



Somos un banco ético y responsable

02

1. Actuamos con ética y transparencia
2. Cultura de prevención de sobornos, corrupción y fraude
3. Gestión de riesgos y crisis
4. Ciber riesgos y protección de datos



“

Nuestra cultura y valores institucionales constituyen el cimiento de todas nuestras actividades. Nos comprometemos diariamente a desarrollarlos, ponerlos en práctica y buscar constantemente su mejora.

”

1. Actuamos con ética y transparencia

[GRI3-3][GRI2-15][GRI2-23][GRI2-24][GRI2-26]
[GRI2-27][DJ1.5.2][DJ1.5.5][DJ1.9.4]

Promovemos una cultura de ética, transparencia y cumplimiento normativo, gracias a la cual hemos podido retribuir confianza a la sociedad, con un alto grado reputacional en las dimensiones económica, social, ambiental. Además, fomentamos el respeto y contribución a la protección de los Derechos Humanos.

De la misma manera, exigimos a todos nuestros colaboradores y socios estratégicos el compromiso de cumplir los lineamientos éticos y de responsabilidad empresarial que promulgamos, fortaleciendo el sistema de cumplimiento de principios y valores. También, generamos espacios de retroalimentación utilizando mecanismos como: talleres, capacitaciones, informativos y un modelo de rendición de cuentas, que aportan a una cultura empresarial robusta.

Nuestros Valores

 **Coherencia**

 **Esfuerzo (ser el mejor)**

 **Responsabilidad**

 **Trascendencia**

Los compromisos que promulgamos se encuentran descritos en el Estatuto, el Código de Buen Gobierno Corporativo, el Código de Ética y Conducta, la Políticas de Sostenibilidad y asociadas; las mismas que conforman los cimientos de nuestra cultura de valores ante los colaboradores, accionistas y partes interesadas. Elamos siempre por el cumplimiento de las leyes y normativa que nos rigen acorde a nuestro giro de negocio. Además, describimos cómo evitar conflictos de interés con los diferentes públicos.

Se encuentran disponibles públicamente los siguientes documentos:

- Código de Ética y Conducta de Banco Pichincha y su Grupo Financiero.
- Código de Ética Microfinanzas.
- Política de Sostenibilidad de Banco Pichincha.
- Código de Ética y Conducta de Proveedores.
- Código de Buen Gobierno Corporativo.
- Certificado de Prácticas de Gobierno Corporativo.
- Estatuto Banco Pichincha.
- Declaratoria de Diversidad e Inclusión.

Revisa nuestras políticas en los siguientes links <https://www.pichincha.com/transparencia> 

El Código de Ética y Conducta aborda la relación con nuestros públicos, incluyendo la temática de conflicto de interés con los clientes y proveedores. Su objetivo es prevenir y mitigar situaciones específicas, delineando las acciones que deben tomar los colaboradores.

1.1. Difusión y formación

Trabajamos arduamente para que nuestros compromisos y valores que promueven la ética y transparencia sean comunicados, documentados y difundidos a través de canales disponibles para colaboradores, accionistas y partes interesadas.

Para garantizar la aplicación efectiva de los códigos mencionados, capacitamos a nuestro personal a través de Workplace, portal de políticas, página web, cursos mandatorios dirigidos a toda la organización, así como, talleres y capacitación a las diferentes unidades.

1.2. Gestión y monitoreo

Adicionalmente, como medida de control preventivo, contamos con un sistema de monitoreo y seguimiento enfocado en el cumplimiento de los compromisos y valores de manera transversal en las diferentes áreas, con el fin de verificar la aplicación obligatoria en todas las actividades que desempeñamos en las operaciones.

Hemos habilitado diferentes canales de contacto como nuestra página web, la intranet, correos y línea telefónica, en las que los colaboradores, proveedores y público en general puedan realizar consultas y denuncias. Estos mecanismos son de carácter anónimo y confidencial para proteger a las personas de posibles retaliaciones. Finalmente, esta información es consolidada y reportada al Comité de Ética.

El mail canalcompliance@pichincha.com es uno de los canales habilitados para consultas y denuncias por parte de nuestros grupos de interés.

Mediante la aplicación oportuna de controles establecidos en las políticas y procedimientos, hemos logrado prevenir la materialización de riesgos negativos en nuestras relaciones comerciales.

De igual manera, estos controles abarcan la gestión de los impactos potenciales e inherentes del sector financiero como la exposición a corrupción, fraude, correcta privacidad de datos, entre otros, los cuales mitigamos a través de diferentes estrategias como:

- Establecimiento de un marco de gobierno y control para administrar y prevenir los diferentes riesgos basados en estándares internacionales como las normativas legales vigentes, Basilea y normas ISO, identificándolos y gestionándolos en una matriz de riesgos.
- Estructura de gobernabilidad basada en diferentes comités los cuales permiten identificar aquellos riesgos que requieran ser atendidos y monitoreados en base a revisiones de auditorías internas y externas, alertas de los propios dueños de los procesos, monitoreos internos o canales de contacto. Se definen planes de acción e indicadores para medir la eficacia de las medidas para remediar y reducir los riesgos levantados. Finalmente, los resultados son comunicados a la Alta Gerencia y a los Comités correspondientes, para que se conozcan cuáles fueron las debilidades y los controles implementados para mitigar los riesgos, para posterior a esto incorporarlos y/o actualizarlos en las políticas y procedimientos institucionales.
- Respeto y promoción de los Derechos Humanos con todos nuestros grupos de interés, en el marco de lo establecido en la Carta Internacional y en la Declaración Universal de los Derechos Humanos. Además, para garantizar un compromiso institucional más extendido, contamos con una Política de Derechos Humanos y durante este año realizamos un mapa de riesgos sobre Derechos Humanos en nuestra cadena de valor realizado por una empresa independiente.

Durante el 2023 no registramos casos de incumplimiento a las normativas que nos rigen y que hayan generado la imposición de multas o sanciones en contra de nuestra Institución.

¹En un siguiente ejercicio de reporte publicaremos la data segmentada por región.

2. Cultura de prevención de soborno, corrupción y fraude

[GRI 2-17][GRI 205-1][GRI205-2][DJ1.5.3][DJ1.5.4]

Para establecer una cultura de prevención de soborno, corrupción y fraude, es necesario el reforzamiento y la capacitación constante en este ámbito. En el marco de incrementar los conocimientos en desarrollo sostenible realizamos continuamente monitoreos y seguimientos a los riesgos de soborno, corrupción y fraude, capacitamos al personal a través de cursos mandatorios y talleres para prevenir y mitigar conductas inadecuadas, desde los miembros del órgano de gobierno hasta las posiciones iniciales en el Banco, y comunicamos a nuestros socios comerciales sobre el obligatorio cumplimiento de nuestras políticas y códigos para prevenir este tipo de riesgos.

- Política de Compliance.
- Política Anticorrupción y Antisoborno.
- Programa de Cumplimiento.
- Política General de Seguridad de la Información y Ciberseguridad.

En nuestra Política Anticorrupción y Antisoborno se exponen responsabilidades y políticas generales y específicas que deben seguir nuestros colaboradores, además de las sanciones pertinentes y los canales para denunciar, de buena fe, un incumplimiento o apariencia de incumplimiento.

Comunicación y formación sobre anticorrupción			
Grupo de interés comunicados sobre las política y procedimientos anticorrupción de la organización	2023		
	Total de personas	Personas alcanzadas	%
Miembros del órgano de gobierno	12	12	100 %
Colaboradores de la organización	5.591	5.591	100 %
Socios de negocio	715	715	100 %
Grupos de interés formados en anticorrupción		Total de personas	Personas alcanzadas
			%
Miembros del órgano de gobierno		12	12
Colaboradores de la organización		5.591	5.431
			33 %
			97 %

Como parte de una buena práctica internacional hemos establecido el Programa de Compliance dentro de la institución; además, contamos con los siguientes instrumentos disponibles públicamente para el conocimiento de todos nuestros stakeholders:

Aplicamos un programa de seguimiento y control para monitorear los riesgos relacionados con la corrupción que fueron identificados y evaluados con posibilidad de impacto. Cabe recalcar que, el departamento de Control y Cumplimiento no ha recibido denuncias sobre eventos de corrupción y soborno, durante el periodo 2023.

3. Gestión de riesgos y crisis

[GRI2-25] [DJ1.5.2] [DJ1.5.4] [DJ1.4.1] [DJ1.4.2]
[DJ1.4.3] [DJ1.4.4]

Tenemos como prioridad la gestión de riesgos y crisis, por lo que contamos con departamentos y comités responsables de su gestión en términos de apetito y tolerancia de riesgo, así como de supervisión e información sobre los mismos. Disponemos de una Política de gestión de apetito y límites de riesgo en la que se detallan las pruebas de estrés (Stress Test) y el cálculo del VAR y la pérdida esperada, en base a la cual están elaboradas las revisiones e informes mensuales de nuestra exposición en este aspecto.

El área responsable de la gestión de riesgos es la Vicepresidencia de Riesgo Integral, y para la supervisión y auditoría es responsable el Comité de Administración de Riesgos (CAR), conformado por miembros delegados del Directorio, el Gerente General y el Vicepresidente de Riesgo Integral.

Como medida de control, se realizan auditorías a los procesos mencionados, además de que nuestra estructura organizacional ha definido de manera independiente al área de Negocio y al área de Riesgos.

Riesgos emergentes:

En el análisis de riesgos emergentes, identificamos los siguientes:

1) Cambio Climático: A través del análisis de la frecuencia e intensidad de fenómenos y estudios climáticos sobre la vulnerabilidad del territorio se evidencia que las afectaciones causadas por el cambio climático cada vez se hacen más crecientes, pues genera fenómenos extremos como



inundaciones, sequías y tormentas intensas, que podrían afectar directamente a nuestros clientes y comunidades, generando inestabilidad en su capacidad de pago y, por ende, riesgos en la cartera de préstamos.

La variabilidad y eventos climáticos extremos representan una amenaza creciente a largo plazo para la estabilidad financiera y la operación del Banco pues impacta directamente en la solvencia de los prestatarios, la devaluación de activos inmobiliarios y la viabilidad de proyectos financiados por el Banco, afectando la calidad de los activos y la rentabilidad institucional.

Para minimizar este peligro, realizamos el análisis de los riesgos climáticos como parte de la evaluación del Sistema de Administración de Riesgos Ambientales y Sociales (SARAS) en los préstamos otorgados. Además, participamos activamente, tanto interna como externamente, en iniciativas que contribuyen a la mitigación y adaptación al cambio climático desde el accionar de las empresas.

2) Ciberseguridad: Como institución nos enfocamos en el desarrollo y en estar a la vanguardia de los últimos avances tecnológicos, pero esto trae consigo riesgos en ciberseguridad a los cuales nos enfrentamos. El aumento de la digitalización y la interconexión de servicios financieros aumenta la exposición a amenazas cibernéticas, como ataques de ransomware, phishing y robos de datos.

Estos eventos podrían comprometer la integridad de los sistemas, la confidencialidad de la información de los clientes y la continuidad de las operaciones, a través de fallos, accesos no autorizados o indebidos a los sistemas de información. Un ataque cibernético exitoso puede resultar en la pérdida de datos sensibles, interrupciones operativas y en consecuencia daño a la reputación del Banco y pérdida de confianza por parte de los clientes, lo que podría afectar la participación del mercado y la retención de clientes.

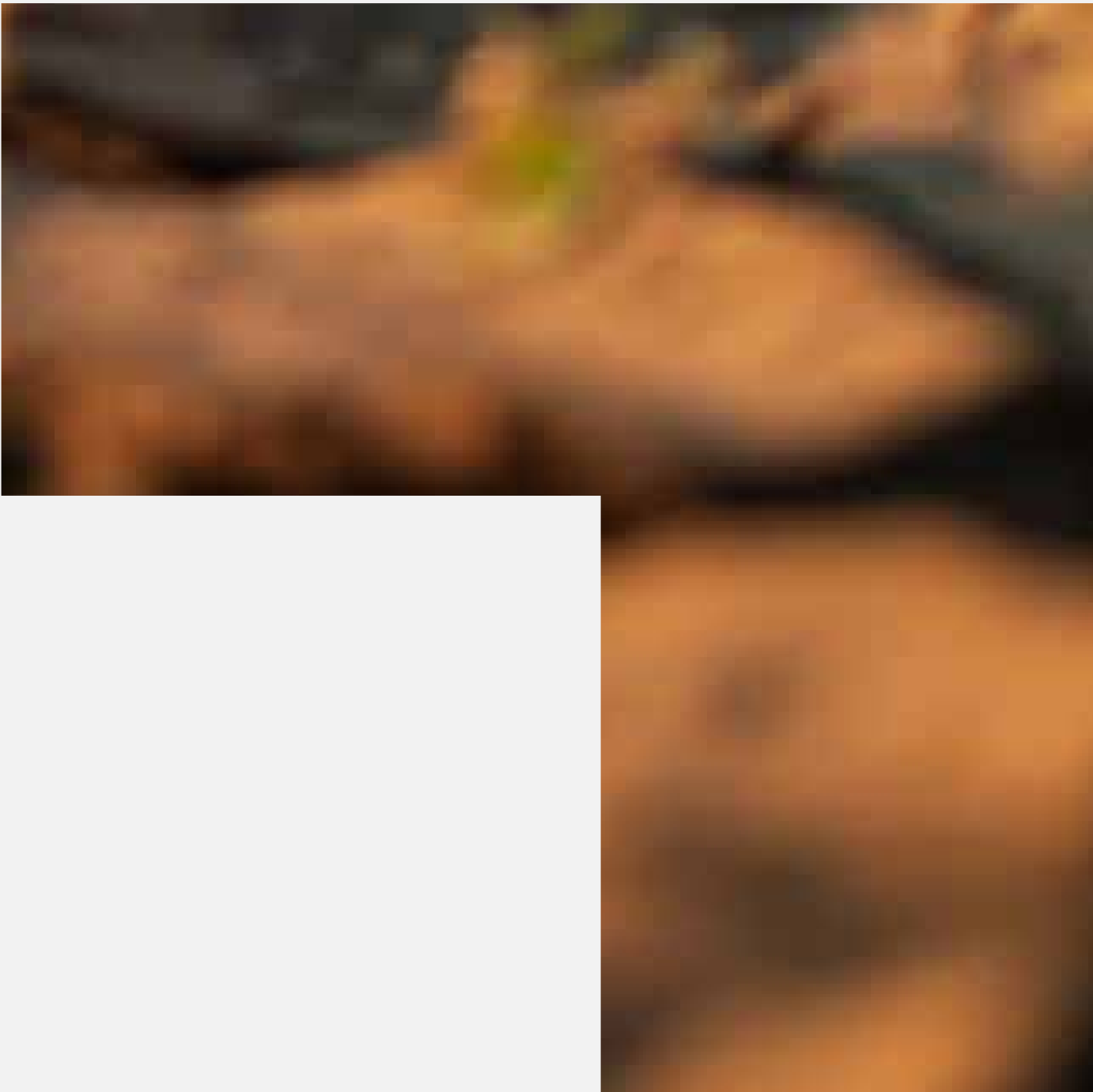
Para prevenir y mitigar este riesgo hemos desarrollado una estrategia de ciberseguridad liderada por la Vicepresidencia de Tecnología y Operaciones y el Comité de Ciberseguridad. Además, varios miembros de la Alta Gerencia y directores velan por su cumplimiento.

Cultura de riesgos

Generamos una cultura de riesgos transversal en la institución mediante acciones para que todas las áreas y colaboradores puedan identificar los riesgos que deben ser gestionados por el Banco.

Un ejemplo de esto es la evaluación que realiza el área de Recursos Humanos que incluye el indicador de madurez cultural que se encuentra enfocado en medir qué tanto estamos alineados a cuidar y gestionar los riesgos desde nuestros principios culturales: “We act as owners” / “We make banking easy”. Por otro lado, realizamos una evaluación de riesgos de estas iniciativas antes de su aprobación, lo cual se detalla en nuestro “Instructivo para la gestión de riesgos en iniciativas/proyectos”.

Para que nuestros colaboradores puedan identificar e informar proactivamente sobre riesgos potenciales, realizamos un ejercicio anual de autoevaluación y testeo de controles en el que los dueños de procesos informan sobre los riesgos, el diseño y la efectividad de sus controles. Asimismo, existe el proceso de Torre de Control en Riesgos No Financieros el cual identifica riesgos potenciales a nivel global y solicita a los dueños de procesos evaluarlos y plantear planes de acción en caso de ser necesario.



4. Ciber riesgos y protección de datos

[GRI3-3][DJ1.5.2]

La gestión de riesgos operativos identifica los riesgos a los que está expuesta la institución con respecto a cuatro factores: procesos, personas, tecnología y eventos externos. Dentro del factor tecnología encontramos la gestión de ciber riesgos, el cual es uno de los pilares fundamentales de la estrategia empresarial del Banco; de esta forma se asegura que la oferta de valor a nuestros clientes se cumple en forma y fondo, protegiendo la información que los mismos nos han proporcionado.

La industria financiera está expuesta a una amplia y recurrente variedad de ciber amenazas. Cor esto, realizamos grandes esfuerzos para gestionar la protección de los datos e información con un enfoque de riesgos, ya que somos conscientes de que, un potencial incidente podría generar intermitencia en nuestros canales y servicios, afectando a aproximadamente el 30% de usuarios del sistema financiero nacional (bancos) que transaccionan a través de los mismos, además de vulnerar el acceso a la información de nuestros clientes.

A través de estas acciones, hemos generado impactos positivos mediante la optimización del uso de canales digitales disminuyendo la huella carbono de sus actividades y también, promoviendo la inclusión financiera de grupos sociales considerados minorías o con difícil acceso a tecnología, brindando disponibilidad de nuevos productos a través de canales digitales.

Conscientes de que los impactos negativos potenciales que pueden generar los ciber riesgos, hemos adoptado medidas para prevenir o disminuir los mismos:

- Actualización de la metodología para valorar ciber riesgos.
- Estructura de expertos asignados por especialidad.
- Implementación de herramientas para detectar ciber amenazas de forma continua.
- Esquemas de capacitación continua para incrementar nuestras capacidades internas.
- Pruebas continuas para mejorar la capacidad de detección de ciber amenazas.
- Mejora en el proceso de respuesta a ciber incidentes en coordinación con las áreas intervinientes en base a la naturaleza del evento.
- Automatización de respuesta ante potenciales ciber incidentes.

Identificamos de forma oportuna aquellas ciber amenazas potenciales, determinamos esquemas de protección y remediación de forma proactiva, y minimizamos impactos en nuestros canales y servicios.

Además, el área de Gobierno de Ciberseguridad cuenta con un proceso transversal que permite diseñar, medir y monitorear diferentes indicadores asociados con procesos y controles de ciberseguridad y seguridad de información.



5. Protección de datos

[GRI 418-1] [DJ3.8.1] [DJ3.8.2]

Establecemos metodologías, políticas, procedimientos, estándares, medidas técnicas, organizativas y legales orientadas a gestionar los ciber riesgos con el fin de proteger los datos e información de nuestros clientes, colaboradores y otras partes interesadas.

En nuestra web, compartimos el "**Aviso de privacidad de canales electrónicos**" ya que somos los responsables de gestionar los datos personales en estos canales y contamos con los siguientes puntos relacionados con la protección de la privacidad:

- Responsabilidad del tratamiento y protección de datos.
- Naturaleza de la información capturada.
- Uso de la información recopilada.
- Información, acceso, eliminación, rectificación, actualización, oposición, portabilidad, suspensión y no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.
- Canal de requerimientos.
- Veracidad de los datos del cliente.
- Tiempo de conservación de la información en los archivos corporativos.
- Divulgación a terceros (entidades públicas y privadas).

La Política General de Protección de Datos Personales se elaboró bajo lo dispuesto en la Ley Orgánica de Protección de Datos Personales. Por otra parte, como medida de control y monitoreo contamos con Indicadores Claves de Riesgo (KRI) y Objetivos y Resultados Claves (OKR) para determinar la eficacia de las medidas implementadas para la protección de datos. En 2023 no contamos con ninguna reclamación fundamentada respecto a la violación de la privacidad de clientes.