

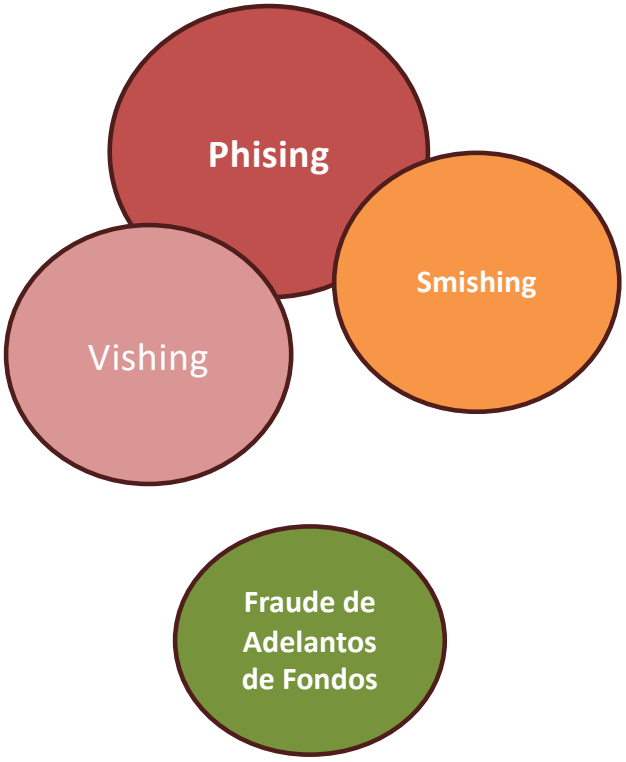
❑ Del Fraude a la Estafa (España)

Fraude	Estafa
No es necesaria la existencia del beneficio económico (Electoral, Procesal, de ley, Laboral, deudor que elude un pago mediante simulaciones)	**Delitos contra el patrimonio de la víctima o la propiedad**
	Artículo 248 del Código Penal (tipo Básico) - De 6 meses a 3 años prisión (se considera el importe)
	Delito Leve: si la estafa no excede de 400 euros, la pena será de multa de 1 a 3 meses (multa por día de 2€ a 400€ x día)
	Delito agravado de estafa: **Artículo 250 del Código Penal** (p.ej. valor de la defraudación supere 50.000 euros o afecte a un elevado número de personas, estafa procesal, bienes de primera necesidad)
	Penas de prisión de 4 a 8 años y multa de 12 a 24 meses

1. Introducción al Fraude como Ciberdelito

❑ Tipos de Fraudes más comunes





1. Introducción al Fraude como Ciberdelito

❑ Tipos de Fraudes más comunes

1.- Phishing

Técnica utilizada para adquirir información confidencial (contraseñas, números de tarjetas de crédito) mediante correos electrónicos o sitios web que se hacen pasar por entidades legítimas.

2.- Smishing y Vishing

- **Smishing**: Similar al phishing, pero a través de mensajes de texto (SMS).-
- **Vishing**: Variante del phishing que utiliza llamadas telefónicas para obtener datos personales

3.- Fraude en Compras en Línea: Sitios web falsos que venden productos inexistentes o envían productos diferentes a los anunciados.

4.- Fraude en Subastas en Línea: Manipulación de subastas en línea para incrementar los precios artificialmente o no entregar el producto subastado

5.- Fraude de Adelantos de Fondos: Prometen ganar dinero fácilmente (inversiones, premios de lotería) a cambio de un adelanto de dinero.

6.- Fraude de Caridad: Creación de organizaciones benéficas falsas para recolectar donaciones fraudulentas

1. Introducción al Fraude como Ciberdelito

❑ Tipos de Fraudes más comunes

7.- Fraude de Suplantación de Identidad:

Uso de la información personal de otra persona para cometer fraudes o delitos.

- **Fraude de Facturas**
- **Fraude del CEO**

2. **Análisis Forense**. Importancia del análisis forense en la lucha contra el fraude y ciberdelitos

Mejorando la detección de fraudes

1 Identificación de patrones de fraude

El análisis forense permite **identificar patrones de fraude a través del examen detallado de evidencia digital**, lo que facilita la detección temprana de actividades delictivas.

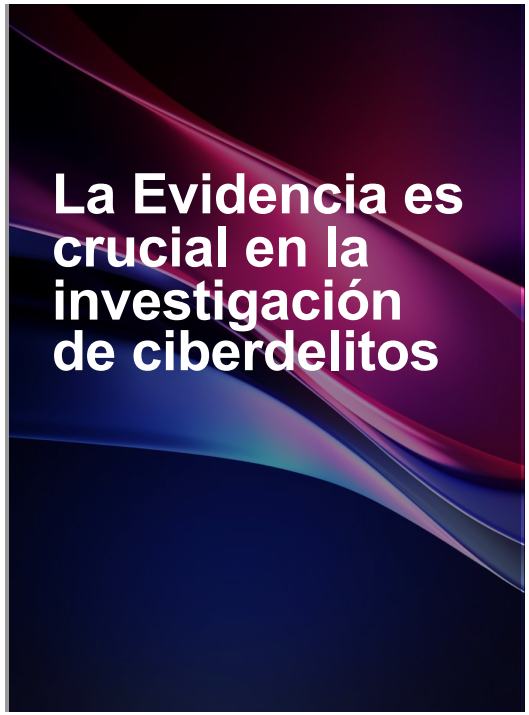
2 Rastreo de transacciones sospechosas

Mediante el análisis forense, es posible **rastrear transacciones sospechosas**, **identificando el origen y destino** de los fondos involucrados en actividades fraudulentas.

3 Reconstrucción de eventos delictivos

El análisis forense permite **reconstruir los eventos delictivos mediante la recopilación y examen de datos digitales**, proporcionando una comprensión completa de los incidentes de fraude.

2. Análisis Forense. Importancia del análisis forense en la lucha contra el fraude y ciberdelitos



Recuperación de datos borrados

El análisis forense posibilita la **recuperación de datos borrados**, lo que resulta **fundamental en la obtención de evidencia para investigaciones de ciberdelitos**.

Análisis de malware y actividades maliciosas

Mediante el análisis forense, se puede **examinar el malware y otras actividades maliciosas** para comprender su funcionamiento y origen, contribuyendo a la **prevención de ciberdelitos**.

Identificación de vulnerabilidades y puntos de acceso

El análisis forense ayuda a **identificar vulnerabilidades y puntos de acceso utilizados por ciberdelincuentes**, fortaleciendo la seguridad cibernética y la prevención de delitos informáticos.

2. **Análisis Forense**. Importancia del análisis forense en la lucha contra el fraude y ciberdelitos

La Práctica Forense en los Procesos Judiciales

Presentación de pruebas sólidas

El análisis forense debe de **proporcionar pruebas sólidas y verificables** que respaldan las investigaciones y procesos judiciales relacionados con fraudes y ciberdelitos, fortaleciendo la persecución de los responsables.

Colaboración con autoridades y expertos legales

La Práctica forense, debe de **facilitar la colaboración con autoridades y expertos**, aportando conocimientos técnicos y evidencia digital para respaldar los casos de fraude y ciberdelitos.

Defensa de la integridad de la evidencia digital

El análisis forense debe de **garantizar la integridad y autenticidad de la evidencia digital** presentada en procesos judiciales, **asegurando la validez y confiabilidad de la información** utilizada en casos legales.

2. Análisis Forense.

Importancia de la tecnología en la prevención del Fraude como Ciberdelito

Avances tecnológicos en la detección de fraudes

Los avances tecnológicos juegan un papel crucial en la identificación y prevención de actividades fraudulentas en entornos digitales.

Herramientas de análisis de datos para detectar anomalías

Las herramientas de análisis de datos son fundamentales para **detectar patrones y anomalías** que puedan indicar posibles intentos de fraude cibernético. El uso de tecnologías para la detección de fraudes plantea **desafíos en términos de privacidad y ética**, lo que requiere un **enfoque cuidadoso en su implementación**

Integración de inteligencia artificial en la prevención

La **integración de la inteligencia artificial** en sistemas de **prevención de fraude cibernético** permite una detección más ágil y precisa.

2. Análisis Forense.

El futuro de la tecnología en la lucha contra el Fraude como Ciberdelito

Desarrollo de tecnologías predictivas

Se espera un desarrollo continuo de **tecnologías predictivas** que **permitan anticipar y prevenir el fraude** cibernético de manera más efectiva.

Enfoque en la ciberseguridad basada en el comportamiento

La ciberseguridad basada en el comportamiento busca utilizar la tecnología para **identificar patrones de conducta** que puedan indicar actividades fraudulentas.

Colaboración internacional en el desarrollo tecnológico

La colaboración entre países y entidades internacionales es esencial para el **desarrollo y la implementación de tecnologías efectivas en la lucha contra el fraude** como ciberdelito.

2. **Análisis Forense**. Impacto

Impacto en la economía global

1

Pérdidas financieras significativas

El fraude como ciberdelito conlleva a **pérdidas financieras significativas** para empresas y gobiernos, afectando la economía global.

2

Costos de recuperación

Las organizaciones deben incurrir en **costos significativos para recuperarse de los ciberdelitos**, impactando negativamente en la economía.

3

Repercusiones en el comercio

El fraude como ciberdelito **afecta el comercio electrónico y la confianza del consumidor**, generando un impacto económico negativo a nivel global.

4

Desafíos para la ciberseguridad

Los ciberdelitos plantean **desafíos significativos para la ciberseguridad, lo que requiere inversiones adicionales** para contrarrestar el impacto en la economía.

2. **Análisis Forense**. Desafíos

Cooperación Internacional en la lucha contra el Cibercrimen

Intercambio de información y buenas prácticas

La colaboración entre agencias internacionales facilita el **intercambio de información y buenas prácticas en la investigación y prevención de ciberdelitos** a nivel global.

Desafíos legales y jurisdiccionales

Los desafíos legales y jurisdiccionales en la cooperación internacional **plantean obstáculos para la investigación y enjuiciamiento de ciberdelitos** que trascienden fronteras.

Desarrollo de protocolos de actuación conjunta

El establecimiento de **protocolos de actuación conjunta entre países** fortalece la capacidad de respuesta ante ciberdelitos transnacionales, mejorando la eficacia de las investigaciones forenses.

Estandarización de procesos y procedimientos

La **estandarización de procesos y procedimientos en el ámbito forense digital** facilita la cooperación internacional al establecer un **marco común para la recopilación y análisis de evidencia**.

2. **Análisis Forense**. Comparativa Evolución Cibercrimen

Evolución de la Cibercriminalidad en España 2023 – 2024 (marzo 24 MIR)
Balance de Criminalidad cuarto trimestre 2024

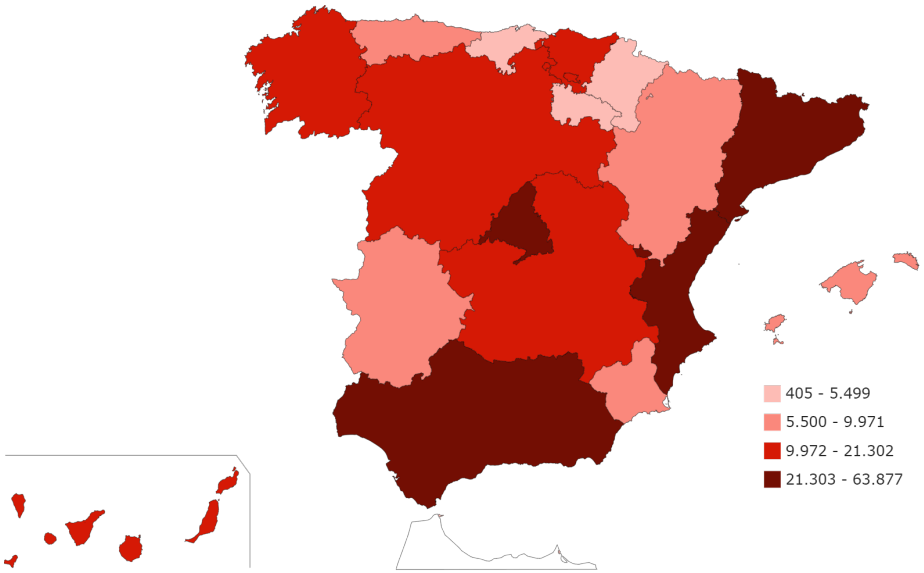
✓ La **Cibercriminalidad** (122.428 infracciones penales, el **20,2% del total**), presenta un **incremento del 13,5% sobre 2023**.

	enero a marzo		
	2023	2024	Var.% 24/23
I. CRIMINALIDAD CONVENCIONAL	480.101	484.467	0,9
II. CIBERCRIMINALIDAD (infracciones penales cometidas en/por medio ciber)	107.826	122.428	13,5
12.-Estafas informáticas	96.482	110.268	14,3
13.-Otros ciberdelitos	11.344	12.160	7,2
III. TOTAL CRIMINALIDAD	587.927	606.895	3,2

Las **estafas informáticas** (110.268 infracciones penales que **representan el 90,1% de toda la cibercriminalidad** y el **18,2% de toda la delincuencia registrada** de enero a marzo) presenta un **incremento del 14,3% sobre** el mismo período de 2023.

2. **Análisis Forense**. Comparativa Evolución Cibercrimen

Distribución por Comunidades Autónomas 2022



Comunidad	2022
CATALUÑA	63.877
MADRID (COMUNIDAD DE)	63.758
ANDALUCÍA	56.908
COMUNITAT VALENCIANA	34.005
CASTILLA Y LEÓN	21.302
GALICIA	20.914
PAÍS VASCO	20.907
CASTILLA - LA MANCHA	15.649
CANARIAS	13.684
MURCIA (REGIÓN DE)	9.971
ARAGÓN	9.620
BALEARS (ILLES)	8.701
ASTURIAS (PRINCIPADO DE)	8.560
EXTREMADURA	7.528
EN EL EXTRANJERO	5.643
NAVARRA (COMUNIDAD FORAL DE)	5.499
CANTABRIA	4.806
RIOJA (LA)	2.433
CIUDAD AUTÓNOMA DE CEUTA	567
CIUDAD AUTÓNOMA DE MELILLA	405

3. Casos Prácticos

❑ Fraude de Suplantación de Identidad

- **Fraude de Facturas:**
  - Estafa basada en la **ingeniería social dirigida a empresas**. Se produce cuando el estafador **suplanta la identidad de un proveedor o de un empleado** con el fin de **desviar el cobro de facturas**.
  - Estudian las empresas a través de su página corporativa, redes sociales e incluso hackeando las cuentas de correo de los empleados. El objetivo es **descubrir las relaciones que mantienen con sus proveedores**, incluidos los detalles de los pagos regulares.
  - El ciberdelincuente **suplanta el proveedor** y se pone en contacto con la empresa para solicitarle un nuevo procedimiento de pago facilitando un nuevo número de cuenta bancaria fraudulenta.
  - A partir de este momento, **la víctima enviará todos los pagos a la cuenta bancaria que controla el estafador**. El fraude solo se puede descubrir cuando el proveedor legítimo reclama el impago de las facturas.

3. Casos Prácticos

❑ Fraude de Suplantación de Identidad

- **Fraude de Facturas. Caso Real.**
  - Empresa Española.
  - Recibe email de falso proveedor (dominio similar), reclamando el pago de la última factura.
  - La empresa realiza transferencia:
    - Mismo Banco (extranjero), Titular de la cuenta empresa con nombre similar
  - El proveedor real escribe reclamando pago de la factura.
  - La empresa contesta al proveedor, enviando justificante de transferencia bancaria.
  - El proveedor contesta que esa cuenta no le pertenece y que su cuenta bancaria no ha cambiado.
  - La empresa detecta el fraude. Solicita información de cuenta al Banco Extranjero. El banco extrajero no contesta.
  - La empresa ha perdido :
    - 350.000€ en pagos a falso proveedor (estafador)

3. Casos Prácticos

❑ Fraude de Suplantación de Identidad

- **Fraude de Facturas. Caso Real.**
  - Emails del Ciberdelincuente

De: Smith, Lava
Enviado el: jueves, 7 de marzo de 2024 12:42
Para: "noelia macías"
CC: 'Boilletot, Patrice A.' ; 'Pruett, John D' ; 'Carpenter, Megan' ; [redacted] 'recepciontecnica' ; [redacted]
Asunto: RE: RV: [EXTERNAL] ConBid 2024 Aluminium - Kaiser- URGENT!

Noelia,

Thank you for your reply, I will be waiting for your payment update.

Thank you,

Megan Toman
Kaiser Aluminum - Corporate
Senior Manager Treasury
Office: (629) 899-7079

De: Smith, Lava <lava.smith@[redacted]aluminum.com>
Enviado el: viernes, 8 de marzo de 2024 11:22
Para: [redacted]
CC: 'Boilletot, Patrice A.' <patrice.boilletot@[redacted]aluminum.com>; 'Pruett, John D' <john.pruett@[redacted]aluminum.com>; 'Carpenter, Megan' <megan.carpenter@[redacted]aluminum.com>; 'Julio Ba[redacted]; 'recepciontecnica' <recepcion.tecnica@[redacted]; 'Mila [redacted]; """"'Ma Ángeles [redacted]"""" <administracion@[redacted]
Asunto: RE: RV: [EXTERNAL] ConBid 2024 Aluminium - Kaiser- URGENT!
Importancia: Alta

Noelia,

Send us the payment confirmation once it has been processed.

Thank you,

Megan Toman
Kaiser Aluminum - Corporate
Senior Manager Treasury
Office: (629) 899-7079

3. Casos Prácticos

❑ Fraude de Suplantación de Identidad

Uso de la información personal de otra persona para cometer fraudes o delitos.

- **Fraude del CEO:**
  - Estafa basada en la **ingeniería social dirigida a empresas**.
  - Los ciberdelincuentes **suplantan un alto cargo de la compañía con el propósito de engañar a los empleados** para que, en la mayoría de los casos, efectúen órdenes de pago fraudulentas.
  - El estafador **estudia las víctimas y recaba información sobre la empresa**. Una vez conoce el organigrama y las operaciones habituales de la compañía, **suplanta la identidad del CEO o de un alto cargo de la organización**, generalmente a través del hackeo de su cuenta correo o de la creación de una dirección falsa.
  - A Continuación, inicia el envío de correos electrónicos o rondas de llamadas para **solicitar el pago a un tercero, siempre de forma urgente y confidencial**. El objetivo es desalentar a la víctima de verificar la operación.
  - El empleado engañado lleva a cabo los pagos solicitados a las cuentas que controla el estafador.

Muchas Gracias

Manuel Hernández