

Del fraude financiero al cibercrimen

Cómo la tecnología está cambiando el riesgo LAFT

11.º Congreso LAFT América 2026 · Bogotá



MAGICSWORD

El punto de partida

“ Durante años hemos aprendido a seguir el dinero. Hoy también tenemos que seguir la tecnología que permite moverlo. ”

Identidad



¿Quién está realmente detrás de una acción digital?

Acceso



¿Cómo obtuvo acceso al entorno o a la cuenta?

Ejecución



¿Qué pudo ejecutar o manipular una vez dentro?

El crimen financiero se digitalizó

ANTES

- Efectivo y documentos físicos
- Empresas fachada
- Identidades falsas
- Transferencias y movimientos opacos
- Investigación centrada en la transacción

AHORA

- Identidades y cuentas digitales
- Credenciales robadas
- Ingeniería social
- Acceso remoto y malware
- Activos virtuales y automatización

IMPLICACIÓN

El análisis financiero sigue siendo esencial, pero debe conectarse con señales de identidad, dispositivo, acceso y comportamiento digital.

Una operación ilícita puede comenzar antes de la transacción

1

Engaño

Phishing,
suplantación,
ingeniería social

2

Acceso

Credenciales o
sesión
comprometida

3

Ejecución

Herramientas,
scripts o procesos
abusados

4

Control

Persistencia,
movimiento o
manipulación

5

Impacto

Fraude, robo,
extorsión o
transacción ilícita

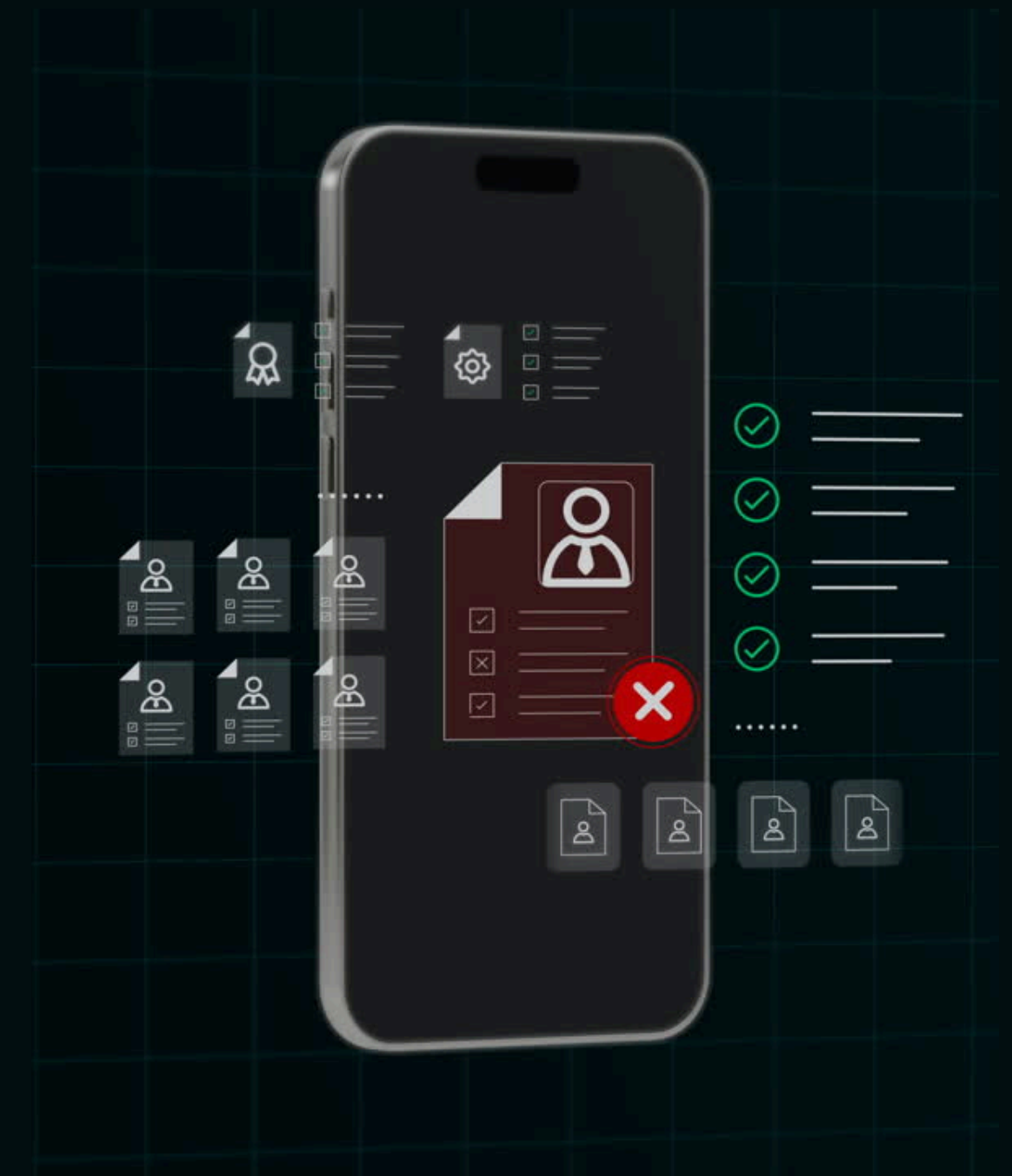
IDEA CLAVE

Si solo observamos el movimiento de dinero, podemos llegar tarde a señales que ya aparecieron en la identidad, el dispositivo o el acceso.



El dispositivo también es parte del riesgo

- Un usuario legítimo puede operar desde una sesión comprometida.
- Un atacante puede aprovechar herramientas legítimas del sistema para parecer actividad normal.
- El acceso remoto autorizado puede convertirse en un canal de abuso si cae en manos equivocadas.
- La señal relevante no siempre es "malware": puede ser una combinación anómala de identidad, acceso, proceso y contexto.



El reto: cuando lo legítimo se usa con fines ilegítimos

> contexto > privilegio > propósito

01

HERRAMIENTAS LEGÍTIMAS

Sistemas operativos y aplicaciones incluyen utilidades potentes para administración, automatización, scripting y soporte remoto.

02

ABUSO

Un atacante puede aprovechar esas mismas capacidades sin introducir necesariamente un archivo claramente malicioso.

03

DESAFÍO

El contexto importa: quién ejecuta, qué ejecuta, desde dónde, con qué privilegios y para qué propósito.

La pregunta cambia de "¿es malware?" a
"¿debería esta acción estar permitida en este contexto?"



Detección y prevención no son lo mismo

Busca reconocer comportamientos, indicadores o anomalías que puedan representar una amenaza.

Pregunta central:
¿Qué está ocurriendo?



PREVENCIÓN



Reduce las acciones que pueden ocurrir, limita privilegios y define qué comportamientos están autorizados.

Pregunta central:
¿Qué debería poder ocurrir?

Una estrategia madura combina visibilidad, detección, prevención y respuesta.

¿Por qué esto importa para LAFT?

01

Toma de cuentas

Una cuenta válida puede ser controlada por una persona no autorizada.

02

Fraude

La infraestructura comprometida puede facilitar operaciones fraudulentas.

03

Robo de credenciales

Las credenciales son un activo que habilita movimientos posteriores.

04

Manipulación de datos

Cambios en información o procesos pueden ocultar o facilitar actividad ilícita.

05

Abuso interno

Usuarios con acceso legítimo pueden exceder su función o ser comprometidos.

06

Extorsión y crimen organizado

Los ataques digitales pueden financiar, facilitar o acompañar otras actividades criminales.

CINCO PREGUNTAS

Para conectar LAFT y ciberseguridad

- 1 ¿Podemos distinguir al usuario legítimo de una sesión comprometida?
- 2 ¿Qué señales digitales observamos antes de una transacción sospechosa?
- 3 ¿Sabemos qué herramientas y procesos pueden ejecutarse en los equipos críticos?
- 4 ¿Compliance y ciberseguridad comparten señales, casos y contexto?
- 5 ¿Nuestros controles están diseñados solo para detectar o también para reducir posibilidades de abuso?

Un modelo simple de colaboración



1 • IDENTIDAD

Quién es el usuario, cómo se autenticó y qué nivel de confianza tenemos.



2 • DISPOSITIVO

Desde qué equipo opera, su postura y su contexto de riesgo.



3 • COMPORTAMIENTO

Qué procesos, accesos y acciones ocurren antes y durante la operación.



4 • TRANSACCIÓN

Qué se movió, a quién, cuánto, cuándo y bajo qué patrón.



Más contexto compartido = mejores decisiones de riesgo.



El riesgo financiero y el riesgo digital ya forman parte de la misma conversación.



No se trata únicamente de seguir el dinero.
Se trata de entender el entorno digital que puede
habilitar el delito financiero.

GRACIAS



MAGICSWORD