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, y 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 socio-ambiental.

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. (GRI 102-15) (GRI 102-16)

Código de ética

Como eje central de nuestro desempeño basado en valores, 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 del holding, representa nuestro compromiso formal con el respeto de los derechos humanos y los estándares laborales.

La erradicación del trabajo infantil o forzoso, el combate contra todo tipo de discriminación, la valoración de la diversidad social, 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. (ODS 5.1) (ODS 5.2) (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.

El Código de Ética de Itaú Paraguay se complementa con una Política de Gestión de Ética Corporativa que, buscando combatir actos de corrupción, establece directrices de actuación sobre temas como coimas, 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.

Difusión del Código de Ética

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 colaboradores 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

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 la misma, 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. (GRI 102-17) (ODS 5.1) (ODS 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 hace un recordatorio. (GRI 102-17)

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 comunicación de desvíos éticos

Canales en Itaú Paraguay

• Correos electrónicos internos genéricos: - Comité de Ética: comitedeetica@itau.com.py

• Correo electrónico externo hablemos@itau.com.py

• Interno con línea telefónica grabada 3777.

• 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 cual pueden hacerse denuncias, seleccionar motivos y el área receptora de la denuncia. El denunciante puede identificarse o mantenerse en el anonimato, si así lo prefiriese.

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:

• Comité de Ética y Ombudsman: ombudsman@ombudsman.itauunibanco.com.br o ombudsman.itub@terra.com.br

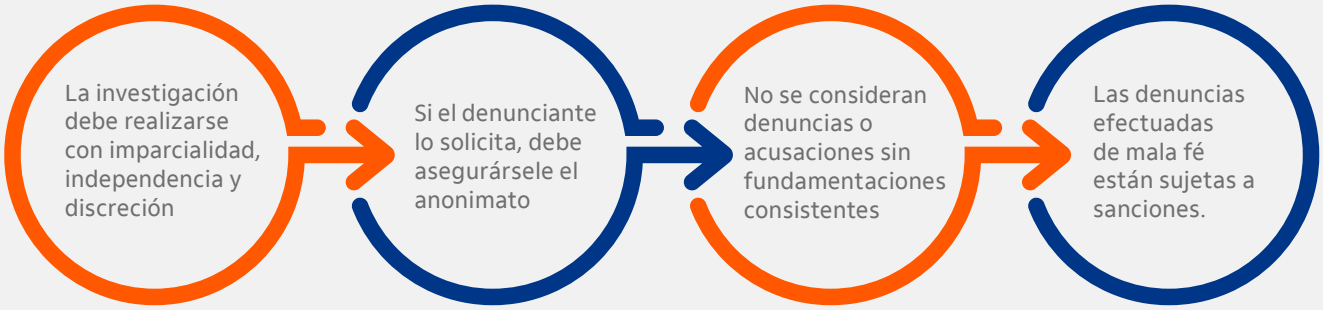
• Comité de Inspectoría: inspetoria@itauunibanco.com.br

• Comité de Auditoría: comitê.auditoria@itau-unibanco.com.br

Cómo actuamos ante denuncias de desviaciones éticas

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.

Para la atención de los casos, los cuales cuentan con un seguimiento trimestral formalizado, se respetan las siguientes condiciones:



En 2021, se han recibido y tratado 13 denuncias realizadas por colaboradores a través de los canales correspondientes. De ellas, 11 han sido resueltas y concluidas dentro del año con planes de acción específicos y 2 continuaban en análisis y seguimiento al cierre del 2021.

Del total de las denuncias, 9 fueron sobre situaciones de asedio moral, 2 casos de conflictos de intereses y 2 casos de discriminación. (GRI 406-1)

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 que 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, prácticas anticorrupción, entre otros asuntos. (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

(GRI 102-17)

Prácticas anticorrupción

(GRI 205-2) (ODS 16.5)

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

La instancia encargada de garantizar la internalización de estas políticas vinculadas a prácticas anticorrupción es la Dirección de Riesgos, Crédito y 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.

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.

Conflictos de interés

(GRI 102-25) (ODS 16.5)

Los conflictos de intereses pueden comprometer la imparcialidad de nuestras acciones y poner en riesgo la reputación del holding así como 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 las 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 en concordancia con la legislación y reglamentaciones locales vigentes, y también 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).

Es por ello que contamos con una Política de Prevención y Combate a Actos Ilícitos, la cual orienta nuestros esfuerzos para identificar y evitar situaciones en las cuales los servicios, productos y recursos operacionales del banco puedan ser utilizados para realizar actividades ilegales, o para ocultar o disimular la verdadera naturaleza de esos fondos.

Nuestro Programa Corporativo de Prevención de Actos Ilícitos -sobre 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 los procesos anteriormente mencionados, es fundamental que nuestros colaboradores entiendan suficientemente estos asuntos y estén concientizados de la responsabilidad que tienen en este proceso dentro de la institución.

En 2021, 1.370 colaboradores participaron de entrenamientos en modalidad híbrida, sobre prevención del lavado de dinero y financiamiento del terrorismo. También tomaron parte en capacitaciones especiales según sus niveles de riesgo y se realizaron visitas a las sucursales de frontera (Ciudad del Este y Encarnación) para otras capacitaciones sobre la misma temática.

En el período que abarca este reporte 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 para los negocios. Así también, el área de Prevención de Lavado de Dinero desarrolló espacios de formación para los sectores del banco que están en contacto con clientes, de modo a interiorizarles sobre los cambios normativos 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 dirigidas a los equipos de otras organizaciones integrantes del holding, como la Fundación Itaú, la casa de bolsa Itaú Invest e Itaú Aseguradora.

Fortalecimiento continuo de los procesos

En lo que respecta a los procedimientos internos, durante el año 2021 trabajamos en la evolución de los flujos de control y en el fortalecimiento de modelos relacionados con los procesos "Conozca a su Cliente" y "Monitoreo de Transacciones". Es así que hemos automatizado alertas adicionales incluyéndolas en el Modelo de Gestión de Monitoreo e implementamos un formulario específico en el proceso de conocimiento del cliente para ciertas actividades económicas relacionadas a rubros de alto riesgo. Adicionalmente, hemos trabajado en la optimización y automatización de datos, mejorando reportes de seguimiento para el área comercial. Así también, creamos un modelo de gestión de alertas para operaciones de colaboradores, el cual repercutió favorablemente en la gestión de controles y en el seguimiento de las tareas, logrando mayor eficiencia y una reducción de la carga operativa, permitiendo así enfocarse mejor en las cuestiones de mayor riesgo.

La automatización de diversos flujos operativos relacionados con los procesos de impedidos fue otro avance del año 2021, el cual permitió optimizar tiempo de trabajo en las áreas operativas. Finalmente, todos estos procesos fortalecen el compromiso de Itaú Paraguay con las regulaciones locales e internacionales existentes, y constituyen el soporte para lograr la continuidad de los negocios y una mayor seguridad para 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, la privacidad y 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 marcan 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, proveedores y al público en general.

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 correos electrónicos con contenido malicioso. En 2021 lanzamos campañas de concientización con consejos de seguridad para utilización de tarjetas de crédito, transacciones en Internet y medidas para evitar ser víctimas de fraudes.

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 2021, en el marco del programa de concientización anual realizado por el área, se ha desarrollado un entrenamiento dirigido a todos los colaboradores del banco, con el fin de reforzar conceptos sobre la importancia del manejo adecuado de la información. Además, se les brindó capacitación sobre ciberseguridad en la empresa y el uso responsable de los equipos de trabajo con acceso a datos de la organización.

Esta capacitación fue acompañada de comunicados vía correo electrónico sobre los diversos temas impartidos en el curso con el fin de reforzar lo aprendido.

Seguridad para clientes

En 2021, seguimos reforzando las comunicaciones a nuestros clientes a través de correos electrónicos con orientaciones que establecían los pasos a seguir ante casos de estafas como de phishing, aconsejándoles en la prevención y seguridad de sus datos.

En el sitio web www.itau.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 servicios y productos.

Complementariamente, el sitio incluye 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 diferentes situaciones, como el uso de internet, el tránsito en las calles, el hogar y la escuela.

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 principales preocupaciones 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 una gerencia 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 para identificar potenciales vulnerabilidades en nuestra infraestructura tecnológica.

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: Definición de 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 remediarlos 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 y remediarlos 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.

Durante 2021 logramos fortalecer nuestros procesos en materia de ciberseguridad, lo cual abarcó la adherencia al “Proyecto Estructurante”, que consistió en la adquisición de servicios especializados de ciberseguridad de la Casa Matriz (Brasil). Así también realizamos una actualización del Mapa de Riesgos del banco, que nos permitió identificar nuestro ambiente de riesgo real.

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:

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

Durante el año 2021, 265 fueron personas fueron capacitadas incluyendo colaboradores y operadores de Servicio de Atención al Cliente a través distintas plataformas digitales.