Prevenir el Lavado de Activos, la Financiación del Terrorismo y el Fraude

¿Qué es el lavado de activos?

El lavado de activos busca esconder el origen de dinero y bienes obtenidos ilegalmente. A través de diferentes medios trata de introducir en la economía activos de procedencia ilícita, dándoles apariencia de legalidad, lo que permite a criminales disfrazar el origen ilegal de sus recursos.

¿Qué es la financiación del terrorismo?

El financiamiento del terrorismo proporciona fondos para la actividad terrorista. Puede tratarse de fondos recaudados de fuentes legítimas, como donaciones personales, ganancias de empresas y organizaciones benéficas, así como de fuentes delictivas, como el tráfico de drogas, el fraude, el contrabando de armas, el secuestro y la extorsión. El financiamiento del terrorismo también puede estar directamente relacionado con el lavado de dinero si el producto del delito se utiliza para financiar actividades terroristas.

¿Qué es el SARLAFT?

Es el Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo. En Nu contamos con este sistema e implementamos procesos y controles para prevenir que nuestros productos sean utilizados para actividades ilegales.

Elementos de prevención de riesgo LAFT en Nu

En cumplimiento con lo establecido en la Circular Básica Jurídica de la Superintendencia Financiera de Colombia y con el Marco Regulatorio para la prevención del lavado de activos y financiación del terrorismo, Nu ha implementado un Sistema de Administración del Riesgo del Lavado de Activos y Financiación del Terrorismo cumpliendo con las recomendaciones y mejores prácticas locales e internacionales.

Conocimiento del cliente

El proceso de conocimiento del cliente busca que todos los potenciales clientes y clientes activos sean identificados adecuadamente y se pueda establecer su perfil de riesgo y su perfil transaccional. Adicionalmente, realiza la debida diligencia para mantener actualizada la información de nuestros clientes.

Sistema de monitoreo

La entidad ha diseñado e implementado sistemas para monitorear los comportamientos transaccionales de los clientes, con el propósito de identificar operaciones inusuales a partir de las señales de alerta que se tienen establecidas.

Capacitación del personal

Nu reconoce la importancia de la construcción y mantenimiento de un programa de capacitación para toda la organización y reconoce que todos los empleados son fundamentales en la lucha contra el lavado de activos y/o financiación del terrorismo, según el rol que desempeñan.

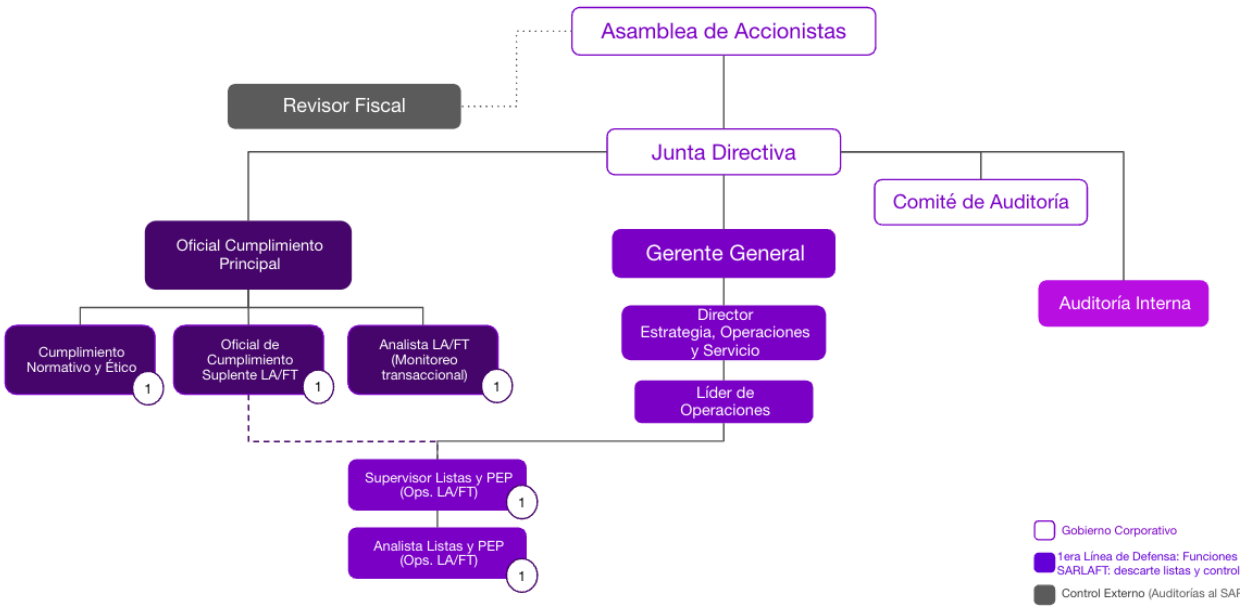
Oficial de Cumplimiento

Para el desarrollo de las funciones establecidas por las normas legales, la Junta Directiva de Nu designó un Oficial de Cumplimiento Principal y un Oficial de Cumplimiento Suplente, los cuales se encuentran debidamente posesionados ante la SFC. El Oficial de Cumplimiento es un colaborador de Nu, con capacidad decisoria, que reporta directamente a la Junta Directiva de Nu.

Auditoría y Control

Nu, cuenta como entes de control como son la Auditoría Interna y la Auditoría Externa. Las cuales cuentan con un programa de revisión basado en riesgos el cual es evaluado anualmente y sus resultados son informados a la Junta Directiva y al Oficial de Cumplimiento.

Estructura orgánica del área de Cumplimiento y SARLAFT



Estos son algunos de los delitos fuente de lavado de activos más comunes

- Tráfico de drogas
- Trata de personas
- Enriquecimiento Ilícito
- Secuestro extorsivo
- Tráfico de armas
- Contrabando
- Extorsión
- Fraude informático

¿Cómo prevenir el lavado de activos?

- No des información personal a desconocidos.
- No participes de negocios con margen de ganancia muy elevado sin justificación.
- No prestes tus productos financieros para recibir dinero de desconocidos.
- Trata de conocer a las personas con quién haces negocios
- Denuncia comportamientos sospechosos en la página de la Unidad de Información y Análisis Financiero - UIAF.

Tipos de fraude más utilizados por ciberdelincuentes

Ingeniería social

Son técnicas de engaño y manipulación que utilizan los delincuentes para obtener información confidencial que les permita suplantar tu identidad y cometer fraudes.

Phishing

Es una estafa realizada a través de un correo electrónico, donde el delincuente engaña al destinatario para que abra un archivo adjunto (con software malicioso), haga clic en un enlace malicioso o entregue información personal.

Smishing

Es un tipo de fraude en donde un atacante trata de obtener información personal o financiera de un usuario mediante un mensaje de texto o a través de redes sociales. Utilizan mensajes con promociones, premios o alertas para que el destinatario sienta la necesidad de responder.

Vishing

Este tipo de fraude se realiza a través de una llamada telefónica, donde el atacante falsifica su identidad y engaña a la persona para que proporcione información confidencial.

Malware

Es un software malicioso que busca infectar los computadores y dispositivos móviles para tomar control remoto de ellos y extraer información confidencial.

Suplantación de identidad

Este tipo de fraude se da cuando un delincuente obtiene información personal de una víctima para suplantar o intentar cometer estafas y fraudes en su nombre.

¿Cómo evitar ser víctima de fraude?

- No compartas tu información personal en redes sociales.
- No uses la misma contraseña en varios portales de internet.
- Navega en páginas web seguras y sitios de confianza.
- No hagas compras en línea o transacciones bancarias conectado a redes de wifi públicas.