ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

POLÍTICA CORPORATIVA DE PREVENCIÓN Y COMBATE A ACTOS ILÍCITOS

Objetivo

Este documento tiene como objetivo consolidar los principios y las directrices de Itaú Unibanco Holding S.A. en lo que se refiere a la prevención y el combate al lavado de dinero, el financiamiento del terrorismo y los fraudes, todo ello en consonancia con la legislación y reglamentación vigentes y con las mejores prácticas de mercado nacionales e internacionales.

Introducción

Las instituciones financieras desempeñan un papel fundamental en la prevención y el combate a actos ilícitos, entre los que se destacan el lavado de dinero, el financiamiento del terrorismo y los fraudes.

El gran desafío es identificar y reprimir operaciones cada vez más sofisticadas que intentan encubrir el origen, la propiedad y el movimiento de bienes y valores provenientes de actividades ilegales.

Itaú Unibanco establece la presente política con el propósito de evitar verse involucrado en actividades ilícitas y proteger su reputación e imagen a los ojos de colaboradores, clientes, aliados estratégicos, proveedores, prestadores de servicios, órganos reguladores y sociedad, por medio de una estructura de gobierno orientada hacia la transparencia, el riguroso cumplimiento de normas y reglamentos y la cooperación con las autoridades policiales y judiciales. Asimismo, mantiene una labor constante de inversión y capacitación de sus colaboradores en el sentido de adherirse a las mejores prácticas nacionales e internacionales de prevención y combate a actos ilícitos.

Conceptos

El lavado de dinero consiste en ocultar o simular la naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes, derechos o valores provenientes, directa o indirectamente, de transgresión penal.

El financiamiento del terrorismo se configura por la estructuración de fuentes de recursos financieros (lícitos o ilícitos), transferidos de forma oculta o simulada, para permitir que los grupos terroristas realicen sus actividades.

El fraude se refiere al acto intencional de omisión/manipulación de información, transacción, apropiación de valores, adulteración de documentos, registros y estados contables.

Público-Objetivo

Esta política se aplica a Itaú Unibanco y a sus empresas controladas y vinculadas en Brasil y en el extranjero.

En caso de existir algún conflicto entre esta política y la legislación local donde se ubiquen las representaciones en el extranjero, prevalecerá el modelo más riguroso, siempre y cuando no se infrinja la legislación local.

Responsabilidades

Conselho de Administração

- Aprobar las directrices de prevención de actos ilícitos de la Institución y sus respectivas modificaciones.

Comitê de Auditoria

- Supervisar el Programa Corporativo de Prevención de Actos Ilícitos.

Comissão Superior de Risco Operacional

- Definir las directrices de prevención de actos ilícitos de la Institución.
- Analizar los resultados de los procesos y actividades de prevención de actos ilícitos.
- Resolver situaciones no previstas en esta política.

Comitês Setoriais de Risco

- Definir las directrices sectoriales de prevención de actos ilícitos según las especificidades de las unidades de negocios.
- Verificar los resultados de los procesos y actividades de prevención de actos ilícitos que hayan sido adoptados en la unidad de negocio.

Comitês de Prevenção à Lavagem de Dinheiro

- Evaluar las transacciones u operaciones sospechosas de ser actividades de lavado de dinero.
- Decidir sobre la comunicación de estos hechos a los órganos reguladores competentes y la gestion de consequencia, en acuerdo con la legislación local vigente.

Diretoria de Segurança Corporativa

- Administrar el Programa de Prevención de Actos Ilícitos de Itaú Unibanco en Brasil y en el extranjero.
- Validar las políticas sectoriales de Prevención de Actos Ilícitos elaboradas por las unidades de negocios.
- Realizar la evaluación previa de los riesgos de lavado de dinero, financiamiento del terrorismo y fraudes en nuevos productos y servicios.
- Definir la metodología y los criterios de clasificación de riesgos de lavado de dinero, financiamiento del terrorismo y fraudes de los clientes, aliados comerciales, proveedores y prestadores de servicios.
- Ayudar a las unidades de negocios a definir e implantar procesos de Prevención de Actos Ilícitos.
- Evaluar riesgos de lavado de dinero, financiamiento del terrorismo y fraudes al entablar relaciones con clientes persona y empresa en Itaú Unibanco Brasil en cuanto a los procesos que estén bajo su gestión directa.
- Seguir y diagnosticar los diferentes tipos de actos ilícitos en el sentido de anticipar tendencias y proponer soluciones preventivas y de combate.
- Monitorear, identificar y analizar las transacciones y operaciones realizadas por los clientes que lleven a pensar o sospechar en la posibilidad de fraude, lavado de dinero o financiamiento del terrorismo y realizar la respectiva comunicación, cuando corresponda, a los órganos competentes en Brasil, así como supervisar tales actividades en el ámbito de las unidades en el extranjero.
- Coordinar el Comitê de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (CFT) en lo que se refiere a las operaciones realizadas por medio de Itaú Unibanco Brasil y seguir y/o participar en los Comitês de PLD/CFT de Banco de Atacado Brasil y de las unidades en el extranjero.
- Elaborar e implementar un programa de entrenamiento y capacitación continua de los administradores y colaboradores sobre prevención y combate al lavado de dinero, al financiamiento del terrorismo y a fraudes.

Unidades de Negocios

- Implantar políticas sectoriales en consonancia con las directrices corporativas de prevención y combate al lavado de dinero, financiamiento del terrorismo y fraudes.
- Definir e implementar procedimientos y controles compatibles con la complejidad y los riesgos asociados a sus operaciones.
- Asegurar que los colaboradores realicen entrenamientos sobre prevención y combate al lavado de dinero, al financiamiento del terrorismo y a fraudes.
- Designar los Puntos Focales de PLD/CFT en sus respectivas unidades de negocios.

Puntos Focales de PLD/CFT- Unidades de Negocios

- Garantizar el cumplimiento de las directrices corporativas de PLD/CFT por parte de la unidad de negocios.
- Monitorear los riesgos de lavado de dinero y respectivos controles de la unidad de negocios bajo la supervisión directa del ejecutivo.

Diretoria de Controles Internos e Compliance

Las responsabilidades del área de Controles Internos, Compliance e Risco Operacional están descritas en política específica.

Adicionalmente, este directorio debe:

- Definir y ejecutar pruebas para verificar los procedimientos de control adoptados para prevenir y combatir actos ilícitos.
- Evaluar las posibles comunicaciones dirigidas a DCIC que hayan sido realizadas por los colaboradores sobre sospechas o casos de actos ilícitos y, cuando corresponda, entrar en contacto con Diretoria de Segurança Corporativa para que se adopten las medidas oportunas.
- Monitorear el cumplimiento de lo que Diretoria de Segurança Corporativa haya solicitado a los gestores comerciales e informar sobre eventuales situaciones de riesgos en los Comitês Setoriais de Risco.
- Verificar si los colaboradores realizan el entrenamiento de prevención y combate al lavado de dinero, al financiamiento del terrorismo y a fraudes.

Jurídico

- Analizar los requerimientos legales y regulatorios de PLD/CFT y respectivos impactos en los negocios.
- Ayudar a los gestores de negocio a elaborar planes de acción para implantar controles de PLD/CFT.
- Apoyar la evaluación de los riesgos y la adopción de las medidas necesarias para tratar los casos de transacciones u operaciones sospechosas de lavado de dinero desde el punto de vista jurídico.

Administradores y Colaboradores

- Conocer y seguir las directrices de esta Política y realizar los entrenamientos de Prevención de Actos Ilícitos ofrecidos por Diretoria de Segurança Corporativa.
- Comunicar toda situación, operación o propuesta sospechosa de implicación con algún acto ilícito a Diretoria de Segurança Corporativa.
- Responder en su debido momento y con objetividad a lo solicitado por Diretoria de Segurança Corporativa.

Auditoria Interna

- Las responsabilidades relacionadas a la actuación de la Auditoría Interna se describen en política específica.

Programa Corporativo de Prevención de Actos Ilícitos

Con el propósito de viabilizar el cumplimiento de las directrices de esta política y evitar que sus productos y servicios se utilicen en actividades ilícitas, Itaú Unibanco estableció un programa de prevención y combate a actos ilícitos que se compone de las siguientes reglas:

Prevención y Combate al Lavado de Dinero y al Financiamiento del Terrorismo

Proceso de Identificación de Clientes:

Se trata de un conjunto de acciones que deben adoptarse para identificar clientes, entre las que se destacan la obtención, actualización y almacenamiento de informaciones de registro. También incluye procedimientos específicos para identificar a Beneficiarios Finales y Personas Expuestas Políticamente (PEP).

Itaú Unibanco no admite la apertura y mantenimiento de cuentas anónimas.

Se prohíbe entablar o mantener relaciones con individuos o entidades mencionadas en las listas de sanciones financieras de Naciones Unidas (ONU), *US Office of Foreign Assets Control* (OFAC) y Unión Europea.

Proceso "Conozca a su Cliente" (KYC):

Se trata de un conjunto de acciones que deben adoptarse para asegurar la identidad y la actividad de los clientes, así como el origen y la constitución de su patrimonio y recursos financieros. En aquellos casos con más riesgo asociado a actos ilícitos deben aplicarse criterios de identificación y actuación más rigurosos, al paso que la relación debe ser aprobada por un nivel jerárquico superior.

Cuanto más precisas sean las informaciones obtenidas y registradas en el momento en que se entable la relación, mayor será la capacidad de identificar riesgos de práctica de actos ilícitos y mayor será también la seguridad para los clientes que depositan su confianza en Itaú Unibanco.

Proceso "Conozca a su Aliado " (KYP):

Se trata de un conjunto de reglas, procedimientos y controles que deben adoptarse para identificar y aceptar aliados comerciales, incluyendo a los corresponsales en el país y en el extranjero, a efectos de prevenir la realización de negocios con contrapartes no idóneas o sospechosas de estar involucradas en actividades ilícitas, así como asegurar que posean procedimientos adecuados de PLD/CFT, cuando corresponda.

Itaú Unibanco no admite relaciones con los denominados Bancos Pantalla (*Shell Banks*).

Proceso "Conozca a su Proveedor" (KYS):

Se trata de un conjunto de reglas, procedimientos y controles que deben adoptarse para identificar y aceptar a proveedores y prestadores de servicios con la finalidad de evitar la contratación de empresas no idóneas o sospechosas de estar implicadas en actividades ilícitas. Con relación a aquellos casos que representen más riesgo se adoptarán procedimientos complementarios y actuaciones más profundas de evaluación y se definirán niveles de competencia específicos para su aprobación, todo según la criticidad del caso en cuestión.

Proceso "Conozca a su Empleado " (KYE):

Se trata de un conjunto de reglas, procedimientos y controles que deben adoptarse para seleccionar y verificar la situación económica financiera con objeto de evitar vínculos con personas implicadas en actos ilícitos.

Evaluación de Nuevos Productos y Servicios:

Los nuevos productos y servicios deben someterse a una evaluación previa, bajo el prisma de PLD/CFT, en conformidad con las directrices establecidas en la Política Interna.

Monitoreo de Transacciones:

Es necesario monitorear las transacciones y operaciones financieras realizadas por los clientes, sean colaboradores o no, con objeto de verificar situaciones que puedan configurar indicios de casos de lavado de dinero o financiamiento del terrorismo. Respecto a los casos que requieran Especial Atención, como la relación con Personas Expuestas Políticamente y operaciones en las que no sea posible identificar al Beneficiario Final, se adoptarán procedimientos más rigurosos de análisis. El monitoreo tiene en cuenta el perfil, origen y destino de los recursos y la capacidad financiera de los clientes.

Comunicación de Transacciones Sospechosas a los Órganos Reguladores:

Las operaciones o propuestas que contengan indicios de casos de lavado de dinero o financiamiento del terrorismo deben comunicarse a los órganos reguladores competentes cuando corresponda, en cumplimiento de las disposiciones legales y reglamentarias. Las comunicaciones hechas de buena fe no acarrean responsabilidad civil o administrativa a Itaú Unibanco ni a sus administradores y colaboradores.

Itaú Unibanco se abstiene de facilitar a los respectivos clientes o terceros informaciones sobre eventuales comunicaciones efectuadas en razón de indicios de lavado de dinero o financiamiento del terrorismo.

Entrenamiento:

El programa de entrenamiento de PLD/CFT es continuo y debe aplicarse a todos los colaboradores elegibles con el objetivo de:

- ampliar el conocimiento que los administradores y colaboradores tienen a respecto de las exigencias y responsabilidades legales y reglamentarias, así como de las directrices corporativas de PLD/CFT;

- capacitar a administradores y colaboradores para identificar, prevenir, tratar y comunicar situaciones de riesgo o con indicios de posibles casos de lavado de dinero o financiamiento del terrorismo en los negocios realizados.

Este programa debe aplicarse por medio de acciones institucionales y en las áreas de negocios, e incluirán cursos presenciales o a distancia (*e-learning*), charlas, teleconferencias, audio conferencias, campañas, comunicados y publicaciones, entre otras modalidades y formas.

Declaración de Observancia de los Requerimientos de PLD/CFT:

Los ejecutivos responsables de las áreas de negocios en Brasil o en el extranjero deben enviar a Diretoria de Segurança Corporativa, anualmente y por escrito, una declaración sobre la observancia y conformidad con las directrices de esta Política. La existencia de legislación o reglamentación que impida o limite la aplicación de lo dispuesto en esta Política deberá informarse en la referida declaración.

Prevención y Combate a Fraudes

Evaluación de Riesgos al Principio de la Relación:

Los procesos de contratación de servicios y productos deben incluir procedimientos para prevenir y mitigar el riesgo de fraude al principio de la relación con proponentes.

Evaluación de Riesgos en Nuevos Productos y Servicios:

Los nuevos productos y servicios deben evaluarse con anterioridad, pensando en la prevención del fraude, y en conformidad con las directrices establecidas en la Política Interna.

Monitoreo de Transacciones:

Es necesario monitorear los productos y servicios contratados por los clientes para detectar y verificar situaciones atípicas o sospechosas de casos de fraude u otros actos ilícitos.

Tratamiento de Ocurrencias:

Las situaciones bajo sospecha o confirmadas deben verificarse para conocer a los responsables y estudiar las medidas que deban tomarse.

Los procedimientos y decisiones tomadas durante el tratamiento de los casos que ocurran deben formalizarse para que puedan utilizarse en expedientes judiciales.

Entrenamiento:

El programa de entrenamiento de prevención de fraudes es continuo y debe llegar a todos los colaboradores elegibles con objeto de:

- ampliar el conocimiento que los administradores y colaboradores tienen de los requerimientos normativos externos e internos de prevención y combate a fraudes;

- capacitar a administradores y colaboradores para identificar, prevenir, tratar y comunicar situaciones sospechosas o relacionadas con fraudes y otros actos ilícitos.

Este programa debe aplicarse por medio de acciones institucionales y en las unidades de negocio, y puede incluir cursos a distancia (e-learning) y presenciales, charlas, teleconferencia, audio conferencia, campañas, comunicados y publicaciones, entre otras modalidades y formas.

Prevención y Combate al Fraude Interno

Itaú Unibanco toma medidas específicas para evitar que ocurran casos de fraude en los que se vean involucrados sus colaboradores, todo ello por medio de directrices y procedimientos de control de prevención y detección de actividades irregulares.

Prevención y Combate al Fraude Contable

Itaú Unibanco toma medidas para resguardar la calidad e integridad de sus estados contables por medio de controles internos, de la realización de auditorías interna y externa y de la supervisión del Comitê de Auditoria.

Mantenimiento y Custodia de Informaciones y Registros

Las informaciones y registros de las operaciones y servicios prestados deben mantenerse en su forma original o en archivos electrónicos, según plazos y responsabilidades establecidos por la legislación vigente.

Auditoria Interna y Evaluaciones Independientes

Itaú Unibanco cuenta con un área de Auditoria Interna que evalúa regularmente la efectividad del programa de prevención y combate a actos ilícitos y propone medidas para perfeccionarlo. El programa también se somete a la evaluación periódica de organizaciones independientes.

Transparencia en las Relaciones con los Clientes

Los clientes de Itaú Unibanco disponen de diversos canales que les dan acceso a sus informaciones financieras, incluyendo recursos invertidos, productos contratados y límites concedidos. Eso convierte al propio cliente en un aliado fuerte y actuante en la prevención y el combate a actos ilícitos.

Itaú Unibanco también advierte sistemáticamente a sus clientes, por medio de los canales de relaciones, sobre las posibilidades de casos de actos ilícitos y acciones y cuidados que deben tomarse para prevenirlos.

Canales de Comunicación de Actos Ilícitos

Los administradores y colaboradores de Itaú Unibanco deben comunicar inmediatamente las situaciones en las que vean indicios o evidencias de actos ilícitos utilizando:

Situaciones Relacionadas con Lavado de Dinero o Financiamiento del Terrorismo

En Brasil, el contacto se establecerá con Superintendência de Prevención à Lavagem de Dinheiro.

En las unidades internacionales será necesario establecer contacto con los canales locales o “Compliance *Officers*”.

Situaciones Relacionadas con Fraudes y Actos Ilícitos

En Brasil, el contacto se establecerá con Superintendência de Prevención à Lavagem de Dinheiro.

En las unidades internacionales será necesario establecer contacto con los canales locales o “Compliance *Officers*”.

Estos canales también están a disposición de clientes, prestadores de servicios y público en general.

Protección a Denunciantes

- Administradores y colaboradores no pueden practicar actos de Represalia contra quien, de buena fe: (i) denuncie, presente una queja o manifieste sospecha, duda o preocupación con relación a posibles transgresiones de las directrices de esta Política; y (ii) facilite información o ayude en las investigaciones referentes a las posibles transgresiones.
- Administradores y colaboradores deben preservar la confidencialidad de las informaciones referentes a la investigación de posibles transgresiones de las directrices de esta Política.
- Los Canales de Denuncia deben recibir las manifestaciones anónimas, así como también deben preservar el anonimato.

- Se aplicará sanción disciplinaria a aquellos administradores o colaboradores que intenten o pongan en práctica cualquier represalia contra quien de buena fe comunique posibles casos de transgresión de las directrices de esta Política.
- Se aplicará sanción disciplinaria a aquellos administradores o colaboradores que, comprobadamente, hayan actuado de mala fe al comunicar posibles transgresiones de las directrices de esta Política o se hagan eco de hechos que sepan que son falsos.

Los administradores y colaboradores que transgredan los términos de esta Política estarán sujetos a las sanciones disciplinarias previstas en normas internas de las empresas del Conglomerado Itaú Unibanco.

Sanciones Previstas

El incumplimiento de las disposiciones legales y reglamentarias somete a los administradores y colaboradores a sanciones que van desde penalidades administrativas hasta criminales por lavado de dinero, financiamiento del terrorismo y fraudes.

La negligencia y el Fallo Voluntario se consideran incumplimiento de esta política y del Código de Ética, por lo que son pasibles de aplicación de medidas disciplinarias previstas en normativas internas de la Institución.

Documentos Relacionados

Esta política debe leerse e interpretarse conjuntamente con los siguientes documentos:

Normas Externas:

Leyes Federales nº 9.613/98 y nº 12.683/12.

Decreto Ley nº 2.848/40 - Código Penal Brasileño.

Resolución nº 2.025/93 del Consejo Monetario Nacional.

Resolución nº 2.747/00 del Consejo Monetario Nacional.

Circular nº 3.461/09 del Banco Central de Brasil.

Circular nº 3.462/09 del Banco Central de Brasil.

Carta Circular nº 3.430/10 del Banco Central de Brasil.

Circular nº 3.517/10 del Banco Central de Brasil.

Circular nº 3.583/12 del Banco Central de Brasil.

Carta Circular nº 3.542/12 del Banco Central de Brasil.

Circular nº 3.654/13 del Banco Central de Brasil.

Instrucción nº 301/99 de la Comisión de Valores Mobiliarios y respectivas modificaciones.

Circular nº 445 de la Superintendencia de Seguros Privados.

Resoluciones COAF nº 006/99 y 021/12.

Instrucción nº 26/08 de la Superintendencia Nacional de Previsión Complementaria.

Normativa de Autorregulación SARB nº 011/2013 de la Federación Brasileña de Bancos.

Wolfsberg Anti-Money Laundering Principles.

Recomendaciones de GAFI (Grupo de Ação Financeira).

Normas Internas:

Política Corporativa de Ética.

Política Corporativa de Seguridad de la Información.

Política Corporativa de Prevención de la Corrupción.

Política de Gobierno Corporativo.

Glosario

Actos Ilícitos: lavado de dinero, corrupción, financiamiento del terrorismo, corrupción y fraudes.

Banco Pantalla (*Shell Bank*): banco constituido en una jurisdicción en la que carezca de cualquier presencia física y sin estar integrado a un grupo financiero reglamentado.

Beneficiario Final: es la persona física que, en última instancia, tiene el control de la persona jurídica.

CFT: Combate al Financiamiento del Terrorismo.

Especial Atención: las situaciones que requieren un monitoreo reforzado son aquellas relacionadas con:

- I - operaciones o propuestas cuyas características, en lo que concierne a las partes involucradas, valores, formas de realización e instrumentos utilizados, o que, por falta de fundamento económico o legal, indiquen riesgo de que ocurran actos ilícitos;

- II - propuestas de inicio de relaciones y operaciones con personas políticamente expuestas;

- III - indicios de burla a los procedimientos de identificación y comunicación;

- IV - clientes y operaciones en que no sea posible identificar al beneficiario final;

- V - transacciones oriundas de países que aplican insuficientemente las recomendaciones de Grupo de Ação Financeira - GAFI; y

- VI - situaciones en las que no sea posible mantener actualizadas las informaciones de registro de los clientes.

Fallo Voluntario: es el acto intencional por el que alguien se involucra en acciones ilícitas como, por ejemplo, estructurar o aconsejar a otras personas a estructurar operaciones con el propósito de burlar las comunicaciones a los órganos reguladores, o involucrarse conscientemente en transacciones cuyos fondos provengan de actos ilícitos.

Institución o Conglomerado Itaú Unibanco: a los efectos específicos de esta Política, tales términos incluyen a Itaú Unibanco Holding S.A. y a todas las empresas que controle con exclusividad en Brasil y en el extranjero.

Itaú Unibanco: Itaú Unibanco Holding S.A.

OCIR: Oficial de Controles Internos y Riesgos.

Personas Expuestas Políticamente (PEP): son los agentes públicos que desempeñan o hayan desempeñado en los últimos cinco años, en Brasil o en países, territorios y dependencias extranjeras, cargos, empleos o funciones públicas relevantes, así como sus representantes, familiares y otras personas de su círculo de relaciones más cercano. También se incluye bajo esta denominación a las personas jurídicas cuyos representantes o controlantes, directos o indirectos, sean PEP.

PLD: Prevención del Lavado de Dinero.

Puntos Focales: administradores o colaboradores indicados por el ejecutivo del área de negocios para celar por el cumplimiento de las directrices corporativas de PLD/CFT por parte de la unidad de negocios.

Represalia: acto de persecución, respuesta o venganza contra administradores o colaboradores que pongan de manifiesto sus dudas, sospechas o constataciones. Ejemplos de represalia: amenazas, descenso de cargo, inclusión en "lista negra", aplicación de suspensión, despido, etc.