



< Integridad y ética

“ ¿Por qué este tema es material?

Tenemos la convicción de que organizaciones que desean permanecer en el tiempo, no admiten ganancias a cualquier precio y que su éxito depende de su capacidad para liderar con integridad y ética.

En nuestra cultura corporativa, estos valores son innegociables y fundamentales para alcanzar nuestra visión de ser el banco líder en performance sustentable y en satisfacción de clientes.

Consideramos que la integridad y ética es la base sobre la cual se sustenta toda la organización y las relaciones con los diversos grupos de interés; son componentes esenciales para nuestras actuaciones, perennidad y sustentabilidad del negocio.

La sociedad demanda en las grandes empresas, transparencia y compromiso con los objetivos y compromisos asumidos. Conscientes de esto y de la responsabilidad social corporativa que tenemos para con la sociedad, conducimos nuestros negocios, procesos y relacionamientos, con el fin de establecer vínculos duraderos con nuestros grupos de interés a la vez de generar valor para todos.

Estamos comprometidos con altos padrones de conducta en los negocios y nos adherimos a las leyes, normas y reglamentaciones que rigen nuestras operaciones. Por medio de la confianza adquirida y de la calidad de nuestros productos y servicios, garantizamos la perennidad de nuestros negocios y la satisfacción de los clientes.
(GRI 102-16)

”



Código de Ética

El Código de Ética de Itaú Paraguay -alineado al del Holding- tiene el objetivo de orientar, prevenir y subsanar dilemas éticos y conflictos de interés en nuestras actividades y relaciones internas y; ofrecer directrices sobre cuáles son las posturas que se consideran adecuadas y las que son inaceptables al momento de actuar.

El Código, representa nuestro compromiso formal con asuntos como la erradicación del trabajo infantil o forzoso, el combate contra todo tipo de discriminación, la valorización de la diversidad social, la prevención de situaciones de acoso, el respeto a los derechos de libre asociación sindical y a la negociación colectiva, entre otros temas. **(ODS 5.1) (ODS 8.7 8.8)**

Principios del Código de Ética

Principio de Identidad



Somos una empresa dedicada al crecimiento, la eficiencia y la satisfacción de los clientes con base en una conducta empresarial ética y en el desarrollo sustentable.

Principio de Interdependencia



Interactuamos con nuestro público y con la sociedad con el fin de compartir valores y acciones que lleven al bien común.

Principio de Buena Fe



Actuamos de buena fe y asumimos la responsabilidad de nuestros actos y elecciones.

Principio de Excelencia



Mejoramos continuamente la calidad de nuestro trabajo y cultivamos ambientes motivadores y que estimulen la cooperación.

La Política de Gestión de Ética Corporativa (actualizada en julio de 2019), a su vez, establece directrices complementarias al Código de Ética con temas como el combate a la corrupción y coimas, ventajas personales, conflictos de interés, soborno, cortesías, contribuciones, actividades externas, relaciones con clientes y proveedores, relaciones de parentesco, y comunicación de sospechas o denuncias de desvíos en la conducta y sus respectivas sanciones.

Difusión del Código de Ética

Estas son las iniciativas que llevamos a cabo para difundir los lineamientos del Código:

- **Adhesión digital:** como requisito obligatorio para poder iniciar las actividades, cada colaborador debe adherirse a los lineamientos del Código mediante la confirmación de lectura en una plataforma digital (esta adhesión se renueva anualmente).
- **Inducción de nuevos colaboradores:** en el proceso de ingreso de nuevos colaboradores y pasantes universitarios, se hace entrega de una copia impresa del Código.
- **Portal interno corporativo:** el documento en

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

- **E-learning “Cultura de Riesgos y Ética”:** de forma anual, se lleva a cabo este entrenamiento online que incluye contenido sobre el Código de Ética y casos prácticos para evaluación. En 2019 la puntuación media en las pruebas de adherencia fue de 99%.

Canales de orientación y comunicación de desvíos éticos

El compromiso que todos los colaboradores asumen con los principios y directrices incluidos en nuestro Código de Ética, es la base de la solidez y la perdurabilidad de la empresa. Esto implica que si se encuentran ante una situación o ante la sospecha de la transgresión de una norma, ley o reglamento; la situación debe ser comunicada.

Para este efecto, se han establecido canales locales -y al nivel del Holding- para casos en que los colaboradores necesiten orientaciones sobre las directrices del Código de Ética y/o realizar denuncias o reclamos sobre incumplimientos en





normativas, maltratos, discriminación, abusos y otras irregularidades en el comportamiento. (GRI 102-17) (ODS 5.1) (ODS 8.8) (ODS 16.1).

Estos canales de comunicación y denuncia tienen la intención de asegurar la responsabilidad y el respeto en nuestras relaciones, de mantener siempre presentes a los principios y valores del Banco y como consecuencia garantizar un ambiente de trabajo armónico y seguro para nuestros colaboradores.

Canales en Itaú Paraguay

- Correos electrónicos internos genéricos:
 - Comité de Ética: comitedeetica@itau.com.py
 - Compliance: complianceetica@itau.com.py
 - Personas: personasetica@itau.com.py
- Correo electrónico externo hablemos@terra.com
- Interno con línea telefónica grabada 3777.
- Correos electrónicos internos y líneas telefónicas del Superintendente de Personas y del Gerente de Controles Internos y Riesgo Operacional.
- Casilla de correo N° 391 de la Dirección Nacional de Correos del Paraguay.
- Voz Activa: es un espacio ubicado en el portal corporativo interno del Banco en el cuál pueden hacerse denuncias, seleccionar motivos y el área receptora de la denuncia. Además, da la posibilidad al denunciante de identificarse o mantenerse en el anonimato.

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, siempre que sea necesario los colaboradores cuentan con estructuras del Holding, tales como:

- Comité de Ética y Ombudsman: ombudsman@ombudsman.itau-unibanco.com.br o ombudsman.itub@terra.com.br
- Comité de Inspectoría: inspetoria@itau-unibanco.com.br
- Comité de Auditoría: comitê.auditoria@itau-unibanco.com.br

Casos de desvíos éticos

El Comité de Ética del Banco es la instancia encargada de gestionar los casos de desvíos éticos, para lo cual se reúne semestralmente y en caso de necesidad; los casos individuales son tratados de forma extraordinaria.

Respecto a las situaciones denunciadas, la atención de los casos se realiza respetando ciertas condiciones: i) la investigación con imparcialidad, independencia y discreción; ii) se asegura el anonimato del denunciante (si así lo prefiere); iii) no se consideran denuncias o acusaciones sin fundamentaciones consistentes y, iv) las denuncias efectuadas de mala fe están sujetas a sanciones. Todos los casos cuentan con seguimientos trimestrales formalizados.

En 2019, se han tratado y finalizado trece denuncias realizadas por colaboradores que llegaron hasta estos canales. Del total de las denuncias, en ocho casos se mencionó situaciones de abuso de poder o asedio moral, tuvimos dos situaciones de asedio sexual, dos situaciones en las que se mencionaron situaciones de conflicto de interés y, un caso sobre discriminación. No hemos recibido en el presente año





denuncias respecto a incumplimientos normativos, ni situaciones de maltrato, así como tampoco hemos recibido denuncias por violación de derechos humanos o corrupción. (GRI 205-3) (GRI 406-1) (ODS 16.3 16.5) (ODS 5.2)

La comunicación de la disponibilidad de los canales de denuncia es realizada a través del Código de Ética entregado a colaboradores al inicio de su relación con el Banco y en el año se realizan comunicaciones internas para recordarlos. Además, los colaboradores reciben capacitaciones sobre los mecanismos de asesoramiento y denuncia a través de las charlas anuales de Riesgo Operacional y Ética, desarrolladas por la Gerencia de Controles Internos y Riesgo Operacional.

Ética en la cadena de suministro

Para el vínculo con los prestadores de servicios o provisión de insumos y bienes, contamos con un Código de Ética de Proveedores en el cual están descriptas las principales directrices de gestión que el Banco aplica en sus operaciones y que se espera sean adoptadas por las empresas, cuando se convierten en proveedores de Itaú.

El documento incorpora contenidos relacionados a ética, seguridad de la información, relacionamiento de colaboradores del Banco (nexo familiar o consanguinidad), con empleados o dueños de empresas proveedoras, manejo de conflictos de interés y cumplimiento tributario.

Todas las empresas proveedoras efectivas o empresas postulantes, están obligadas a adherirse al cumplimiento del Código. Esto las compromete a observar las políticas presentadas 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, prácticas anticorrupción, entre otros. (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.

En 2019, no se han recibido denuncias de proveedores a través de estos canales.

Prácticas anticorrupción (GRI 205-2) (ODS 16.5)

En Itaú, los temas vinculados a la lucha contra la corrupción están delimitados en varios documentos institucionales, como los Códigos de Ética (con Colaboradores y Proveedores), y las Políticas Corporativas, en las que se hace explícito cada aspecto vinculado y los comportamientos y prácticas que se desalientan y sancionan.

• **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- sobre la prevención y combate a la corrupción en todas sus formas. Así también, la misma establece orientaciones para la concepción, efectividad y mejora continua del programa corporativo destinado al desarrollo y mantenimiento de prácticas de prevención, monitoreo y combate, y determina el establecimiento y gerenciamiento de canales de denuncia y la realización de acciones de concienciación y entrenamiento de administradores y colaboradores sobre el tema.

• **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 y recibimiento de cortesías, entre otros temas que guardan relación con potenciales situaciones de corrupción. La Dirección de Riesgos, Crédito y Compliance, es la encargada de garantizar la





internalización de estas políticas vinculadas a prácticas anticorrupción y de monitorear el cumplimiento de sus delineamientos. La lectura y adherencia a políticas relacionadas al Código de Ética y a lucha contra la corrupción son de carácter obligatorio para todos los colaboradores. El e-learning “Cultura de Riesgos y Ética”, realizado anualmente, también cuenta con contenido sobre prácticas anticorrupción.

En 2019, dentro del plan de formación dirigido a colaboradores sobre prácticas anticorrupción, fueron desarrollados los siguientes entrenamientos:

Prevención de la corrupción: tenía el objetivo de establecer claramente qué es la corrupción, cómo actuar ante la sospecha o identificación de una situación de corrupción; exponer las principales orientaciones para prevenir la corrupción dentro del Programa de Integridad y Ética y; conseguir una mayor concientización sobre los riesgos de corrupción. La formación fue en formatos específicos para miembros del Comité Ejecutivo y para representantes de áreas críticas del Banco.

• **Volcker Rule:** esta regla, persigue el objetivo de limitar los riesgos excesivos tomados por las instituciones de depósitos y sus filiales. Cualquier banco extranjero con sucursales, agencias y filiales, así como las empresas en las que este banco tenga control, son entidades sujetas a las restricciones impuestas por la Volcker Rule. Desde el conglomerado, se realizaron análisis de negocio y se puso en práctica un programa para asegurar y supervisar que las actividades de la institución cumpla con las especificaciones establecidas por la Volcker Rule.

Conflictos de Interés (GRI 102-25)(ODS 16.5)

Las Políticas de Actividades Externas y de Relación de Parentesco establecen los lineamientos para gestionar conflictos de interés en el contexto laboral. La primera define el proceso de comunicación y de evaluación de riesgos o conflictos vinculados al ejercicio de actividades fuera del Banco por parte del colaborador, en organizaciones ya sea como propietario o con participaciones (con o sin remuneración). La segunda, establece criterios para evaluar casos de relaciones de parentesco entre

colaboradores dentro de la organización. Todos los colaboradores, anualmente, tienen como requisito completar declaraciones sobre actividades externas que puedan estar desempeñando y su parentesco con otros colaboradores.

Prevención de lavado de dinero y financiamiento del terrorismo (ODS 16.10 a)

Como institución financiera -en concordancia con la legislación vigente, reglamentaciones locales y de acuerdo con las mejores prácticas de mercado internacional- cumplimos un papel fundamental en la tarea de prevenir y combatir hechos ilícitos tales como el lavado de dinero (LD) o el financiamiento del terrorismo (FT).

Nuestros esfuerzos están orientados a identificar y evitar situaciones en las que los servicios, productos y recursos operacionales del Banco sean utilizados para realizar movimientos y/u ocultar o disimular la verdadera naturaleza de fondos provenientes de actividades ilegales.

Nuestra Política de Prevención y Combate

a Actos Ilícitos está alineada a un Programa Corporativo de Prevención de Actos Ilícitos, dentro del cual se encuentra el Proceso de Prevención y Combate de Lavado de Dinero y Financiamiento del Terrorismo. Las principales herramientas vinculadas al Programa son:

- Conozca a su colaborador.
- Conozca a su cliente.
- Conozca a su proveedor.
- Clasificación de clientes por su nivel de riesgo LD/FT
- Monitoreo de transacciones.
- Informe de transacciones sospechosas a autoridades y entes reguladores.

Para garantizar la efectividad de estos procesos, es esencial asegurar el entendimiento de los colaboradores sobre estos asuntos y sobre la responsabilidad que representan para ellos y para la institución.

En 2019, 1.217 colaboradores participaron de entrenamientos sobre prevención del lavado de dinero y financiamiento del terrorismo. En el año, además, se llevaron a cabo actividades adicionales al programa de cultura, incluyendo encuentros de tipo





focus group entre representantes de las áreas comerciales y el Chief Risk Officer enfocadas a conocer riesgos de prevención de lavado de dinero. Así también, el área de Prevención de Lavado de Dinero desarrolló espacios de formación para áreas del Banco en contacto con clientes con el objetivo de interiorizarlas con los cambios normativos. Adicionalmente, se realizó una capacitación exclusiva con enfoque jurídico-penal en temas relacionados a la prevención del lavado de dinero y financiamiento del terrorismo dirigida a integrantes del Comité Ejecutivo y a gerentes de todas las áreas de la empresa.

Fortalecimiento en procesos

Sobre nuestros procedimientos internos, en el año se trabajó en el fortalecimiento del proceso de renovación catastral de datos del cliente lo que permitió posteriormente realizar mejores evaluaciones que derivaron en una mejor atención. En este sentido la actualización de datos en forma digital, permitió actualizar informaciones de más de 200.000 clientes.

También, se rediseñaron los controles relacionados al monitoreo transaccional y comportamental del cliente, en pos de lograr

una mayor eficiencia en las gestiones con el mismo.

Estos procesos fortalecen el compromiso del Banco con las regulaciones locales e internacionales existentes y constituyen el soporte para lograr la sustentabilidad de sus negocios y una mayor seguridad para sus clientes.

Seguridad de la información y privacidad del cliente

Desde el área de Seguridad de la Información del Banco, se invierte en infraestructura, recursos tecnológicos y entrenamientos tanto para colaboradores como para proveedores con la intención de proteger las informaciones que gestionamos y de asegurar la privacidad de los clientes en las operaciones que realizamos.

Políticas de seguridad y privacidad

La Política Corporativa de Seguridad de la Información, cuya lectura es obligatoria para todos los colaboradores, y la Política de Funciones y Responsabilidades de Seguridad de la Información, Cyber Security y Propiedad Intelectual, establecen las directrices para el tratamiento de la

información en la empresa. Su propósito es garantizar que los lineamientos y principios de propiedad intelectual y seguridad de la información sean aplicados para proteger al Banco, a los clientes y al público en general.

Entrenamientos

El área de Seguridad de la Información participa de la Inducción Corporativa de nuevos colaboradores, con un entrenamiento 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.

De la misma forma, en el año se desarrolló un entrenamiento en línea, dirigido a todos los colaboradores del Banco con el fin de reforzar los conceptos y formar a los colaboradores sobre la importancia del manejo de la información. Además nos enfocamos en un tema muy recurrente en estos días como lo es la ciberseguridad en una empresa, concienciando a los empleados sobre el uso responsable de los equipos de trabajo con acceso a datos de la organización.

Certificación Norma ISO/IEC 27001

Contamos con esta norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

En 2019, trabajamos en el mantenimiento de esta ISO, con alcance sobre ciertos procesos de la Banca Digital, aplicando las recomendaciones que nos fueron realizadas.





Consejos de seguridad en redes sociales

Aprovechamos nuestros perfiles en redes sociales, en diferentes momentos del año, para reforzar medidas de seguridad y protección de datos en Internet, en nuestras plataformas digitales y específicamente para prevenir situaciones de fraudes y robos a través de llamadas telefónicas y cajeros automáticos.

En 2019 lanzamos campañas de concientización con consejos de seguridad para utilización de tarjetas de crédito, transacciones en Internet y evitar ser víctimas de fraudes en épocas determinadas de gran movimiento comercial.

Seguridad para clientes

En el sitio web www.itaú.com.py, se encuentra disponible el espacio “Más Seguridad” el cual proporciona recomendaciones de seguridad en la utilización de los servicios y productos que ofrece el Banco; contiene consejos sobre transacciones en el sitio 24 horas en Internet, el uso de cajeros automáticos y terminales de auto atención, la utilización de cheques, tarjetas de crédito, entre otros.

Complementariamente, se incluyen

informaciones sobre medidas de seguridad para el manejo de la información en redes sociales, correos electrónicos y mensajería instantánea, recomendaciones útiles para el mantenimiento de la seguridad física y la salud en el ambiente de los hogares, la calle, en viajes e incluso situaciones de asaltos y secuestros. El sitio también incorpora una sección con medidas de seguridad en el cuidado de los niños en situaciones, como el uso de internet, el tránsito en las calles, el hogar y la escuela.

Gestión de Prevención de Fraudes

Desde el área de Prevención de Fraudes del Banco, se implementan y aplican procedimientos de prevención y detección oportunos 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 al producto préstamo y cuentas.

- Herramientas de seguridad y control como la tecnología chip y contactless para tarjetas, los códigos token para validación de transferencias de ciertos importes, el servicio de alerta de transacciones Click Banking y toda la plataforma digital con acceso constante a la información sobre sus productos.

- 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 tanto presenciales como virtuales a los colaboradores del Banco, en los que se exponen las tipologías de fraude tradicionales (falsificación, clonación, robo de identidad, etc.) y las relacionadas a las nuevas tecnologías o al mundo digital

(ingeniería social o phishing). En el e-learning “Prevención de Fraudes” dirigido a los colaboradores, se muestran los tipos de fraude que circulan en la actualidad y se brindan recomendaciones para estar más protegidos ante estos ataques. En el período del 2019, fueron capacitadas en total 1.392 personas (1.077 colaboradores de Itaú y 242 operadores del Servicio de Atención al Cliente).

