BANCO CHN
CRÉDITO HIPOTECARIO NACIONAL

Tipologías de lavado de dinero a través de

PAGOS ELECTRÓNICOS Y E-COMMERCE

riesgos cibernéticos asociados al lavado de dinero e identificación de patrones sospechosos

Gerencia de Cumplimiento

¿QUÉ ES LAVADO DE DINERO?

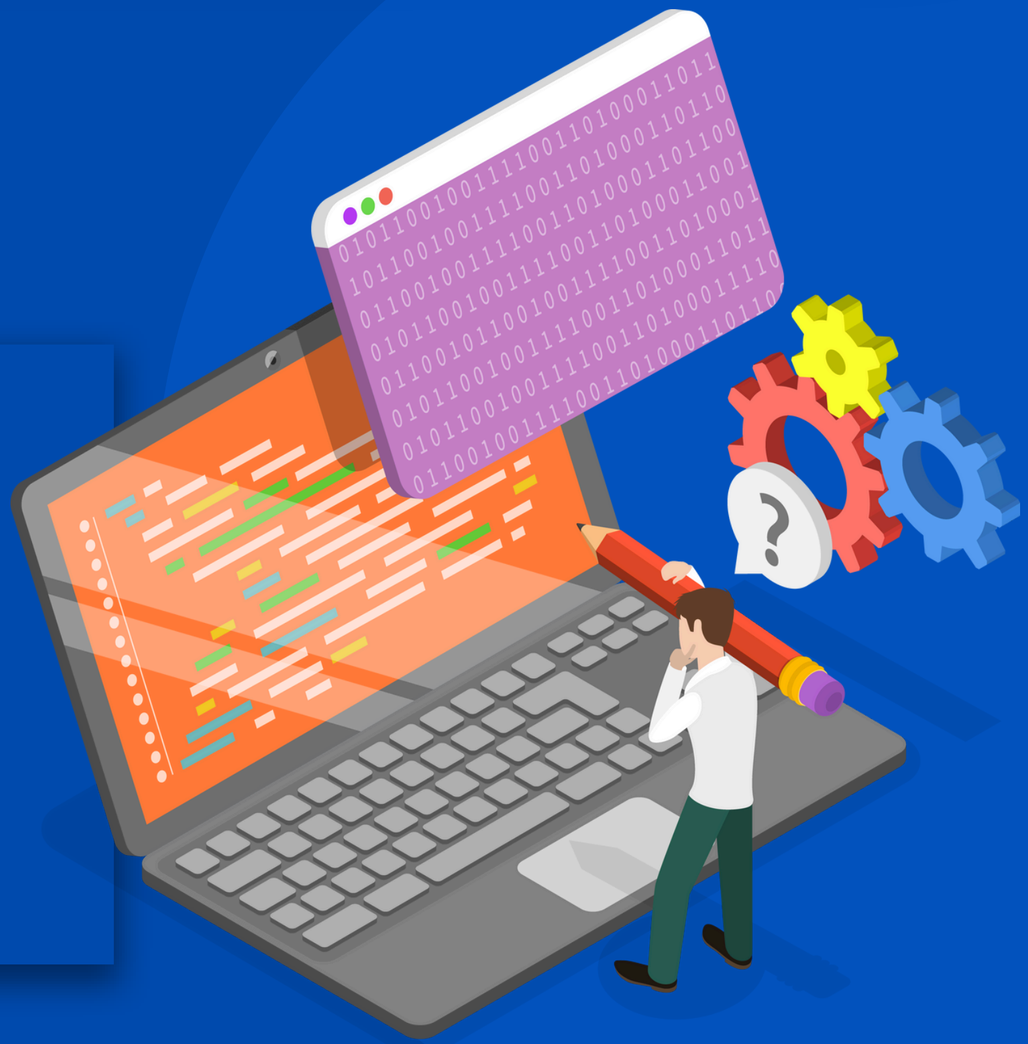
Es el conjunto de operaciones realizadas por una persona individual o jurídica, con el fin de ocultar o disfrazar el origen ilícito de bienes o recursos los cuales son producto de actividades delictivas.

¿CÓMO SE PUEDE IDENTIFICAR EL LAVADO DEINERO A TRÁVES DE MEDIOS ELECTRÓNICOS?

Los lavadores de dinero utilizan también los sistemas financieros digitales para ocultar el origen ilícito de fondos. Esto puede incluir el uso de tarjeta prepagadas, billeteras electrónicas o criptomonedas para transferir dinero de manera que sea difícil rastrear su procedencia. Por ejemplo: los delincuentes pueden dividir grandes sumas de dinero en transacciones más pequeñas para evitar alertas, o utilizar plataformas de pago en línea que no tienen controles estrictos contra el lavado de dinero.

¿QUÉ ES TIPOLOGÍA DE LD/FT?

Es la forma utilizada por las organizaciones criminales para lavar dinero dando apariencia de legalidad a los fondos de origen ilícito y transferirlos de un lugar a otro o entre personas para financiar sus actividades criminales.



¿QUÉ ES SEÑAL DE ALERTA DE LAVADO DE DINERO?

Son elementos que permiten detectar la posible presencia de operaciones de “lavado de activos”. Situaciones fuera del comportamiento habitual o particular de los clientes, empleados o asociados, es decir que salen de lo normal, por lo que se consideran atípicas.

¿QUÉ ES UN PATRÓN?

Es una serie de variables, sucesos o eventos, los cuales son constantes y/o recurrentes.

ALGUNOS EJEMPLOS DE COMERCIOS ELECTRÓNICOS, PUEDEN SER:

01

TIENDAS EN LÍNEA

Plataformas como Amazon, Shein, Ebi Mall, Pacíficko, Kemik, donde los usuarios pueden comprar productos directamente.

02

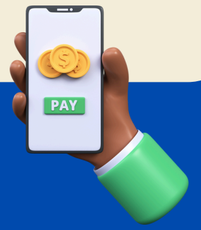
SERVICIOS DIGITALES

La adquisición de software como servicios en la nube de Google o creación de Marketplace, suscripciones o contenido digital, como música o películas.

03

PAGOS EN LÍNEA

El uso de sistemas como PayPal, Stripe o tarjetas de crédito para completar transacciones.



04

MARKETPLACE

Sitios que conectan que compradores con vendedores, como Mercado Libre o AliExpres.

Otro ejemplo: el uso de billeteras electrónicas P2P.

Peer-to-Peer, son plataformas digitales que permiten a los usuarios transferir dinero directamente entre ellos, sin necesidad de intermediarios como bancos tradicionales.

El e-commerce ha transformado el comercio tradicional, ofreciendo comodidad, alcance global y diversas opciones de pago, sin embargo, como todo sistema en el cual se utiliza dinero en este caso virtual, existen amenazas y vulnerabilidades que surgen del uso de tecnologías digitales.

Las plataformas en línea pueden utilizarse en actividades ilícitas. Algunos ejemplos claves son:

1. Uso indebido de criptomonedas: debido a su anonimato y descentralización, son utilizadas para ocultar el origen de fondos ilícitos, dificultando el rastreo de transacciones.
2. Fraude cibernético: los delincuentes pueden usar técnicas como el phishing o malware para obtener acceso a cuentas bancarias o plataformas de pago electrónico, transfiriendo fondos ilícitos sin ser detectados.
3. Plataformas de comercio electrónico falsas: se crean en tiendas en línea ficticias para procesar pagos fraudulentos y lavar dinero bajo la apariencia de transacciones legítimas.
4. Ataques a sistemas financieros: hackers pueden comprometer sistemas de instituciones financieras para desviar fondos o manipular registros, facilitando el lavado de dinero.

5. Uso de mezcladores y tumblers: estas herramientas digitales se utilizan para mezclar transacciones de criptomonedas, dificultando la identificación del origen y destino de los fondos.

6. Uso de gift cards y tarjetas prepago: como medio de movimiento de fondos.

7. El uso de Merchat Account: o cuenta de comerciante, es un tipo de cuenta bancaria diseñada específicamente para que los negocios puedan aceptar y procesar pagos electrónicos, como tarjetas de crédito u otras transferencias electrónicas.

PATRONES SOSPECHOSOS O SEÑALES DE ALERTA.

- Alto volumen de ventas en cortos periodos de tiempo.
- Actividad comercial no consistente con el perfil del cliente.
- Compras reiteradas de productos caros sin justificación comercial.
- Uso frecuente de métodos de pago difíciles de ratrear.
- Envíos internaciones a países de alto riesgo según Grupo de Acción Financiera Internacional -GAFI-
- Envió de bienes de alto valor a jurisdicciones sin justificación.
- Transacciones con valores redondeados o sin lógica comercial.

- Simulación de operaciones comerciales con facturación electrónica falsa.
- Venta de productos con precios irregulares o sin lógica comercial.
- Tarjetas abiertas con identidades robadas o falsas.
- Pagos con tarjetas robadas en tiendas del mismo lavador.
- Abuso de sistema de puntos o recompensas para lavar activos.
- Transferencias de saldo entre cuentas de juegos online.
- Movimiento de valor en plataformas tipo Steam, Roblox, etc.
- Cuentas inactivas que se activan con volúmenes altos en corto tiempo

TIPOLOGÍAS DE LAVADO DE DINERO A TRAVÉS DE PAGOS ELECTRÓNICOS:

1. Integración de fondos ilícitos mediante compras simuladas en tiendas en línea propias o de terceros.

2. Movimiento transfronterizo de fondos sin necesidad de pasar por canales tradicionales (uso de pasarelas de pago globales **).

3. Los delincuentes pueden utilizar tarjetas prepagadas para lavar dinero. Compran estas tarjetas con fondos ilícitos y luego las usan para realizar transacciones electrónicas o retiradas de efectivo. Esto dificulta el rastreo del origen del dinero, ya que las tarjetas prepagadas no están vinculadas directamente a cuentas bancarias ni a identidades verificadas

** Las pasarelas de pagos permiten aceptar pagos con tarjeta de crédito o de débito (tanto en persona como online), mediante la transferencia de dinero entre la cuenta bancaria de tu comercio y un procesador de pagos, por medio de un datáfono o de un procesador

4 El uso de empresas ficticias o fantasma en plataformas de e-commerce. Un delincuente podría crear una tienda en línea que parece legítima, pero que no vende productos reales. Luego procesa transacciones electrónicas simuladas, como si estuviera recibiendo pagos por ventas, pero en realidad está moviendo dinero ilícito a través de estas transacciones falsas. Esto da la apariencia de ingresos legítimos y dificulta el rastreo del origen del dinero

5 Clientes informan que están recibiendo una gran cantidad de correos electrónicos de phishing, esto podría ser una señal de una operación de lavado de dinero que puede estar próxima o incluso ya en marcha. Esto se debe a que muchos de los estafadores que intentan lavar dinero en un sitio de comercio electrónico intentarán acceder a varios inicios de sesión para ayudar a difundir el dinero lavado y evitar ser detectados.

6 Utilización de datos robados para abrir cuentas en plataformas de pago o e-comerce.

MUCHAS GRACIAS!!

Gerencia de Cumplimiento