



## INTRODUCCIÓN

Por medio de este documento CISCO COLOMBIA divulga a todas sus contrapartes las políticas generales del SAGRILAFT (Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, de la Financiación del Terrorismo y de la Financiación a la Proliferación de Armas de Destrucción Masiva) implementado en la Compañía en cumplimiento de lo estipulado en el capítulo X de la Circular Básica Jurídica por la Superintendencia de Sociedades.

### **POLÍTICA DE GESTIÓN DE RIESGOS LA/FT/FPADM**

Cisco Colombia es una empresa multinacional comprometida con hacer negocios de forma correcta, con integridad, transparencia y honestidad. Tomar la decisión empresarial ética y hacer lo correcto, forman parte del ADN de la Compañía. Por ello, Cisco Colombia no tolera cualquier actividad asociada al LA/FT/FPADM y reconoce que estas conductas ilícitas violan la confianza del público, amenazan el desarrollo económico y social, y perjudican el comercio justo.

Estamos comprometidos a llevar nuestro negocio de forma justa, con transparencia e integridad y a cumplir de manera estricta todas las obligaciones legales a nuestro cargo. Por ello, implementamos normas y estándares de seguridad que ayudan a generar confianza y credibilidad en sus actividades nacionales e internacionales.

Estas normas y estándares de seguridad se materializan en el Manual del Sistema de Autocontrol y Gestión del Riesgo Integral del Lavado de Activos, la Financiación del Terrorismo y de la Financiación a la Proliferación de Armas de Destrucción Masiva ("SAGRILAFT"), cuya metodología y controles se expresan en el Manual SAGRILAFT y en la Matriz de Riesgos LA/FT/FPADM. El Manual SAGRILAFT, así como todas las políticas y procedimientos diseñados por la Empresa para gestionar los riesgos LA/FT/FPADM son de obligatorio cumplimiento y buscan establecer los lineamientos y procedimientos para evitar, detectar y dar una respuesta apropiada a los Riesgos LA/FT/FPADM.

### **LINEAMIENTOS PARA LA GESTIÓN Y PREVENCIÓN DE LOS RIESGOS LA/FT/FPDAM**

La Compañía imparte los siguientes lineamientos y políticas destinadas a la prevención, detección y reporte de LA/FT/FPADM que son de obligatorio cumplimiento para las contrapartes que establezcan algún vínculo con Cisco Colombia, de conformidad con los requerimientos de la normativa en Colombia y por las políticas corporativas globales de Grupo Cisco, del cual hace parte Cisco Colombia y, en general, de las políticas y procedimiento establecidos por la Compañía para Colombia.

#### **Manejo de dinero en efectivo**

Cisco Colombia limita la utilización de efectivo en sus operaciones con Contrapartes. Razón por la cual, no es permitido recibir o efectuar pagos en efectivo, en todos los casos las transacciones deberán realizarse a través de transferencia bancaria.

## **Incursión en nuevos mercados y apertura de nuevas líneas de negocio**

Previo al lanzamiento de cualquier producto, a la modificación de sus características, a la incursión en un nuevo mercado, a la apertura de operaciones en nuevas jurisdicciones o al lanzamiento o modificación de los canales de distribución, los departamentos de negocio involucrados deberán comunicar al Oficial de Cumplimiento a fin de que éste realice un análisis, identificación, evaluación de Riesgos LA/FT/FPADM que el lanzamiento pueda generar a la Empresa, asimismo y de ser necesario, propondrá nuevos controles para mitigar los riesgos LA/FT/FPADM.

## **Registro de pagos y control de operaciones**

Para el caso de Clientes, la Compañía registra todos los pagos a través del sistema de la Compañía y son aplicados a las facturas o cuentas que se encuentren abiertos a los clientes.

En el caso de Proveedores, el equipo de Accounts Payable verifica que el pago se haya realizado a la cuenta bancaria registrada para el Proveedor que en ningún caso podrá ser de un tercero, de acuerdo con lo establecido en las políticas de Cisco sobre Compras e Impuestos.

La Compañía ha diseñado procesos de identificación de operaciones sospechosas e intentadas, y cuando ellas se detecten las reportará a la UIAF mediante el SIREL, salvaguardando su confidencialidad.

## **Debida Diligencia**

Cisco Colombia reconoce que el principal instrumento para prevenir y controlar el riesgo LA/FT/FPADM es la debida diligencia. Con el objeto de conocer a las distintas contrapartes con las que Cisco Colombia potencialmente desea desarrollar relaciones contractuales y de negocios, la Compañía ha diseñado un procedimiento que parte de la calidad de la Contraparte para determinar el responsable, los documentos y pasos a desarrollar en la debida diligencia.

La Compañía conducirá procesos de debida diligencia con todas sus contrapartes, solicitando la documentación pertinente para su onboarding y conocimiento adecuadamente, a la vez que consulta si están registrados en listas restrictivas. No habrá excepciones a estos procedimientos. El proceso de debida diligencia podrá intensificarse en los casos descritos en el SAGRILAFT de Cisco Colombia.

## **Recepción e investigación de denuncias**

Cuando evidencie que una situación puede afectar a la Compañía o a algún Empleado o puede constituir una violación a las políticas de Grupo Cisco o la normativa colombiana, es su obligación reportarlo inmediatamente a través de los siguientes canales:

- Línea ética online que está habilitada para Empleados y Contrapartes es: <http://www.cisco.com/c/en/us/about/corporate-social-responsibility/ethics-office/ethicsline.html>.
- También se encuentran a disposición los correos electrónicos: [ethics@cisco.com](mailto:ethics@cisco.com) o [auditcommittee@external.cisco.com](mailto:auditcommittee@external.cisco.com).