



Integridad y ética

¿Por qué este tema es relevante para nosotros?

Itaú Paraguay considera que la integridad y la ética son componentes fundamentales sobre los cuales debe asentarse toda organización. Por eso, en nuestra cultura corporativa, estos valores son innegociables y están alineados con nuestra visión de ser el banco líder en performance sustentable y en satisfacción de clientes.

Tenemos la convicción de que las organizaciones que deseen permanecer en el tiempo deben priorizar la ética por encima de las ganancias a cualquier precio. Trabajamos para reflejar esta línea de pensamiento en nuestro accionar cotidiano: en las relaciones con los diversos grupos de interés; en la calidad de los productos y servicios que ofrecemos; en el desempeño financiero y en nuestra responsabilidad socioambiental.

Es así que estamos comprometidos con altos estándares de conducta en los negocios y respetamos estrictamente las leyes, normas y reglamentaciones que rigen nuestras operaciones.

Código de ética

Contamos con un Código de Ética mediante el cual buscamos orientar, prevenir y subsanar dilemas éticos y conflictos de interés en nuestras actividades y relaciones internas. En él están descriptas las conductas que nuestra organización considera adecuadas, así como aquellas que califica de inaceptables.

Este instrumento, cuyos preceptos están en consonancia con el código de ética de nuestra Casa Matriz, representa nuestro compromiso formal con el respeto por los derechos humanos y los estándares laborales. [\(Contenido 2-23\)](#)

La erradicación del trabajo infantil o forzoso, el combate contra todo tipo de discriminación,

la valoración de la diversidad, la prevención de situaciones de acoso, la libre asociación sindical y la negociación colectiva, son algunos de los temas de derechos humanos que están contemplados en el Código de Ética de Itaú Paraguay. [\(Contenido 2-23\)](#) [\(ODS 5.1 5.2\)](#) [\(ODS 8.7 8.8\)](#)

El Código de Ética de Itaú Paraguay se complementa con una Política de Gestión de Ética Corporativa que establece directrices de actuación sobre temas como ventajas personales, conflictos de interés, soborno, cortesías, contribuciones, actividades externas, relaciones con clientes y proveedores, relaciones de parentesco, comunicación de sospechas o denuncias de desvíos en la conducta y sus respectivas sanciones.

Principios del Código de Ética



Principio de identidad corporativa

Somos una empresa dedicada a la satisfacción de los clientes, al crecimiento y a la eficiencia, con base en una conducta empresarial ética, en la transparencia y en el desarrollo sostenible, en todos los países donde operamos.



Principio de interdependencia

Interactuamos con diferentes públicos de interés con el fin de compartir valores y acciones que lleven al bien común. Creemos que el valor compartido es beneficioso para todas las partes involucradas, proporcionando perennidad a las relaciones.



Principio de buena fe y postura profesional

Actuamos de buena fe y asumimos la responsabilidad de nuestros actos y elecciones. Para esto, debemos dar a los demás el trato justo que esperan recibir, ser responsables de nuestras acciones y elecciones, demostrando la buena fe y honestidad de nuestros propósitos, y estableciendo un ambiente de confianza entre las partes.

Difusión del Código de Ética (Contenido 2-23)



Adhesión digital: como requisito obligatorio para incorporarse al equipo de colaboradores del banco, cada persona debe adherirse a los lineamientos de nuestro código, lo cual se formaliza a través de la confirmación de lectura y aceptación del mismo en una plataforma digital de Itaú Paraguay. Esta adhesión se renueva anualmente.



Inducción de nuevos colaboradores: en el proceso de ingreso de nuevos funcionarios y pasantes universitarios, se expone la importancia de este código y se presentan sus principales términos.



Portal interno corporativo: el documento, en su versión digital, se encuentra disponible en el portal corporativo interno para consultas en todo momento.

Canales de orientación y comunicación de desvíos éticos (Contenido 2-25) (Contenido 2-26)

Cada uno de nuestros colaboradores debe adherirse al Código de Ética y actuar sobre la base de los principios y directrices que se establecen en este documento. Ante cualquier transgresión de una norma, ley o reglamento o ante la sospecha de ésta, la situación debe ser comunicada.

Para ello existen canales establecidos -tanto a nivel local como en el holding- a través de los cuales los colaboradores pueden solicitar orientaciones, realizar denuncias o reclamos sobre incumplimientos de normativas, situaciones de maltrato, discriminación, abusos u otras irregularidades. (ODS 5.1 5.2) (ODS 8.8) (ODS 16.1)

Cada colaborador es informado sobre la disponibilidad de los canales de denuncia, tanto al momento de la inducción corporativa al ingresar a la empresa, como también posteriormente, cada cierto tiempo, a través del envío de correos electrónicos en los que se hacen recordatorios.

Con estos canales de comunicación y denuncia buscamos propiciar una conducta responsable y el respeto en nuestras relaciones, así como mantener siempre presentes los principios y valores del banco y, de esta manera, garantizar un ambiente de trabajo armónico y seguro para nuestros colaboradores.

Canales de orientación y denuncia para colaboradores

Canales en Itaú Paraguay

- Ombudsmand Regional:
silvia.calvani@mailier.com.uy
- Voz Activa (Intranet Corporativa): deriva directamente al Ombudsman Regional
- Línea telefónica con WhatsApp:
+5491131025031
- Denuncias externas en el sitio web institucional:
www.itaui.com.py/denuncias

Canales de Itaú Unibanco Holding

Cada país que compone el Holding es responsable de recibir y tratar consultas o denuncias referentes al Código de Ética a través de sus canales establecidos; sin embargo, de ser necesario los colaboradores cuentan con estructuras del holding, tales como:

Superintendencia de Ombudsman

- Contacto en IU Conecta
- Teléfono: 0800 721 4040
- Correo electrónico externo: ombudsman@ombudsman.itaui-unibanco.com.br

Comité de Auditoría

- Correo electrónico interno: casilla Comité Auditoría.
- Correo electrónico externo: comite.auditoria@itaui-unibanco.com.br
- Correo físico: Comité de Auditoría Itaú Unibanco Holding S.A. Praça Alfredo Egydio de Souza Aranha, 100 Torre Olavo Setubal, 9º Andar, São Paulo - SP - CEP: 04344-902

Cómo actuamos ante denuncias de desviaciones éticas

La instancia de Ombudsman Regional es la encargada de gestionar los casos de desvíos éticos de manera objetiva e imparcial. El Comité de Ética es un órgano colegiado que se reúne semestralmente y, en caso de necesidad, los casos individuales son tratados de forma extraordinaria.

En 2025 se han tratado cinco denuncias realizadas por colaboradores que llegaron hasta estos canales, de las cuales todas han sido resueltas y concluidas dentro del año con planes de acción específicos. Del total de denuncias, cuatro fueron por asedio moral y una por desvíos éticos, pero no fue procedente. (GRI 406-1)

También se recibió una denuncia de discriminación por parte de un cliente, la cual derivó en la cancelación del relacionamiento con ese cliente.

Ética en la cadena de suministro

La Política de Ética de Banco Itaú también contempla a los prestadores de servicios y proveedores de insumos y bienes. Es así como contamos con una herramienta exclusiva para este público: nuestro Código de Ética de Proveedores. En él se describen las directrices de gestión que el banco aplica en sus operaciones y que se espera sean adoptadas por las empresas que se conviertan en proveedores de Itaú.

Este código hace referencia a temas como seguridad de la información, el relacionamiento de colaboradores del banco con empleados o dueños de empresas proveedoras (nexo familiar o consanguinidad), el manejo de conflictos de interés y el cumplimiento tributario.

Todas las empresas proveedoras efectivas o empresas postulantes están obligadas a adherirse al Código de Ética. Esto las compromete a cumplir las políticas establecidas por el banco y las normas legales aplicables a derechos de propiedad intelectual, derechos del consumidor, comportamiento ambiental y de responsabilidad social, trabajo forzado e infantil, sigilo bancario, y prácticas anticorrupción, entre otros aspectos. (ODS 8.7) (ODS 16.2)

Canales de denuncia para Proveedores



Correo electrónico:
hablemos@itau.com.py



Casilla de correo
N° 391



Área de Compras por
su relacionamiento constante con
proveedores



Sitio web institucional:
www.itau.com.py/denuncias

Prácticas anticorrupción

(GRI 205-2) (ODS 16.5)

Tanto en los códigos de ética por los cuales se rige el relacionamiento con el público interno y con los proveedores del banco, como en nuestras políticas corporativas, se contemplan medidas para el combate a la corrupción.

Política Corporativa de Combate a la Corrupción

Refuerza el compromiso del holding de cooperar proactivamente con las iniciativas de cada país -y con las internacionales- para prevenir y combatir la corrupción en todas sus formas. Esta política también establece orientaciones para la implementación eficaz y la mejora continua del programa corporativo destinado al desarrollo y mantenimiento de prácticas de prevención, monitoreo y combate. Así también, dispone la implementación y el gerenciamiento de canales de denuncia y la puesta en práctica de acciones de concienciación y entrenamiento sobre el tema, dirigidas a administradores y colaboradores.

Política de Gestión de Ética Corporativa

Proporciona orientaciones sobre el uso de información, registros y know-how de la empresa, participación de los colaboradores en otras empresas, actividades externas de los colaboradores, relaciones de parentesco y proximidad, relaciones con clientes y proveedores, comportamiento ante regalos de cortesía, entre otros temas que guardan relación con potenciales situaciones de corrupción.

La instancia encargada de garantizar la internalización de estas políticas vinculadas a prácticas anticorrupción es el área de Compliance, que también se ocupa de monitorear el

cumplimiento de sus delineamientos. La lectura y adherencia a las políticas relacionadas con el Código de Ética y la lucha contra la corrupción es de carácter obligatorio para todos los colaboradores.

Conflictos de interés

(Contenido 2-15) (ODS 16.5)

Los conflictos de interés pueden comprometer la imparcialidad de nuestras acciones y poner en riesgo la reputación del holding, así como la de los colaboradores. Por esto, hemos establecido políticas que determinan cómo se debe manejar este tipo de casos.

Actividades externas y relaciones de parentesco: contamos con políticas específicas que establecen los lineamientos para gestionar conflictos de interés en el contexto laboral. Una de ellas define cómo debe ser el proceso de comunicación y de evaluación de riesgos o conflictos vinculados a la realización de actividades fuera del banco por parte del colaborador, ya sea como propietario en organizaciones o con alguna participación en las mismas (con o sin remuneración). Otra política determina criterios para evaluar posibles casos de conflicto de intereses en relaciones de parentesco o proximidad entre colaboradores dentro de la organización. Anualmente, todos los colaboradores deben completar una declaración sobre actividades externas que pudieran estar desempeñando y sobre su parentesco con otros colaboradores.

Informaciones y know-how: es importante para nosotros hacer un uso correcto de la información, el conocimiento y la propiedad intelectual respetando las normas establecidas en favor de nuestro público. Entendemos que la manera en que utilizamos las informaciones y el know-how impacta en los negocios y en la reputación de las personas, por eso consideramos fundamental mantener en secreto y tratar correctamente las informaciones que nuestra organización maneja en el día a día. Así también, implementamos medidas de seguridad y control restringiendo y mitigando posibles desviaciones de estas conductas de manera proactiva y garantizando la confidencialidad de los datos.

Cortesías y regalos: nuestra Política de Integridad, Ética y Anticorrupción establece reglas para los casos de relaciones externas o prácticas comerciales que puedan considerarse intentos o formas de influir en las personas que toman decisiones, comprometiendo la transparencia de los negocios. Es así que en Itaú está prohibido ofrecer y aceptar regalos o atenciones que puedan llevar a establecer -directa o indirectamente- vínculos o compromisos que puedan ser confundidos con mecanismos para burlar reglas, o interpretados como medios ilícitos para facilitar negocios.

Prevención de lavado de dinero y financiamiento del terrorismo

(ODS 16.4) (ODS 16.10 a)

Como institución financiera, mantenemos nuestro compromiso con la prevención y el combate de actividades ilícitas, en línea con la legislación paraguaya vigente y con las mejores prácticas internacionales. Nuestra gestión busca asegurar que los productos, servicios y recursos operativos del banco no sean utilizados con fines de lavado de dinero (LD) o financiamiento del terrorismo (FT).

Este enfoque se encuentra estructurado en nuestra Política de Prevención y Combate a Actos Ilícitos, que establece los lineamientos para identificar, evaluar y mitigar riesgos, garantizando una actuación responsable y transparente en todas nuestras operaciones.

Nuestro Programa Corporativo de Prevención de Actos Ilícitos -en el cual se basa nuestro proceso de Prevención y Combate de Lavado de Dinero y Financiamiento del Terrorismo- se encarga de asegurar el cumplimiento de las directrices de la mencionada política, a través de las siguientes iniciativas:



Capacitar para prevenir

Para garantizar la efectividad de todos los procesos anteriormente mencionados, en Itaú consideramos que la capacitación de nuestros colaboradores constituye un componente esencial para fortalecer la cultura interna de prevención. En el periodo de este reporte, más de 1.550 participaron de entrenamientos, en modalidad híbrida, sobre prevención del lavado de dinero y financiamiento del terrorismo, además de recibir entrenamientos específicos según sus funciones, nivel de riesgo y responsabilidades.

Se realizaron visitas y sesiones presenciales en sucursales, incluyendo aquellas de frontera (Ciudad del Este y Encarnación) para capacitaciones sobre la misma temática, de manera a permear constantemente nuestra cultura de prevención, reforzar la comprensión de los riesgos y promover buenas prácticas.

En el año se realizaron, además, actividades orientadas a la prevención de actos ilícitos desde el programa de cultura, como el lanzamiento de una serie de comunicados enfocados a conocer los riesgos del lavado de dinero y financiamiento del terrorismo en los negocios. También se desarrollaron capacitaciones dirigidas a colaboradores enfocadas en temas relacionados con sanciones y embargos internacionales, con la participación de disertantes externos especializados en la materia, como parte de la mejora continua relacionada con el financiamiento del terrorismo. Asimismo, el área de Prevención de Lavado de Dinero (PLD) desarrolló espacios de formación ampliada para distintos sectores del banco, de modo a interiorizarlos sobre los cambios normativos y matriciales que se han producido en este campo.

Además de las acciones realizadas en Banco Itaú, se buscó fortalecer la cultura corporativa de prevención de riesgos a través de capacitaciones compartidas con los equipos de la Fundación Itaú, la Casa de Bolsa Itaú Invest, la administradora de fondos Itaú Asset Management, y la aseguradora Itaú Seguros.

Fortalecimiento continuo de los procesos

En lo que respecta a los procesos internos, durante el año 2025 trabajamos en la evolución de los flujos de control y fortalecimiento de modelos relacionados, afianzando de manera constante los focos de “Conozca a su Cliente” y “Monitoreo de Transacciones”. Se revisaron y optimizaron modelos de riesgo para mantener su alineación con los estándares regulatorios locales y regionales, reforzando la capacidad del banco para identificar comportamientos atípicos y realizar una gestión eficiente.

Adicionalmente, se consolidaron procesos vinculados a embargos y sanciones, siguiendo lineamientos del conglomerado y de referentes internacionales. También se automatizaron procesos y reportes clave, facilitando la disponibilidad ágil de información para equipos internos y contribuyendo a una respuesta más eficiente hacia clientes y autoridades.

Estas acciones reafirman el compromiso del banco con la mejora continua y con el cumplimiento de las regulaciones vigentes, fortaleciendo la seguridad y contribuyendo a la sostenibilidad del negocio y a la confianza de nuestros clientes.

Seguridad de la información y privacidad del cliente

Desde el área de Seguridad de la Información invertimos en infraestructura, recursos tecnológicos y capacitación para colaboradores y proveedores, con la intención de proteger la información que gestionamos y garantizar la integridad, privacidad y la confidencialidad de los datos que nos confían nuestros clientes en las operaciones que realizamos.



Políticas de seguridad y privacidad

Las directrices para el tratamiento de la información en la organización se encuentran establecidas en nuestra Política Corporativa de Seguridad de la Información, cuya lectura y aceptación es obligatoria para todos los colaboradores. Así también, están contempladas en la Política de Funciones y Responsabilidades de Seguridad de la Información/Cyber Security y Propiedad Intelectual, donde se demarcan los lineamientos a seguir para garantizar que los principios de propiedad intelectual y seguridad de la información sean aplicados, y de este modo, proteger al banco, a los clientes, a los proveedores y al público en general.



Entrenamientos

Al momento de la inducción corporativa de nuevos colaboradores del banco, el área de Seguridad de la Información les brinda capacitación sobre principios de seguridad, clasificación de la información, manejo y comportamiento en las redes sociales, lineamientos de seguridad sobre accesos a sistemas y utilización del correo electrónico, entre otros temas.

Durante el año 2025, en el marco del programa de concientización anual realizado por el área, se ha desarrollado un entrenamiento en modalidad e-learning dirigido a todos los colaboradores del banco con el fin de reforzar conceptos sobre la importancia del manejo adecuado de la información.

Asimismo, se realizó una simulación de phishing para promover el fortalecimiento de la cultura de seguridad entre los colaboradores, evaluando su nivel de concienciación y reforzando las buenas prácticas frente a correos potencialmente maliciosos.



Consejos de seguridad en redes sociales

En 2025 continuamos con las campañas de concientización con consejos de seguridad para nuestros clientes, lanzando la campaña “Si algo te suena raro, no abras” con la publicación de materiales audiovisuales sobre casos de phishing reales en nuestros perfiles de redes sociales. Además, durante el año se compartieron orientaciones sobre temas diversos de seguridad, a través de videos realizados por influencers de alcance local.



Ciberseguridad y seguridad de la información

Somos conscientes de que gestionamos información sensible de nuestros clientes en el contexto nacional e internacional, por eso la seguridad y la ciberseguridad de esos datos constituye una de nuestras prioridades y al mismo tiempo un compromiso que nos impulsa a reforzar permanentemente nuestros procesos en esta materia.

Para ofrecer la confianza y seguridad que los clientes merecen en la gestión de sus datos, contamos con un área especializada en ciberseguridad que se encarga de implementar planes de continuidad y contingencia, tanto a nivel operacional como del lugar de trabajo. Además, nos guiamos por procedimientos de disaster recovery acordes a nuestros procesos más críticos, que son probados de manera frecuente, permitiendo así corroborar que la institución mantenga sus actividades en un nivel aceptable.

Nuestro Modelo de Gestión en Ciberseguridad se enfoca en los siguientes aspectos:



Gestión de Incidentes:

Monitoreo y tratamiento de los tipos de ataques e incidentes de seguridad con el apoyo del equipo de respuestas a incidentes.



Seguridad de Sistemas:

Define los principios, directrices y la gestión de seguridad de la información adoptados por la institución.



Arquitectura de Referencia:

Aplicación de baselines de mejores prácticas de seguridad y fortalecimiento de equipos tecnológicos.



Gestión de Crisis y Continuidad del Negocio:

Establecimiento de directrices que aseguren acciones inmediatas frente a diversas crisis que pongan en peligro la continuidad de los procesos más críticos del negocio.



Protección de Datos:

Protección, clasificación y privacidad de datos e información del banco y clientes.



Gestión de Vulnerabilidades:

Gestión de vulnerabilidades con escaneos internos y externos con el fin de detectar brechas de seguridad para remediarlas de forma proactiva.



Cumplimiento de Normativas:

Aplicación, definición y cumplimiento de los principios y directrices de Seguridad de la Información y Ciberseguridad.



Red Team:

Equipo especializado en realizar pruebas de intrusión con el fin de detectar vulnerabilidades de forma proactiva a fin de remediarlas a tiempo.



Gestión de Riesgos:

Gestión y administración de los asuntos de ciberseguridad, mapas de riesgo y medición del ambiente de control de ciberseguridad.



Concientización y Cultura Ciber:

Generación y aplicación de acciones de concientización para elevar el nivel de cultura de riesgos en materia de ciberseguridad.

Gestión de Prevención de Fraudes

Desde el área de Prevención de fraudes del banco se implementan y aplican procedimientos de prevención y detección oportunas de situaciones de fraudes que puedan afectar a nuestros clientes. Las principales medidas y herramientas son:

- Medidas para hacer frente a casos de uso indebido de tarjetas de crédito y débito (clonación, falsificación), de operaciones con cheques adulterados y billetes falsos, y otras operaciones fraudulentas relacionadas a los productos préstamo y cuenta.
- Método de autenticación 3D Secure para nuestras tarjetas de crédito VISA y MASTERCARD y tarjetas de débito MASTERCARD. Con este método hacemos que las compras en plataformas de e-commerce sean más seguras.
- Sistema de monitoreo de transacciones, que genera alertas conforme a determinadas reglas y parámetros, como los hábitos de consumo del cliente, rubros de las compras, y países de riesgo, entre otros controles. Además, se utilizan y alimentan listas restrictivas de control como las de números de teléfonos celulares utilizados para llamadas extorsivas o fraudulentas.
- Herramienta de bloqueo para situaciones de exposición o compromiso de datos en los diversos productos que ofrece el banco.

Anualmente, se ofrecen entrenamientos a los colaboradores del banco, en los que se exponen los distintos tipos de fraude tradicionales como falsificación, clonación, robo de identidad, etc. También los relacionadas con las nuevas tecnologías o con el mundo digital (ingeniería social o phishing).

En el año, más de 450 personas fueron capacitadas (incluyendo colaboradores y operadores de Servicio de Atención al Cliente) a través de distintas plataformas digitales. Así también, hemos brindado capacitaciones a empresas clientes contratantes del servicio de pago de salarios del banco.