# Cultura y gestión de riesgo

Asumir y administrar riesgos, tanto en nombre propio como en nombre de clientes y accionistas, es parte fundamental del negocio de Itaú. Los resultados de la gestión de riesgos dependen de la conducta de las personas. Por eso, fomentamos prácticas que generen una cultura que profundice el entendimiento, la identificación y la mitigación de los riesgos de manera transversal a toda la organización.

Tenemos el compromiso de promover la creación de un ecosistema financiero íntegro, ético y alineado con la agenda de desarrollo sostenible, a partir de la promoción de la Cultura de Riesgos a la interna de la organización y en concientizar y capacitar en temas de Prevención de Lavado de Dinero.

# Gestión de riesgo 102-15, 102-44, FS2

Tenemos el compromiso de promover la creación de un ecosistema financiero íntegro, ético y alineado con la agenda de desarrollo sostenible, a partir de promover la cultura de riesgos dentro de la organización y de concientizar y capacitar en la prevención de lavado de dinero.

El negocio de Banco Itaú Uruguay (BIU) implica asumir y administrar riesgos, tanto en nombre propio como en nombre de clientes y accionistas. Los resultados de la gestión de riesgos dependen fundamentalmente de la conducta de las personas. Entender, identificar, medir, administrar y mitigar riesgos son prácticas esenciales e inherentes a las actividades.


**Delineamos un conjunto de políticas, procedimientos y metodologías que propician la identificación, la medición, el control y el monitoreo de dichos riesgos.**

## Apetito de Riesgo

El Marco de Apetito de Riesgo, aprobado por el Directorio, determina los niveles de tolerancia a los distintos riesgos que Banco Itaú Uruguay está dispuesto a asumir para alcanzar sus objetivos de negocio. Estos se expresan en términos de capitalización, liquidez, resultados, diversificación y franquicia.

El apetito de riesgo está integrado en la gestión y determina lineamientos básicos de actividad, ya que establece el marco en el que desarrolla su presupuesto.

## Declaración de Apetito de Riesgo

"Somos un banco universal operando en Uruguay, subsidiario de un banco que opera predominantemente en América Latina. Nos apoyamos en nuestra cultura de riesgo para actuar de acuerdo con los más rigurosos estándares éticos, cumplimos la regulación y buscamos resultados elevados y crecientes con baja volatilidad, mediante una relación duradera con el cliente, la fijación correcta del precio de los riesgos, capacitación diversificada de recursos y una adecuada utilización del capital"

## Principios generales de la gestión de riesgos

Nuestro modelo de gestión de riesgos se basa en principios:

### Sustentabilidad y satisfacción de clientes

Nos preocupamos por generar valor compartido para quienes trabajan en Itaú, quienes nos eligen, los accionistas y la sociedad, garantizando la sustentabilidad del negocio. Hacemos negocios que sean buenos para los clientes y para el Banco.

### Diversificación

Tenemos bajo apetito de riesgo por volatilidad de nuestros resultados, y por eso actuamos en una base diversificada de clientes, productos y negocios, buscando la diversificación de los riesgos a que estamos expuestos y priorizando lo negocios de riesgo menor.

### Cultura de riesgos

Nuestra cultura de riesgos va más allá de las políticas, los procedimientos y procesos, y fortalece la responsabilidad individual y colectiva de colaboradores para que hagan lo que corresponde en el momento apropiado y de manera correcta, respetando nuestra forma ética de hacer negocios.

### Excelencia operacional:

Queremos ser un Banco ágil, con infraestructura robusta y estable, de forma de ofrecer un servicio de alta calidad.

### Evaluación de riesgos

Actuamos y asumimos riesgos en negocios que conocemos y entendemos y evitamos riesgos que no conocemos o en los cuales no tenemos ventaja competitiva, tras evaluar cuidadosamente la relación riesgo-retorno.

### Ética y respeto a la regulación:

Para Banco Itaú la ética es innegociable. Promovemos un ambiente institucional íntegro, orientamos a los colaboradores a cultivar la ética en las relaciones y los negocios, así como el respeto a las normas, velando por nuestra reputación.

### Identificación de riesgos.

La identificación de riesgos tiene como objetivo mapear los eventos de riesgo de naturaleza interna y externa que puedan afectar las estrategias y el cumplimiento de objetivos, con posibilidad de impactos negativos en el capital asignado y en los resultados.

La identificación de riesgos debe tratarse de forma metódica, para garantizar que todas las actividades relevantes estén identificadas y todos los riesgos catalogados.

### Evaluación de los Riesgos.

Las evaluaciones de eventos de riesgo se realizan desde dos perspectivas: cuantitativa y cualitativa. En el enfoque cuantitativo se utilizan modelos para evaluar las eventuales pérdidas esperadas e inesperadas. En el enfoque cualitativo los riesgos se evalúan de acuerdo a la calidad de los procesos y a los resultados de las pruebas de controles manuales y automatizados, con planes de acción dimensionados con base en la severidad y en la probabilidad de materialización del evento para indicar el grado de exposición al riesgo.

### Respuesta al Riesgo.

En los procesos de gestión de riesgos se identifican y evalúan las opciones de respuesta a los riesgos y se consideran sus efectos en la probabilidad y en el impacto del evento, con relación a la tolerancia al riesgo y a la relación costo/beneficio. La respuesta al riesgo incluye las actividades de evitar, aceptar, mitigar, compartir o transferir el riesgo, dentro de los parámetros establecidos.

### Actividades de Control.

Las actividades de control son los procedimientos utilizados para alcanzar los objetivos establecidos, que garantizan que las respuestas al riesgo se ejecuten efectivamente. Se refieren a una serie de actividades tales como verificaciones de aprobaciones y autorizaciones, reconciliaciones y revisiones de desempeño, seguridad de los recursos y segregación de funciones.

### Información y Comunicación.

Las informaciones internas y externas relacionadas con el riesgo se comunican de forma sistemática a los diferentes niveles jerárquicos del Banco. Cada participante exige niveles diferentes de información, que varían en función del alcance de su actuación.

### Monitoreo.

El proceso de monitoreo tiene el objetivo de garantizar los controles internos que están implantados y que son adecuados para las actividades de la institución. El monitoreo evalúa también los niveles de exposición al riesgo definidos.

## Estructura de Gestión de Riesgo 103-1, 103-2, 103-3

La estructura de gestión de riesgos asegura que la administración tenga procesos para definir objetivos y que estos estén en línea con la misión y la visión, consistentes con el Marco de Apetito de Riesgo de la institución.

El modelo de gestión de riesgos se integra por tres líneas de defensa:

### 1 Áreas ejecutivas

Comprenden las áreas comerciales, operativas y de soporte. Son responsables de identificar, medir y evaluar posibles riesgos y de implementar planes de acción para redireccionar procesos y controles ineficientes.

### 2 Áreas de la Dirección de Riesgos

Son responsables de desarrollar y generar metodologías, sistemas, herramientas e infraestructura para estructurar el gerenciamiento de riesgos. Dan soporte a la primera línea de defensa y se encargan de diseminar la cultura de riesgos y controles internos.

### 3 Auditoría Interna

Es un área independiente de la Dirección de Riesgos, encargada de evaluar la eficiencia y eficacia de los procesos de manera independiente a través de la aplicación de controles complementarios.

## Compromisos de Impacto Positivo 102-11, 103-1, 103-2, 413-2

Desde el Área de Riesgos, junto con Banca Empresa y Corporate Investment Banking, se asumió el compromiso de aumentar el financiamiento y los servicios para sectores de impacto positivo, lo que implica realizar una primera revisión de las industrias locales para definir los sectores de impacto positivo relevantes de Uruguay, así como formar a los equipos en temas de evaluación social, ambiental y de gobernanza.

Se trabajará en adoptar y aprobar localmente la política corporativa de riesgos y oportunidades socioambientales y, en paralelo, identificar a quienes puedan elegirnos dentro de la cartera con vistas a generar oportunidades de negocio de impacto positivo. Para llevar adelante este compromiso es prioritario generar acercamiento y alianzas con quienes desarrollan acciones clave en el sector público, a fin de poder escalar el impacto.

# Gerenciamiento de riesgos

102-15, 102-44, 103-1, 103-2, 103-3, FS2, FS4

### 1 Riesgo de mercado

El riesgo de mercado se deriva del riesgo de pérdidas resultantes de la oscilación en los valores de mercado de las posiciones mantenidas por la institución, así como su margen financiero, e incluye los riesgos de las operaciones sujetas a variación de las cotizaciones de las monedas, tasas de interés, precio de acciones y precios de mercadería. Los principales riesgos de mercado en Banco Itaú son los que se desprenden de los riesgos de tasa de interés y tipo de cambio. El proceso de gestión del riesgo de mercado consiste en administrar y controlar dichos riesgos.

### 2 Riesgo de liquidez

Se genera cuando las reservas y disponibilidades de una institución no son suficientes para honrar sus obligaciones en el momento en que ocurren, como consecuencia del descalce de plazos o de volumen entre los pagos a realizar y los posibles ingresos de fondos, sin afectar sus operaciones diarias y sin incurrir en pérdidas significativas. El proceso de gestión de este riesgo está orientado a preservar y reforzar la estabilidad, la flexibilidad y la diversidad de fondos.

### 3 Riesgo de crédito

Se deriva de las operaciones que generan derechos directos y contingentes con determinada contraparte (deudor) y surge de la posibilidad de que el deudor no cumpla con sus obligaciones crediticias en las condiciones pactadas. El Banco divide la gestión de este riesgo en dos grandes áreas, Banca Empresa y Banca Personas y Comercios, y para llevarla a cabo utiliza un amplio conjunto de herramientas que se engloban en políticas, sistemas de información y comités, entre otras.

### 4 Riesgo operacional

Es definido como la posibilidad de que ocurran pérdidas a consecuencia de fallos, deficiencias o falta de adecuación de procesos internos, personas y sistemas, y también de eventos externos. Contempla el riesgo legal asociado a la falta de adecuación o deficiencia en contratos firmados, así como a las sanciones en virtud de incumplimientos de disposiciones legales y a las indemnizaciones por daños a terceros como resultado de las actividades desarrolladas por la institución.

### 5 Riesgo reputacional

Es el impacto actual y futuro sobre las ganancias y el patrimonio que surgen de una valoración negativa de la institución por parte del público, así como el riesgo de incumplir con las expectativas razonables de las partes interesadas sobre el desempeño y el comportamiento de la organización. El Banco ha desarrollado iniciativas para la gestión del riesgo reputacional que comprenden a sus principales grupos de interés: clientes, colaboradores, proveedores, comunidad y regulador, entre otros.

### 6 Riesgo de cumplimiento

Es el riesgo presente y futuro de que las ganancias o el patrimonio de la entidad se vean afectados por violaciones a las leyes, regulaciones, estándares y prácticas de la industria o estándares éticos. El riesgo de cumplimiento también aparece en situaciones en que las leyes o regulaciones que rigen ciertos productos o actividades bancarias son ambiguas o no han sido debidamente probadas. Este riesgo expone a la institución a multas, penalidades civiles monetarias, pago de daños y cancelación de contratos. Puede llevar a reducir el valor del negocio, limitar sus oportunidades, reducir la expansión potencial y la capacidad de mejorar los contratos.

### 7 Riesgo de seguridad de la información

Se define como la posibilidad de sufrir daños o pérdidas derivados de vulnerabilidades vinculadas con la gestión de la información. Estos acontecimientos pueden derivarse de la pérdida, la modificación o la divulgación de información, o de la pérdida de acceso a la información.
Banco Itaú tiene un fuerte foco en los controles destinados a evitar la fuga de información, mediante la realización de controles preventivos de diferentes acciones o actividades.
Con el objetivo de asegurar la continuidad de las operaciones en eventuales situaciones extremas originadas por diferentes motivos, se dispone de un plan de contingencia que incluye un sitio de contingencia con un sistema de replicación activa.

### 8 Riesgo de lavado de activos y financiamiento del terrorismo

Refiere a la posibilidad de pérdida o daño que puede sufrir una entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos o la canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.
En Itaú hemos implementado un Programa de Prevención de Lavado de Dinero conformado por los siguientes elementos:

- Políticas y procedimientos
- Sistemas y procedimientos de monitoreo
- Designación de un oficial de cumplimiento
- Supervisión y gerenciamiento
- Capacitación
- Evaluaciones periódicas

### 9 Prevención de delitos financieros

Tenemos políticas y procedimientos que establecen requisitos mínimos para aceptar una nueva relación: Política Anti Lavado de Dinero; Conozca a su Cliente y Política de Prevención del Financiamiento del Terrorismo.

# Cultura de riesgo 102-44, FS4

**Asumimos riesgos conscientemente**
Evaluamos todos los tipos de riesgo que pueden impactar en nuestras operaciones, así como procuramos conocer y entender los riesgos existentes e identificar de forma proactiva y estructurada aquellos que pueden surgir a corto, mediano y largo plazo.

**Somos gestores de riesgo**
Somos responsables, individual y colectivamente, de los riesgos de los negocios que proponemos, administramos o controlamos, independientemente del cargo, el área o la función. No actuamos aisladamente; mantenemos informada a la gerencia; colaboramos con las áreas de negocio, soporte y control, sin delegar la responsabilidad en lo que refiere a la gestión de riesgos.

**La cultura de riesgo de Banco Itaú se basa en cuatro principios:**


**Discutimos riesgos**
Fomentamos que se comparta información relevante que brinde la oportunidad de hacer una gestión de riesgos más eficiente, por medio de debates internos donde se discute abiertamente sobre los riesgos y el apetito de riesgo.

**Actuamos sobre los riesgos**
Mitigamos de forma sistémica los riesgos que superen el apetito previamente definido. Para ello actuamos directamente sobre la raíz de los riesgos de forma asertiva y simple, respetando los principios éticos, las reglas internas y externas de la corporación, y priorizando siempre la perdurabilidad de la organización.

El Programa de Cultura de Riesgo tiene como objetivo profundizar el tema en todas las áreas, ya que es uno de los focos de mejora continua y un tema transversal en la organización. El Programa impulsa diversas actividades, como capacitaciones presenciales, cursos virtuales y campañas de comunicación interna, dirigidas a concientizar y sensibilizar a colaboradores sobre la importancia de su rol en la gestión de riesgos y brindarles herramientas que les permitan administrar mejor los riesgos inherentes al negocio del Banco.

En el marco del Programa Cultura de Riesgo se llevó adelante la Trilha Digital, un *e-learning* completo sobre los distintos tipos de riesgo a los que se enfrentan en su actividad diaria quienes trabajan en Itaú.

Se llevó adelante también el Programa de Integridad Corporativa sobre Ética, Seguridad de la Información, Prevención de Fraudes, y Sustentabilidad. Estos cursos transmiten y fortalecen los valores y principios que nos destacan y llenan de orgullo, para seguir actuando de manera ética, transparente y responsable.

En paralelo se realizaron capacitaciones sobre ambiente de control en temas de cultura de riesgo y prevención de fraudes, comunicaciones y una charla de nuestro director de Riesgos sobre apetito de riesgos.

## Capacitaciones

| Cultura de Riesgos | Seguridad de la información | Sustentabilidad | Prevención de lavado de dinero | Integridad y ética |
|---|---|---|---|---|
| **504** colaboradores | **403** colaboradores | **406** colaboradores | **412** colaboradores | **409** colaboradores |

# Programa de prevención de lavado

103-1, 103-2, 103-3, 205-2, FS4

Tenemos un fuerte compromiso con el cumplimiento de las leyes, la normativa y los estándares aplicables en lo referente a la prevención del lavado de dinero y el financiamiento del terrorismo, así como para impedir fondos ilegítimos o destinados a financiar actos terroristas. Para ello se ha implementado un Programa de Prevención de Lavado de Dinero (en adelante, Programa de PLD) conformado por los siguientes elementos:

1) Políticas y Procedimientos

Se han implementado políticas y procedimientos para cumplir los requerimientos normativos locales y los estándares corporativos que establecen requisitos mínimos al aceptar una nueva relación y mientras esta se mantenga. Las políticas están alineadas con las directrices corporativas.

2) Proceso de Conozca a su Cliente (CSC)

El proceso de CSC provee la información necesaria para entender y conocer las actividades de los clientes y, consecuentemente, establecer parámetros que permitan detectar comportamientos inusuales, lo que permite cumplir con las leyes y regulaciones que obligan a las instituciones financieras a reportar actividades sospechosas o inusuales.

## Organización de riesgo de lavado de activos y financiamiento del terrorismo

Los roles y las responsabilidades varían según la línea de negocios o el área de Itaú, del colaborador y de su función. Las áreas de negocios son las responsables de recolectar, verificar y mantener actualizada la información, y de detectar operaciones inusuales o sospechosas.

Compliance es la responsable de determinar la dirección estratégica del Programa PLD, definir su implementación y establecer las herramientas necesarias para su cumplimiento, no solo bajo la difusión y el entrenamiento sobre las políticas y los procedimientos aplicables, sino también asistiendo a las áreas comerciales y supervisando el cumplimiento de los estándares establecidos.

Itaú ha designado un oficial de Cumplimiento responsable del desarrollo, la implementación y la actualización del Programa de PLD.

Existe un Comité que se reúne mensualmente, donde se analizan las operaciones inusuales y se realiza un seguimiento del Programa de Prevención de Lavado de Dinero.

## Capacitaciones

Hemos implementado un programa de capacitación periódica para las personas del equipo de Compliance y para las áreas comerciales, de soporte y operaciones. Este programa de capacitación busca asegurar que las personas que trabajan en Itaú estén en conocimiento de las políticas y los procedimientos, de los cambios normativos y de sus responsabilidades en lo que se refiere a la prevención de lavado de dinero y financiamiento del terrorismo.

El equipo de Compliance participa al menos una vez al año en cursos o talleres de actualización vinculados a temas de prevención de lavado de dinero o financiamiento del terrorismo. Para las áreas comerciales o las personas responsables con relación directa con clientes se coordinan capacitaciones presenciales y cada dos años se imparte una capacitación general a través de e-learning o campañas de comunicación. Quienes ingresan deben realizar dentro de los 60 días un e-learning completo que contiene una evaluación final obligatoria.

En total 49 personas realizaron esta capacitación y aprobaron el examen final exigido.

## Evaluaciones periódicas 103-3, 205-2, FS4

Periódicamente se realizan revisiones a efectos de verificar el cumplimiento de las políticas y los procedimientos. Se verifica el cumplimiento de las directrices establecidas en la Política PLD/CSC y la Política de Embargos. Los resultados de estas pruebas de control son reportados al Comité PLD/CSC y a la Superintendencia de Controles Internos y Compliance de la entidad controlante. Asimismo, el Programa de PLD se revisa y ajusta periódicamente a efectos de reflejar los cambios normativos y corporativos en la materia, los cambios en los negocios y las tendencias nacionales e internacionales en lavado de dinero y financiamiento del terrorismo.

A partir de 2019 se incorporaron a los programas de revisiones periódicas los diagnósticos de riesgo operacional (DRO).
El Programa de PLD es objeto de revisiones anuales tanto por Auditoría Interna como por quienes auditan externamente y por el regulador.

# Contexto regulatorio

103-1, 103-2, 103-3

### Circular 2311.

En diciembre de 2018 se publicó la Circular 2.311 que introduce modificaciones en la normativa de prevención del uso de las instituciones supervisadas para el lavado de activos y financiamiento del terrorismo.
Esta circular tiene como objetivo adecuar la normativa existente en consonancia con las disposiciones contenidas en la Nueva Ley Integral de Lavado de Activos, 19.574, y su modificativa a los efectos de mejorar la implementación de las recomendaciones aprobadas por el Grupo de Acción Financiera (GAFI) y sus notas interpretativas.

### Tercerizaciones.

Se publicaron la Circular 2337 y la Comunicación 2020/016 con el nuevo régimen para autorización de tercerizaciones. Se debe solicitar autorización expresa a la SSF para la contratación de terceros en servicios inherentes al giro, cuando el servicio es prestado por terceros radicados en el extranjero o cuando el tercero está en Uruguay pero el servicio se presta en el extranjero. Asimismo, se debe contar con políticas y procedimientos que permitan monitorear los riesgos asociados a la tercerización.

### Protección de Datos Personales.

El 21 de febrero se publicó el Decreto 64/020 que reglamenta:
- el ámbito territorial de la Ley de Protección de Datos Personales 18 331 (en adelante, LPDP);
- las medidas de seguridad y el mecanismo de notificaciones en caso de vulneraciones de seguridad;
- las medidas de responsabilidad proactiva que deben asumir quienes son responsables y encargados de tratamiento;
- las funciones y los requerimientos para la designación de delegados y delegadas de protección de datos personales respecto de determinadas entidades, y las sanciones aplicables.