

Código de Ética

Oficina de Ética / Secretaría / Asesoría Jurídica

AI.ANX.DCM.CódigoDeÉtica

Público Una Vez Aprobado

De conformidad con el marco normativo de la Política de Acceso a la Información, el presente documento será divulgado en el sitio web externo del Banco después de su aprobación.

DESARROLLO

TÍTULO I. CÓDIGO DE ÉTICA

CAPÍTULO I. ASPECTOS GENERALES

Artículo 1. Del objeto. El objeto del presente código es establecer un marco de conducta adecuado, regido por principios institucionales y valores éticos, articulado por el Banco Centroamericano de Integración Económica (BCIE) mediante normas que establecen los comportamientos que son esperados de su personal y que el personal espera de sus compañeros de trabajo, en el ejercicio de sus funciones laborales e interpersonales, entendiendo que es un documento vivo que deberá revisarse continuamente. Lo anterior con el propósito de generar y fortalecer una cultura y ambiente ético que permitan el cumplimiento de los objetivos institucionales.

Artículo 2. Ámbito de aplicación. Al tenor de lo establecido en el Reglamento de la Organización y Administración (ROA) del BCIE, el contenido de este Código de Ética será de aplicación y observancia general a todos los niveles jerárquicos del Banco, incluyendo Directores, funcionarios y empleados del Banco, personal regular, contratistas, jóvenes profesionales, pasantes externos, practicantes profesionales y cualquier otro integrante de los diferentes programas de dotación de personal que sean aprobados en el Banco y de acuerdo a lo establecido en el Reglamento General de Administración de Recursos Humanos.

El BCIE espera que cualquier contraparte que tenga relación con la Institución, no obstante que pueda tener su propio Código de Ética, actúe de conformidad con el presente código. En el caso específico de los procedimientos de adquisiciones para el funcionamiento del Banco, así como aquellos en los que el BCIE realice la función de ejecutor de dichos procedimientos, el incumplimiento de los principios institucionales y valores éticos de la Institución dará lugar a las consecuencias previstas en los instrumentos que respectivamente regulan esas relaciones.

Artículo 3. Relación con otras políticas del Banco. Este código constituye el principal documento de política relativo a la ética, estableciendo los principios generales y las expectativas de conducta del personal del Banco en el lugar de trabajo y, en lo aplicable, fuera del mismo. Sin embargo, otros documentos podrán brindar orientación y reglas concernientes específicamente a ciertas funciones e interacciones a efecto de complementarse entre sí.

La Oficina de Ética, en el desempeño de sus funciones y con el afán de crear sinergias, coordinará, en su caso, con las oficinas adscritas la identificación de iniciativas que por su naturaleza pudieran ser objeto de trabajo conjunto o complementario. Además de los mencionados anteriormente, podrá coordinar esfuerzos para realizar actividades de manera conjunta con la Administración, así como con los comités respectivos. Lo anterior, tomando en consideración la independencia de la Oficina de Ética y la confidencialidad de los asuntos bajo revisión.

Artículo 4. Dudas relacionadas con la aplicación del Código de Ética (orientación y asesoría). El Código de Ética deberá ser una fuente de guía, orientación y asesoría para todo el personal del BCIE, mientras trabajan como parte de un equipo para lograr su objetivo, establecido en el artículo 2 del Convenio Constitutivo.

El Código de Ética y las campañas educativas, que para su implementación diseñe la Oficina de Ética, deben constituirse en los instrumentos que ayuden al personal del BCIE a convertir en acciones los principios institucionales y los valores éticos.

Consultar el Código de Ética para obtener información y confiar en el buen juicio del personal del BCIE ayudará a resolver la mayoría de las situaciones, especialmente aquellas que sean desafiantes y desconocidas, tomando en cuenta que ningún documento puede anticipar o proveer respuestas u orientación para toda situación que pueda surgir en el lugar de trabajo. Por lo tanto, si surgen dudas sobre el modo ético de actuar, el personal del BCIE, previo a proceder, debe procurar la asesoría de su supervisor o del Oficial de Ética. El Oficial de Ética y el personal de dicha oficina ayudarán a comprender el Código de Ética cuando no se tenga claro cuál es el curso de acción apropiado en un caso particular.

Artículo 5. Conducta indebida. Cuando este código o sus Normas Complementarias se refiera a los términos “infracción” o “conducta indebida”, esto incluye, pero no se limita, al incumplimiento de las obligaciones adquiridas como integrantes del personal del BCIE contenidas en el mismo:

- a) Acciones u omisiones que transgreden los principios institucionales o valores éticos desarrollados en el presente Código.
- b) Inobservancia de los estándares o comportamientos esperados del personal de un organismo internacional como el BCIE que forman parte de la conciencia y comportamiento organizacional.

No es necesario que una acción implique mala intención o culpa para ser considerada como conducta indebida.

Artículo 6. Principios institucionales. Los principios institucionales que el Banco tiene como base para atender de manera apropiada sus objetivos deberán contemplarse como guía en todas las actuaciones institucionales de todo el personal del Banco, los cuales se enuncian a continuación:

- (a) **El cumplimiento eficiente de su objeto y de su marco institucional:** todo el personal del Banco actuará diligentemente en cada una de sus operaciones, dando fiel cumplimiento a su objeto, al Convenio Constitutivo y a las normas, reglamentos, resoluciones y acuerdos que regulan el Banco.

Asimismo, actuarán diligentemente en aras de proteger el interés y asegurar el tratamiento equitativo a todos los miembros de la Institución en los términos establecidos en el Convenio Constitutivo y en la reglamentación correspondiente, de forma tal que atiendan con objetividad e imparcialidad sus programas de integración económica y de desarrollo económico y social.

- (b) **Atención oportuna al cliente:** el personal del Banco atenderá a sus clientes con prontitud, dedicación, transparencia y profesionalismo, facilitándoles la gestión de operaciones y brindándoles la información que les permita el acceso a los servicios del Banco, protegiendo su confidencialidad y privacidad.

- (c) **El cumplimiento eficiente con las fuentes:** el personal del Banco honrará los compromisos de este con las fuentes de recursos, cumpliendo los términos y condiciones aceptadas en los contratos de préstamos. Asimismo, deben asegurar que estos compromisos sean consistentes con la integridad patrimonial del Banco, que fortalezcan su participación en los mercados internacionales de capital, así como su prestigio institucional.

El personal del Banco observará el cumplimiento de los convenios y las regulaciones vigentes en sus relaciones con los organismos internacionales y multilaterales de crédito y demás instituciones, manteniendo una honorable imagen.

- (d) **Valoración de los recursos humanos del Banco:** los órganos de gobierno del Banco, implementando el tono desde arriba, fomentarán un clima organizacional propicio para la estabilidad y la realización integral de los miembros de su personal. En ese sentido, deberán promover la sinergia de trabajo entre las diferentes áreas, el respeto a la dignidad humana y favorecer el crecimiento y bienestar individual de sus miembros y deberán tomar acciones concretas para prevenir de manera efectiva cualquier conducta inapropiada. Asimismo, dichos órganos garantizarán la investigación de las denuncias existentes en este sentido, así como la eventual sanción del o los denunciados y la reparación moral del daño causado, cuando corresponda, al tenor de lo dispuesto en la normativa vigente.

- (e) **Cultura de trabajo en equipo y cooperación:** todo el personal del Banco, por ser el BCIE una institución que trabaja por la integración y el desarrollo de los países miembros, fomentarán un ambiente laboral que propicie un clima organizacional positivo, que permita la generación de una cultura de trabajo en equipo y de respeto y cooperación entre los miembros de su personal.

- (f) **Fundamentación de actuaciones:** las actuaciones de todo el personal del Banco se desarrollará fundamentada exclusivamente en criterios técnicos establecidos en su normativa y amparándose en los más altos estándares de la banca multilateral de desarrollo, así como en las sanas prácticas de la industria bancaria; lo anterior, en apego a lo establecido en el Convenio Constitutivo. El personal del Banco, independientemente de su nivel jerárquico, no podrá rebasar ni ignorar los mandatos previstos en la normativa para el cumplimiento de sus funciones, evitándose a toda costa la discrecionalidad.

Además, estos no aceptarán, de los clientes o las fuentes de recursos, condicionamientos de carácter político o que contravengan el objeto del Banco.

CAPÍTULO II. DE LOS VALORES ÉTICOS

Artículo 7. Valores éticos y compromiso institucional. El BCIE está comprometido a fomentar y mantener un ambiente de trabajo que favorezca un comportamiento ético y que estimule activamente un diálogo abierto en esta materia. Se espera que, mediante sus acciones y comunicaciones, todo el personal del BCIE demuestre adherencia a los siguientes valores éticos: (1) respeto; (2) equidad; (3) lealtad; (4) integridad y (5) transparencia.

La implementación exitosa del Código de Ética depende del compromiso de todo el personal del Banco de regirse y observar estrictamente las directrices que en él se establecen. Dicho compromiso se asume desde la incorporación al Banco, por lo que es responsabilidad de todo su personal leer, comprender y asumir los compromisos establecidos en el Código de Ética para contribuir a mantener un ambiente positivo, cumpliendo las responsabilidades de conformidad con los principios institucionales y valores éticos.

Considerando el ánimo preventivo de este código y para tal efecto, la Oficina de Ética requerirá del personal del Banco la suscripción anual de una declaración jurada mediante la cual certifiquen haber leído, comprendido y asumido los compromisos establecidos en el Código de Ética. Asimismo, la Oficina de Ética podrá desarrollar guías prácticas, programas y actividades para fomentar el buen comportamiento relacionadas con estos principios institucionales y valores éticos, y así facilitar su comprensión, difusión e implementación.

SECCIÓN 1. DEL VALOR DEL RESPETO

Artículo 8. Respeto. Las relaciones interpersonales del personal del Banco deben desarrollarse con la debida consideración, tolerancia, búsqueda de armonía, imparcialidad y sin causar daño, ofensa o perjuicio.

Por su parte, el Directorio y la Administración Superior implementarán acciones concretas de tal forma que permitan crear un entorno de trabajo positivo y profesional en el que todos reciban un trato digno y respetuoso.

Considerando la diversidad del personal del Banco, todos deben mostrar respeto por quienes les rodean, trátense de sus compañeros u otras personas que se encuentren en las instalaciones del Banco o estén prestando servicios a este. Todo el personal tiene que rendir cuenta de sus acciones y, en consecuencia, asumir la responsabilidad de mantener una conducta profesional, imparcial y respetuosa, plantear inquietudes que puedan tener ante conductas indebidas que falten al respeto a otro u otros miembros del personal, así como denunciarlos y tomar medidas para corregir cualquier falta en su comportamiento. Las acciones irrespetuosas tales como insultos, ofensas, afirmaciones maliciosas y deliberadamente falsas sobre otros y el maltrato verbal y físico, entre otros comportamientos, se consideran conductas indebidas.

El personal del Banco debe estar consciente que en todo momento representa a la Institución y, por tanto, se espera que siempre se comporte con profesionalismo, cortesía y tolerancia al tratar con los demás. También debe abordar su trabajo con empatía, escuchando atentamente, abierto a escuchar nuevas ideas y hablando amablemente con cualquier contraparte, sea esta colega, cliente, socio, proveedor o miembro del público. En el mismo sentido, esto también conlleva a la responsabilidad de salvaguardar los activos físicos del Banco, utilizándolos de manera adecuada.

Al ser el BCIE un organismo internacional, requiere que su personal esté consciente de las diversas costumbres locales, las tradiciones y las diferentes culturas de trabajo de los países miembros y contrapartes. El Banco se compromete a ofrecer al personal un entorno de trabajo que se caracterice por la apertura, la confianza, el respeto, la imparcialidad, la creatividad, la

motivación y la innovación, reconociendo que respetar y valorar las diferencias es clave para el éxito colectivo.

El Banco tomará medidas necesarias para crear y mantener una cultura inclusiva en la que se apoye con lo que se requiera y no se tenga temor de solicitar ayuda unos de otros.

El personal del BCIE que desempeña labores de supervisión tiene la responsabilidad adicional de crear y mantener un entorno de trabajo que sea respetuoso e imparcial con todos. El personal tiene derecho a sentirse seguro y cómodo, y a estar libre de cualquier clase de acoso, abuso u otras formas de comportamiento no deseado en el trabajo.

Artículo 9. Prevención del acoso en todas sus manifestaciones. El acoso no será tolerado en el BCIE. Por consiguiente, se prohíbe cualquier forma de acoso u hostigamiento en todas sus modalidades y formas, sin importar quien sea la víctima (incluyendo al personal de apoyo, contratistas, practicantes, jóvenes profesionales o clientes) o el ofensor, ni cual sea su nivel jerárquico.

Artículo 10. Del acoso. El acoso implica un trato irrespetuoso que se produce una sola vez o de manera repetida, pudiendo ser este verbal o físico. Normalmente tiene por finalidad o efecto crear un entorno de trabajo intimidatorio, hostil u ofensivo. Dicho comportamiento no deseado interfiere con la capacidad para desempeñarse de manera óptima en el empleo de una persona, pudiendo acontecer tanto dentro como fuera del lugar de trabajo formal.

Cualquiera que sea su forma, el acoso resulta inaceptable y exige una respuesta inmediata de parte de la víctima o de cualquier miembro del personal que lo presencie.

Es idóneo que todo el personal del BCIE comunique claramente a sus colegas cualquier comportamiento que considere objetable y pida que dicho comportamiento termine. Igualmente, podrá solicitar asistencia a la Oficina de Ética o a la instancia que corresponda, si estas acciones persisten.

Las siguientes conductas son ejemplos ilustrativos más no limitativos de acoso:

- (a) Trato diferenciado por razones de raza, color, idioma, género, edad, ascendencia, nacionalidad, posición económica, estado de salud, discapacidad, estado civil, preferencias religiosas, políticas, sexuales o cualquier otra condición personal, sea esta real o percibida.
- (b) Comentarios o comportamientos denigrantes y la exhibición o circulación en el lugar de trabajo de material escrito o gráfico que denigre o demuestre hostilidad hacia una persona o grupo; hacer bromas ofensivas, racistas o discriminatorias con respecto a una persona o grupo en relación con su condición personal, sea esta real o percibida, que denigre a los colaboradores del Banco.
- (c) Creación y propagación de rumores, falsas noticias, mentiras, acusaciones en contra de una persona o grupo en relación con su entorno laboral.
- (d) Comportamientos hostiles contra cualquier persona que labore en el Banco, pudiendo incluir insultos y/o amenazas.

- (e) Gritar o agredir verbalmente a los compañeros de trabajo o colegas; exhibir un comportamiento agresivo o intimidante; ridiculizar o interferir en la realización del trabajo y responsabilidades encomendadas a uno o varios miembros del personal del Banco.
- (f) Conductas de hostigamiento, intimidación, maltrato, rumores de mala fe hacia cualquier persona que labore en el Banco.

Artículo 11. Acoso laboral. El acoso laboral representa una conducta inadecuada o abusiva que se manifiesta en el ámbito de trabajo por uno o más individuos, que atenta contra la dignidad, integridad psicológica o bienestar físico de la persona afectada.

Para entender mejor la amplitud de este comportamiento, se incluyen algunos ejemplos de manera ilustrativa pero no exhaustiva:

- (a) Insultos asociados con rasgos personales o competencia profesional.
- (b) Comportamiento cuyo propósito sea aislar o humillar a una persona o grupo, tal como la exclusión injustificada de reuniones o la denegación injusta de información o de equipo necesario para el desempeño de las funciones.
- (c) La amenaza o toma de medidas adversas en contra de una persona o un grupo por haberse opuesto o negado a participar en un acto indebido o por diferencias de criterio.
- (d) Intimidación, incluyendo el abuso físico o verbal.
- (e) El desestimar sin fundamento y con intención de atentar contra la dignidad, integridad psicológica o bienestar físico del subordinado, por parte de una persona con cargo jerárquicamente superior, sus ideas, opiniones, trabajo o bloquear las posibilidades de crecimiento laboral dentro de la Institución.
- (f) Hacer señalamientos sin fundamento, en relación con el incumplimiento de normas, procedimientos, requisitos o cualquier acción u omisión en las cuales se diera a entender o se pusiera en duda la honorabilidad de un colaborador del Banco o se afirmara que ha cometido faltas de conducta, éticas, morales, sociales o de cualquier otra índole.
- (g) Gritar o agredir verbalmente; hacer bromas ofensivas o racistas con respecto a una persona o grupo; exhibir por parte del superior inmediato un comportamiento agresivo; intimidar, ridiculizar o interferir en la realización de su trabajo.
- (h) Cargar injustamente de trabajo a un subalterno.

Artículo 12. Acoso sexual. El acoso sexual representa una conducta que, por su naturaleza, alcance, contexto y magnitud, conlleva entre el personal del Banco cualquier tipo de proposición sexual no deseada, solicitud de favores sexuales u otra manifestación de naturaleza sexual, explícita o sutil, que provoca objetivamente en la víctima una ofensa, sufrimiento o humillación. El acoso sexual puede abarcar una serie de comportamientos e involucrar a personas del mismo o de distinto género.

A continuación, se enumeran, de forma enunciativa más no limitativa, algunos comportamientos que podrían considerarse como acoso sexual:

- (a) Invitaciones a actividades sociales o citas cuando la persona a quien se dirigen haya manifestado no estar interesada.
- (b) Coqueteo, insinuaciones o propuestas sexuales indeseadas.
- (c) Pedidos explícitos, implícitos o sutiles de favores sexuales a cambio de beneficios laborales reales o prometidos, tales como evaluaciones favorables, promociones o la permanencia en el puesto.

- (d) Comentarios sexuales, degradantes o sugestivos; epítetos, bromas y burlas de carácter sexual; referencias escritas o verbales a la sexualidad, o bien comentarios sobre el cuerpo de una persona.
- (e) Represalias o amenaza de represalias tras una respuesta negativa a insinuaciones sexuales.
- (f) Exhibición de objetos, imágenes o contenido en general de connotación sexual.
- (g) Gestos obscenos o contacto físico indeseado de connotación sexual.
- (h) Indagaciones o discusiones sobre las experiencias o actividades sexuales de una persona.
- (i) Envío de textos o imágenes u otro tipo de comunicación inapropiada y no solicitada de connotación sexual, por medio de celulares, correo electrónico, internet, redes sociales o cualquier otro medio.

Artículo 13. Cero tolerancia al acoso. Los comportamientos irrespetuosos y el acoso no tienen cabida en el BCIE. En tal sentido, el personal con funciones de autoridad sobre otros deben desempeñar funciones especiales que consisten en lo siguiente:

- (a) Comunicar a sus colaboradores que el comportamiento irrespetuoso y el acoso no serán tolerados.
- (b) Asegurar que el colaborador que plantee inquietudes reciba apoyo y no sean objeto de represalias.
- (c) Nunca excusar o minimizar una conducta indebida o comportamiento inapropiado.
- (d) Cuando sea necesario, llevar las quejas e inquietudes a la Oficina de Ética.

SECCIÓN 2. DEL VALOR DE LA EQUIDAD

Artículo 14. Equidad. En el contexto del presente código, equidad significa que el personal del BCIE debe cumplir las normas y políticas en forma consistente, congruente, justa y uniforme para asegurar un ambiente de trabajo libre de favoritismos, abuso en el ejercicio de la autoridad y decisiones arbitrarias o caprichosas.

También quiere decir que cualquier colaborador del Banco debe ofrecer un tratamiento inclusivo y equitativo al resto del personal, a los proveedores, a los consultores externos, a los clientes y demás partes interesadas.

Artículo 15. Uso apropiado de la autoridad. El personal a quien el BCIE ha confiado funciones de autoridad sobre otros tiene la especial responsabilidad de ejercer dicha autoridad con discernimiento y equidad, respetando los principios institucionales y valores éticos, promoviendo su respeto por parte de sus subalternos. Incluso quienes no actúan formalmente como supervisores deben cuidar de no valerse de su posición en el Banco para perseguir fines no apropiados, ya sea internamente o con proveedores, consultores externos, clientes y partes interesadas o socios de negocio.

Los siguientes son ejemplos ilustrativos y no exhaustivos de abuso de autoridad:

- (a) Incurrir en conductas de intimidación o acoso.
- (b) Interferir con la capacidad de otros para trabajar eficazmente, por ejemplo, obstaculizando su acceso a información o recursos.
- (c) Exigir tareas o favores personales a los subordinados.
- (d) Plantear habitualmente exigencias laborales no razonables.

- (e) Valerse de las credenciales o la posición en el Banco para obtener atención o trato especial.

Artículo 16. Prohibición de la discriminación. El BCIE promoverá un lugar de trabajo donde todo el personal sea valorado, se respeten las diferencias y se brinden oportunidades y un trato equitativo e incluyente para todos. El BCIE respeta y valora la diversidad porque representa un conjunto de experiencias, culturas y antecedentes. En la Institución se tiene el convencimiento de que la diversidad contribuye al éxito de las actividades que se desarrollan. Consecuentemente, el BCIE tiene una política de cero tolerancia ante cualquier forma de discriminación y fomenta la inclusión, por lo que los colaboradores del Banco no pueden discriminar a sus compañeros de ninguna forma.

El BCIE prohíbe de manera enérgica la discriminación con el objetivo de impulsar la igualdad laboral, prevenir y eliminar todo tipo de violencia laboral y discriminación ya sea por motivos de origen étnico o nacional, cultura, color de piel, apariencia física, sexo, género, identidad y expresión de género, orientación sexual, edad, discapacidad, religión, idioma, condición social, económica, jurídica, así como de salud, embarazo, estado civil o conyugal y situación migratoria, entre otras, sea esta real o percibida.

Artículo 17. Violencia en el lugar de trabajo. El activo más valioso del BCIE son sus colaboradores, por lo tanto, la seguridad y comodidad en el lugar de trabajo es primordial. Los miembros de los órganos de gobierno del BCIE y en general todo el personal brindará un entorno laboral seguro, en el que la violencia es inaceptable.

La violencia en el lugar de trabajo también puede constituir un delito en los países miembros del Banco por lo que el BCIE podrá referir a las autoridades nacionales a miembros del personal que cometan o amenacen con cometer actos de violencia, en atención a la normativa y naturaleza del Banco, siguiendo para ello los procedimientos establecidos.

En ese sentido, cualquier acción, incidente o conducta que razonablemente le cause a un miembro del personal del Banco temor por su seguridad personal o la de sus compañeros de trabajo, familia, amigos, o propiedad, constituye violencia en el lugar de trabajo. Esta puede ocurrir en las instalaciones del Banco, o fuera de ellas en determinadas circunstancias, y puede abarcar las siguientes acciones ejemplificativas y no limitativas:

- (a) Agredir físicamente.
- (b) Amenazar con agresión física o mediante contacto agresivo dirigido contra otra persona.
- (c) Amenazar con causar daño a una persona o su familia, amigos, asociados o a su propiedad.
- (d) Destruir o amenazar con destruir intencionalmente bienes propiedad del Banco o de otras personas.
- (e) Acosar con llamadas telefónicas amenazantes o intimidantes.
- (f) Acechar.
- (g) Intimidar o amenazar veladamente con daño físico.

SECCIÓN 3. DEL VALOR DE LA LEALTAD

Artículo 18. Lealtad. Lealtad significa que el personal del BCIE, en el desempeño de sus funciones, rinde cuentas exclusivamente al Banco y a sus autoridades, estando comprometido

con la Institución, así como con sus pares de trabajo, promoviendo en todas las actividades una imagen institucional positiva, evitando comentarios y actuaciones que puedan causar perjuicio al BCIE o a sus pares de trabajo. Igualmente, supone proteger y mantener en reserva toda la información proveída y generada por la Institución o sus clientes, cuando así corresponda, de acuerdo con las disposiciones establecidas al efecto.

Artículo 19. Conflictos de intereses. Un conflicto de interés es una situación en la que se genera una disyuntiva entre los intereses personales y los intereses de la Institución o de sus clientes. Es decir, que los intereses privados de una persona interfieran o puede entenderse que interfieren con su toma de decisiones y con el cumplimiento cabal de sus funciones oficiales.

Desde esa perspectiva, el **conflicto de interés** es una situación en la que un miembro del personal del BCIE tiene un interés que influye de manera indebida en su criterio, decisiones, acciones, atribuciones y responsabilidades con el Banco, sus clientes o contrapartes. Tales situaciones vulneran los principios institucionales y valores éticos del presente código, así como los deberes que los miembros del personal del Banco adquieren como colaboradores de un organismo internacional.

En la gestión de los conflictos de intereses se reconoce que estos pueden ser directos o indirectos. Se entiende que existe un **interés directo** si la situación que origina el conflicto de interés pudiera generar un beneficio al propio miembro del personal, o cuando la gestión o decisión que corresponda a un miembro del personal involucre a un tercero que sirve de nexo entre el propio miembro del personal y sus intereses.

Por su parte, se entenderá como **interés indirecto** aquellos casos en los que la situación que origina el conflicto de interés puede generar un beneficio a un tercero, ya sea una persona natural o jurídica, dentro de los límites, parámetros y relaciones que se establecen en este código. Además, se considera un **interés indirecto** si la gestión o decisión que corresponda a un miembro del personal, aún sin existir un beneficio, involucre a alguno de los parientes del miembro del personal (hasta el cuarto grado de consanguinidad y segundo de afinidad) o a alguna persona con la que este mantenga una relación personal.

Un **conflicto de interés real** sucede cuando un miembro del personal del Banco efectivamente tiene un interés que pudiera entrar en conflicto con los intereses del Banco para una situación presente o una potencial. Entendiendo como situación presente cuando el interés del miembro del personal entra en conflicto con una situación que está ocurriendo. Un **conflicto de Interés potencial** es aquella situación que puede ocurrir cuando un miembro del personal del Banco tiene un interés actual que podría entrar en conflicto con la Institución en una situación o circunstancias futuras.

Los **conflictos de interés aparentes** podrían ser cuando el personal del Banco no tiene un interés actual, pero terceros podrían estimar, suponer o percibir que sí existe dicho conflicto, lo cual puede tener efectos reputacionales, ya sea para el personal del Banco y/o para la Institución misma.

Por lo tanto, los miembros del personal del Banco deben prevenir, evitar o gestionar, de acuerdo con las circunstancias propias de cada caso, cualquier situación que cree o pueda crear un conflicto de interés en alguna operación, sea esta activa o pasiva, o en algún procedimiento de adquisiciones, así como cualquier asunto que influya de manera indebida en su criterio. Con ese propósito y para mejorar la comprensión de situaciones de esta índole, el Banco implementará acciones que ayuden al personal a identificar aquellas que pudieran generar algún tipo de conflicto. Para este efecto, la Oficina de Ética deberá desarrollar la normativa y los protocolos requeridos en ese sentido.

Artículo 20. Posibles conflictos de interés. Un conflicto de interés puede surgir de varias maneras. A continuación, se describen, de forma enunciativa más no limitativa, algunos de los conflictos de intereses más comunes y se brinda información sobre cómo resolverlos.

(a) Interés financiero. Se entiende por interés financiero cualquier posibilidad de recibir intereses, dividendos, apreciaciones de capital, honorarios u otros pagos o beneficios monetarios, económicos o en especie.

El personal del Banco deberá evitar conflictos de interés, **reales** o **aparentes** entre sus propios intereses financieros, los de su cónyuge o de sus parientes y los intereses del Banco.

Por lo anterior, el personal del Banco deberá abstenerse de participar, conocer e influir en cualquier etapa del proceso de toma de decisiones, en cualquier asunto en las que tenga una relación de propiedad la persona jurídica que sea contraparte directa y receptora o beneficiaria de recursos del BCIE.

Una relación de propiedad se establece cuando el miembro del personal, su cónyuge o sus parientes poseen participación accionaria o de capital de al menos 5% por ciento en la persona jurídica contraparte del BCIE o al menos el 25% de participación en una persona jurídica que a su vez posea un 5% por ciento de acciones en la contraparte directa del BCIE.

A continuación, se enumeran, de manera ilustrativa y no limitativa, algunas prácticas con tendencias adversas como ejemplos de conflicto de interés que podrían presentarse y que, según proceda, siempre estarán sujetas a la valoración de la Oficina de Ética y, en su caso, al Comité de Ética:

- (i)** Realizar transacciones a corto plazo en títulos emitidos por el Banco.
- (ii)** Poseer un interés financiero en un préstamo otorgado por el Banco a terceros o a una entidad con la que exista relación de propiedad.
- (iii)** Poseer un interés financiero en una entidad vinculada a una operación activa o pasiva del BCIE, que mantenga otro tipo de relación financiera con este o que sea proveedora del Banco.

Lo anterior incluye cualquier interés financiero en prestatarios, acreedores o proveedores del Banco, o en un organismo executor de una actividad financiada por este que razonablemente pudiera ser percibido como una influencia en la toma de decisiones.

(b) Participación en actividades fuera del Banco (actividad política o de otra índole). El personal del Banco deberá trabajar para el BCIE a tiempo completo. Consecuentemente, el

referido personal deberá cumplir con lo establecido en el Reglamento de Organización y Administración (ROA) del BCIE y en el Reglamento General de Administración de Recursos Humanos, indistintamente de cuál sea su cargo, y no podrá dedicarse a ocupaciones distintas a las del Banco o asumir cargos o posiciones que sean incompatibles con el desempeño correcto de sus deberes o que puedan ocasionar compromisos o dificultades para la Institución.

Si bien el personal puede tener interés en asuntos cívicos y políticos de sus respectivos países, se debe mantener cautela a fin de no afectar su condición de miembros del personal del BCIE. Consecuentemente, debe abstenerse de participar en actividades políticas partidarias o emitir comentarios, juicios u opiniones de esa naturaleza en ámbitos que puedan comprometer la reputación del Banco. Asimismo, ningún miembro de su personal podrá aceptar cargo público o político alguno, sea remunerado o no. El miembro del personal del Banco deberá renunciar a su empleo en el BCIE antes de aceptar una candidatura o ser electo o nombrado para cargos políticos o de elección popular.

En atención a lo indicado en el primer párrafo de este acápite, un miembro del personal no podrá ejercer relaciones y funciones de administración en otra persona jurídica. Una relación de administración se establece cuando el miembro del personal ejerce algún cargo de director o miembro de la junta directiva, representante legal, administrador único, gerente general o similares, o tiene firma autorizada, ya sea que tenga o no participación en el capital de tales personas jurídicas.

Lo anterior no es aplicable a sociedades mercantiles familiares creadas con el propósito exclusivo de administrar el patrimonio familiar, o asociaciones civiles cuyo ámbito de acción no tenga relación alguna con las del BCIE o que no implique alguna incompatibilidad con el desempeño de sus funciones en el Banco, siempre que se efectúen a título individual y no como empleado del Banco. Por incompatibilidad se entenderá que estén dentro del mismo giro del Banco, que puedan proveer servicios a este o que, de alguna manera, puedan suponer un conflicto de interés.

(c) Empleos anteriores y posteriores al BCIE. El personal del Banco deberá evitar conflictos relacionados con un antiguo o un probable empleador.

(i) Empleo anterior. Salvo con la autorización del Comité de Ética, y durante un período de cinco años a partir de su incorporación al Banco, el personal se debe abstener de participar en decisiones que afecten a un antiguo empleador. Si al cabo de ese período aún existe un posible conflicto de intereses, real o aparente, se debe consultar a la Oficina de Ética antes de desempeñar cualquier tarea relacionada con el antiguo empleador. Lo anterior no es aplicable en caso que el empleador anterior haya sido el Estado o un organismo internacional.

(ii) Empleo probable. Se prohíbe que el desempeño de las funciones del personal del Banco se vea condicionado o afectado de cualquier manera por la posibilidad de obtener un empleo o poder dedicarse a futuro a actividades profesionales o técnicas independientes fuera del BCIE.

(iii) Empleo subsiguiente. El Banco reconoce la libertad de cada miembro del personal de obtener empleos o de dedicarse a actividades en el ejercicio de su profesión a partir de la terminación de su relación con el BCIE. En el desarrollo del nuevo empleo, o de sus actividades posteriores, podrán utilizar la experiencia y conocimiento acumulados durante la vigencia de su relación con el Banco, a menos que implique la divulgación de información considerada como de uso interno, confidencial o restringida por el plazo que determine la Política de Seguridad de la Información.

No obstante, durante un período de cinco años posterior a la terminación de la relación con el BCIE, las dependencias responsables dentro del Banco evitarán que exmiembros del personal participen en operaciones o actividades del BCIE con el sector privado, siempre que el exmiembro de que se trate haya tenido alguna participación directa en esa operación o actividad particular durante la vigencia de su relación con el BCIE.

(d) Relaciones familiares o personales. El personal del Banco deberá evitar conflictos de interés que deriven de una relación familiar, de parentesco o personal con otro miembro del personal del BCIE.

En el marco del Código de Ética, la definición de pariente o familiar incluye al cónyuge o compañero de hogar de un miembro del personal del BCIE, así como los individuos relacionados con este por lazos de consanguinidad (incluyendo vínculos por adopción) hasta el cuarto grado o por lazos de afinidad hasta el segundo grado, pudiendo derivarse estos de relación de matrimonio o de unión de hecho. Cuando se utilice el término "pariente" o "parentesco" deberá entenderse que se refiere a los individuos que quedan incluidos en esta definición o al vínculo que existe en virtud de los lazos antes referidos.

Tener a un pariente dentro de la línea de mando, ejercer supervisión o control sobre un pariente o que ambos laboren en la misma dependencia, podrían crear o dar la apariencia de un conflicto de interés para un miembro del personal del BCIE. Asimismo, los miembros del personal del Banco no podrán tomar decisiones en el ámbito laboral o comercial que involucren a un individuo con quien tiene una relación personal, familiar, de parentesco, sentimental o de amistad cercana o íntima, ya sea que este se desempeñe como personal del BCIE, o bien, como proveedor, contratista o cliente del Banco. En tal sentido, su personal no deberá involucrarse en la asignación de tareas, evaluación de desempeño, encuestas de satisfacción o evaluación de servicios, entre otras, que se den con respecto a esa persona.

Adicionalmente, se considerará conflicto de interés cualquier relación sentimental entre un superior y un subordinado que no haya sido reportada oportunamente. En concordancia con lo anterior, el Banco insta al personal a evitar este tipo de relaciones.

Para prevenir conflictos de interés, todas las situaciones anteriores deben ser informadas a su superior inmediato y a la Oficina de Ética en cuanto tenga conocimiento de forma inmediata. A tal efecto, esta Oficina desarrollará la normativa y los protocolos necesarios.

Además, en el caso específico que un miembro del personal del BCIE se entere que un familiar se está postulando para trabajar en el Banco, debe informarlo a la Oficina de Recursos

Humanos y a la Oficina de Ética en cuanto tome conocimiento de lo anterior a fin que se adopten las medidas preventivas necesarias.

(e) Adquisiciones y contrataciones. Los colaboradores del BCIE deben abstenerse de favorecer a cualquier persona en un proceso de contratación de bienes y servicios o laboralmente por tener una relación cercana o de parentesco con esta, lo mismo que influir para que dicha persona obtenga un beneficio.

En el caso que un miembro del personal del Banco identifique una situación en la cual un pariente, amigo o socio tiene un interés en alguna operación o actividad del BCIE (incluyendo un interés en el ámbito laboral o de contratación de bienes y servicios) que podría generarle un conflicto de interés (real o aparente), deberá comunicar la situación a su superior inmediato, abstenerse de participar en el proceso y, en su caso, solicitar asesoramiento en la Oficina de Ética.

(f) Regalos y favores. Se refiere a cualquier tipo de gratificación que se reciba de personas externas al Banco, tales como alimentación, transporte, alojamiento, invitaciones a eventos de entretenimiento (culturales, deportivos o de otra índole), descuentos, préstamos, dinero en efectivo o sus equivalentes, pudiendo ser estas tarjetas de regalo, vales o créditos y, en general, cualquier tipo de compensación, beneficio económico, contribución monetaria o en especie.

En términos generales, el personal del Banco no podrá aceptar regalos o favores de terceros relacionados que puedan comprometer o dar la apariencia de comprometer su objetividad e integridad en el cumplimiento de sus funciones, salvo los que la normativa vigente autorice. Asimismo, se prohíbe que el personal del Banco solicite regalos o favores de un tercero relacionado.

Terceros relacionados. A los efectos de aplicación de esta disposición, se entiende como terceros relacionados con el BCIE a toda persona natural o jurídica con la que el Banco planea establecer o establezca una relación comercial o un vínculo contractual de cualquier naturaleza, ya sea con la intención de otorgar o autorizar todo tipo de operación activa, pasiva, de preinversión, cooperación técnica o financiera, donación, patrocinio o como proveedor de bienes, servicios o consultorías dentro de los procedimientos de adquisiciones institucionales o aquellos que se realicen con recursos del BCIE en sus operaciones.

Lo anterior incluye, más no se limita, a cualquier prestatario, beneficiario, contratista, proveedor u oferente, que lo sea actualmente o que haya demostrado formalmente su interés en serlo.

Tomando en cuenta lo anterior, únicamente se podrán aceptar regalos o invitaciones cuando se cumpla con todas las siguientes condiciones:

- (i)** Su valor nominal no exceda de los doscientos dólares, moneda de Estados Unidos de América o su equivalente en moneda local.
- (ii)** El valor acumulado de todos los regalos o invitaciones provenientes de una misma persona o entidad jurídica no exceda en los últimos doce (12) meses el valor establecido en el inciso anterior.

- (iii) No se trate de dinero en efectivo, monedas electrónicas o sus equivalentes.
- (iv) No hayan sido solicitados por el personal del BCIE.
- (v) Sean consistentes con los estándares éticos y las prácticas comerciales generalmente aceptadas.
- (vi) El regalo o la invitación no sea contingente a la realización de una contraprestación ni cree una obligación o una expectativa a la contraparte.

Invitaciones. En el caso de invitaciones, seminarios o talleres, el personal del Banco podrá aceptar que un tercero relacionado realice pagos (parciales o totales) de gastos asociados a eventos que atenderá el personal, si cuenta con la autorización previa y declara ante el Oficial de Ética que no existe un conflicto de interés actual y que con su participación no se generará un conflicto de interés.

Instancias de autorización.

- (1) El Directorio para el Presidente Ejecutivo, los Directores y los titulares de las dependencias adscritas al Directorio.
- (2) Para el Vicepresidente Ejecutivo, el Presidente Ejecutivo.
- (3) Para el Contralor, el Comité de Contraloría.
- (4) Para el personal de las direcciones, el Director correspondiente.
- (5) Para el personal de las oficinas adscritas a la Asamblea de Gobernadores o al Directorio, el jefe respectivo.
- (6) Para el resto del personal del BCIE, el Vicepresidente Ejecutivo.

Asimismo, el personal del Banco podrá aceptar alimentación o transporte local y cortesías conexas siempre que su valor nominal no exceda de los límites establecidos en la presente normativa, cuando estén naturalmente asociadas a sus funciones relacionadas con los negocios del Banco y siempre que su aceptación no comprometa la objetividad e independencia de criterio en forma real o aparente.

Si en determinadas circunstancias la negativa a aceptar un regalo o favor no solicitado con un valor nominal superior a los límites antes señalados, puede causar una molestia al donante o al BCIE, o interpretarse como una ofensa, el miembro del personal del Banco podrá aceptarlo en representación de la Institución, siempre y cuando comunique de manera inmediata la situación a la Oficina de Ética, quien emitirá un Dictamen de Conflicto de Interés con su opinión técnica y solicitará, si aplica, su registro a la dependencia de Servicios Administrativos y Adquisiciones Institucionales (SAAI) como activo propiedad del Banco.

Para efectos prácticos de lo anterior, la Oficina de Ética estará facultada para emitir instructivos, protocolos y guías que se consideren convenientes.

El personal del Banco se abstendrá de brindar regalos o hacer favores de valor significativo que puedan influir en las decisiones o acciones de personas que hacen negocios con el BCIE.

Obsequios institucionales. Se excluye de esta disposición los obsequios institucionales que de tiempo en tiempo el Banco adquiere para ser distribuidos como obsequio a los miembros del personal del BCIE, los proveedores y clientes actuales y potenciales de la Institución. No obstante, por medio de la normativa del Banco se procurará que estos obsequios sean de bajo

costo, evitando que haya grandes erogaciones en este sentido, aplicando para este cometido los principios de la razonabilidad y la austeridad.

Artículo 21. Divulgación de conflictos de intereses. Cuando surja un conflicto o una situación con potencial de convertirse en un conflicto, el personal del BCIE debe procurar solicitar orientación de su supervisor y comunicarlo inmediatamente a la Oficina de Ética. La Oficina de Ética puede asesorarle para evitar entrar en un conflicto o, si un conflicto ya se ha identificado, puede ayudarle a actuar de manera proactiva para prevenir que la situación escale a una denuncia de conducta indebida.

SECCIÓN 4. DEL VALOR DE LA INTEGRIDAD

Artículo 22. Integridad. El personal del BCIE debe observar una conducta honesta, veraz y libre de toda influencia corrupta, sustentada en la verdad, la honradez, la rectitud, la justicia, la excelencia, la prudencia y la discreción en todas sus actuaciones, salvaguardando la información confidencial y evitando cualquier declaración pública o acción que pueda comprometer o dar la apariencia de comprometer el desempeño de sus funciones oficiales o perjudicar la reputación del Banco. Asimismo, el personal debe cumplir las normas y reglamentos del Banco, así como las leyes locales aplicables.

El personal del BCIE debe proveer información verdadera, exacta y oportuna en el desempeño de sus funciones o en otras situaciones en que se requiera divulgación de información, nunca se debe tergiversar intencionalmente la verdad. La integridad y la discreción deben guiar sus acciones cuando se brinde información a otros, tanto dentro como fuera del Banco.

Artículo 23. Fraude interno u ocupacional y corrupción. Fraude interno u ocupacional se define como el uso de la ocupación o empleo para el enriquecimiento personal del individuo, en forma directa o indirecta, a través del mal uso deliberado o mala aplicación de los procesos, recursos o activos del Banco.

El personal del Banco deberá realizar sus funciones con integridad, ética y transparencia, por lo que la participación en cualquier situación que se pueda calificar como fraude interno u ocupacional se considerará como una acción que atenta directamente contra los principios institucionales y los valores éticos del Banco y contra el desempeño de sus obligaciones como colaboradores. A su vez, el Banco establecerá los mecanismos de control interno necesarios y, por medio de la Oficina de Ética, capacitará continuamente a su personal en contra de dichas prácticas.

Fraude interno u ocupacional. Se considera que hay fraude interno u ocupacional cuando el personal del BCIE incurre en algunas de las formas de corrupción que a continuación se enlistan, de manera enunciativa más no limitativa:

- (a) Un esquema de fraude por el cual un miembro del personal abusa de su influencia en una transacción de negocios de manera tal que viola su deber hacia el Banco con el fin de obtener un beneficio directo o indirecto. La corrupción puede materializarse cuando existe conflicto de interés, por lo que es obligatorio que cualquier situación que se considere como tal se gestione de acuerdo con lo estipulado en el apartado respectivo del presente código y en sus normas y procedimientos complementarios.

- (b) Cuando se ofrece, da, recibe o solicita una cosa de valor para influir en una decisión de negocio.
- (c) Cuando exista malversación y apropiación ilegal de activos, que ocurre cuando un miembro del personal sustrae o hace mal uso de los recursos o información del Banco.

Los siguientes son ejemplos ilustrativos, más no limitativos, de malversación y apropiación ilegal de activos:

- (i) Sustracción de dinero en efectivo disponible.
 - (ii) Desembolsos fraudulentos.
 - (iii) Uso indebido o sustracción de los activos del Banco.
- (d) Un esquema de fraude en estados financieros por el cual un miembro del personal intencionalmente realiza una declaración falsa u omite información relevante en los informes financieros del Banco.

Algunos ejemplos de fraude en estados financieros pueden ser los siguientes:

- (i) Sobrestimación de ingresos/activos.
- (ii) Subestimación de ingresos/activos.

Artículo 24. Uso adecuado de la información. Los activos físicos de información y la propiedad intelectual son esenciales para las actividades del BCIE y son considerados, después del capital humano, uno de los activos más valiosos, por lo que el personal del BCIE tiene el deber de protegerlos. En tal sentido, todo el personal debe administrar y usar la información del Banco de manera responsable y proteger los registros y la información, tanto si pertenece al BCIE como a sus socios estratégicos, clientes o colaboradores, de conformidad con la Política de Seguridad de la Información del BCIE.

Por otra parte, el personal del BCIE deberá abstenerse de emitir comentarios, en público o frente a terceros, que desprestigien la buena imagen e institucionalidad del Banco. De forma enunciativa más no exhaustiva, se señalan las siguientes formas de uso inadecuado de la información:

(a) Declaraciones públicas. A fin de que el Banco se exprese clara y uniformemente, el personal no debe hacer declaraciones públicas en nombre del Banco o acerca de él, a menos que haya sido expresamente autorizado para hacerlo. Es importante que el personal tenga en cuenta que las opiniones o la información en nombre o acerca del Banco compartidas en internet también constituyen declaraciones públicas. Similarmente, solo representantes designados por el Banco podrán hacer declaraciones a la prensa en su nombre, quienes, por consiguiente, deberán evitar toda referencia u opinión personal.

(b) Uso personal de información. El personal del Banco que utilice información que haya obtenida en el curso de su relación laboral con este, debe adherirse a las políticas de Seguridad de la Información y de Acceso a la Información del BCIE, a sus principios institucionales, a los valores éticos y a las directrices específicas que figuran a continuación:

(i) Manejo de información interna, confidencial, reservada o no pública. Es obligación de todo el personal del BCIE proteger la confidencialidad de la información a la que haya tenido acceso por motivo de su cargo y en el ejercicio de sus funciones, tanto dentro como fuera del lugar de trabajo.

La información clasificada como no pública solamente puede compartirse con otros miembros del personal del Banco exclusivamente cuando sea necesaria para el ejercicio de sus funciones y nunca se debe revelar tal información fuera del Banco, sin aprobación previa. En el caso de las direcciones por país, este tipo de información podrá ser trasladada, según la línea de mando establecida, a los gobernadores por país, cuando así se considere prudente.

Asimismo, el personal del BCIE no debe utilizar información interna, confidencial, reservada o no accesible al público para favorecerse en lo personal o para favorecer a terceros.

Estas obligaciones permanecen vigentes aún después de la terminación de la relación de trabajo con el Banco, conforme con la normativa vigente en la Institución.

(ii) Información a disposición del público. La información obtenida en el ejercicio de funciones oficiales podrá ser usada únicamente para fines personales o para beneficio de otros, únicamente si dicha información se encuentra a disposición del público en general.

(iii) Información protegida por derechos de autor. El Banco es propietario de los derechos de autor de todo el material que su personal produzca como parte de sus funciones oficiales y por lo tanto tiene el derecho exclusivo de publicar o utilizarlo en la forma que juzgue apropiado. Si un miembro del personal del BCIE desea publicar o utilizar material que no se haya producido como parte de sus funciones en el Banco, pero que se refiera a este, debe obtener la autorización previa del Comité de Directores de Comunicaciones y de Acceso a la Información.

Todo el personal tiene la obligación de cumplir con la ley, respetar los derechos de autor de otros, al reproducir o transmitir material literario impreso o electrónico que haya sido suministrado por el Banco.

(c) Uso de los activos físicos y financieros del Banco. Los bienes propiedad del Banco comprenden activos físicos y financieros tales como instalaciones, equipos, materiales de oficina, computadoras y recursos financieros. El BCIE encomienda a su personal el uso de tales activos en el mejor interés institucional y de las partes interesadas, con el propósito de facilitar la labor asignada. Esto implica la responsabilidad del personal en su utilización apropiada y la protección contra daños, pérdida, hurto o uso inadecuado.

(d) Propiedad intelectual. La propiedad intelectual del BCIE es otro activo valioso que el personal debe proteger en todo momento. La propiedad intelectual incluye derechos de autor, patentes, marcas, derechos de diseño, logotipos y nombres distintivos, así como el nombre y los símbolos del Banco.

(e) Uso de los sistemas computarizados del Banco, dispositivos y el acceso a Internet. La propiedad del Banco también incluye sus sistemas de computación, *hardware*, *software*, correo electrónico, acceso a Internet, teléfonos y cualquier otro dispositivo electrónico de comunicación y almacenamiento de información.

Es responsabilidad del personal del BCIE hacer uso profesional, ético y lícito de los equipos del Banco. Está prohibido crear, descargar, buscar, almacenar, copiar o transmitir material que sea sexualmente explícito o que muestre o promueva la discriminación racial, étnica, religiosa o de cualquier otro tipo. En toda circunstancia se espera que el personal haga uso de buen juicio al utilizar los bienes propiedad del Banco, tomando en cuenta la posibilidad de que el uso y la transmisión de determinados contenidos pueden ofender o incomodar a otros. También es importante recordar que no existe ninguna expectativa de privacidad en la utilización de los equipos o sistemas del Banco.

(f) Uso apropiado de las redes sociales. Las redes sociales representan, entre otras cosas, la apertura a nuevos espacios de conexión, socialización, encuentro, intercambio y conocimiento. Gracias a ellas hoy en día es muy sencillo compartir información y los colaboradores del BCIE deben mantener y cuidar su imagen al compartir información.

El BCIE reconoce la dificultad que puede haber en desvincular el ámbito personal de la función institucional que se desempeña, por lo que el uso de las redes sociales personales nunca deberá poner a la Institución en riesgo. Los colaboradores del BCIE deben hacer buen uso de las redes sociales, respetar a la audiencia y a sus compañeros, no publicar opiniones personales o alguna otra referencia no autorizada en nombre de la Institución.

En ese entendido, reconoce que estas herramientas pueden brindar canales actuales e innovadores para interactuar entre colaboradores y en ocasiones utilizarse con fines personales, empleando tecnologías suministradas por el Banco. Al hacer uso de las redes sociales –asociadas o no al BCIE– se deben tener presentes las siguientes normas:

- (i)** Proteger siempre los activos, la reputación y la información confidencial del Banco, sin olvidar que el Internet es un espacio público.
- (ii)** Utilizar de guía el presente código al tomar decisiones de carácter ético.
- (iii)** Seguir las políticas y estándares del Banco para el uso de sus activos tecnológicos, tanto si se interviene en calidad de agentes autorizados por este, como si se utilizan las redes y medios sociales a título personal.
- (iv)** Abstenerse de utilizar las redes sociales para ejercer cualquier tipo conducta indebida, contraria a las buenas costumbres en el ámbito de los principios institucionales y los valores éticos contenidos en el presente código.

SECCIÓN 5. DEL VALOR DE LA TRANSPARENCIA

Artículo 25. Transparencia. Las actividades y comunicaciones del BCIE se llevarán a cabo con claridad, sin duda ni ambigüedad y sin esconder u omitir cualquier tipo de información, evitando, en toda circunstancia, incurrir en situaciones de riesgo.

Artículo 26. Reportes y mantenimiento de registros. Los libros y registros del BCIE deben reflejar las transacciones operativas de forma completa y precisa. Estos registros deben estar

siempre de acuerdo con el sistema de control interno y las normas financieras y contables vigentes.

Artículo 27. Gestión, retención y eliminación de registros. Los registros del BCIE son un componente fundamental para fomentar la confianza de los clientes, proveedores y socios del Banco. A tal efecto, la Institución cuenta con políticas que orientan la gestión de los registros y plazos de conservación. Por tanto, el personal debe observar las políticas de gestión de registros y los plazos de conservación de estos en todos los países en los que opera el BCIE. Asimismo, tiene la obligación de denunciar a las instancias respectivas, cuando exista alguna sospecha o indicio de que alguien haya indebidamente ocultado, alterado o destruido algún registro.

CAPÍTULO III. DE LAS RESPONSABILIDADES DERIVADAS DEL CÓDIGO DE ÉTICA

Artículo 28. Los órganos de gobierno del Banco en materia de Ética. La promoción de los principios institucionales y de los valores éticos y la prevención de conductas indebidas son prioritarios para el Banco. En ese sentido, los miembros de los órganos de gobierno del Banco están comprometidos a fomentar y mantener un ambiente de trabajo que favorezca un comportamiento ético que estimule activamente un diálogo abierto en materia deontológica.

Los miembros de dichos órganos, mediante sus acciones y comunicaciones, demostrarán su adherencia a los siguientes comportamientos básicos:

- (a) Asegurar un tratamiento justo e imparcial para todo el personal;
- (b) Garantizar un entorno de trabajo basado en los valores éticos;
- (c) No tolerar el abuso en el ejercicio de autoridad;
- (d) Rendir cuentas sobre los asuntos inherentes a las obligaciones y responsabilidades de su personal como tomadores de decisión.
- (e) Proporcionar las herramientas pertinentes para lograr una adecuada gestión de la ética.
- (f) Proteger a los miembros del personal del Banco contra las represalias de todo tipo, incluyendo las que se pudieran tomar en contra de denunciantes y testigos de buena fe, que reporten o colaboren en investigaciones que se lleven a cabo sobre supuestas conductas indebidas.

SECCIÓN I. DEL DIRECTORIO

Artículo 29. Del Directorio. El Directorio, como órgano responsable de la dirección del Banco y superior inmediato del Presidente Ejecutivo, está sujeto a las disposiciones contenidas en el Convenio Constitutivo, en el Reglamento de la Organización y Administración (ROA) y en cualesquiera otras disposiciones vigentes o las que, en el futuro, dicte la Asamblea de Gobernadores y le resulten aplicables. En tal sentido, ejercerá todas las facultades que le delegue la Asamblea de Gobernadores en materia de ética, entre ellas:

- a) La aprobación del presente Código de Ética y sus Normas y Procedimientos Complementarios, así como sus modificaciones.
- b) Poner en conocimiento de la Asamblea de Gobernadores el texto aprobado del Código de Ética y sus Normas y Procedimientos Complementarios, así como cuando sean objeto de cualquier modificación.
- c) La designación del Director propietario y suplente para integrar el Comité de Ética, quien tendrá las funciones de Presidente del Comité.

- d) Realizar la interpretación auténtica, con carácter normativo, del Código de Ética y sus Normas y Procedimientos Complementarios en los casos de ambigüedad o falta de claridad de dichas disposiciones.

SECCION II: DE LA PRESIDENCIA EJECUTIVA

Artículo 30. De la Presidencia Ejecutiva. El Presidente Ejecutivo es el funcionario de mayor jerarquía en la conducción administrativa del Banco y tiene la representación legal de la institución. Bajo la dirección del Directorio le corresponde cumplir y hacer cumplir el Convenio Constitutivo, los reglamentos, las resoluciones y los acuerdos de la Asamblea de Gobernadores y el Directorio, así como las demás disposiciones que regulan el Banco y particularmente todas aquellas relativas al Código de Ética y sus Normas y Procedimientos Complementarios.

Entre su autoridad y funciones en materia de ética, le corresponderá la aprobación, a propuesta de la Oficina de Etica, de la normativa necesaria para una efectiva implementación del Código de Ética y sus Normas y Procedimientos Complementarios.

SECCION III. DEL COMITÉ DE ÉTICA

Artículo 31. Del Comité de Ética. El Comité de Ética es el órgano responsable de coadyuvar en el fortalecimiento de la ética institucional de acuerdo a lo establecido en las disposiciones contenidas en el Código de Ética y en las Normas y Procedimientos Complementarios al Código de Ética.

Artículo 32. De las Funciones del Comité de Ética. La función principal del Comité de Ética es la de ser el órgano responsable de conocer y resolver sobre los asuntos relacionados con las conductas indebidas y las infracciones a los principios institucionales y valores éticos contenidos en el Código de Ética.

Además, coadyuvará al fortalecimiento de la ética institucional, desarrollando las funciones adicionales:

- (a) Monitorear y evaluar los lineamientos y el desempeño de la organización y su personal en materia de ética.
- (b) Promover la cultura ética en todos los estratos de la organización del Banco mediante un plan de acción anual propuesto por la Oficina de Ética, que contenga al menos los siguientes aspectos:
 - 1. Programación de charlas o exposiciones institucionales sobre temas de ética.
 - 2. Planificación de actividades orientadas a promover una cultura de ética y de los principios y valores institucionales.
- (c) Recomendar el informe anual sobre el cumplimiento de dicho plan de acción y del cumplimiento del personal del Banco en cuanto a la remisión de las declaraciones exigidas por la normativa vigente en relación con la gestión de la ética.
- (d) Proponer las actualizaciones de las normativas éticas o de una nueva normativa.

Asimismo, le corresponden las funciones de apoyar al Directorio en conocer y evaluar las acciones realizadas por la Oficina de Ética enfocadas al desarrollo de estrategias relacionadas con la promoción de la cultura ética y el monitoreo del desempeño de la Institución y su

personal en dicha materia, incluyendo sus propuestas de actualización o de una nueva normativa.

También corresponderá al Comité de Ética, de así considerarlo pertinente, sobre la base de caso por caso y en atención a la complejidad y naturaleza de la presunta infracción al Código de Ética, determinar la necesidad de contar con apoyo especializado interno o externo para efectos de llevar a cabo la investigación de los procedimientos administrativos correspondientes.

Artículo 33. De la Conformación del Comité de Ética del Banco. El Comité de Ética, para los propósitos señalados en los párrafos precedentes, estará conformado por:

- (a) Un Director, quien tendrá las funciones de Presidente del Comité. Dicho Director será designado por el Directorio del Banco con rotación anual. El Directorio designará, además, a su suplente con rotación anual.
- (b) El Vicepresidente Ejecutivo.
- (c) El Contralor.
- (d) El Asesor Jurídico.
- (e) Oficial de Ética.

Todos los miembros del Comité de Ética actuarán con voz y voto, a excepción del Oficial de Ética y el Asesor Jurídico, quienes actuarán con voz pero sin voto. En el caso de que el Director que funge como miembro suplente participe en las reuniones del Comité, también lo hará con voz pero sin voto.

El Presidente del Comité de Ética deberá convocar a los miembros de dicho Comité para conocer los asuntos de su competencia. Una vez instalado el Comité, para conocer de un asunto en particular, será responsabilidad de este cumplir con las respectivas etapas del procedimiento administrativo a fin de resolver sobre el mérito de la causa.

Todas las cuestiones de procedimiento necesarias para la buena marcha del Comité de Ética que no estuvieren previstas expresamente en la presente normativa serán definidas por el Directorio, en coordinación con el Presidente del Comité de Ética.

Un funcionario de la Oficina de Ética designado por el o la Oficial de Ética desempeñará el papel de Secretario del Comité de Ética y estará a cargo de la gestión de los trámites administrativos.

El proceso administrativo comenzará tras la aceptación de la competencia por parte del Comité de Ética.

Los miembros del Comité de Ética no podrán delegar su participación en dicho Comité. No se considerará que se ha delegado la participación cuando se haya nombrado un encargado temporal de la dependencia de manera oficial.

Artículo 34. De la Sustitución de los miembros del Comité de Ética. Cuando así lo resuelva el Comité de Ética, la sustitución de cualesquiera de sus miembros en el evento que alguno

de ellos deba excusarse o sea recusado para conocer un caso en particular, se hará de la siguiente forma:

- (a) Cuando se trate del Director que funge como miembro titular del Comité de Ética, será sustituido por el Director que funge como miembro suplente.
- (b) Cuando se trate del Vicepresidente Ejecutivo, será sustituido por el Presidente Ejecutivo.
- (c) Cuando se trate del Contralor, será sustituido por el Auditor Interno del Banco.

El miembro titular del Comité de Ética que deba excusarse o sea recusado para conocer de un caso particular, no podrá participar en dicho Comité cuando el caso por el que se excusó o fue recusado esté en discusión, a menos que sea requerido por este para evacuar alguna diligencia, tal como ocurriría con cualquier otro miembro del personal.

Para los efectos de lo dispuesto en los párrafos precedentes, son causas de recusación o excusa las siguientes:

- (i) Cuando el denunciado como infractor a los valores éticos sea de la misma nacionalidad de alguno de los miembros del Comité de Ética.
- (ii) Cuando el denunciado sea miembro del Comité o de su grupo familiar inmediato, entendiéndose por este al cónyuge o compañero de hogar, o familiar dentro del cuarto grado de consanguinidad o segundo grado de afinidad.
- (iii) Cuando cualquier miembro del Comité o su grupo familiar inmediato o familiares dentro del cuarto grado de consanguinidad y segundo de afinidad tienen vínculos de negocios directos o indirectos con el denunciado como infractor a los principios institucionales o valores éticos.
- (iv) Cuando un miembro del Comité esté o haya sido denunciado por el encausado por supuestas infracciones a los principios institucionales y valores éticos.
- (v) Cuando un miembro del Comité mantenga una amistad íntima o enemistad manifiesta con el denunciado.
- (vi) Cuando el denunciado como infractor sea o haya sido subordinado del miembro del Comité de que se trate.
- (vii) En cualquier otro supuesto en que, a criterio del Comité de Ética, existan circunstancias que fundamenten la excusa o recusación de un miembro titular del mismo para conocer de un caso particular, con el propósito de garantizar la objetividad del procedimiento.

El miembro del Comité que corresponda, con la debida diligencia y anticipación, deberá declarar la existencia de los vínculos señalados en los numerales ii), iii) y v), así como de cualquier conflicto de interés que pudiera surgir en su relación con el denunciado.

SECCIÓN IV. DE LA OFICINA DE ÉTICA

Artículo 35. De la Oficina de Ética. La Oficina de Ética es una dependencia adscrita al Directorio del Banco. Su titular es el Oficial de Ética, quien tendrá bajo su responsabilidad promover y dar seguimiento al cumplimiento de las disposiciones contenidas en el Código de Ética y en las Normas y Procedimientos Complementarios al Código de Ética, principalmente por medio de programas educativos, de manera que contribuya a la buena gobernanza del Banco y ayude a preservar y promover la integridad institucional, implementando un enfoque preventivo que fortalezca el ambiente ético de la Institución. Asimismo, tendrá la responsabilidad de la aplicación, implementación y seguimiento de las disposiciones y resoluciones emitidas por el Comité de Ética.

Artículo 36. Del Oficial de Ética. El Oficial de Ética será el encargado de brindar asesoramiento, en todos los niveles del Banco, sobre el comportamiento ético e informar sobre los problemas de ética a las instancias pertinentes. Asimismo, le corresponde investigar las denuncias que se interpongan a través de los canales correspondientes sobre las conductas que se aducen contrarias al Código de Ética y trabajará con otras dependencias del Banco para promover el cumplimiento de la normativa ética. Además, velará que todos los niveles de la organización cumplan o excedan las expectativas en esta materia.

Las responsabilidades del Oficial de Ética y de la Oficina de Ética serán las establecidas en el Reglamento Interno del Directorio y de las Dependencias Adscritas (RIDDA), además de aquellas que se señalen en otra normativa vigente.

SECCIÓN V. DE LA ASESORÍA JURÍDICA

Artículo 37. Del Asesor Jurídico. El Asesor Jurídico del Banco participará en el Comité de Ética para velar por el cumplimiento del debido proceso y mantener el orden y la equidad en las sesiones del comité. Acompañará, además, al Oficial de Ética en la presentación de información, documentación, participación de las partes, pruebas en el procedimiento y tendrá la responsabilidad de informar al Comité sobre cualquier irregularidad identificada durante el proceso administrativo, asegurando su integridad.

SECCION VI. DE LA OFICINA DE RECURSOS HUMANOS

Artículo 38. De la Oficina de Recursos Humanos. La Oficina de Ética, en el cumplimiento de sus atribuciones, deberá mantener una estrecha colaboración con la Oficina de Recursos Humanos como instancia encargada de diligenciar los conflictos laborales que se originen en la implementación de este código. Para este efecto, se deberá implementar la figura de la mediación como fórmula alterna de solución de conflictos, la que deberá gestionarse desde esta oficina. La Oficina de Recursos Humanos desarrollará la normativa y los protocolos necesarios y establecerá los procesos requeridos para este efecto. En ningún momento se debe entender este proceso como un obstáculo para acceder a la Oficina de Ética.

SECCION VII. DEL SUPERVISOR

Artículo 39. Del Supervisor. El personal del Banco que desempeña puestos a nivel de dirección, administración superior, gerencial y mandos medios que realicen funciones de autoridad inmediata superior, para efectos del proceso de evaluación del desempeño, juegan un papel activo y tienen responsabilidades adicionales en materia de ética y conducta, así como en la promoción de una cultura deontológica en el Banco. En particular, son obligaciones de las y los supervisores, las siguientes:

- (a) Actuar como modelos a seguir, demostrando consistentemente comportamientos y actitudes que reflejen los estándares de este código.
- (b) Respalda el código y asegurar que el personal que les colabora entiende los comportamientos que se les requieren.
- (c) Generar un entorno de trabajo positivo, inclusivo y de respeto en el que el personal al que supervisa se sienta cómodo en plantear preguntas e inquietudes.
- (d) Ser los primeros en actuar para atender situaciones en el lugar de trabajo que, de no ser atendidas adecuadamente, podrían escalar a violaciones a las disposiciones del Código u otros problemas más serios.

- (e) Comunicar inmediatamente a la Oficina de Ética toda conducta indebida.
- (f) Nunca tomar ni permitir que se tomen represalias contra personas que hayan informado de buena fe sobre sospechas de conductas indebidas.

Los supervisores también cumplen en el Banco un rol particular en el manejo de las inquietudes de los empleados sobre asuntos que se refieren a funciones asignadas de acuerdo con el puesto que ocupan. Los supervisores son responsables de mantener buenas relaciones de trabajo y un ambiente de respeto. Además de brindar a los empleados el consejo y la orientación adecuados, los supervisores deben estar disponibles a escuchar y responder a toda pregunta o queja que puedan tener los colaboradores sobre asuntos de trabajo.

Los conflictos de oficina deben abordarse en forma proactiva y, en lo posible, resolverse en una fase inicial con la necesaria sensibilidad e imparcialidad; en ese sentido, los supervisores pueden solicitar la asistencia de un representante, ya sea de la Oficina de Recursos Humanos o de la Oficina de Ética, con el propósito específico de intervenir como mediadores de cualquier conflicto suscitado.

En ese aspecto, el comportamiento ético comienza con las y los supervisores. Liderar con el ejemplo es la mejor manera de inspirar en otros un comportamiento ético y mantener un entorno de trabajo positivo y productivo.

SECCION VIII. DEL PERSONAL DEL BANCO.

Artículo 40. Del personal del Banco. El compromiso compartido para la gestión de la ética se asume desde la incorporación al Banco, y se reafirma al certificar el conocimiento del Código y al participar en cursos de capacitación sobre la materia. Es responsabilidad de cada miembro del personal del Banco leer, comprender y asumir los compromisos emanados del Código. Si en alguna ocasión no estuviese seguro de cómo actuar, cualquier miembro del personal del Banco podrá consultar con la Oficina de Ética.

El personal de todos los niveles del Banco son responsables de sus propias conductas o acciones y esperan que los demás colaboradores también lo sean.

Los valores éticos contenidos en el presente código y, en lo aplicable, los principios institucionales son de cumplimiento obligatorio y deberán ser la guía de comportamiento de cada integrante del personal del Banco de todos los niveles. Para su adecuada implementación, se recomienda al personal que exprese su opinión, solicite orientación o informe de cualquier acción que pudiera ser perjudicial para el colaborador o la imagen del Banco ante las autoridades institucionales. Si necesita orientación en su labor cotidiana, se puede consultar a cualquiera de las siguientes personas o dependencias:

- (a) Superior inmediato o supervisor.
- (b) Oficina de Recursos Humanos.
- (c) Oficina de Ética.

Además de esto, todo el personal del Banco tiene el deber de cooperar en investigaciones por conductas indebidas.

De presenciar una vulneración a una disposición de este código y negarse a participar en el proceso de investigación o, en su caso, no denunciarlo cuando por su posición jerárquica está en posibilidad de hacerlo, a juicio del Comité de Ética, podrá ser sujeto del proceso de investigación y las sanciones correspondientes.

Por lo anterior si fuera testigo de una conducta indebida deberá realizar las siguientes acciones:

- (i) Reportar de buena fe a través de los canales de denuncias establecidos o solicitar orientación sobre las acciones a realizar al supervisor o a la Oficina de Ética.
- (ii) Documentar o emplear cualquier medio a su alcance para dejar evidencia de la conducta indebida o las acciones que podrían estar en contra de lo establecido en el Código de Ética.
- (iii) Colaborar en el proceso de investigación a realizarse por la instancia correspondiente.

Con respecto al miembro del personal que fuese víctima o denunciante de una conducta indebida, además de las acciones anteriores, deberán cumplir con las medidas correctivas o preventivas que establezca la instancia correspondiente durante el proceso de investigación.

SECCION IX. DEL TRIBUNAL ADMINISTRATIVO.

Artículo 41. Del Tribunal Administrativo. El Tribunal Administrativo es un órgano colegiado, con función jurisdiccional y con atribuciones privativas y competencia para conocer, de conformidad con la normativa interna del BCIE que determine los casos específicos de procedencia, de los conflictos que puedan surgir entre el Banco y personal, tanto bajo eventual responsabilidad patronal del BCIE y con el cual el BCIE no tiene responsabilidad patronal, conforme lo establecido en el presente Código de Ética y sus Normas y Procedimientos Complementarios. Dicho Tribunal se regirá y funcionará conforme con las disposiciones de su Estatuto y por las propias disposiciones procedimentales que adopte el Tribunal en cada caso. Por lo anterior, las decisiones del Comité de Ética podrán ser apeladas ante dicho tribunal.

TÍTULO II. OTRAS DISPOSICIONES

Artículo 42. Normativa vinculante. Las normas internas, reglamentarias y administrativas del Banco deberán tutelar los principios institucionales y valores éticos contemplados en el presente código.

Artículo 43. Interpretación auténtica. En los casos en los que el Directorio realice una interpretación auténtica con carácter normativo del Código de Ética, deberán ser publicadas regularmente de manera que sean accesibles a todo el personal del Banco.

ANEXO

Disposiciones de Integridad

A. Contrapartes y sus Relacionados:

Todas las personas naturales o jurídicas que proporcionen al BCIE bienes y/o servicios, ya sea en su condición de proveedores, contratistas, consultores, (en adelante todos los anteriores serán denominados en este documento como “el proveedor”), así como cualesquiera otra condición análoga, en adelante referidos como Contrapartes y sus Relacionados, deberán abstenerse de realizar cualquier acto o acción que se enmarque o pueda catalogarse como Práctica Prohibida conforme lo establece el literal (B) siguiente del presente Anexo.

B. Prácticas Prohibidas:

En virtud de lo anterior, el BCIE ha establecido un Canal de Reportes como el mecanismo para denunciar irregularidades, así como la comisión de cualquier Práctica Prohibida, en el uso de los fondos del BCIE o de los fondos administrados por éste, mediante el sitio web institucional: <https://www.bcie.org/acerca-del-bcie/medios-de-denuncias>.

El personal del BCIE involucrado en los procesos de adquisiciones de bienes y/o contratación de servicios, así como las personas físicas y los representantes, funcionarios y empleados de las personas naturales o jurídicas que participen como proveedores de dichos bienes y servicios, han y deberán observar los más altos niveles éticos durante todo el proceso de adquisición y durante la fase de ejecución contractual. En tal sentido y sin que esta enumeración sea taxativa, se considerarán prácticas prohibidas las siguientes:

- a) Soborno: Consiste en el ofrecimiento, suministro, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir impropriamente en la actuación o decisión de la persona competente para tomar decisiones en el proceso de adquisición de bienes y servicios que el BCIE esté realizando.
- b) Práctica Fraudulenta: Cualquier actuación u omisión, incluyendo una tergiversación de los hechos, que desoriente o pretenda desorientar a otra persona con el fin de obtener un beneficio indebido, financiero o de otra índole.
- c) Colusión: Consiste en las acciones entre oferentes destinadas a que se obtengan precios en cualquiera de los métodos de adquisición utilizados por el BCIE a niveles artificiales, no competitivos, capaces de privar a los demás participantes de los beneficios de una competencia libre y abierta.
- d) Práctica Coercitiva: Consiste en el hecho de amenazar a otro con causarle a él mismo o a miembros de su familia, en su persona, honra, o bienes un mal que constituyere delito, para influir en las decisiones durante cualquiera de los procesos de adquisición o contratación o durante la ejecución del contrato correspondiente, ya sea que el objetivo se hubiere logrado o no.

El Banco se reserva el derecho de resolver de forma unilateral el contrato sin necesidad de declaración judicial o extrajudicial alguna en caso se llegare a determinar que el proveedor seleccionado ha promovido o ejecutado estas prácticas.

C. Declaraciones y Obligaciones del Proveedor:

El proveedor trasladará a sus Relacionados (contratistas, subcontratistas, proveedores, supervisores, oferentes y similares) de forma expresa, las declaraciones y obligaciones del presente Anexo a la documentación contractual que rija la relación entre el proveedor con sus Relacionados, cuando la misma tenga relación directa con la contratación y suministro de bienes y servicios requeridos por el BCIE.

Declaraciones Particulares del proveedor:

El proveedor declara que:

a. Conocen el Canal de Reportes del BCIE, como un mecanismo para informar sobre irregularidades o la comisión de cualquier Práctica Prohibida en el uso de los fondos del BCIE o de los fondos administrados por éste.

b. Conservarán todos los documentos y registros relacionados con actividades contratadas por el BCIE por un período de hasta siete (7) años, contados a partir de la finalización del presente contrato.

c. A la fecha de suscripción del presente contrato no se ha cometido de forma propia ni a través de relacionados (funcionarios, empleados, representantes y agentes) o como cualquier otro tipo de relación análoga, en Prácticas Prohibidas.

d. Toda la información presentada es veraz y por tanto no ha tergiversado ni ocultado ningún hecho durante los procesos de selección, adjudicación o ejecución del presente contrato.

e. Ni ellos, ni sus agentes, su personal, contratistas, consultores, directores, funcionarios o accionistas (a) han sido inhabilitados o declarados por una entidad como inelegibles para la adjudicación de contratos financiados por cualquier otra entidad, o (b) han sido declarados culpables de delitos vinculados con Prácticas Prohibidas por parte de la autoridad competente.

f. Ninguno de sus directores, funcionarios o accionistas ha sido director, funcionario o accionista de una entidad que (a) se encuentre inhabilitada o declarada inelegible por cualquier otra entidad, o (b) haya sido declarado culpable de un delito vinculado con Prácticas Prohibidas por parte de la autoridad competente.

Obligaciones del Proveedor:

Son obligaciones del proveedor las siguientes:

- a. No incurrir en ninguna Práctica Prohibida en la ejecución del contrato de prestación de servicios requerido por el BCIE con fondos propios o fondos administrados por éste.

- b. Reportar, durante la ejecución del contrato, por medio del Canal de Reportes, cualquier irregularidad o la comisión de cualquier Práctica Prohibida relacionada con la contratación de bienes y servicios requeridos por el BCIE con fondos propios o fondos administrados por éste.

- c. En relación con las prácticas prohibidas reportadas, ya sea por el proveedor o por terceros, por medio del Canal de Reportes y en relación con el servicio objeto del Contrato, permitir y facilitar la realización de entrevistas a sus accionistas, directivos, ejecutivos o empleados de cualquier estatus, debiendo prestar toda la colaboración y asistencia que fuese necesaria en caso de cualquier auditoría o investigación proveniente del BCIE o de cualquier investigador contratado por el BCIE para tales efectos.

- d. En relación con las prácticas prohibidas reportadas, ya sea por el proveedor o por terceros, por medio del Canal de Reportes y en relación con el servicio objeto del Contrato, atender en el plazo establecido en las comunicaciones efectuadas por el BCIE, las consultas relacionadas con cualquier, indagación, inspección, auditoría o investigación proveniente del BCIE o de cualquier investigador, agente, auditor, o consultor apropiadamente designado, ya sea por medio escrito, virtual o verbal, sin ningún tipo de restricción.

- e. En los casos aplicables, reembolsar a solicitud del BCIE, los gastos o costos razonables vinculados con las actividades e investigaciones efectuadas en relación con la comisión de Prácticas Prohibidas.

Las Declaraciones y Obligaciones efectuadas por el proveedor contenidas en el literal C. son veraces y permanecerán en vigencia desde la fecha de firma del presente contrato, durante su vigencia y hasta la finalización del presente contrato a satisfacción del Banco.

D. Proceso de Auditoría e Investigación:

El BCIE se reservará el derecho de ejecutar los procedimientos de auditoría e investigación que le asisten.

El BCIE otorgará a las Contrapartes y sus Relacionados la oportunidad procesal para presentar sus argumentos de descargo a través de un procedimiento administrativo. Esto incluye, sin estar limitado solo a ello, el derecho del BCIE de compartir o hacer público el contenido de esa lista.

E. Lista de Contrapartes Prohibidas:

El BCIE podrá incorporar, a su entera discreción, a las Contrapartes y sus Relacionados en la Lista de Contrapartes Prohibidas, que para tal efecto ha instituido. La inhabilitación de

forma temporal o permanente en dicha Lista de Contrapartes Prohibidas será determinada caso por caso por el BCIE.

F. Aceptación de las Disposiciones de Integridad:

El proveedor reconoce que con la aceptación del presente Anexo se compromete a cumplir con la Política Antifraude, Anticorrupción y otras Prácticas Prohibidas del BCIE y demás normativa aplicable sobre la materia, acatando las acciones y decisiones del BCIE en caso de comprobarse la existencia de cualquier práctica contraria a estas regulaciones (normativas). La Política Antifraude, Anticorrupción y otras Prácticas Prohibidas del BCIE se encuentra disponible en el sitio web: <https://www.bcie.org/acerca-del-bcie/oficina-de-integridad-y-cumplimiento>

Este Anexo forma parte integral del presente contrato, por lo que el Proveedor acepta cada una de las disposiciones aquí estipuladas

POLÍTICA DE GESTIÓN DE RIESGO DE LAVADO DE ACTIVOS, FINANCIAMIENTO AL TERRORISMO, PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA, INTEGRIDAD Y SANCIONES

Versión 3

Gerencia de Riesgos

Público Una Vez Aprobado

De conformidad con el marco normativo de la Política de Acceso a la Información, el presente documento será divulgado en el sitio web externo del Banco después de su aprobación.

TABLA DE CONTENIDO

I. INTRODUCCIÓN	3
II. OBJETIVO	3
III. ALCANCE	4
IV. ABREVIATURAS Y TÉRMINOS	4
V. DEFINICIONES	5
VI. DOCUMENTACIÓN RELACIONADA	8
VII. DESARROLLO	9
1. GESTIÓN DE RIESGOS Y PRINCIPIOS BÁSICOS	9
2. RESPONSABLES EN LA GESTIÓN DE LA POLÍTICA	10
3. SISTEMA DE ADMINISTRACIÓN DE RIESGOS LA/FT/FPDAM, INTEGRIDAD Y SANCIONES	15
4. CONSIDERACIONES DEL RIESGO LA/FT/FPADM	17
5. CONSIDERACIONES DEL RIESGO DE INTEGRIDAD	17
6. CONSIDERACIONES DEL RIESGO DE SANCIONES	18
7. OTRAS DISPOSICIONES	19

I. INTRODUCCIÓN

En atención a los estándares internacionales, el Banco Centroamericano de Integración Económica (BCIE) dirige sus esfuerzos para la administración de los riesgos de Lavado de Activos, Financiamiento del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) con el fin de que sus productos y servicios no sean utilizados para dar apariencia de legalidad a los fondos que sean producto de actividades ilícitas o sirvan para canalizar recursos lícitos o ilícitos destinados a actividades terroristas o proliferación de armas de destrucción masiva.

Asimismo, el BCIE tiene la responsabilidad, en atención a su deber fiduciario, de cuidar los recursos de sus países miembros, previniendo la desviación de sus fondos hacia fines incompatibles con sus objetivos estratégicos y, por ello, mantiene controles en materia de integridad.

Por otro lado, las sanciones económicas y financieras tienen una variedad de fuentes y se emiten en apoyo de políticas nacionales e internacionales para prevenir y controlar el terrorismo, su financiación, el lavado de activos, sus delitos fuente, corrupción, la financiación de la proliferación de armas de destrucción masiva, abusos y violación en contra de los derechos humanos y diversos objetivos de relaciones internacionales.

El BCIE está comprometido a combatir los delitos financieros y hace su aporte en proteger la integridad del sistema financiero global, por medio de la ejecución de negocios responsables y seguros en las distintas jurisdicciones a nivel mundial en las que el Banco realiza operaciones con diferentes grupos de interés.

La emisión de la presente política es parte del compromiso del BCIE en la lucha contra el lavado de activos, financiamiento del terrorismo y financiación de la proliferación de armas de destrucción masiva y otras prácticas prohibidas, la administración del riesgo de sanciones, así como otros delitos financieros, que tengan relación directa con el riesgo de LA/FT/FPADM.

II. OBJETIVO

La presente política ha sido desarrollada con el propósito de establecer los lineamientos generales y complementarios que norman la administración del riesgo de LA/FT/FPADM, Integridad, Sanciones y Otros Delitos Financieros de manera conjunta, que tengan relación directa con el riesgo de LA/FT/FPADM en el BCIE; los cuales serán de aplicación y observancia general en todos los niveles del BCIE para generar una cultura institucional orientada a la prevención.

Estos lineamientos representan una guía para prevenir y mitigar los efectos que podrían producirse si la organización, sus operaciones o actividades son utilizadas como vehículo para lavado de activos, financiamiento del terrorismo y la financiación de la proliferación de armas de destrucción masiva y que se materialicen en prácticas prohibidas o cualquier delito financiero que tenga una relación directa con el riesgo LA/FT/FPADM, que impida el cumplimiento del deber fiduciario del BCIE, daños a la imagen y reputación derivados de sanciones y otras actividades conexas.

III. ALCANCE

La presente política, en conjunto con la normativa interna sobre la materia, es aplicable a todo el personal al servicio del BCIE en todos los niveles (directores, alta gerencia, funcionarios, empleados, contratistas, jóvenes profesionales, programas especiales y cualquier otra categoría establecida o que se establezca para la dotación de recurso humano al Banco) y a todas sus contrapartes según se define en esta política.

Estas directrices deberán observarse en todas las operaciones activas, pasivas, donaciones, patrocinios y de adquisición de bienes y/o servicios, institucionales o en el marco de las operaciones, en las que el BCIE participe con sus contrapartes y los relacionados de estas.

Estas directrices son complementarias al marco normativo vigente en materia de sanciones e integridad ya diseñado para el BCIE.

En aquellos casos en que el BCIE se vea afectado en sus intereses, patrimonio u obligaciones contractuales, como producto de la actuación u omisión de su personal, de cualquier contraparte o de un relacionado que conlleve el incumplimiento de los principios y normas incluidos en la presente política y demás normativa interna en la materia, se le aplicarán, según corresponda, las sanciones previstas en el Código de Ética del BCIE vigente y sus Normas y Procedimientos Complementarios, las obligaciones establecidas contractualmente referentes a la presente política o en la normativa que resultare aplicable, sin perjuicio de la responsabilidad legal que correspondiere.

IV. ABREVIATURAS Y TÉRMINOS

- Administración Superior: **Presidencia y Vicepresidencia Ejecutivas.**
- BCIE o Banco: **Banco Centroamericano de Integración Económica.**
- LA/FT/FPADM: **Lavado de Activos, Financiamiento del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.**
- GAFI: **Grupo de Acción Financiera.**

- GERIES: **Gerencia de Riesgos.**
- OFIC: **Oficina de Integridad y Cumplimiento.**

V. DEFINICIONES

- Actos sancionables: **significa cualquier trato, acuerdo, operación, o la entrada o ejecución de cualquier transacción que: (i) esté prohibido o sujeto a la aplicación de una sanción de cualquier naturaleza por un organismo sancionador, o (ii) podría esperarse razonablemente que forme la base de cualquier consecuencia negativa de sanciones para el BCIE.**
- Análisis de riesgo: **consiste en determinar la frecuencia (probabilidad de ocurrencia) con la que determinados eventos se pueden producir y la magnitud (impacto) de sus consecuencias. El análisis puede ser cualitativo y cuantitativo y debe tener en cuenta los controles existentes.**
- Banderas rojas: **serie de alertas que se deben observar y tener en cuenta tanto en la prevención como en la detección de LA/FT, sus delitos fuente, FPADM, sanciones y otras prácticas prohibidas, las cuales pueden variar según la naturaleza del delito.**
- Consecuencia negativa de sanciones: **significa cualquier determinación adversa material, multa, penalidad, castigo, orden administrativa, sanción (ya sea secundaria o no) u otra declaración, determinación o decisión de cualquier organismo sancionador que pueda tener una consecuencia material negativa para la persona aplicable.**
- Contraparte: **persona natural o jurídica con la que el BCIE planea establecer o establece una relación comercial o un vínculo contractual, o cualquier operación activa, pasiva, de preinversión, cooperación técnica, donaciones, patrocinio, de adquisición de bienes y/o servicios de cualquier otra naturaleza.**
- Control del Riesgo de LA/FT/FPADM: **comprende la implementación de políticas, procesos, prácticas u otras acciones existentes que actúan para minimizar el riesgo LA/FT/FPADM en las operaciones, negocios o contratos que realice el BCIE.**
- Debida diligencia: **es actuar con el cuidado que sea necesario para el adecuado conocimiento de la contraparte, la procedencia y, en su caso, destino de sus fondos, de su actividad y de cualquier otro elemento que permita adoptar decisiones suficientemente informadas para determinar que la contraparte no está vinculada a**

actividades ilícitas como el Lavado de Activos, Financiamiento al Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), Integridad, Sanciones y Otros Delitos Financieros que tenga una relación directa con el riesgo LA/FT/FPADM. Lo anterior permite reducir la posibilidad de incurrir en negligencia y en responsabilidades administrativas, civiles o penales. La debida diligencia se clasifica en simplificada, normal y mejorada.

- Delito fuente, subyacente, determinante, precedente o grave: **es una conducta delictiva consagrada en la normatividad penal de la cual provienen los activos, bienes, fondos o recursos ilícitos que luego son lavados. Reciben la denominación de delitos "fuente", "subyacentes", "determinantes," "precedentes" porque son anteriores al delito de lavado de activos y de "graves" por la pena a imponer y la importancia y lesividad del delito. Se consideran como tales, de acuerdo con el GAFI: estafa; terrorismo, incluyendo financiamiento del terrorismo; tráfico de seres humanos y tráfico ilícito de migrantes; explotación sexual, incluyendo la explotación sexual de menores; tráfico ilícito de estupefacientes y sustancias psicotrópicas; tráfico ilegal de armas; tráfico ilícito de mercancías robadas y otros bienes; corrupción y soborno; fraude; falsificación de dinero; falsificación y piratería de productos; delitos ambientales; homicidio, lesiones corporales graves por precio; secuestro extorsivo, privación ilegítima de la libertad y toma de rehenes; robo o hurto; contrabando; (incluyendo los impuestos y cargos aduaneros); delitos fiscales (relacionado con impuestos directos, impuestos indirectos y evasión fiscal); extorsión; falsificación; piratería; y uso indebido de información confidencial o privilegiada y manipulación del mercado. La lista anterior no es taxativa, sino enunciativa y debe tener en cuenta la regulación de cada jurisdicción en la que el Banco opera.**
- Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM): **es todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, transferencia, depósito o uso dual de armas u otros objetos para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable.**
- Financiamiento al Terrorismo (FT): **delito reconocido internacionalmente, en el cual incurre la persona que, por el medio que fuere, directa o indirectamente, ilícita y deliberadamente, provea o recolecte fondos con la intención que se utilicen, o a sabiendas que serán utilizados en todo o en parte, para el financiamiento de actos terroristas y de terroristas y organizaciones terroristas.**

- Gestión del Riesgo: **actividades coordinadas para dirigir y controlar la organización en relación con el riesgo.**
- Lavado de Activos (LA): **es el procedimiento que se lleva a cabo para encubrir el origen de fondos o activos generados mediante la comisión de uno o varios delitos fuentes, subyacentes, determinante, precedente o grave. Su propósito es ocultar o encubrir que los fondos o activos obtenidos a través de actividades ilícitas aparezcan como el producto de actividades lícitas y circulen sin problema en el sistema económico y financiero. El lavado de activos también es conocido como lavado de dinero, blanqueo de capitales o legitimación de capitales.**
- Listas de Sanciones: **registros emitidos o divulgados por cualquier organismo sancionador bajo el amparo de las leyes y normas sobre sanciones económicas, financieras o comerciales, los embargos u originadas de las medidas restrictivas administradas, promulgadas o aplicadas por cualquier organismo sancionador, entre estas: lista Consolidada de Sanciones del Consejo de Seguridad de las Naciones Unidas (ONU), lista consolidada de personas, grupos y entidades sujetas a las sanciones financieras de la Unión Europea (UE), lista de entidades e individuos inelegibles del Banco Mundial (BM), lista consolidada de la Oficina de Control de Activos del Extranjero (OFAC)–y lista “HM Treasury Sanctions List de la Oficina de Implementación de Sanciones Financieras (OFSI) y cualquier otra que sea de observancia para el BCIE en sus actividades financieras. Dichos listados serán consolidados por la OFIC y presentados al comité definido en el apartado b, inciso iii, del artículo 4 de la presente política.**
- Organismo sancionador: **se refiere, sin estar limitado, a las Naciones Unidas, a la Unión Europea, al Reino Unido, al Banco Mundial y a los gobiernos e instituciones u organismos oficiales de observancia para el BCIE en sus actividades financieras.**
- Otros delitos financieros: **son conductas delictivas tipificadas en la regulación penal en las jurisdicciones en las que opera el Banco y que atentan contra la seguridad en el tráfico jurídico, operaciones, patrimonio y el sano y eficiente manejo de las entidades financieras, los cuales se tipifican de manera enunciativa más no limitativa, siempre que tenga una relación directa con el riesgo LA/FT/FPADM.**
- Práctica prohibida: **es cualquier práctica fraudulenta, corruptiva, coercitiva, colusoria u obstructiva según se define en la Política Antifraude, Anticorrupción y Otras Prácticas Prohibidas del BCIE.**

- Relacionados: **personas naturales o jurídicas que participen o presten servicios a las contrapartes en proyectos u operaciones, ya sea en su condición de coordinadores, supervisores, contratistas, subcontratistas, consultores, proveedores, beneficiarios de donaciones (y a todos sus empleados, representantes y agentes), así como cualquier otro tipo de relación análoga.**
- Responsable primario: **persona que establece una relación o tiene contacto con una contraparte del BCIE. Sin distinción del cargo o posición, ya sea personal bajo responsabilidad patronal del BCIE, personal bajo eventual responsabilidad patronal del BCIE y personal con el cual el BCIE no tiene responsabilidad patronal, será considerado responsable primario aquella persona que mantenga contacto directo y constante con la contraparte.**
- Sistema de Administración de Riesgo Integral: **es el Sistema de Administración de Riesgo de LA/FT/FPADM, Integridad y Sanciones.**

VI. DOCUMENTACIÓN RELACIONADA

- **Política Antifraude, Anticorrupción y Otras Prácticas Prohibidas del BCIE.**
- **Reglamento del Mecanismo de Ring Fence para las Actividades y Operaciones Relacionadas con la República de Cuba o sus Nacionales.**
- **Política para la Gestión Integral de Riesgos.**

VII. DESARROLLO

1. GESTIÓN DE RIESGOS Y PRINCIPIOS BÁSICOS

Artículo 1. **El Banco debe cautelar en su operación la gestión de los siguientes tipos de riesgos:**

- a. Riesgo de Lavado de Activos, Financiamiento al Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM): **es la probabilidad de pérdida, daño o exposición que puede sufrir una entidad que, por la naturaleza de sus operaciones, está propensa a ser utilizada directa o indirectamente como vehículo para el lavado de activos, la canalización de recursos hacia la realización de actividades terroristas y/o actividades encaminadas al Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM). Este riesgo conlleva en forma inherente aspectos reputacionales, legales, operativos y de contagio.**
- b. Riesgo de integridad: **es la gestión de los riesgos de fraude, corrupción y otras prácticas prohibidas. Estas prácticas pueden exponer a la entidad a desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la Institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.**
- c. Riesgo de sanciones: **puede definirse como el riesgo de acciones legales, normativas, pérdida financiera, material o daños reputacionales que una entidad puede sufrir como resultado de la imposición de una sanción económica establecida por un organismo sancionador.**

Artículo 2. **Para la gestión de este tipo de riesgos, el Banco y su personal debe actuar bajo los siguientes principios básicos:**

- a. Cumplimiento normativo: **cumplimiento de la normativa interna vigente de LA/FT/FPADM, Integridad y Sanciones y cualquier otra aplicable.**
- b. Debida diligencia: **observancia de la debida diligencia con respecto al conocimiento de las contrapartes, de acuerdo con la normativa interna vigente en materia LA/FT/FPADM, Integridad, Sanciones y Otros Delitos Financieros, que tenga una relación directa con el riesgo LA/FT/FPADM.**

- c. Cultura de cumplimiento: **el Banco promoverá una cultura de observancia a las buenas prácticas internacionales en materia de LA/FT/FPADM, Integridad y Sanciones para demostrar el compromiso del BCIE con la ejecución de negocios responsables y la adecuada gestión de riesgos.**
- d. Confidencialidad: **la información que custodia y administra la Oficina de Integridad y Cumplimiento, así como la información que sea suministrada por las contrapartes, los registros y los documentos referentes a las operaciones respectivas que sean remitidos a dicha oficina para el cumplimiento de sus funciones, será clasificada en las categorías “no públicas” de conformidad con la Política de Seguridad de la Información, quedando a criterio del Jefe de la Oficina de Integridad y Cumplimiento la clasificación como restringida de la información sensible.**
- e. Colaboración: **la colaboración de todo el personal del BCIE y sus contrapartes es esencial para el adecuado funcionamiento del Sistema de Administración del Riesgo de LA/FT/FPADM, Integridad, Sanciones y que el cumplimiento de esta política y demás normativa interna en la materia se anteponga al logro de las metas comerciales.**

Artículo 3. **Para la adecuada gestión de este tipo de riesgo, el Banco deberá establecer un Sistema de Administración del Riesgo de LA/FT/FPADM, Integridad y Sanciones considerando como referencia los estándares internacionales en cada materia, emitidos por entidades tales como el Grupo de Acción Financiera (GAFI)- del cual el Banco participa como observador en los grupos regionales GAFILAT y GAFIC-, los pronunciamientos del Comité de Basilea, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO por sus siglas en inglés), Ley Sarbanes-Oxley, la Organización para la Cooperación y el Desarrollo Económicos (OECD), la Asociación de Examinadores de Fraudes Certificados (ACFE por sus siglas en inglés), el Foro Global sobre Transparencia e Intercambio de Información con Fines Tributarios, Convención de las Naciones Unidas contra la Corrupción, Convención de Viena, el Marco COBIT y la ISO31,000, entre otros.**

Todo el personal, las contrapartes y sus relacionados actuarán respetando los lineamientos que se establezcan en la normativa interna que regula el Sistema de Administración del Riesgo de LA/FT/FPADM, Integridad y Sanciones.

2. RESPONSABLES EN LA GESTIÓN DE LA POLÍTICA

Artículo 4. **Para la implementación y ejecución de la presente política se establecen los siguientes actores y responsabilidades:**

a. Del Directorio y la Administración Superior:

- i. El Directorio, a través de la aprobación de la presente política, establece el tono institucional respecto a la relevancia e importancia de la gestión de los riesgos descritos en la misma.***
- ii. El Directorio y la Administración Superior velarán porque el personal de la OFIC mantenga una preparación y especialización que permita contar con las capacidades y condiciones necesarias para su adecuado desempeño.***
- iii. El Directorio y la Administración Superior se comprometen a proporcionar todos los medios necesarios para que se impartan capacitaciones en materia de prevención de LA/FT/FPADM, Integridad y Sanciones dirigidas al personal, de manera que el modelo se convierta en parte de la cultura institucional empoderando al personal e integrando esta cultura dentro de las actividades diarias de la organización.***
- iv. El Directorio y la Administración Superior apoyan y reconocen la autoridad e independencia del Gerente de Riesgos y del Jefe de la Oficina de Integridad y Cumplimiento y su personal para proponer políticas y procedimientos de forma tal que se controlen efectivamente los riesgos de LA/FT/FPADM, Integridad y Sanciones que enfrenta el BCIE.***

b. De la Administración Superior:

- i. La Administración Superior velará por la existencia de una estructura organizacional para el eficiente funcionamiento de la Oficina de Integridad y Cumplimiento dentro de la Gerencia de Riesgos y para la adecuada Administración del Riesgo de LA/FT/FPADM, Integridad y Sanciones, incluyendo el recurso humano dedicado a dicha función, conforme con la experiencia requerida, profesionalización del personal, tecnologías de información que apoyen la función, y otros recursos acorde al volumen de las operaciones, mercados en los que opera, y otros factores que afectan el perfil de riesgo del BCIE.***
- ii. Establecer las líneas de reporte y comunicación al Directorio, por medio de la Gerencia de Riesgos, sobre asuntos relacionados con los riesgos LA/FT/FPADM, Integridad y Sanciones, incluyendo la emisión de informes sobre estos.***

- iii. Deberá mantener un comité de administración de riesgos y cumplimiento para atender los temas relacionados con la administración del riesgo LA/FT/FPADM.**
 - iv. Designar al Jefe de la Oficina de Integridad y Cumplimiento, quien fungirá como Oficial de Integridad y Cumplimiento del Banco.**
 - v. Propiciar los medios idóneos de denuncia para el reporte de situaciones en las que se detecte incumplimientos a la normativa y/o ilícitos en materia de LA/FT/FPADM, Integridad y Sanciones por parte del BCIE, su personal o contrapartes.**
 - vi. Velar a través de las distintas dependencias, que se realicen esfuerzos coordinados para proteger al BCIE de los efectos que representan las acciones derivadas de la materialización de un riesgo de LA/FT/FPADM, Integridad, Sanciones u Otros Delitos Financieros que tenga una relación directa con el riesgo LA/FT/FPADM.**
 - vii. Instruir a las distintas áreas remediar cualquier brecha identificada en las revisiones internas o independientes.**
- c. De la Gerencia de Riesgos, a través de su Oficina de Integridad y Cumplimiento:
- i. El Jefe de la Oficina de Integridad y Cumplimiento, en su función de Oficial de Integridad y Cumplimiento, y su personal, son responsables de coordinar el Sistema de Administración del Riesgo de LA/FT/FPADM, Integridad y Sanciones, aplicando y velando por el cumplimiento de la presente política y su normativa complementaria, estableciendo los controles para administrar estos riesgos.**
 - ii. Administrar el proceso de identificación, valuación, seguimiento y control de los riesgos relacionados con el LA/FT/FPADM en el BCIE, mediante la implementación de herramientas de gestión de riesgo, así como el diseño, desarrollo, implementación, monitoreo, actualización, difusión y capacitación del marco normativo y procedimientos vigentes a nivel de toda la organización conforme mejores prácticas que permitan la prevención y mitigación de estos riesgos.**
 - iii. Coordinar sus recursos a manera de efectuar de forma efectiva los análisis propios y especializados para el adecuado “Conocimiento del Cliente” en las operaciones del BCIE y las actividades de mitigación de sanciones.**

Asimismo, asesorar y apoyar a los responsables primarios en la aplicación de los lineamientos normativos definidos.

- iv. Establecer y mantener actualizados los principios y normas que serán de aplicación y observancia general a todos los niveles de la organización relacionados con materia de cumplimiento, integridad y sanciones y atender las operaciones que presenten elementos de riesgo y, en su caso, elevarlas a la instancia respectiva para su consideración.***
- v. Evaluar la gestión de cumplimiento, integridad y sanciones en las diferentes áreas y dar seguimiento a los planes de acción que las mismas propongan y a las recomendaciones planteadas.***
- vi. Propiciar la prevención y detección de elementos de riesgo en materia de LA/FT/FPADM, prácticas prohibidas y sanciones, mediante el programa de comunicación y capacitación, el desarrollo y actualización del marco normativo, el asesoramiento y debida diligencia, la administración de los distintos medios de denuncias habilitados, entre otros.***
- vii. Coordinar procesos de investigación y sanción de prácticas prohibidas, con el acompañamiento del Comité de Integridad y sobre la base de los principios del debido proceso.***
- viii. Gestionar y mantener el programa de cumplimiento de sanciones, coordinando los procesos especiales de atención del Ring Fence y los controles necesarios para las potenciales operaciones y transacciones con países, entidades y/o personas sancionadas, con el propósito de salvaguardar impactos negativos en el BCIE derivados de las regulaciones impuestas por entidades sancionadoras.***
- ix. Monitorear las actualizaciones de órganos sancionadores y establecer o actualizar las políticas y procedimientos que pudieran tener implicaciones en la operatividad del BCIE. Escalaría las respectivas instancias los riesgos de sanciones presentes en la operatividad del BCIE. Desarrollar, implementar y monitorear las capacitaciones en sanciones de acuerdo con las necesidades del personal, con el fin de permear los riesgos de sanciones en la Institución. Coordinar la implementación de acciones correctivas al programa de sanciones.***
- x. Coordinar y asistir en las distintas revisiones internas o independientes al programa de cumplimiento, integridad y/o sanciones.***

- xi. Liderar la atención de consultas y debida diligencia por parte de las fuentes de recursos sobre los esquemas y procedimientos especiales sobre sanciones, los controles LA/FT/FPADM y su sistema de integridad.**
 - xii. Representar al Banco ante entidades externas (nacionales e internacionales) en materia de prevención de LA/FT/FPADM, integridad y sanciones.**
- d. Del responsable primario:
- i. Aplicar las medidas de debida diligencia de ingreso y seguimiento y documentar oportunamente los controles y lineamientos señalados en la normativa vigente, utilizando las herramientas disponibles en el BCIE.**
 - ii. Gestionar con el apoyo del Jefe de la Oficina de Integridad y Cumplimiento el riesgo de LA/FT/FPADM, integridad y sanciones en las contrapartes y operaciones a su cargo.**
 - iii. Participar en las convocatorias de capacitación especializadas derivadas del programa de capacitación sobre el Riesgo de LA/FT/FPADM, Integridad, Sanciones y Otros Delitos Financieros que tenga una relación directa con el riesgo LA/FT/FPADM.**
 - iv. Realizar un permanente seguimiento de las contrapartes involucradas cumpliendo con los controles de ingreso y seguimiento establecidos en la normativa interna; así como cuando se identifiquen algunas señales de alerta en el transcurso de la relación. Para el cumplimiento de lo anterior, y en caso de ser necesario, las contrapartes y sus relacionados son responsables de atender las solicitudes realizadas por el responsable primario en tiempo y forma.**
- e. De las contrapartes:
- i. Cumplir en tiempo y en forma con los requisitos que exige la normativa del BCIE relacionada con la prevención de LA/FT/FPADM, Integridad, Sanciones y Otros Delitos Financieros.**
 - ii. Comunicar cualquier modificación en su estructura accionaria, organizativa, de los miembros de la junta directiva, fusiones, adquisiciones y cualquier información significativa conforme con el perfil de riesgo de la contraparte.**

- iii. En los casos aplicables, asegurar que los fondos aportados para la ejecución de los proyectos no provengan ni se encuentren vinculados con LA/FT/FPADM u otra actividad ilícita.**
 - iv. Cautelar la idoneidad de los relacionados financiados con los recursos del BCIE y con otros recursos. Esto incluye el cumplimiento de las buenas prácticas internacionales reconocidas en la materia, así como búsquedas realizadas en las listas de sanciones.**
 - v. Cumplir en tiempo y en forma la presentación de la documentación de sus relacionados, en el caso que el BCIE lo requiera.**
 - vi. Según su naturaleza y en atención al marco jurídico aplicable, adoptar o mantener un programa de prevención de los riesgos de LA/FT/FPADM, Integridad y Sanciones en lo que resulte aplicable.**
 - vii. Reportar cualquier señal de alerta o banderas rojas identificadas durante la ejecución de la operación, a través del Canal de Reportes del BCIE.**
 - viii. Cumplir con todas las disposiciones establecidas en la presente política, normativa relacionada y disposiciones contractuales establecidas.**
- f. De la Auditoría Interna:
- i. El rol de la Auditoría Interna del Banco es buscar los mecanismos para verificar la aplicación y la efectividad de las políticas del Sistema de Administración de Riesgos LA/FT/FPADM, Integridad y Sanciones.**

3. SISTEMA DE ADMINISTRACIÓN DE RIESGOS LA/FT/FPDAM, INTEGRIDAD Y SANCIONES

Artículo 5. **El Sistema de Administración de Riesgos LA/FT/FPDAM, Integridad y Sanciones está compuesto por el conjunto de políticas, manuales, instructivos y procedimientos de debida diligencia, documentación, metodologías de evaluación de riesgos, estructura organizacional, órganos de control, infraestructura tecnológica, mecanismos de divulgación de información y capacitación establecidos y que se establezcan para promover la cultura de administración del riesgo y prevenir la ocurrencia del LA/FT/FPADM, prácticas prohibidas y de sanciones en las relaciones u operaciones del BCIE.**

Artículo 6. ***Para la administración del riesgo se deberán considerar las directrices para identificar, medir, controlar y monitorear los riesgos de LA/FT/FPADM, Integridad y Sanciones cautelando la segregación de funciones.***

Artículo 7. ***Para el adecuado conocimiento de las contrapartes y sus relacionados, se deberá realizar una debida diligencia considerando lo siguiente:***

- a. ***Aplicar los lineamientos indicados en la presente política, de manera integral, a todas las contrapartes y sus relacionados con las cuales el Banco mantiene o pretende mantener algún tipo de relación.***
- b. ***Definir requisitos para el establecimiento de relaciones comerciales con contrapartes y sus relacionados, debiendo rechazar el establecimiento o la renovación de una relación que no cumpla con los requerimientos exigidos en la normativa interna.***
- c. ***Determinar el nivel de riesgo de LA/FT/FPADM, Integridad y Sanciones de acuerdo con la naturaleza de sus contrapartes y negocios conforme con los requerimientos establecidos en la normativa interna.***
- d. ***Establecer procedimientos que permitan la identificación del beneficiario final, de acuerdo con los requerimientos establecidos en la normativa interna.***
- e. ***Implementar procedimientos de debida diligencia simplificada, debida diligencia normal y debida diligencia mejorada, de conformidad con el nivel de riesgo de LA/FT/FPADM, Integridad y Sanciones de sus contrapartes y atendiendo la naturaleza de los negocios que realiza.***
- f. ***Considerar en el proceso de debida diligencia las listas de sanciones y jurisdicciones sujetas a sanciones. Adicionalmente, los controles deben abarcar el filtrado de transacciones y la gestión de listas de sanciones, incluyendo las adiciones a listas y los filtrados de las bases de datos de contrapartes.***
- g. ***Establecer mecanismos que impidan promover vínculos con contrapartes que apoyen la construcción, distribución y financiamiento de armas de destrucción masiva.***
- h. ***Implementar controles para evitar que las operaciones del BCIE se encuentren relacionadas con el financiamiento del terrorismo.***

- i. **Desarrollar mecanismos, desde un enfoque preventivo, para identificar, implementar y mantener controles antifraude, anticorrupción y otras prácticas prohibidas en las operaciones del BCIE.**
- j. **Implementar controles y tomar medidas de aislamiento u otras aplicables, cuando se identifiquen riesgos de sanciones en las contrapartes y sus relacionados.**

Si como resultado de la debida diligencia realizada, surgen dudas sobre la idoneidad de una contraparte y/o sus relacionados, la Oficina de Integridad y Cumplimiento, la dependencia responsable de la operación o la instancia que corresponda, deberá abstenerse de recomendar o, en su caso, de aprobar cualquier operación activa, pasiva, de donación, patrocinios o de adquisición de bienes y/o servicios.

4. CONSIDERACIONES DEL RIESGO LA/FT/FPADM

Artículo 8. **Previo a la emisión de nuevos productos, al uso de nuevas prácticas comerciales, incluyendo nuevos canales, a la modificación de las características de un producto, a la incursión en un nuevo mercado, a la apertura de operaciones en nuevas jurisdicciones, se realizará un análisis por parte de la Oficina de Integridad y Cumplimiento en conjunto con el área responsable del mismo para definir su nivel de riesgo y determinar si requiere de lineamientos especiales de debida diligencia según las características aplicables.**

Artículo 9. **El BCIE dispondrá la conservación de todos los documentos, con la debida seguridad, relacionados con el Riesgo de LA/FT/FPADM, hasta por un período de siete (7) años.**

Artículo 10. **Se deberá contar con una revisión independiente cada dos años, que deberá velar por que existan los controles suficientes y necesarios para prevenir que el BCIE sea utilizado como vehículo para canalizar recursos provenientes de actividades delictivas o tendientes a financiar actos terroristas o armas de destrucción masiva.**

5. CONSIDERACIONES DEL RIESGO DE INTEGRIDAD

Artículo 11. **El Directorio y la Administración Superior están comprometidos en combatir las prácticas prohibidas en sus operaciones, por lo que han adoptado una política de cero tolerancia a la comisión de estas prácticas.**

Artículo 12. **Los mecanismos y lineamientos complementarios para administrar el riesgo de integridad se establecen en la Política Antifraude, Anticorrupción y otras Prácticas Prohibidas y demás normas vigentes.**

6. CONSIDERACIONES DEL RIESGO DE SANCIONES

Artículo 13. **El BCIE actuará en observancia de las distintas sanciones económicas y financieras en las jurisdicciones en las que se hacen negocios, incluyendo los negocios conducidos en o a través de instituciones financieras extranjeras (corresponsalías).**

Artículo 14. **El BCIE realizará una evaluación de riesgos de sanciones cada dos (2) años, que refleje de manera integral y adecuada los posibles riesgos a los cuales está expuesto el BCIE tomando en consideración los siguientes factores que, de manera enunciativa más no limitativa, puedan tener puntos de contacto o nexos a lo externo de la organización: clientes, productos, servicios, intermediarios, contrapartes, transacciones y localización geográfica. Asimismo, por medio de su metodología de gestión de riesgos deberá identificar, analizar y administrar cualquier riesgo de sanciones identificado, proceso que servirá de base para actualizar las políticas, procedimientos, controles y las necesidades de entrenamiento para mitigar este riesgo.**

Artículo 15. **Los controles internos deberán permitir al BCIE prevenir, identificar, prohibir, escalar y reportar al personal competente las transacciones y actividades que pudiesen estar prohibidas, así como establecer los mitigantes en los casos aplicables. Las distintas áreas del BCIE deberán gestionar el riesgo de sanciones que derivado de sus funciones se identifique se encuentren expuestos. Asimismo, las áreas gestionarán el almacenamiento de los registros relacionados con estos controles.**

Artículo 16. **El BCIE no fomentará relaciones o realizará operaciones de ningún tipo, directa o indirectamente, en países sujetos a sanciones exhaustivas por los organismos sancionadores, excepto cuando dicho país sea un socio del BCIE, para lo cual se deberá evaluar y definir el mecanismo especializado de atención y tomar las medidas pertinentes. Las actividades indirectas incluyen, sin limitaciones, las compras a terceras partes intermediarias de bienes, productos o servicios que originan de o se destinan hacia las jurisdicciones enlistadas, o con bancos o instituciones financieras que se asocian a estas transacciones. En lo que respecta a la República de Cuba, prevalecerá lo establecido en el Reglamento del Mecanismo de Ring Fence para las Actividades y Operaciones Relacionadas con la República de Cuba o sus Nacionales.**

Artículo 17. **El BCIE monitoreará cualquier riesgo emergente en jurisdicciones que expongan al Banco al riesgo de sanciones debiendo establecer los mitigantes necesarios para limitar la exposición identificada.**

Artículo 18. **Los fondos que eventualmente deban ser recibidos en concepto de pagos de parte de individuos, entidades¹ y entes² que se encuentren en cualesquiera de las listas de sanciones de los organismos sancionadores deberán ser manejados adecuadamente, de forma separada, sin ser mezclados con el resto de los caudales del Banco.**

Artículo 19. **El BCIE no establecerá relaciones de ninguna naturaleza con individuos, entidades o entes que se encuentren en listas de sanciones de los organismos sancionadores. En relaciones existentes en las que emerja un riesgo de sanciones se aplicarán las medidas de aislamiento, mitigación o terminación según sea necesario.**

Artículo 20. **En caso de identificar que una contraparte o relacionado se encuentre o sea incluido en resoluciones del Consejo de Seguridad de las Naciones Unidas relativas a la prevención y represión del terrorismo, el financiamiento del terrorismo y de la proliferación de armas de destrucción masiva, se procederá al congelamiento inmediato, es decir, la retención de los fondos o desembolsos respectivos en un plazo de 24 horas.**

Artículo 21. **Todo el personal deberá cumplir con las disposiciones y directrices definidas para evitar el riesgo de sanciones y deberán abstenerse de realizar acciones para evadir las limitaciones derivadas de sanciones, ya sea en los mensajes de transferencia y transacciones transfronterizas, así como el borrado, la reemisión y/o alteración de información relevante de sanciones.**

Artículo 22. **El personal del BCIE sujeto a regulaciones sancionadoras tiene prohibido participar, autorizar o aprobar financiamientos a una contraparte sancionada, ni podrá facilitar o indicar a otro miembro del personal que intervenga o apruebe una operación con una contraparte sancionada.**

7. OTRAS DISPOSICIONES

Artículo 23. **Es responsabilidad del personal del BCIE en todos los niveles y estamentos comprender, cumplir y aplicar la presente política, normativa interna y cualquier otro documento que forme parte del Sistema de Administración del Riesgo de LA/FT/FPADM, Integridad y Sanciones, así como asesorarse adecuadamente cuando existan dudas o**

¹ Incluye entidades propiedad en 50% o más, o controlada (directa o indirectamente) por uno o más individuos o entidades sancionadas, o un individuo o entidad actuando en nombre de partes sancionadas.

² Navíos, embarcaciones, aeronaves.

consultas sobre su aplicación. Asimismo, es deber de todo el personal participar en las convocatorias anuales derivadas del programa de capacitación sobre el Riesgo de LA/FT/FPADM, Integridad, Sanciones y Otros Delitos Financieros que tenga una relación directa con el riesgo LA/FT/FPADM.

Artículo 24. **El personal del BCIE tiene el deber de informar de inmediato a sus superiores, a la Oficina de Integridad y Cumplimiento y/o a través de los medios de denuncia disponibles cuando se identifiquen aspectos inusuales o sospechosos en las actividades u operaciones del Banco, de conformidad con lo establecido en la normativa interna.**

Artículo 25. **El BCIE prestará, conforme con su Convenio Constitutivo y conforme con las normativas que rigen su actividad en esta materia, la colaboración a las autoridades competentes que así lo requieran.**

Artículo 26. **El BCIE se asegurará que los contratos de todas las operaciones activas del Banco, así como los contratos con sus proveedores de bienes y servicios, contengan las disposiciones contractuales necesarias para mitigar, prevenir y contrarrestar el riesgo de LA/FT/FPADM, Integridad y Sanciones, siendo responsabilidad de la Oficina de Integridad y Cumplimiento el diseño de las cláusulas pertinentes que permitan dicho propósito.**

Artículo 27. **La Administración Superior, a través de la Gerencia de Riesgos y de su Oficina de Integridad y Cumplimiento, velará por la actualización oportuna de la presente política, de conformidad con el avance en las mejores prácticas y estándares internacionales en la materia.**

onómica

Anexo
Resolución No. DI-36/2023

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 5

Gerencia de Tecnología de Información

Público una vez aprobado

De conformidad con el marco normativo de la Política de Acceso a la Información, el presente documento será divulgado en el sitio web externo del Banco después de su aprobación.

PÚBLICO: UNA VEZ APROBADO

TABLA DE CONTENIDO

I. INTRODUCCIÓN.....	4
II. OBJETIVO	4
III. ALCANCE.....	4
IV. ABREVIATURAS Y TÉRMINOS	4
V. DEFINICIONES.....	5
VI. DOCUMENTACIÓN RELACIONADA.....	6
VII. DESARROLLO.....	8
RESPONSABILIDADES ANTE EL SISTEMA DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	8
DISPOSICIONES DE CONFIDENCIALIDAD Y PROPIEDAD DE LA INFORMACIÓN.....	9
ACCESO A LOS ACTIVOS DE INFORMACIÓN	9
UTILIZACIÓN Y ADMINISTRACIÓN DEL RECURSO INFORMÁTICO	10
CONTROL Y CLASIFICACIÓN DE LA INFORMACIÓN.....	10
SEGURIDAD FÍSICA.....	12
REVISIONES PERIÓDICAS DE SEGURIDAD.....	12
CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN.....	12
RETENCIÓN Y CONSERVACIÓN DE REGISTROS DE ARCHIVO.....	13
USO DE INTERNET Y CORREO ELECTRÓNICO	13
DESARROLLO Y MANTENIMIENTO DE SISTEMAS	14
GESTIÓN DE INCIDENTES DE SEGURIDAD	14
RELACIÓN CON TERCERAS PARTES	14
SISTEMAS DE DIVULGACIÓN Y COMUNICACIÓN INTERNA DEL BCIE.....	14
REDES SOCIALES	15
IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA.....	15
ACCIONES JURÍDICAS Y DISCIPLINARIAS.....	15

I. INTRODUCCIÓN

En alineación a COBIT, Marco de Gobierno de las Tecnologías de Información adoptado por el Directorio se define la presente Política de Seguridad de la Información del Banco Centroamericano de Integración Económica como documento normativo de mayor jerarquía para regular la Tecnología de Información del Banco y la seguridad requerida para la protección de la información del Banco.

II. OBJETIVO

Establecer los principios y las normas que deben ser aplicados en el Banco Centroamericano de Integración Económica al generar y hacer uso de información, de forma que se cumplan los siguientes principios básicos:

- a. **Integridad:** Se refiere a la exactitud y a la completitud de la información y de los métodos para su procesamiento.
- b. **Confidencialidad:** Se refiere a que la información sea accesible solo para las personas que tengan la debida autorización.
- c. **Disponibilidad:** Se refiere a que los usuarios autorizados tengan acceso a la información en el momento en que se requiera.

Para lograr lo anterior, se establecerán controles para administrar la información del Banco. Estos controles abarcan a las personas, a los procesos y a la tecnología de información, de acuerdo con los estándares y a las mejores prácticas internacionales en la materia.

III. ALCANCE

La presente política, en conjunto con su Manual de Seguridad de la Información y con los procedimientos complementarios, será de aplicación y observancia dentro de todas las actividades del Banco.

Todo el personal que labore en el Banco, así como cualquier persona natural o jurídica que tenga una relación contractual con el Banco, como es el caso de pasantes, jóvenes profesionales, contratistas, practicantes, personal de servicios tercerizados, proveedores y consultores, estará sujeto a aceptar formalmente, a acatar y a desempeñarse bajo esta Política. No estarán sujetos a aceptar y acatar la presente Política prestatarios, contrapartes y clientes del Banco en general. Los requisitos de integridad, confidencialidad y disponibilidad de información para estos casos estarán sujetos a las condiciones establecidas en cada contrato específico según corresponda.

El alcance de esta Política no incluye ni tutela los principios de integridad, confidencialidad y disponibilidad de equipos, servicios de información y cuentas de correo electrónico o de otra forma de activos tangibles e intangibles propiedad de terceros, a menos que el Banco y el propietario lo establezcan expresamente por escrito.

IV. ABREVIATURAS Y TÉRMINOS

- **Administración Superior:** Presidencia y Vicepresidencia Ejecutivas.
- **BCIE o Banco:** Banco Centroamericano de Integración Económica.
- **GTI:** Gerencia de Tecnología de Información.
- **GERSEC:** Gerencia de Servicios Generales y Control Financiero.
- **SAAI:** Departamento de Servicios Administrativos y de Adquisiciones Institucionales.
- **SIATI:** Departamento de Seguridad de la Información y Aseguramiento de la Calidad de TI.

- **TI:** Tecnología de Información.

V. DEFINICIONES

- **Activo:** Cualquier bien tangible o intangible que tenga valor para el Banco.
- **Activo de Información:** Activo que contiene información en forma intangible, incluyendo, pero no limitado a datos y archivos digitales, bases de datos, aplicaciones desarrolladas internamente, propiedad intelectual, documentos físicos y electrónicos, copias de respaldo, imágenes o video, así como activos tecnológicos en forma de infraestructura tecnológica, incluyendo pero no limitado a equipos, servidores, computadoras personales, dispositivos móviles (portátiles, tabletas, teléfonos inteligentes, entre otros) dispositivos de almacenamiento central y de usuario final (ej. discos duros extraíbles), equipo de comunicaciones o sistemas de control de accesos.
- **Amenaza:** Una causa potencial de un incidente no deseado que puede resultar en daño a un sistema o al Banco o en la pérdida de confidencialidad, integridad o disponibilidad de la información del Banco.
- **Bitácora Técnica:** Registro en forma electrónica de los estados, eventos y acciones que ocurren durante la ejecución de un proceso, trabajo o tarea. Este registro incluye los sucesos relevantes que tuvieron lugar durante la realización de dicha tarea y las fallas que se produjeron, sin hacer referencia al contenido de la información que se procesa.
- **Control:** Conforme con lo definido en la Política para la Gestión Integral de Riesgos del BCIE, es cualquier acción tomada por el Directorio, por la Administración u otros miembros de la entidad dirigida a mitigar o a minimizar un riesgo identificado y asegurar la consecución de los objetivos.
- **Custodio de Información:** Persona a quien se le han delegado las funciones y las responsabilidades de administrar, a nombre de los propietarios de información, los controles de acceso a la información. Para el caso específico del Banco corresponde única y exclusivamente al Coordinador de Seguridad de Información, los Supervisores de Seguridad de Información o a quien la Presidencia Ejecutiva designe a través del Manual de Seguridad de la Información.
- **Cuenta Privilegiada:** Las cuentas privilegiadas son aquellas que confieren capacidades extraordinarias no disponibles para las cuentas y usuarios normales. Son identificadores de usuario (User ID) creados por el fabricante de una plataforma tecnológica que posee privilegios de súper usuario y los cuales son utilizados regularmente por personal técnico de la GTI para la administración y soporte a sistemas operativos, bases de datos, dispositivos de redes y comunicación y aplicativos. Ejemplos de estos usuarios son Admin, Root, System, entre otros.
- **Evento de Seguridad de la Información:** Una ocurrencia identificada en el estado de un sistema, servicio o red indicando una posible violación de la seguridad de la información o una falla en controles o una situación previamente desconocida que puede ser relevante para la seguridad de la información del Banco.
- **Incidente de Seguridad de la Información:** Evento o serie de eventos de seguridad de información que atenta contra la operación del Banco o que compromete la confidencialidad, integridad o disponibilidad de la información del Banco.
- **Información:** Se refiere a toda comunicación o representación de conocimiento incluyendo formas textuales, numéricas, gráficas, cartográficas, orales o audiovisuales

y en cualquier medio de transmisión o almacenamiento, ya sea impreso, magnético, óptico, digital o audiovisual.

- **Instalaciones de Procesamiento de Información:** Sitio físico en donde se alberga cualquier sistema, servicio o infraestructura de procesamiento de información de forma centralizada.
- **Originadores de Documentos:** Calidad que adquiere todo el personal del BCIE que produce documentos o informes finales y que son sujetos de clasificación de conformidad con el modelo contenido en la presente Política.
- **Plan de Gestión de la Seguridad de Información:** Conjunto de iniciativas, proyectos y actividades que deben ser realizadas anualmente para soportar, mantener y mejorar continuamente el Sistema de Seguridad de Información del Banco. Este Plan hace parte del Plan Operativo Anual de Tecnología de Información del BCIE.
- **Responsable de la Información:** Por regla general, los responsables de la información serán los titulares de cada dependencia del Banco, salvo que se haya designado a un funcionario específico para ejercer este rol. Para el caso de activos de información aprobados en los diferentes comités, el propio comité será el Responsable de la Información. Los Responsables de la Información tienen la responsabilidad final de que los activos de información de sus respectivas dependencias estén debidamente clasificados. Asimismo, deben mantener un registro actualizado de los activos de información que están bajo su cargo, incluyendo aquellos considerados como datos estructurados. Para el caso de activos de información que no sean considerados oficiales de la dependencia y que son creados y administrados por cada colaborador en particular, como es el caso de documentos de *office* y correo electrónico, corresponde a cada colaborador la responsabilidad de clasificación de estos.
- **Riesgo:** Se define como la posibilidad de que ocurran eventos que representen una desviación de lo esperado, que pudieran causar daños o pérdidas que afecten la consecución de los objetivos de la Institución.
- **Registros de Archivo:** Información creada o recibida, conservada como información y prueba en el desarrollo de las actividades del Banco o en virtud de sus obligaciones legales.
- **Seguridad de la Información:** La salvaguarda de la confidencialidad, integridad y disponibilidad de la información.
- **Seguridad Física:** La salvaguarda de la información a través del establecimiento de áreas seguras, protegidas por un perímetro de seguridad definido, con barreras de seguridad apropiadas y controles de ingresos y egresos.
- **Usuario de Información:** Persona que utiliza activos de información creados por sí mismo o por otros usuarios, para realizar sus funciones.
- **Vulnerabilidad:** Una debilidad en un activo o grupo de activos que puede ser explotado por alguna amenaza.

VI. DOCUMENTACIÓN RELACIONADA

- Reglamento de la Organización y Administración (ROA) del Banco Centroamericano de Integración Económica (Código de Ética).
- Reglamento General de Administración de Recursos Humanos.
- Política de Acceso a la Información.
- Manual de Seguridad de la Información.

- Manual de Normas de Conducta.
- Manual de Funcionamiento del Comité de Tecnología de Información.
- Manual de Formulación y Monitoreo del Plan Estratégico y el Plan Operativo Anual de la Tecnología de Información del BCIE.

VII. DESARROLLO

RESPONSABILIDADES ANTE EL SISTEMA DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 1. Se establece el Sistema de Administración de la Seguridad de la Información como el conjunto de personas, procesos, herramientas y sistemas tecnológicos que a través de un enfoque sistemático permiten asegurar razonablemente la debida utilización y protección de la información del BCIE.

Artículo 2. Se establecen las principales responsabilidades para la adecuada gestión del Sistema de Administración de la Seguridad de la Información de la siguiente manera:

- 2.1.** Corresponde al Directorio del Banco direccionar el sistema de Administración de la Seguridad de la Información a través de las siguientes funciones:
 - a. Aprobar la Política de Seguridad de la Información, sus actualizaciones y modificaciones.

- 2.4.** Corresponde a la Presidencia Ejecutiva asegurar el alineamiento y efectividad del Sistema de Administración de la Seguridad de la Información a través de las siguientes funciones:
 - d. Aprobar el Manual de Seguridad de la Información del BCIE y los procedimientos complementarios que se requieran para asegurar la debida implementación y cumplimiento de la Política de Seguridad de la Información.

- 2.5.** Corresponde al Comité de Tecnología de Información el monitoreo y supervisión del Sistema de Administración de la Seguridad de la Información a través de las siguientes funciones:
 - d. Analizar y recomendar a la Presidencia Ejecutiva cualquier modificación a la Política de Seguridad de la Información y a su Manual de Seguridad de la Información.

- 2.6.** Corresponde a la GTI:
 - b. Proponer las modificaciones que correspondan a la Política de Seguridad de la Información, Manual de Seguridad de la Información, así como a los procedimientos y a las actividades relacionadas con dicha Política.
 - c. Diseñar e implantar los mecanismos necesarios y adecuados para la divulgación y conocimiento de esta Política a todos los niveles de la Institución, así como a las personas y a las entidades relacionadas con el Banco.
 - g. Asegurar la adecuada implementación de los lineamientos establecidos en esta Política y el manual correspondiente.

- 2.7.** Corresponde al personal del Banco, al responsable de la Información, al Usuario de Información y en general a los sujetos obligados al cumplimiento de la Política de Seguridad de Información, producir, salvaguardar y hacer uso adecuado, confidencial

y responsable de la información del Banco, de acuerdo con lo establecido en la presente Política y en los procedimientos, manuales y actividades asociadas.

- 2.8.** Corresponde al personal del Banco, así como a las demás personas naturales y jurídicas que están incluidas en el alcance de esta política, suscribir la aceptación formal de esta política y de su Manual de Seguridad de la Información al momento del inicio de su relación laboral o contractual con el Banco. Adicionalmente, y cada vez que se modifique la Política de Seguridad de la Información, se deberá exigir al personal del Banco, contratistas y jóvenes profesionales la suscripción de un nuevo acuerdo de aceptación de la misma y de su correspondiente manual.

DISPOSICIONES DE CONFIDENCIALIDAD Y PROPIEDAD DE LA INFORMACIÓN

Artículo 3. Las personas naturales y jurídicas que conforme con lo establecido en el alcance de esta política son sujetos de aplicación de la presente política, están obligados al cumplimiento del principio de confidencialidad con respecto a la información propiedad del Banco que llegue a ser de su conocimiento y que sea catalogada como de uso interno confidencial o restringida o a la que ellos mismos generen durante su relación contractual, salvo aquella información que sea catalogada como pública. La obligación de confidencialidad de la información subsistirá hasta por diez (10) años después de concluida la relación entre el Banco.

Artículo 4. Toda la información a la que cada uno de los sujetos obligados al cumplimiento de la presente Política tenga acceso durante su vínculo contractual se considera propiedad del Banco. Dicha información incluye, pero no se limita a toda información internamente generada, procesada, transformada, editada o cualquier otra actividad análoga de creación, transformación o consulta y la información legalmente adquirida o cedida de forma voluntaria por alguna contraparte con la que el Banco tiene relaciones.

Artículo 5. Los sujetos obligados al cumplimiento de la presente Política están obligados a respetar los derechos intelectuales de propiedad de terceros o de otros derechos incorporados a la simple propiedad física.

Artículo 6. Para asegurar la debida protección de la información propiedad del Banco, la Administración Superior, a través de la GTI, el Banco contará con herramientas automáticas para la prevención de pérdidas de datos que permitan prevenir, detectar e investigar eventos de fuga de información sensible en medios electrónicos.

Artículo 7. Los clientes y a los proveedores que realicen transacciones con el Banco por medios electrónicos deben suscribir un documento que establezca los acuerdos de uso y de confidencialidad que el Banco defina, según se establezca en el Manual de Seguridad de la Información. Asimismo, deberán suscribir la aceptación y cumplimiento de la presente Política de Seguridad de la Información, así como del Manual de Seguridad de la Información.

ACCESO A LOS ACTIVOS DE INFORMACIÓN

Artículo 8. La GTI podrá negar cualquier acceso a activos de información que pudieren comprometer la seguridad de la información o que no sean racionales en términos de costos para el Banco.

Artículo 9. La plataforma tecnológica del Banco cuenta con la capacidad de generar las bitácoras requeridas para el monitoreo y cumplimiento de la Política.

Artículo 11. Los custodios de la información y órganos de control del BCIE podrán tener acceso a toda la información contenida en activos de información de propiedad o bajo el control del Banco, única y exclusivamente con fines de monitorear el debido cumplimiento de la Política de Seguridad de la Información o de prevenir o contener posibles incidentes de seguridad.

Artículo 13. En caso de potenciales riesgos o incidentes de seguridad, el Banco se reserva el derecho, y los sujetos obligados por esta Política consienten el acceso, a revisar equipos de usuario final que los sujetos obligados por esta Política utilicen en el desempeño de sus funciones oficiales o servicios contratados, sean estos de su propiedad o de propiedad del Banco.

UTILIZACIÓN Y ADMINISTRACIÓN DEL RECURSO INFORMÁTICO

Artículo 14. La GTI, a través del Departamento de Tecnología y Comunicaciones, es la encargada de la administración de la plataforma tecnológica del Banco, que incluye el equipo de cómputo, equipo de comunicaciones y servicios tercerizados en Internet.

A tal efecto, Los sujetos obligados al cumplimiento de la presente Política deben cumplir los controles que establezca la GTI para gestionar y controlar los elementos que forman parte de la infraestructura tecnológica con el fin y garantizan que serán utilizados en un entorno adecuado de seguridad.

Asimismo, cualquier adquisición, instalación o actualización de los activos de información que conforman la plataforma tecnológica del Banco deberá estar autorizada por la GTI a través del Departamento de SIATI o del Departamento de Tecnología y Comunicaciones, según corresponda.

Artículo 17. Se deben mantener controles automáticos que permitan restringir la conexión a la red del Banco de equipos de personal externo o visitantes, así como el uso de memorias USB, discos externos y cualquier otro dispositivo o servicio de almacenamiento de información en la plataforma tecnológica y de usuario final del Banco.

CONTROL Y CLASIFICACIÓN DE LA INFORMACIÓN

Artículo 18. Toda información propiedad del Banco, independientemente del medio en el que se encuentre, prepare o distribuya debe gestionarse en un entorno de confidencialidad, conforme con lo establecido en las "Disposiciones de Confidencialidad y Propiedad de la Información" de esta Política.

Artículo 19. Los responsables de la información deben clasificar la información de acuerdo con el siguiente modelo:

19.1. Categorías Públicas:

- a. Información no clasificada:** Se refiere específicamente a información propiedad del empleado que no contiene ningún tipo de información del Banco y que el empleado por decisión propia decide categorizarla como "No Clasificada".
- b. Información Pública:** Es aquella información propiedad del Banco que puede ser divulgada a la sociedad y público en general de conformidad con la presente Política y con la Política de Acceso a la Información. Esta información puede ser obtenida, ofrecida y circular sin reserva alguna y, en caso de su publicación en los canales autorizados, debe ser revisada y aprobada previamente por los responsables de información, según sea cada caso.

19.2. Categorías no Públicas:

- a. **Información de Uso Interno:** Es aquella información que se genera, recibe o procesa en el BCIE para el desarrollo de todas las actividades internas institucionales y cuyo acceso y uso se limita exclusivamente al personal del Banco. Por defecto toda la información del Banco será catalogada como de Uso Interno. La Información de uso interno también puede ser categorizada como confidencial en los casos en que solo pueda ser conocida por un grupo específico de usuarios.
- b. **Información Confidencial:** Es aquella que contiene información cuyo acceso y uso debe ser limitado a algunas áreas del Banco o a un grupo de colaboradores o personas en particular.
Dentro de esta categoría se incluirá, no solo la información institucional que corresponda, sino también la información personal de empleados y pensionados gestionada por la Oficina de Recursos Humanos, el Fondo de Prestaciones Sociales y demás dependencias que pudiesen manejar algún tipo de información personal.
Igualmente, se incluye dentro de esta categoría, información que el BCIE debe administrar (conocer, entregar, intercambiar, notificar) en el curso de la interacción con contrapartes para el desarrollo de sus operaciones activas, pasivas, servicios prestados, contratación de bienes y servicios, trámites administrativos y, en general, cualquier actividad con terceros que sea necesaria para las operaciones o funcionamiento del BCIE.
En los casos en que existan acuerdos de confidencialidad suscritos con una contraparte y en el evento de que se requiera compartir información cubierta dentro del acuerdo de confidencialidad con una segunda contraparte o tercero ajeno al Banco, deberá contarse con la autorización de la contraparte con la cual se suscribió el acuerdo y del área del Banco responsable de la relación con la contraparte.
- c. **Información Restringida.** Es aquella información clasificada como confidencial y que, además, por su sensibilidad su acceso está limitado exclusivamente al Directorio, a los Órganos de Control, al Oficial de Ética y a la Administración Superior (Presidencia y Vicepresidencia Ejecutivas).

Artículo 20. La entrega de información propiedad del BCIE por requerimientos judiciales, solicitudes de entes contralores del orden público o instancias similares externas deberá ser atendida conforme con la Política de Acceso a la Información.

Artículo 21. Los gobernadores, los directores, el Contralor, el Auditor Interno y el Oficial de Ética tendrán acceso a toda la información de propiedad del Banco, observando las disposiciones particulares de la información clasificada como confidencial o restringida y siguiendo los canales que en tal sentido se definan en el Manual de Seguridad de la Información.

Artículo 22. En el Manual de Seguridad de la Información se establecerán las actividades específicas para la administración de la información institucional y ejemplos que faciliten la clasificación de la información del Banco en cada una de las categorías establecidas.

Artículo 23. Los jefes de cada dependencia del Banco y los sujetos obligados al cumplimiento de la presente Política deben mantener el debido control de sus activos de información clasificados como de uso restringido o confidencial. Será responsabilidad de los responsables de la información identificar expresamente la información clasificada como confidencial en

cada documento que corresponda, sea este físico o electrónico, haciendo uso de las herramientas que para tal efecto se dispongan.

Artículo 24. Los responsables de la información tienen la responsabilidad final de clasificar la información y de definir los niveles de acceso a la misma, otorgando autorizaciones de acceso y revisando periódicamente los niveles de acceso otorgados. Asimismo, son responsables de mantener un registro actualizado de los activos de información que están bajo su responsabilidad.

Artículo 25. La información debe ser catalogada por los originadores de documentos al momento de generarla, considerando las categorías antes descritas y de acuerdo con los niveles de importancia, sensibilidad y criticidad. Si la información debe ser conocida por sujetos no obligados por la política, la transferencia es responsabilidad del Usuario de Información. No obstante, el Usuario de Información no podrá compartir aquella información catalogada como confidencial o restringida sin antes obtener la autorización del responsable de la información, de acuerdo con los términos de esta política y su Manual de Seguridad de la Información.

Artículo 26. Cada dependencia del Banco debe mantener un inventario actualizado con la tipología de información que considera confidencial o restringida. Asimismo, el Banco deberá contar con herramientas tecnológicas que faciliten la clasificación de la información del Banco.

SEGURIDAD FÍSICA

Artículo 27. Los sujetos obligados al cumplimiento de la presente Política deberán cumplir los lineamientos de administración de seguridad física y ambiental que defina la GERSEC, a través del Departamento de Servicios Administrativos y de Adquisiciones Institucionales (SAAI).

REVISIONES PERIÓDICAS DE SEGURIDAD

Artículo 29. El Banco realizará revisiones éticas a la plataforma de seguridad apoyadas por firmas o por terceros especializados con el fin de detectar, valorar y controlar nuevas amenazas y riesgos que atenten contra los activos de información del Banco y de asegurar la efectividad de todos los controles implementados a nivel físico y lógico para salvaguardar los activos de Información. Los sujetos obligados al cumplimiento de la presente Política podrán ser sujetos a estas y cualquier otra auditoría.

Artículo 30. En caso de que a algún proveedor o contraparte contractual se le reporte alguna vulnerabilidad, ésta deberá establecer un plan de cierre de las vulnerabilidades identificadas que permitan el cierre de las mismas.

CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN

Artículo 31. Los sujetos obligados al cumplimiento de la presente Política deben cumplir con los documentos normativos que correspondan que permitan controlar la asignación de derechos de acceso a los sistemas y servicios de información.

Artículo 32. Los contratistas o proveedores con accesos a la plataforma tecnológica del Banco, o con vinculación directa a los servicios prestados al Banco, deberán notificar con al Banco todo movimiento de personal asociado a procesos y servicios prestados incluyendo de vinculación, desvinculación, licencias, traslados, ausencias prolongadas o cualquier otro relacionado con la gestión del recurso humano que pudiese afectar el servicio o que tengan accesos otorgados a las plataformas tecnológicas del banco y que pudiesen requerir de una

creación, modificación o cancelación de privilegios de acceso de algún usuario. Asimismo, dentro del proceso de reclutamiento del personal que presta servicios al Banco, se deberán realizar estudios de seguridad que incluyan la verificación de antecedentes al personal que estará asignado.

Artículo 33. Se asignará una identificación única, personal y no transferible a cada Usuario de Información que requiera, por sus funciones, acceso a la plataforma tecnológica del Banco. Esta identificación debe ser asignada y revocada conforme con lo que se establezca en el Manual de Seguridad de la Información, el cual debe establecer además los parámetros técnicos de esta identificación. Los usuarios no deberán compartir sus identificaciones y contraseñas de acceso a ningún otro usuario y mucho menos a terceros ajenos al Banco y estarán obligados a hacer uso de las herramientas de seguridad tecnológica que implemente la GTI y a seguir las prácticas de control que en tal sentido se definan en el Manual de Seguridad de la Información.

RETENCIÓN Y CONSERVACIÓN DE REGISTROS DE ARCHIVO

Artículo 37. Los Usuarios de Información son responsables del contenido de las computadoras de escritorio, portátiles y equipos de computación móvil como teléfonos inteligentes, tabletas y cualquier otro activo o recurso de información que le fueren asignadas, siguiendo las indicaciones técnicas establecidas por la GTI.

USO DE INTERNET Y CORREO ELECTRÓNICO

Artículo 38. El acceso a Internet es proporcionado a los Usuarios de Información para facilitar la ejecución de sus actividades y labores diarias relacionadas con el Banco. En este sentido, el uso de recursos disponibles en Internet debe enmarcarse en los lineamientos de uso aceptable de Internet, descritos en el Manual de Seguridad de la Información.

Artículo 39. Toda información transmitida, recibida, procesada, almacenada y, en general, administrada a través del correo electrónico institucional es propiedad del Banco. El correo electrónico institucional es proporcionado a los usuarios de información como una herramienta de apoyo para el desarrollo de las operaciones de negocios, administrativas y técnicas de la Institución, por lo que su uso debe enmarcarse en los lineamientos de uso aceptable de correo electrónico, descritos en el Manual de Seguridad de la Información.

Artículo 40. El correo electrónico no se usará para el envío de mensajes masivos a todo el personal, salvo aquellos que contiene información de interés institucional, como por ejemplo los relacionados con temas de continuidad del negocio (BCP), seguridad de la información y el caso de encargos temporales, entre otros. Para este efecto la Administración Superior establecerá las áreas del Banco autorizadas a enviar correos masivos.

Artículo 41. Se prohíbe el envío de mensajes masivos de carácter personal a grupos de correos electrónicos o a todo el personal, tales como anuncios de cadenas, colectas, propaganda, publicidad, compraventa, invitaciones y toda clase de transacciones de carácter personal.

Artículo 42. El intercambio de información con contratistas, proveedores de servicios, contrapartes y clientes se hará por los medios oficiales establecidos por el Banco y a través de las herramientas que en tal sentido se implementen. Se prohíbe el uso de repositorios públicos en la nube para el intercambio de información de uso interno o confidencial con terceros.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

GESTIÓN DE INCIDENTES DE SEGURIDAD

Artículo 51. Los usuarios de información deben reportar al Departamento de SIATI cualquier actividad sospechosa, amenaza real o potencial de eventos que comprometan la confidencialidad, integridad o disponibilidad de la información o que contravenga la política de la seguridad de la información, incluyendo actividades como pérdidas o robo de equipos o medios de almacenamiento, ataques de virus, fugas de información, mal uso de información o mal uso de los activos tecnológicos o de información asignados a los usuarios u otros eventos.

Artículo 52. Mediante el Manual de Seguridad de la Información, se definen los procedimientos para que oportunamente se comuniquen, clasifiquen, investiguen, solucionen y documenten los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia, y se escale los incidentes de acuerdo con su criticidad y mantendrá registros y estadísticas de eventos que afecten la seguridad de la información.

Artículo 53. La Administración Superior, a través de la Oficina de Comunicación y Relaciones Externas o a través de la dependencia que designe, serán los únicos canales válidos para realizar pronunciamientos oficiales ante entidades externas sobre incidentes de seguridad ocurridos.

Artículo 54. En caso de que se materialice algún incidente de seguridad asociado con secuestro de datos, ni el Banco ni su personal está autorizado a pagar rescate por los mismos. Cualquier excepción a esta disposición debe ser aprobada por la Presidencia Ejecutiva.

Artículo 55. A fin de poder detectar y contener oportunamente cualquier ataque cibernético que pudiera atentar contra la disponibilidad de las operaciones y servicios del Banco, este, a través del Departamento de SIATI, deberá asegurar que se implemente y mantenga operativa una plataforma de seguridad tecnológica robusta que permita proteger razonablemente al Banco de ataques externos. Asimismo, deberá asegurar que se realice un monitoreo permanente a dicha plataforma los siete días a la semana y 24 horas al día, para lo cual podrá contar con el apoyo permanente de firmas especializadas.

RELACIÓN CON TERCERAS PARTES

Artículo 56. Cada dependencia del Banco responsable de servicios o relaciones con terceros, según su ámbito de trabajo, deberá establecer contractualmente los controles necesarios en aquellas operaciones y servicios realizados por terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas cumplan con las políticas y con los procedimientos de seguridad de la información.

SISTEMAS DE DIVULGACIÓN Y COMUNICACIÓN INTERNA DEL BCIE

Artículo 57. Se consideran como canales oficiales de comunicación interna el correo electrónico, el Intranet, el sistema telefónico, el sistema de videoconferencia o cualquier otro sistema electrónico, digital o impreso utilizado para las comunicaciones internas y externas.

Artículo 58. La Administración Superior, a través de la Oficina de Comunicación y Relaciones Externas, debe normar las condiciones de uso y restricciones de los canales de comunicación interna relacionados con las funciones oficiales y no oficiales del personal del BCIE.

REDES SOCIALES

Artículo 59. La contratación de servicios para la divulgación de información institucional por Internet y redes sociales será responsabilidad exclusiva de la Oficina de Comunicación y Relaciones Externas, la que deberá contar con el visto bueno del área de SIATI desde la perspectiva de seguridad de dichos servicios. En este sentido, ningún área del Banco podrá tener su propia red social pública sin que la misma no cuente con las autorizaciones respectivas.

Artículo 60. La creación y el manejo de las cuentas oficiales del Banco en redes sociales públicas es responsabilidad exclusiva de la Oficina de Comunicación y Relaciones Externas, la que debe monitorear diariamente las redes sociales que mencionen al Banco y dar seguimiento en caso de que sean publicaciones que potencialmente puedan dañar la imagen o reputación institucional. Para el caso de redes sociales públicas asociadas al proceso de reclutamiento de personas o a la gestión del recurso humano, estas serán administradas por la Oficina de Recursos Humanos.

Artículo 61. El contenido y publicaciones en redes sociales del Banco, así como en los portales web del BCIE para el público en general deben ser previamente validados por la Oficina de Comunicación y Relaciones Externas. En este sentido, en la página web, publicaciones y redes sociales del Banco solo se publicará información clasificada como de carácter pública y en cumplimiento de la presente política y de la Política de Acceso a la Información.

Artículo 62. La Administración Superior, a través de la Oficina de Comunicación y Relaciones Externas, debe normar los procedimientos y estándares que deben cumplirse en el uso y administración de las redes sociales utilizadas por el BCIE como mecanismos de divulgación y comunicación, así como las actividades que los colaboradores del Banco deben seguir para realizar publicaciones o comentarios en las redes del BCIE.

IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

Artículo 63. Corresponde a la Presidencia Ejecutiva aprobar y dar a conocer todos los mecanismos necesarios para implementar la presente Política mediante manuales, procedimientos y cualquier otro documento normativo que estime necesario, con el fin de que todo usuario de información conozca y aplique esta Política.

Artículo 64. La presente Política debe ser revisada cada vez que haya cambios significativos en los componentes del Sistema de Administración de la Seguridad de la Información y periódicamente como parte de un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo del cumplimiento y la aceptación de las directrices y de la estrategia de implantación en todos los niveles del Banco.

ACCIONES JURÍDICAS Y DISCIPLINARIAS

Artículo 65. El BCIE se reserva el derecho de tomar las acciones legales que corresponda en caso de violaciones a lo establecido en esta Política que tengan como consecuencia pérdidas financieras o daño de cualquier índole.



CODE OF ETHICS

Ethics Office / Secretariat / Legal Counsel
AI.ANX.DCM.CodeofEthics

Public Once Approved

In accordance with the regulatory framework of the Access to Information Policy, this document will be published on the Bank's external website after its approval.

DEVELOPMENT

TITLE I. CODE OF ETHICS

CHAPTER I. GENERAL ASPECTS

Article 1. On the objective. The objective of this code is to establish a framework of appropriate conduct, governed by institutional principles and ethical values articulated by the Central American Bank for Economic Integration (CABEI), through rules that establish the behaviors that are expected of its personnel and that the personnel expects of their co-workers in the exercise of their work and interpersonal functions, understanding that it is a living document that must be continually reviewed. The foregoing with the purpose of generating and strengthening an Ethical culture and environment that allow the fulfillment of institutional objectives.

Article 2. Scope of application. In accordance with the provisions of CABEI's Organization and Administration Regulations (ROA), the content of this Code of Ethics will be applicable and generally observed at all hierarchical levels of the Bank, including Directors, officers and employees of the Bank, regular staff, contractors, young professionals, external interns, professional trainees, and any other member of the different staffing programs that are approved in the Bank and in accordance with the provisions of the General Regulation of Human Resources Administration.

CABEI expects that any counterparty that has a relationship with the Institution, despite the fact that it may have its own Code of Ethics, will act in accordance with this code. In the specific case of the procurement procedures for the operation of the Bank, as well as those in which CABEI performs the function of executing said procedures, non-compliance with the institutional principles and ethical values of the Institution will give rise to the consequences foreseen in the instruments that respectively regulate these relations.

Article 3. Relation to other Bank Policies. This code serves as the primary policy document related to Ethics, establishing the general principles and expectations of conduct of the Bank's personnel in the workplace and, where applicable, including, outside the workplace. However, other documents may offer guidance and rules regarding specific functions and interactions in order to complement each other.

The Ethics Office, in the performance of its functions and with the aim of creating synergies, will coordinate, where appropriate, with the attached offices the identification of initiatives that due to their nature could be the subject of joint or complementary work. In addition to those mentioned above, it can coordinate efforts to carry out activities jointly with the Administration, as well as with the respective committees. The foregoing, taking into consideration the independence of the Ethics Office and the confidentiality of the matters under review.

Article 4. Doubts related to the application of the Code of Ethics (Guidance and advice). The Code of Ethics should be a source of guidance, orientation, and advice for all CABEI staff while they work as part of a team to achieve their objective, established in article 2 of the Constitutive Agreement.

The Code and the educational campaigns designed by the Ethics Office for its implementation must become the instruments that help CABEI staff convert institutional principles and ethical values into actions.

Consulting the Code of Ethics to obtain information and relying on the good judgment of CABEI staff will help resolve most situations, particularly those that are challenging and unknown, considering that no document can anticipate or provide answers or guidance for every situation that may arise in the workplace. Therefore, if doubts arise about the ethical way of acting, CABEI staff, before proceeding, must seek the advice of their supervisor or the Ethics Officer. The Ethics Officer and the staff of that office will assist in understanding the Code of Ethics when it is not clear what the appropriate course of action is in a particular case.

Article 5. Improper conduct. When this code refers to the terms "infraction" or "improper conduct", this includes, but is not limited to, non-compliance with the obligations acquired as CABEI staff members as specified :

1. Actions or omissions that violate the institutional principals or ethical values established in this Code
2. Failure to adhere to the standards or expected behaviors of personnel within an international organization such as CABEI, which are integral to the organizational consciousness and conduct.

An action does not need to involve malicious intent or fault to be considered improper conduct.

Article 6. Institutional principles. The institutional principles that the Bank has as a basis to appropriately meet its objectives should be considered as a guide in all institutional actions of the Bank's personnel. These are listed below:

(a) Efficient fulfillment of its purpose and its institutional framework: all Bank personnel shall act diligently in each of its operations, faithfully complying with its purpose, the Constitutive Agreement, and the rules, regulations , resolutions, and agreements that regulate the Bank.

Likewise, they will act diligently in order to protect the interest and ensure equitable treatment to all the members of the Institution in the terms established in the Constitutive Agreement and in the corresponding regulations in such a way that they attend with objectivity and impartiality their programs of economic integration and of economic and social development.

(b) Proper customer service: the Bank's staff will serve their clients promptly, with dedication, transparency, and professionalism, facilitating the processing of operations and providing them with the information that allows them access to the Bank's services, protecting their confidentiality and privacy.

(c) Efficient compliance with sources: the Bank's personnel will honor the Bank's commitments to the sources of funds, complying with the terms and conditions accepted in the loan contracts. Likewise, they must ensure that these commitments are consistent

with the Bank's equity integrity and that they strengthen its participation in international capital markets, as well as its institutional prestige.

The Bank's personnel will comply with the agreements and regulations in force in their relations with international and multilateral credit organizations and other institutions, maintaining and cultivating an honorable image.

- (d) Valuing the Bank's human resources:** the Bank's governing bodies, implementing the tone from the top, will promote an organizational climate conducive to the stability and comprehensive development and well-being of its staff members. In this sense, they must promote the synergy of work between the different areas, respect for human dignity and favor the growth and individual well-being of its members and must take concrete actions to effectively prevent all improper conduct. Likewise, these bodies will guarantee the investigation of existing complaints in this regard, as well as the possible sanction of the offender or offenders and moral reparation for the damage caused, when appropriate, in accordance with the provisions of current regulations.
- (e) Culture of teamwork and cooperation:** all the Bank's personnel, as CABEI is an institution that works for the integration and development of member countries, will foster a work environment that promotes a positive organizational climate, which allows the generation of a culture of teamwork and respect and cooperation among the members of its staff.
- (f) Basis for actions:** the actions of all the Bank's personnel will be based exclusively on established technical criteria in its regulations and based on the highest standards of multilateral development banking, as well as sound practices of the banking industry; the foregoing in accordance with the provisions of the Constitutive Agreement. The Bank's personnel, regardless of their hierarchical level, may not exceed or ignore the mandates provided in the regulations for the fulfillment of their functions, avoiding any form of discretion.

In addition, they will not accept conditions of a political nature from clients or sources of resources or that contravene the purpose of the Bank.

CHAPTER II. ON ETHICAL VALUES

Article 7. Ethical values and institutional commitment. CABEI is committed to fostering and maintaining a work environment that favors ethical behavior and that actively stimulates an open dialogue on these matters. Through their actions and communications, all CABEI personnel are expected to demonstrate adherence to the following ethical values: (1) respect; (2) equality; (3) loyalty; (4) integrity; and (5) transparency.

The successful implementation of the Code of Ethics depends on the commitment of all Bank's personnel to abide by and strictly adhere the guidelines established therein. This commitment is assumed upon joining the Bank, so it is the responsibility of all its personnel to read, understand, and assume the commitments established in the Code of Ethics to contribute to

maintaining a positive environment by fulfilling the responsibilities in accordance with the institutional principles and ethical values.

Considering the preventive spirit of this code and for this purpose, the Ethics Office will require the Bank's staff to annually sign a sworn statement by which they certify that they have read, understood, and assumed the commitments established in the Code of Ethics. Likewise, the Ethics Office may develop practical guides, programs, and activities to promote good conduct in lines with these institutional principles and ethical values, thereby facilitating their understanding, dissemination, and implementation.

SECTION I. ON THE VALUE OF RESPECT

Article 8. Respect. The Bank's staff must develop interpersonal relations with due consideration tolerance, harmony, impartiality, and without causing harm, offense, or damage.

For their part, the Board of Directors and the Senior Administration will implement specific actions in such a way as to create a positive and professional work environment in which everyone is treated with dignity and respect.

Considering the diversity of the Bank's staff, it is expected that everyone shows respect towards their colleagues and other individual present in the Bank's facilities or providing service to it. All staff are held accountable for their actions and therefore take responsibility for maintaining professional, impartial, and respectful conduct, raising concerns they may have about improper conduct that is disrespectful to other staff member(s) , as well as report them and take action to correct any fault in their behavior. Disrespectful actions such as insults, offenses, malicious and deliberately false statements about others, and verbal and physical abuse, among other behaviors, are considered improper conduct.

Bank personnel must be aware that they represent the Institution at all times and, as such , are expected to demonstrate professionalism, courtesy, and tolerance when dealing with others. They should approach their work with empathy, listening carefully, being open to hearing new ideas, and speaking kindly to any counterparty, be they colleague, client, partner, supplier, or member of the public. In the same vein, this also entails the responsibility of safeguarding the Bank's physical assets by using them appropriately.

As CABEI is an international organization, it requires its staff to be aware of the various local customs, traditions, and different work cultures of the member countries and counterparts. The Bank is committed to offering staff a work environment characterized by openness, trust, respect, impartiality, creativity, motivation, and innovation, recognizing that respecting and valuing differences is key to collective success.

The Bank will take the necessary steps to create and maintain an inclusive culture in which support is provided and there is no fear to ask each other for help.

CABEI staff performing supervisory duties have the additional responsibility of creating and maintaining a work environment that is respectful and impartial to all. Staff have the right to

feel safe and comfortable, and to be free from any kind of harassment, abuse, or other forms of unwanted behavior at work.

Article 9. Prevention of harassment in all its manifestations. Therefore, all forms of harassment or bullying in any of its modalities are prohibited, regardless of who the victim is (including support staff, contractors, interns, young professionals, or clients) or the offender, or whatever their hierarchical level.

Article 10. On harassment. Harassment involves disrespectful treatment that occurs once or repeatedly, and may be verbal or physical. It typically has the purpose or effect of creating an intimidating, hostile, or offensive work environment. Such undesirable behavior interferes with a person's ability to perform optimally in a person's job and can occur both inside and outside the formal workplace.

Whatever its form, harassment is unacceptable and requires an immediate response from the victim or any member of staff who witnesses it. It is desirable that all CABEI staff clearly communicate to their colleagues any behavior that they consider objectionable and request that such behavior cease. Likewise, you may request assistance from the Ethics Office or the corresponding instance, if these actions persist.

The following behaviors are illustrative and non-limiting examples of harassment:

- (a) Differential treatment for reasons of race, color, language, gender, age, ancestry, nationality, economic position, health status, disability, marital status, religious, political, sexual preferences, or any other personal condition, whether real or perceived.
- (b) Derogatory comments or behavior and the display or circulation in the workplace of written or graphic material that demeans or shows hostility towards a person or group; making offensive, racist, or discriminatory jokes regarding a person or group in relation to their personal condition, whether real or perceived, that denigrates the Bank's collaborators.
- (c) Spreading rumors, false information, lies, or making baseless accusations against an individual or group in relation to their work environment
- (d) Hostile behavior against any person who works at the Bank, which may include insults and/or threats.
- (e) Yelling or verbally abusing co-workers or colleagues; exhibiting aggressive or intimidating behavior; ridiculing or interfering in the performance of the work and responsibilities entrusted to one or more members of the Bank's staff.
- (f) Behaviors of harassment, intimidation, mistreatment, or bad faith rumors towards any person who works at the Bank.

Article 11. Workplace harassment. Workplace harassment represents inappropriate or abusive conduct that is manifested in the workplace by one or more individuals, which threatens the dignity, psychological integrity, or physical well-being of the affected person.

To better understand the extent of this behavior, some examples are included in an illustrative but not exhaustive manner:

- (a) Insults associated with personal traits or professional competence.

- (b) Behavior whose purpose is to isolate or humiliate a person or group, such as the unjustified exclusion from meetings or the unjust denial of information or equipment necessary for the performance of functions.
- (c) The threat or taking of adverse measures against a person or group for opposing or refusing to participate in an improper act or for differences of opinion.
- (d) Bullying, including physical or verbal abuse.
- (e) The dismissal of the ideas, opinions, work, or blocking the possibilities of job growth within the institution without foundation and with the intention of attacking the dignity, psychological integrity, or physical well-being of the subordinate, by a person with a hierarchically superior position.
- (f) Making unsubstantiated remarks in relation to non-compliance with rules, procedures, requirements, or any action or omission in which the honorability of a Bank collaborator is implied or questioned or it is affirmed that they have committed breaches of conduct, ethics, morals, social, or of any other nature.
- (g) Yelling at or verbally abusing coworkers or colleagues, exhibiting aggressive or intimidating behavior, ridiculing, or interfering with the performance of work and responsibilities entrusted to one or more staff members of the Bank.
- (h) Unfairly loading a subordinate with work.

Article 12. Sexual harassment. Sexual harassment represents conduct that, due to its nature, scope, context, and magnitude involves Bank personnel in any form of unwelcome sexual advances, requests for sexual favors, or other manifestations of a sexual nature, explicit or subtle, that objectively causes the victim to feel offended, distressed, or humiliated. Sexual harassment may include various behaviors and affect individuals of the same or different genders.

Listed below, including but not limited to, some behaviors that could be considered sexual harassment:

- (a) Invitations to social activities or appointments when the person to whom they are addressed has stated that they are not interested.
- (b) Unwelcome sexual flirting, advances, or proposals.
- (c) Overt, implied, or subtle requests for sexual favors in exchange for actual or promised job benefits, such as favorable reviews, promotions, or tenure.
- (d) Sexual, demeaning, or suggestive comments; epithets, jokes, and teasing of a sexual nature; written or verbal references to sexuality, or comments about a person's body.
- (e) Retaliation or threat of retaliation following a negative response to sexual advances.
- (f) Exhibition of objects, images, or general content with a sexual connotation.
- (g) Obscene gestures or unwanted physical contact with a sexual connotation.
- (h) Inquiries or discussions of a person's sexual experiences or activities.
- (i) Sending texts or images or other types of inappropriate and unsolicited communication of sexual connotation, through cell phones, email, internet, social networks, or any other means.

Article 13. Zero-tolerance of harassment. Disrespectful behavior and harassment have no place at CABEI. In this regard, personnel with authority over others must perform special functions that consist of the following:

- (a) Communicate to their collaborators that disrespectful behavior and harassment will not be tolerated.
- (b) Ensure that the employee who raises concerns is supported and not subject to retaliation.
- (c) Never excuse or minimize improper conduct or inappropriate behavior.
- (d) When it is necessary to take complaints and concerns to the Ethics Office.

SECTION 2. ON THE VALUE OF EQUALITY

Article 14. Equality. In the context of this code, equality means that all CABEI staff must comply with the rules and policies consistently, congruently, fairly, and uniformly to ensure a work environment that is free of favoritism, abuse in the exercise of authority, and arbitrary or capricious decisions.

It also means that any Bank collaborator must offer inclusive and equitable treatment to the rest of the staff, suppliers, external consultants, clients, and other stakeholders.

Article 15. Appropriate use of authority. Personnel entrusted with authority over other by CABEI have a special responsibility to exercise said authority with discernment and equity, respecting the institutional principles and basic ethical values, and promoting respect from their subordinates. Even those who do not formally act as supervisors must take care not to use their position in the Bank to pursue inappropriate ends, either internally or with suppliers, external consultants, clients, and stakeholders or business partners.

Examples of such actions include but are not limited to:

- (a) Engaging in intimidating or harassing conduct.
- (b) Interfering with the ability of others to work effectively, for example, by hindering their access to information or resources.
- (c) Demanding personal tasks or favors from subordinates.
- (d) Habitually make unreasonable job demands.
- (e) Use of credentials or position in the Bank to obtain attention or special treatment.

Article 16. Prohibition of discrimination. CABEI will promote a workplace where all personnel are valued, differences are respected, and opportunities for equal and inclusive treatment are provided to all. CABEI respects and values diversity because it represents a range of experiences, cultures, and backgrounds. The Institution is convinced that diversity contributes to the success of its activities.

Consequently, CABEI has a policy of zero-tolerance for any form of discrimination and encourages inclusion, therefore, Bank collaborators cannot discriminate against their colleagues in any way.

CABEI energetically prohibits discrimination in order to promote labor equality, prevent and eliminate all types of workplace violence and discrimination, whether for reasons of ethnic or national origin, culture, skin color, physical appearance, sex, gender, gender identity and expression, sexual orientation, age, disability, religion, language, social, economic, legal status, as well as health, pregnancy, marital or civil status and immigration status, among others, whether real or perceived.

Article 17. Violence in the workplace. CABEI's most valuable asset is its collaborators, therefore, safety and comfort in the workplace are paramount. The members of CABEI's governing bodies and all personnel in general will provide all staff with a safe work environment, in which violence is unacceptable.

Violence in the workplace can also constitute a crime in the Bank's member countries, so CABEI may refer staff members who commit or threaten to commit acts of violence to the national authorities, in accordance with the regulations and nature of the Bank, following the established procedures.

In that sense, any action, incident, or conduct that reasonably causes a Bank staff member to fear for the personal safety of their co-workers, family, friends, or property constitutes violence in the workplace. This may occur at the Bank's facilities, or outside of them in certain circumstances.

Examples of such actions include but are not limited to:

- (a) Physical assault.
- (b) Threatening physical aggression or through aggressive contact directed against another person.
- (c) Threatening to cause harm to a person or their family, friends, associates, or their property.
- (d) Intentionally destroying or threatening to destroy property owned by the Bank or by others.
- (e) Harassing with threatening or intimidating phone calls.
- (f) Stalking.
- (g) Making intimidating or veiled threat of physical harm.

SECTION 3. ON THE VALUE OF LOYALTY

Article 18. Loyalty. Loyalty means that CABEI staff, in the performance of their duties, are accountable exclusively to the Bank and its authorities, being committed to the Institution, as well as to their work peers, promoting a positive institutional image in all activities, avoiding comments and actions that may harm CABEI or their work peers. Likewise, it implies protecting and maintaining the confidentiality all the information provided and generated by the Institution or its clients, when appropriate, in accordance with the provisions established for that purpose.

Article 19. Conflicts of interest. A conflict of interest is a situation in which a dilemma arises between personal interests and the interests of the institution or its clients. It means that the private interests of a person interfere or can be understood to interfere with their decision-making and with the full performance of their official duties.

From this perspective, a **conflict of interest** is a situation in which a CABEI staff member has an interest that unduly influences their criteria, decisions, actions, powers, and responsibilities with the Bank, its clients, or counterparts. Such situations violate the institutional principles and ethical values outlined in this code, as well as the duties that Bank staff members acquire as collaborators of an international organization.

Conflict of interest can be categorized as direct or indirect. It is understood that there is a **direct interest** if the situation that gives rise to the conflict of interest could generate a benefit for the staff member, or when the management or decision that corresponds to a staff member involves a third party that serves as a link between the staff member and their interests.

On the other hand, **indirect interest** will be understood as those cases in which the situation that gives rise to the conflict of interest can generate a benefit to a third party, whether a natural or legal person, within the limits, parameters, and relationships established in this code. In addition, an **indirect interest** is considered if the management or decision that corresponds to a staff member, even without a benefit, involves any of the staff member's relatives (up to a fourth degree of consanguinity and second degree of affinity) or a person with which they maintain a personal relationship.

A **real conflicts of interest** occurs when a Bank staff member actually has an interest that could conflict with the Bank's interests for a current or potential situation. A current situation when the interest of the staff member conflicts with a situation that is occurring. A **potential conflict fo interest** is a situation that may occur when a Bank staff member has a current interest that could conflict with the Institution in a future situation or circumstances.

Apparent conflicts of interest could be when Bank personnel do not have a current interest, but third parties could estimate, assume, or perceive the existence of such conflict , which may have reputational effects, both for Bank personnel and/or or for the institution itself.

Therefore, Bank staff members must prevent, avoid, or manage, according to the circumstances of each case, any situation that creates or could create a conflict of interest in any operation, whether active or passive, or in any procurement procedure, as well as any matter that improperly influences their judgment. For this purpose and to improve the understanding of situations of this nature, the Bank will implement actions that help staff identify those that could generate some type of conflict. For this purpose, the Ethics Office must develop the regulations and protocols required in this regard.

Article 20. Possible conflicts of interest. A conflict of interest can arise in various ways. The following are some of the most common conflicts of interest described in a illustrative but not limit manner, along with information on how to address and resolve them.

(a) Financial interest. Financial interest refers to the possibility of receiving interest, dividends, capital appreciation, fees, or other monetary, economic, or in-kind payments or benefits.

Bank personnel must avoid **real** or **apparent** conflicts of interest between their own financial interests, those of their spouse, or their relatives and the interests of the Bank.

Therefore, Bank personnel must refrain from participating, knowing and influencing at any stage of the decision-making process, in matters involving legal entities that are direct counterparts or beneficiaries of resources from CABEI.

A property relationship is established when the staff member, their spouse, or their relatives have a shareholding or capital interest of at least 5% percent in the CABEI counterpart legal entity or at least 25% participation in a legal entity that in turn owns 5% percent of shares in CABEI's direct counterpart.

The following practices, among others, are listed as examples of conflicts of interest that may arise but are subject to assessment by the Ethics Office and, if applicable, the Ethics Committee:

- (i) Carrying out short-term transactions in securities issued by the Bank.
- (ii) Having a financial interest in a loan granted by the Bank to third parties or to an entity with which there is a property relationship.
- (iii) Possessing a financial interest in an entity linked to an active or passive operation of CABEI, which maintains another type of financial relationship with it, or which is a supplier of the Bank.

The foregoing includes any financial interest in borrowers, creditors, or suppliers of the Bank, or in an executing agency of an activity financed by it that could reasonably be perceived as influencing decision-making.

(b) Participation in activities outside the Bank (political or other activity). Bank staff must work for CABEI full time. Consequently, the aforementioned personnel must comply with the provisions of CABEI's Organization and Administration Regulations (ROA) and the General Regulations for Human Resources Administration, regardless of their position, and may not engage in occupations other than those of the Bank or assume charges or positions that are incompatible with the correct performance of their duties or that may cause commitments or difficulties for the Institution.

Although staff may have an interest in civic and political issues in their respective countries, caution must be exercised so as not to affect their status as CABEI staff members. Consequently, they must refrain from participating in partisan political activities or issuing comments, judgments, or opinions of that nature in areas that could compromise the Bank's reputation. Likewise, no member of its staff may accept any public or political position, whether paid or not. The Bank's staff member must resign from their employment at CABEI before accepting a candidacy or being elected or appointed to political or popularly elected positions.

In accordance with what is indicated in the first paragraph of this section, a staff member may not hold administrative relationships or functions in another legal entity. A management relationship is established when the staff member holds a position of director or member of the board of directors, legal representative, sole administrator, general manager, or similar, or has an authorized signature, whether they participate in the capital of such legal persons or not.

The foregoing does not apply to family business companies created with the exclusive purpose of managing family assets, or civil associations whose scope of action has no relation to those of CABEI or that does not imply any incompatibility with the performance of their duties at the Bank, provided that they are made individually and not as an employee of the Bank. By incompatibility it will be understood that they are within the same line of business as

the Bank, that they can provide services to it or that, in some way, could suppose a conflict of interest.

(c) Employment before and after CABEI. Bank staff should avoid conflicts related to a former or prospective employer.

(i) Previous Employment. Unless authorized by the Ethics Committee, for a period of five years from joining the Bank, staff members must refrain from participating in decisions that affect their former employer. If at the end of that period there is still a potential conflict of interest, real or apparent, the Ethics Office should be consulted before performing any work related to the former employer. The foregoing does not apply if the previous employer was the State or an international organization.

(ii) Probable employment. It is prohibited that the performance of Bank staff functions be influenced or affected in any way by the possibility of obtaining a job or being able to engage in future independent professional or technical activities outside CABEI.

(iii) Subsequent employment. The Bank recognizes the freedom of each staff member to obtain jobs or engage in activities in the exercise of their profession as of the termination of their relationship with CABEI. In the development of the new job, or their subsequent activities, they may use the experience and knowledge accumulated during the term of their relationship with the Bank, unless this implies the disclosure of information considered to be of internal, confidential, or restricted use for the period determined by the Information Security Policy.

However, for a period of five years after the termination of the relationship with CABEI, the responsible dependencies within the Bank will prevent former staff members from participating in CABEI operations or activities with the private sector, provided that the former staff member in question has had any direct participation in that particular operation or activity during their tenure with CABEI.

(d) Family or personal relationships. The Bank's staff must avoid conflicts of interest that derive from a family, kinship, or personal relationship with another CABEI staff member.

Within the framework of the Code of Ethics, the definition of relative or family member includes the spouse or household partner of a CABEI staff member, as well as individuals related to them by blood ties (including adoption ties) up to the fourth degree or by ties of affinity up to the second degree, these being able to derive from a marriage relationship or de facto union. When the term "relative" or "kinship" is used, it should be understood that it refers to the individuals that are included in this definition or to the link that exists by virtue of the aforementioned ties.

Having a relative within the chain of command, exercising supervision or control over a relative, or both working in the same dependency could create or give the appearance of creating a conflict of interest for a CABEI staff member. Likewise, members of the Bank's staff may not make decisions in the labor or commercial field involving an individual with whom they have a personal, family, kinship, sentimental, or close or intimate friendship relationship,

whether they work as CABEI personnel, or as a supplier, contractor, or client of the Bank. Its personnel should not be involved in the assignment of tasks, performance evaluation, satisfaction surveys, or evaluation of services, among others, that occur with respect to that person.

Additionally, any sentimental relationship between a superior and a subordinate that has not been timely reported will be considered a conflict of interest. In accordance with the foregoing, the Bank urges staff to avoid this type of relationship.

To prevent conflicts of interest, all of the above situations must be reported to the Ethics Office as soon as they become aware. To this end, the Ethics Office will develop the necessary regulations and protocols.

In addition, in the specific case that a CABEI staff member learns that a family member is applying to work at the Bank, they must inform the Human Resources Office and the Ethics Office as soon as they become aware of the foregoing, so that the necessary preventive measures can be taken.

(e) Procurement and contracting. CABEI's collaborators must refrain from favoring any person in the process of procuring goods and services or in the workplace due to a close relationship or kinship that could influence the person's benefit.

In the event that a member of the Bank's staff identifies a situation in which a relative, friend, or partner has an interest in any operation or activity of CABEI (including an interest in the labor field or in the contracting of goods and services) that could generate a conflict of interest (real or apparent), they must report the situation to their immediate superior, abstain from participating in the process, and, if applicable, request advice from the Ethics Office.

(f) Gifts and favors. Refers to any type of gratuity received from people outside the Bank, such as food, transportation, accommodation, invitations to entertainment events (cultural, sports, or otherwise), discounts, loans, cash or its equivalent, these may be gift cards, vouchers or credits and, in general, any type of compensation, economic benefit, monetary or in-kind contribution.

Bank personnel are generally prohibited from accepting gifts or favors from related third parties that may compromise or give the appearance of compromising their objectivity and integrity in the performance of their duties, except those authorized by current regulations. Likewise, Bank personnel are prohibited from soliciting gifts or favors from a related third party.

Related third parties. For the purposes of applying this provision, third parties related to CABEI are understood to be any natural or legal person with whom the Bank plans to establish or establishes a commercial relationship or a contractual relationship of any nature, either with the intention of granting or authorize any type of active, passive, pre-investment, technical or financial cooperation, donation, sponsorship operation, or as a supplier of goods, services, or consultancies within institutional procurement procedures or those carried out with CABEI resources in its operations.

The foregoing includes, but is not limited to, any borrower, beneficiary, contractor, supplier, or offeror, who is currently or has formally demonstrated their interest in being so.

Considering the above, gifts or invitations can only be accepted when all the following conditions are met:

- (i) Their nominal value does not exceed two hundred dollars, currency of the United States of America or its equivalent in local currency.
- (ii) The accumulated value of all gifts or invitations from the same person or legal entity does not exceed in the last twelve (12) months the value established in the previous point.
- (iii) They are not cash, electronic currencies, or their equivalents.
- (iv) They have not been requested by CABEI staff.
- (v) They are consistent with ethical standards and generally accepted business practices.
- (vi) The gift or invitation is not contingent on the realization of a consideration nor does it create an obligation or an expectation to the counterparty.

Invitations. In the case of invitations, seminars, or workshops, the Bank's staff may accept a related third party to make payments (partial or total) of expenses associated with events that the staff will attend, if they have prior authorization and declare to the Ethics Officer that there is no current conflict of interest and that their participation will not generate a conflict of interest.

Authorization instances:

- (1) The Board of Directors for the Executive President, the Directors, and the heads of the dependencies attached to the Board of Directors.
- (2) For the Executive Vice President, the Executive President.
- (3) For the Controller, the Controller's Committee.
- (4) For the personnel of the directorates, the corresponding Director.
- (5) For the personnel of the offices attached to the Board of Governors or the Board of Directors, the respective head of that office.
- (6) For the rest of CABEI staff, the Executive Vice President.

Likewise, Bank personnel may accept local food or transportation and related courtesies provided as long as their nominal value does not exceed the limits established in these regulations, and when they are naturally associated with their functions related to the Bank business and provided that its acceptance does not compromise the objectivity and independence of criteria in a real or apparent way.

If, in certain circumstances, the refusal to accept an unsolicited gift or favor with a nominal value greater than the limits indicated above may cause inconvenience to the donor or to CABEI, or be interpreted as an offense, the Bank staff member may accept on behalf of the Institution, as long as they report the situation **timely** to the Ethics Office, who will issue Conflict of Interest Report with their technical opinion and request, if applicable, its registration with the Administrative Services and Institutional Procurement (SAAI) dependency as an asset owned by the Bank.

For practical purposes of the above, the Ethics Office will be authorized to issue instructions, protocols, and guidelines as deemed necessary.

Bank personnel should refrain from offering significant-value gifts or favors that could influence the decisions or actions of individuals engaged in business with CABEI.

Institutional gifts. Institutional gifts that the Bank acquires from time to time to be distributed as gifts to CABEI staff members, suppliers, and current and potential clients of the Institution are excluded from this provision. However, by means of the Bank's regulations, it will be ensured that these gifts are low cost, avoiding large outlays in this regard, applying the principles of reasonableness and austerity for this purpose.

Article 21. Disclosure of conflicts of interest. When a conflict or a situation with the potential to become a conflict arises, CABEI staff must seek guidance from their supervisor and communicate immediately to the Ethics Office. The Ethics Office can advise them in how to avoid getting into a conflict or, if a conflict has already been identified, can help them take proactive action to prevent the situation from escalating to a report of improper conduct.

SECTION 4. ON THE VALUE OF INTEGRITY

Article 22. Integrity. CABEI staff must demonstrate honest, truthful, and incorruptible conduct, based on truth, honesty, rectitude, justice, excellence, prudence, and discretion in all their actions, safeguarding confidential information and avoiding any public statement or action that may compromise or give the appearance of compromising the performance of their official duties or harm the reputation of the Bank. In addition, staff must comply with the Bank's rules and regulations, as well as applicable local laws.

CABEI staff must provide true, accurate, and timely information in the performance of their duties or in other situations in which disclosure of information is required, the truth should never be intentionally distorted. Integrity and discretion should guide their actions when providing information to others, both inside and outside the Bank.

Article 23. Internal or occupational fraud and corruption. Internal or occupational fraud refers to the misuse of one's occupation or employment for personal enrichment, directly or indirectly, through the deliberate misuse or misapplication of the Bank's processes, resources, or assets.

The Bank's personnel must carry out their functions with integrity, ethically, and transparently. Therefore, engaging in any activity that can be classified as internal or occupational fraud will be considered as an action that directly violates the institutional principles and ethical values of the Bank and against the performance of their obligations as collaborators. In turn, the Bank will establish the necessary internal control mechanisms and, through the Ethics Office, will continuously train its personnel against said practices.

Internal or occupational fraud. Internal or occupational fraud occurs when CABEI staff incurs in some of the forms of corruption that are listed below, which are illustrative but not limiting:

- (a)** A fraud scheme whereby a staff member abuses their influence in a business transaction in such a way as to violate their duty to the Bank in order to obtain a direct or indirect benefit. Corruption can materialize when there is a conflict of interest, so it is mandatory

that any situation considered as such be managed in accordance with the provisions of the respective section of this code and its complementary regulations and processes.

- (b) When something of value is offered, given, received, or requested to influence a business decision.
- (c) When there is embezzlement and illegal appropriation of assets, which occurs when a staff member steals or misuses the Bank's resources or information.

The following are illustrative, but non-limiting examples of embezzlement and misappropriation of assets:

- (i) Theft of petty cash.
 - (ii) Fraudulent disbursements.
 - (iii) Improper use or theft of the Bank's assets.
- (d) A financial statement fraud scheme whereby a staff member intentionally makes a false statement or omits material information from the Bank's financial reports.

Some examples of financial statement fraud may include the following:

- (i) Overstatement of income/assets.
- (ii) Understatement of income/assets.

Article 24. Proper use of information. Physical information assets and intellectual property are essential for CABEI's activities and are considered, after human capital, one of the most valuable assets, for which reason CABEI personnel have the duty to protect them. In this regard, all personnel must manage and use the Bank's information responsibly and protect the records and information, whether it belongs to CABEI or its strategic partners, clients, or collaborators, in accordance with the CABEI Information Security Policy.

Additionally, CABEI personnel must refrain from issuing comments, in public or in front of third parties, that discredit the good image and institutional integrity of the Bank. By way of example but not exhaustively, the following forms of inappropriate use of information are indicated:

(a) Public statements. In order for the Bank to express itself clearly and consistently, staff must not make public statements on behalf of or about the Bank unless expressly authorized to do so. It is important for staff to note that opinions or information on behalf of or about the Bank shared on the internet also constitute public statements. Similarly, only designated representatives of the Bank may make statements to the press on its behalf. They, therefore, must avoid any personal reference or opinion.

(b) Personal Use of Information. Bank personnel who use information obtained in the course of their employment relationship with the Bank must adhere to CABEI's Information Security and Access to Information policies, institutional principles, ethical values, and the specific guidelines below:

(i) Handling of confidential, reserved, or non-public internal information. It is the obligation of all CABEI personnel to protect the confidentiality of the information to which

they have had access due to their position and in the exercise of their functions, both inside and outside the workplace.

Information classified as non-public can only be shared with other members of the Bank's staff exclusively when it is necessary for the exercise of their functions and such information should never be disclosed outside the Bank without prior approval. In the case of country directorates, this type of information may be transferred, according to the established line of command, to the country governors, when it is considered prudent.

Likewise, CABEI staff must not use internal, confidential, reserved information, or information not accessible to the public to favor themselves personally or to favor third parties.

These obligations remain in force even after the termination of the employment relationship with the Bank, in accordance with the regulations in force in the Institution.

(ii) Information available to the public. The information obtained in the exercise of official functions may be used only for personal purposes or for the benefit of others only if said information is available to the general public.

(iii) Information protected by copyright. The Bank owns the copyright to all material produced by its staff as part of their official duties and therefore has the exclusive right to publish or use it in any way it deems appropriate. If a CABEI staff member wishes to publish or use material that has not been produced as part of their functions at the Bank, but that refers to it, they must obtain prior authorization from the Communications and Access to Information Directors Committee.

All staff have the obligation to comply with the law, respect the copyrights of others, when reproducing or transmitting printed or electronic literary material provided by the Bank.

(c) Use of the physical and financial assets of the Bank. The assets owned by the Bank include physical and financial assets such as facilities, equipment, office supplies, computers, and financial resources. CABEI entrusts its staff with the use of such assets in the best institutional interest and that of the stakeholders, with the purpose of facilitating the assigned work. This implies the responsibility of the personnel for its proper use and protection against damage, loss, theft, or improper use.

(d) Intellectual property. CABEI's intellectual property is another valuable asset that staff must protect at all times. Intellectual property includes copyrights, patents, trademarks, design rights, logos and distinctive names, as well as the Bank's name and symbols.

(e) Use of the Bank's computerized systems, devices, and Internet access. The Bank's property also includes its computer systems, hardware, software, email, Internet access, telephones, and any other electronic communication and information storage device.

It is the responsibility of CABEI staff to make professional, ethical, and lawful use of the Bank's equipment. Creating, downloading, searching, storing, copying, or transmitting material that

is sexually explicit or depicts or promotes racial, ethnic, religious, or any other discrimination is prohibited. In all circumstances, staff are expected to exercise good judgment when using Bank property, taking into account the possibility that the use and transmission of certain content may offend or annoy others. It is also important to remember that there is no expectation of privacy in the use of the Bank's equipment or systems.

(f) Appropriate use of social networks. Social networks represent, among other things, the opening to new spaces for connection, socialization, meeting, exchange and knowledge. Thanks to them, today it is very easy to share information and CABEI collaborators must maintain and take care of their image when sharing information.

CABEI recognizes the difficulty that there may be in separating the personal sphere from the institutional function performed, so the use of personal social networks should never put the Institution at risk. CABEI employees must make good use of social networks, respect the audience and their colleagues, not publish personal opinions or any other unauthorized reference on behalf of the Institution.

In this understanding, it recognizes that these tools can provide current and innovative channels to interact between employees and sometimes be used for personal purposes using technologies provided by the Bank. When making use of social networks –associated or not with CABEI– the following rules must be kept in mind:

- (i)** Always protect the assets, reputation, and confidential information of the Bank, without forgetting that the Internet is a public space.
- (ii)** Use this code as a guide when making decisions of an ethical nature.
- (iii)** Follow the Bank's policies and standards for the use of its technological assets, whether intervening as agents authorized by the Bank, or using social networks and media in a personal capacity.
- (iv)** Refrain from using social networks to exercise any type of inappropriate behavior contrary to good customs, within the scope of the institutional principles and ethical values contained in this code.

SECTION 5. ON THE VALUE OF TRANSPARENCY.

Article 25. Transparency. CABEI's activities and communications will be carried out clearly, without doubt or ambiguity, and without hiding or omitting any type of information, while avoiding at all times incurring in risky situations.

Article 26. Reports and record keeping. CABEI's books and records must reflect operational transactions fully and accurately. These records must always be in accordance with the internal control system and the financial and accounting regulations in force.

Article 27. Management, retention, and elimination of records. CABEI's records are a fundamental component for fostering trust among the Bank's clients, suppliers, and members. To this end, the Institution has policies that guide the management of records and retention periods. Therefore, the staff must observe the records management policies and their retention periods in all the countries in which CABEI operates. Additionally, they have an obligation to report to the respective authorities, when there is any suspicion or indication that someone has improperly hidden, altered, or destroyed any record.

CHAPTER III. ON THE RESPONSIBILITIES DERIVED FROM THE CODE OF ETHICS

Article 28. The Bank's governing bodies in matters of Ethics. The promotion of institutional principles and ethical values, and the prevention of improper conduct are priorities for the Bank. In this sense, the members of the Bank's governing bodies are committed to fostering and maintaining a work environment that favors ethical behavior and that actively stimulates an open dialogue on ethical matters.

Through their actions and communications, the members of these bodies, will demonstrate their adherence to the following basic behaviors:

- (a) Ensure fair and impartial treatment for all its personnel.
- (b) Guarantee a work environment based on ethical values.
- (c) Do not tolerate abuse in the exercise of authority.
- (d) Be accountable for matters inherent to the obligations and responsibilities of their personnel as decision makers.
- (e) Provide the pertinent tools to achieve adequate ethics management.
- (f) Protect Bank staff members against retaliation of all kinds, including those that could be taken against whistleblowers and witnesses in good faith who report or collaborate in investigations carried out on alleged improper conduct.

SECTION I. ON THE BOARD OF DIRECTORS

Article 29. Of the Directory. The Board of Directors, as the body responsible for the management of the Bank and immediate superior of the Executive President, is bound by the provisions contained in the Constitutive Agreement, in the Regulations of the Organization and Administration (ROA), and in any other current provisions or those that, in the future, is dictated by the Board of Governors and are applicable to it. In this regard, it will exercise all the powers delegated to it by the Board of Governors in matters of ethics, including:

- a) The approval of this Code of Ethics and its Complementary Regulations and Procedures, as well as their modifications.
- b) Inform the Board of Governors of the approved text of the Code of Ethics and its Complementary Regulations and Procedures, as well as when they are subject to any modification.
- c) The designation of the titular and alternate Director to integrate the Ethics Committee, who will have the functions of Chairman of the Committee.
- d) Carry out the authentic interpretation, with a regulatory character, of the Code of Ethics and its Complementary Regulations and Procedures in cases of ambiguity or lack of clarity in these provisions.

SECTION II: ON THE EXECUTIVE PRESIDENCY

Article 30. Of the Executive Presidency. The Executive President is the highest-ranking officer in the Bank's administrative management and has the legal representation of the institution. Under the direction of the Board of Directors, it is responsible for complying with and enforcing the Constitutive Agreement, the regulations, resolutions and agreements of the Board of Governors and the Board of Directors, as well as the other provisions that regulate the Bank and particularly all those related to the Code of Ethics and its Complementary Regulations and Procedures.

Among its authority and functions in matters of ethics, it will be responsible for the approval, at the proposal of the Ethics Office, of the necessary regulations for an effective implementation of the Code of Ethics and its Complementary Regulations and Procedures.

SECTION III. OF THE ETHICS COMMITTEE

Article 31. Ethics Committee. The Ethics Committee is the body responsible for contributing to the strengthening of institutional ethics in accordance with the provisions contained in the Code of Ethics and in the Regulations and Procedures Complementary to the Code of Ethics.

Article 32. On the Functions of the Ethics Committee. The primary role of the Ethics Committee is to serve as the body responsible for reviewing and resolving matters related to misconduct and violations of the institutional principles and ethical values contained in the Code of ethics

In addition, it will contribute to the strengthening of institutional ethics, developing the additional functions of:

- (a) Monitoring and evaluating the guidelines and performance of the organization and its personnel in matters of ethics.
- (b) Promoting an ethical culture in all levels of the Bank's organization through an annual action plan proposed by the Ethics Office, which contains at least the following aspects:
 1. Scheduling talks or institutional exhibitions on ethical issues.
 2. Planning of activities designed to foster an ethical culture and uphold institutional principles and values.
- (d) Recommending the annual report on compliance with said action plan and compliance of the Bank's personnel regarding the submission of the statements required by current regulations in relation to ethics management. Proposing updates to the ethical regulations or a new regulation.

It will also correspond to the Ethics Committee, if it considers it pertinent, on a case-by-case basis and in view of the complexity and nature of the alleged violation of the Code of Ethics, to determine the need for internal or external specialized support for the purposes of carrying out the investigation of the corresponding administrative procedures.

Additionally, it will be the body responsible for reviewing and resolving, at the proposal of the Ethics Office, matters related to complaints regarding conduct contrary to what is established in the Code of Ethics, ensuring compliance with the due process established in the complementary regulations and procedures, without prejudice to other powers and attributions that the Board of Directors assigns to this Committee.

Article 33. Conformation of the Bank's Ethics Committee. The Ethics Committee, for the purposes indicated in the preceding paragraphs, will be made up of:

- (a) A Director, who will have the functions of Chairperson of the Committee. Said Director will be appointed by the Board of Directors of the Bank with annual rotation. The Board of Directors will also designate its substitute with annual rotation, who will be able to participate in the Committee meetings.
- (b) The Executive Vice President
- (c) The Controller

- (d) The Legal Counsel
- (e) The Ethics Officer

All members of the Ethics Committee shall act with voice and vote, with the exception of the Ethics Officer and the Legal Counsel, who shall act with voice but no vote. In the event that the Director who acts as an alternate member participates in the Committee meetings, they will also do so with voice but without vote.

The Chairperson of the Ethics Committee must convene the members of said Committee to discuss matters within their competence. Once the Committee is convened to address a specific matter, it will be the Committee's responsibility to comply with the respective stages of the administrative procedure in order to decide on the merits of the case.

All procedural issues necessary for the proper functioning of the Ethics Committee that are not expressly provided for in these regulations, will be defined by the Board of Directors in coordination with the Chairperson of the Ethics Committee.

The Ethics Officer will designate **someone** of his office to serve as the Secretary of the Ethics Committee and will be responsible for managing administrative procedures.

The administrative process shall commence upon the Ethics Committee's acceptance of jurisdiction.

The members of the Ethics Committee may not delegate their participation in said Committee. Participation shall not be deemed to have been delegated when a temporary manager of the unit has been officially appointed.

Article 34. On the Substitution of the members of the Ethics Committee. If decided by the Ethics Committee, the substitution of any of its members in the event that one of them must excuse themselves or is challenged to hear a particular case, will be done as follows:

- (a) In the case of the Director who acts as a titular member of the Ethics Committee, they shall be replaced by the Director who acts as alternate member.
- (b) In the case of the Executive Vice President, they will be replaced by the Executive President.
- (c) In the case of the Controller, they will be replaced by the Internal Auditor of the Bank.

The titular member of the Ethics Committee who must excuse themselves or is challenged to hear a particular case, they may not participate in said Committee when the case for which they excused themselves or was challenged is under discussion, unless required by it to evacuate some process, just as any other staff member would.

For the purposes of the provisions of the preceding paragraphs, the following are grounds for recusal or excuse:

- (i) When the person reported as violating ethical values is of the same nationality as one of the members of the Ethics Committee.
- (ii) When the person reported as violating ethical values is of the same nationality as one of the members of the Ethics Committee.

- (iii) When the accused is a member of the Committee or of their immediate family group, understood as the spouse or housemate, or relative within the fourth degree of consanguinity or second degree of affinity.
- (iv) When any member of the Committee or the immediate family group or their relatives within the fourth degree of consanguinity and second degree of affinity have direct or indirect business ties with the person reported as infringing institutional principles or ethical values.
- (v) "When a member of the Committee is or has been reported by the accused for alleged violations of institutional principles and ethical values
- (vi) "When a member of the Committee maintains an intimate friendship or displays clear enmity with the accused."
- (vii) When the person reported as accused is or has been a subordinate of the member of the Committee in question.
- (viii) In any other case in which, at the discretion of the Ethics Committee, there are circumstances that justify the excuse or challenge of a titular member of the Committee to hear a particular case, with the purpose of guaranteeing the objectivity of the procedure.

The respective Committee member, exercising due diligence and foresight, must disclose the existence of the connections mentioned in numerals ii), iii), and v), as well as any conflicts of interest that may arise in their relationship with the accused or regarding institutional principles or ethical values.

SECTION IV. FROM THE OFFICE OF ETHICS

Article 35. On the Ethics Office. The Ethics Office is a dependency attached to the Bank's Board of Directors. The Ethics Officer serves as its head, who will be responsible for promoting and monitoring compliance with the provisions contained in the Code of Ethics and in the Complementary Regulations and Procedures of the Code of Ethics, mainly through educational programs, in order to contribute to the good governance of the Bank and help to preserve and promote institutional integrity, by implementing a preventive approach that strengthens the Institution's ethical environment. Likewise, they will be responsible for the application, implementation, and monitoring of the provisions and resolutions issued by the Ethics Committee.

Article 36. On the Ethics Officer. The Ethics Officer will be in charge of providing advice at all levels of the Bank on ethical behavior and reporting ethical problems to the appropriate authorities. Likewise, they are responsible for investigating the complaints that are filed through the corresponding channels regarding conduct that is alleged to be contrary to the Code of Ethics and will work with other Bank dependencies to promote compliance with ethical regulations. In addition, they will ensure that all levels of the organization meet or exceed expectations in this matter.

The responsibilities of the Ethics Officer and the Ethics Office will be those established in the Internal Regulations of the Board of Directors and Attached Dependencies (RIDDA), in addition to those indicated in other regulations in force.

SECTION V. OF THE LEGAL ADVISORY OFFICE

Article 37. The Legal Advisor. The Legal Advisor of the Bank shall participate in the Ethics Committee to ensure compliance with due process and maintain order and fairness in the committee's sessions. Additionally, the Legal Advisor shall assist the Ethics Officer in the presentation of information, documentation, participation of the parties, evidence in the procedure, and shall be responsible for reporting to the Committee any irregularities identified during the administrative process, ensuring its integrity.

SECTION VI. OF THE HUMAN RESOURCES OFFICE

Article 38. On the Human Resources Office. The Ethics Office, in compliance with its powers, must maintain close collaboration with the Human Resources Office as the body in charge of handling labor disputes arising from the implementation of this code. For this purpose, the figure of mediation must be implemented as an alternative conflict resolution formula, which must be managed from this office. The Human Resources Office will develop the necessary regulations and protocols and will establish the processes required for this purpose. At no point should this process be perceived as an obstacle to accessing the Ethics Office.

SECTION VII. ON THE SUPERVISOR

Article 39. On the Supervisor. The Bank's personnel who hold positions at the management, senior administration, and managerial and middle management levels who exercise immediate superior authority, for the purposes of the performance evaluation process, play an active role and have additional responsibilities in matters of ethics and conduct, and in promoting an ethical culture in the Bank. In particular, supervisors have the following obligations:

- (a) Act as role models, consistently demonstrating behaviors and attitudes that reflect the standards of this code.
- (b) Support the code and ensure that the personnel who collaborate with them understand the behaviors that are required of them.
- (c) Create a positive, inclusive, and respectful work environment in which staff you supervise feel comfortable raising questions and concerns.
- (d) Be the first to act to address situations in the workplace that, if not addressed properly, could escalate to violations of the provisions of the Code or other more serious problems.
- (e) Immediately report any improper conduct to the Ethics Office.
- (f) Never retaliate or allow retaliation against individuals who have reported suspected improper conduct in good faith.

Supervisors also play a particular role in the Bank in handling the concerns of employees on matters that refer to functions assigned according to the position they hold. Supervisors are responsible for maintaining good working relationships and an environment of respect. In addition to providing employees with appropriate advice and guidance, supervisors must be available to listen and respond to any questions or complaints employees may have about work matters.

Office conflicts should be proactively addressed and, where possible, resolved at an early stage with the necessary sensitivity and impartiality, in this regard, supervisors may request the assistance of a representative from either the Human Resources Office or the Ethics Office for the specific purpose of mediating any conflicts that arise.

In that regard, ethical behavior begins with supervisors. Leading by example is the best way to inspire ethical behavior in others and maintain a positive and productive work environment.

SECTION VIII. OF THE BANK STAFF.

Article 40. On the Bank staff. The shared commitment to ethics management is assumed upon joining the Bank, and is reaffirmed by certifying knowledge of the Code and by participating in training courses on the subject. It is the responsibility of each member of the Bank's staff to read, understand, and assume the commitments emanating from the Code. If they are ever unsure how to proceed, any Bank staff member may consult with the Ethics Office.

All staff at all levels are responsible for their own conduct or actions and expect other employees to be as well.

The ethical values contained in this code and, where applicable, the institutional principles are mandatory and must be the behavior guide of each member of the Bank's staff at all levels. For its proper implementation, staff are recommended to express their opinion, request guidance, or report any action that could be detrimental to the collaborator or the image of the Bank, before the institutional authorities. If they need guidance in their daily work, they can consult any of the following people or agencies:

- (a) Immediate superior or supervisor.
- (b) Human Resources Office.
- (c) Ethics Office.

In addition to this, all Bank personnel have a duty to cooperate in investigations of improper conduct.

If they witness a violation of a provision of this code and refuse to participate in the investigation process or, where appropriate, do not report it when they are able to do so due to their hierarchical position, in the opinion of the Ethics Committee, they may be subject to the investigation process and the corresponding sanctions.

Therefore, if they were to witness improper conduct, they must carry out the following actions:

- (i) Report in good faith through the established reporting channels or request guidance on the actions to be taken from the supervisor or the Ethics Office.
- (ii) Document or use any means at their disposal to leave evidence of improper conduct or actions that could be against the provisions of the Code of Ethics.
- (iii) Collaborate in the investigation process to be carried out by the corresponding instance.

With respect to the staff member who was the victim or complainant of improper conduct, in addition to the above actions, they must comply with the corrective or preventive measures established by the corresponding instance during the investigation process.

SECTION IX. ON THE ADMINISTRATIVE TRIBUNAL.

Article 41. On the Administrative Tribunal. The Administrative Tribunal is a collegiate body, with a jurisdictional function and with exclusive powers and competence to hear, cases specified by CABEL's internal regulation that determine their specific origin, the conflicts that may arise between the Bank and personnel, both under possible employer responsibility of CABEL and with which CABEL has no employer responsibility, based on the provisions of this Code of Ethics and its Complementary Regulations and Procedures. Said Tribunal will be governed and will function in accordance with the provisions of its Statute and by the procedural provisions adopted by the Tribunal in each case. Hence decisions made by the Ethics Committee may be appealed before said tribunal.

TITLE II. OTHER PROVISIONS

Article 42. Binding regulations. The internal, regulatory, and administrative rules of the Bank must protect the institutional principles and ethical values contemplated in this code.

Article 43. Authentic interpretation. In the cases in which the Board of Directors makes an authentic interpretation of the Code of Ethics with a regulatory nature, this must be published regularly so that it is accessible to all Bank personnel.

ANNEX IV

Integrity Provisions

A. Counterparties and their Related Parties:

All natural or legal persons that provide goods and/or services to CABEL, whether in their capacity as suppliers, contractors, consultants, (hereinafter all of the foregoing shall be referred to in this document as "the supplier"), as well as any other similar condition, hereinafter referred to as Counterparties and their Related Parties, shall refrain from performing any act or action that is or may be classified as a Prohibited Practice as established in paragraph (B) below of this Annex.

B. Prohibited Practices:

By virtue of the foregoing, CABEL has established a Reporting Channel as the mechanism to denounce irregularities, as well as the commission of any Prohibited Practice, in the use of CABEL funds or funds administered by CABEL, through the institutional website: <https://www.bcie.org/acerca-del-bcie/medios-de-denuncias>.

CABEL personnel involved in the procurement of goods and/or contracting of services, as well as the natural persons and the representatives, officials and employees of the natural or legal persons that participate as suppliers of such goods and services, have and shall observe the highest ethical standards throughout the procurement process and during the contractual execution phase. In this regard and without this list being exhaustive, the following shall be considered prohibited practices:

- a) Bribery: Consists of the direct or indirect offer, supply, acceptance or solicitation of anything of value for the purpose of improperly influencing the performance or decision of the competent decision maker in the process of procurement of goods and services that CABEL is carrying out.
- b) Fraudulent Practice: Any act or omission, including a misrepresentation of the facts, that misleads or seeks to mislead another person with the purpose of obtaining an undue benefit, financial or otherwise.
- c) Collusion: Consists of actions among bidders aimed at obtaining prices in any of the procurement methods used by CABEL at artificial, non-competitive levels, capable of depriving the other participants of the benefits of free and open competition.
- d) Coercive Practice: Consists in the fact of threatening another with causing to himself or to members of his family, in his person, honor, or property a harm that constitutes a crime, in order to influence decisions during any of the procurement or contracting processes or during the execution of the corresponding contract, whether or not the objective has been achieved.

The Bank reserves the right to unilaterally terminate the contract without the need for any judicial or extrajudicial declaration if it is determined that the selected supplier has promoted or executed these practices.

C. Supplier's Statements and Obligations:

The supplier shall expressly transfer the statements and obligations of this Annex to its Related Parties (contractors, subcontractors, suppliers, supervisors, bidders and similar) in the contractual documentation that governs the relationship between the supplier and its Related Parties, when such relationship is directly related to the contracting and supply of goods and services required by CABEL.

Supplier's Particular Statements:

The supplier states that:

- a. They are familiar with the CABEL Reporting Channel, as a mechanism to report irregularities or the commission of any Prohibited Practice in the use of CABEL funds or funds administered by CABEL.
- b. They shall retain all documents and records related to activities contracted by CABEL for a period of up to seven (7) years, counted from the termination of this contract.
- c. As of the date of execution of this contract, the supplier has not committed any Prohibited Practices, either on its own or through related parties (officers, employees, representatives and agents) or as any other type of analogous relationship.
- d. All information submitted is truthful and therefore has not misrepresented or concealed any facts during the selection, award or execution processes of this contract.
- e. Neither they, their agents, personnel, contractors, consultants, directors, officers or shareholders (a) have been debarred or declared by an entity as ineligible for the award of contracts financed by any other entity, or (b) have been convicted of offenses related to Prohibited Practices by the competent authority.
- f. None of its directors, officers or shareholders has been a director, officer or shareholder of an entity that (a) is disqualified or declared ineligible by any other entity, or (b) has been convicted of a Prohibited Practices offense by the competent authority.

Supplier Obligations:

The following are supplier obligations:

- a. Not to incur in any Prohibited Practice in the execution of the contract for the provision of services required by CABEL with its own funds or funds administered by it.
- b. Report, during the contract execution, through the Reporting Channel, any irregularity or the commission of any Prohibited Practice related to the contracting of goods and services required by CABEL with CABEL's own funds or funds administered by CABEL.
- c. In relation to the reported Prohibited Practices, either by the supplier or by third parties, through the Reporting Channel and in relation to the service object of the Contract, allow and facilitate interviews to its shareholders, directors, executives or employees of any status, and must provide all the collaboration and assistance that may be necessary in case of any audit or investigation coming from CABEL or any investigator hired by CABEL for such purposes.
- d. In relation to the reported prohibited practices, either by the supplier or by third parties, through the Reporting Channel and in relation to the service object of the Contract, to attend within the term established in the communications made by CABEL, the consultations related to any inquiry, inspection, audit or investigation coming from CABEL or from any investigator, agent, auditor, or consultant appropriately designated, whether by written, virtual or verbal means, without any type of restriction.
- e. In applicable cases, reimburse, at CABEL's request, reasonable expenses or costs associated with the activities and investigations carried out in connection with the commission of Prohibited Practices.

The Statements and Obligations made by the supplier contained in paragraph C. are true and shall remain in effect from the date of signature of this contract, during its term and until the termination of this contract to the satisfaction of the Bank.

D. Investigation and Auditing process:

CABEL shall reserve the right to carry out the audit and investigation procedures to which it is entitled.

CABEL will grant the Counterparties and their Related Parties the procedural opportunity to present their arguments through an administrative proceeding. This includes, but is not limited to, CABEL's right to share or make the contents of such list public.

E. List of Prohibited Counterparties:

CABEL may incorporate, at its sole discretion, the Counterparties and their Related Parties in the List of Prohibited Counterparties, which it has instituted for such purpose. Temporary or permanent debarment from the List of Prohibited Counterparties shall be determined on a case-by-case basis by CABEL.

F. Integrity Provisions Acceptance:

The supplier acknowledges that by accepting this Annex it agrees to comply with CABEL's Anti-Fraud, Anti-Corruption and Other Prohibited Practices Policy and other applicable regulations on the subject, abiding by CABEL's actions and decisions in the event that any practice contrary to these regulations (norms) is proven. CABEL's Anti-Fraud, Anti-Corruption and Other Prohibited Practices Policy is available at the following website: <https://www.bcie.org/acerca-del-bcie/oficina-de-integridad-y-cumplimiento>

This Addendum forms an integral part of this contract, whereby the Supplier accepts each of the provisions herein stipulated.



RISK MANAGEMENT POLICY FOR MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION OF WEAPONS OF MASS DESTRUCTION, INTEGRITY AND SANCTIONS.

Version 3

R i s k M a n a g e m e n t

Public Once Approved

In accordance with the regulatory framework of the Information Access Policy, this document will be disclosed on the Bank's external website after approval.

TABLE OF CONTENTS

I.	INTRODUCTION	3
II.	OBJECTIVE	3
III.	SCOPE	4
IV.	ABBREVIATIONS AND TERMS	4
V.	DEFINITIONS	4
VI.	RELATED DOCUMENTATION	7
VII.	DEVELOPMENT	7
1.	RISK MANAGEMENT AND BASIC PRINCIPLES	7
2.	THOSE RESPONSIBLE FOR POLICY MANAGEMENT	9
3.	LA/FT/FPDAM RISK MANAGEMENT, INTEGRITY, AND SANCTIONS SYSTEM	13
4.	LA/FT/FPADM RISK CONSIDERATIONS	14
5.	INTEGRITY RISK CONSIDERATIONS	14
6.	PENALTY RISK CONSIDERATIONS	15
7.	OTHER PROVISIONS	16

I. INTRODUCTION

In compliance with international standards, the Central American Bank for Economic Integration (CABEL) directs its efforts to manage the risks of Money Laundering, Terrorism Financing and Financing of the Proliferation of Weapons of Mass Destruction (LA/FT/FPDAM) so that its products and services are not used to give the appearance of legality to funds that are the product of illicit activities or serve to channel licit or illicit resources destined for terrorist activities or the proliferation of weapons of mass destruction.

Likewise, CABEL has the responsibility, in accordance with its fiduciary duty, to take care of its member countries' resources, preventing the detour of its funds for purposes incompatible with its strategic objectives and, therefore, it maintains Integrity controls.

On the other hand, economic and financial sanctions have a variety of sources and are issued in support of national and international policies to prevent and control terrorism, its financing, money laundering, its source crimes, corruption, the financing of the proliferation of weapons of mass destruction, human rights abuses and violations, and various international relations objectives.

CABEL is committed to combating financial crime and contributes to protecting the integrity of the global financial system by conducting responsible and secure business in the different jurisdictions around the world where the Bank conducts operations with different stakeholders.

The issuance of this policy is part of CABEL's commitment in the fight against money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction and other prohibited practices, sanctions' risk management, as well as other financial crimes, which are directly related to the LA/FT/FPADM risk.

II. OBJECTIVE

This Policy has been developed with the purpose of establishing the general and complementary guidelines that regulate the management of LA/FT/FPADM, Integrity, Sanctions and Other Financial Crimes risk in a joint manner, which are directly related to LA/FT/FPADM risk at CABEL; which will be of general application and observance at all of CABEL's levels in order to generate an institutional culture oriented to prevention.

These guidelines represent a guide to prevent and mitigate the effects that could occur if the organization, its operations or activities are used as a vehicle for money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction, and that materialize through prohibited practices or any financial crime that has a direct relationship with the LA/FT/FPADM risk, that prevents the fulfillment of CABEL's fiduciary duty, damage to the image and reputation derived from sanctions and other related activities.

III. SCOPE

This Policy, together with internal regulations on the matter, is applicable to all levels of CABEI's personnel (directors, senior management, officers, contractors, Young Professionals, Special Programs and any other category contemplated for the provision of human resources to the Bank); and all its Counterparties as defined in this Policy.

These guidelines must be observed in all active and passive operations, donations, sponsorships, and acquisition of goods and/or services in which CABEI participates with its Counterparties and their Related Parties.

These guidelines are complementary to the current regulatory framework regarding Sanctions and Integrity already designed for CABEI.

In those cases in which CABEI's interests, assets or contractual obligations are affected as a result of the actions or omissions of its personnel, of any Counterparty or of a Related Party that entails non-compliance with the principles and norms included in this Policy and other internal regulations on the matter, shall be subject to the sanctions established in the current CABEI's Code of Ethics and its Complementary Norms and Procedures, the obligations established contractually in this Policy or the regulations that may result from it, without prejudice to the corresponding legal liability.

IV. ABBREVIATIONS AND TERMS

- **Senior Management:** Executive Presidency and Vice-Presidency.
- **CABEI or Bank:** Central American Bank for Economic Integration.
- **LA/FT/FPADM:** Money Laundering, Terrorism Financing and Financing of the Proliferation of Weapons of Mass Destruction.
- **FATF:** Financial Action Task Force
- **GERIES:** Risk Management
- **OFIC:** Integrity and Compliance Office.

V. DEFINITIONS

- **Sanctionable Acts:** Means any dealings, agreements, operations or the entry into or performance of any transaction that: (i) is prohibited or subject to the application of a sanction of any nature by a Sanctioning Agency, or (ii) could reasonably be expected to form the basis of any Negative Sanction Consequences for CABEI.
- **Risk Analysis:** Consists of determining the frequency (probability of occurrence) with which certain events may occur and the magnitude (impact) of their consequences. The analysis can be qualitative and quantitative and must consider existing controls.

- **Red Flags:** A series of alerts that must be observed and considered both in the prevention and detection of ML/FT, its source crimes, FPADM, sanctions and other prohibited practices, which may vary according to the nature of the crime.
- **Adverse Sanction Consequence:** Means any material adverse determination, fine, penalty, punishment, administrative order, Sanction (whether secondary or otherwise) or other statement, determination or decision of any Sanctioning Body that may have a material adverse consequence to the applicable Person.
- **Counterparty:** Natural or legal person with which CABEL plans to establish or establishes a commercial relationship or contractual link, or any active, passive, pre-investment, technical cooperation, donations, sponsorship, acquisition of goods and/or services of any other nature.
- **LA/FT/FPADM Risk Control:** Comprises the implementation of policies, processes, practices, or other existing actions that act to minimize the LA/FT/FPADM risk in the operations, businesses or contracts carried out by CABEL.
- **Due Diligence:** It is to act with the necessary care for the adequate knowledge of the Counterparty, the origin and, if applicable, destination of its funds, its activity and any other element that allows making sufficiently informed decisions to determine that the Counterparty is not linked to illicit activities such as Money Laundering, Terrorism Financing and Financing of the Proliferation of Weapons of Mass Destruction (LA/FT/FPADM), Integrity, Sanctions and Other Financial Crimes that has a direct relationship with the LA/FT/FPADM risk. This reduces the possibility of incurring negligence and administrative, civil or criminal liabilities. Due diligence is classified as simplified, normal and enhanced.
- **Source, underlying, predicate, precedent or serious offences:** It is a criminal conduct established in the criminal law from which the illicit assets, goods, funds or resources that are later laundered originate: These offences are called "source", "underlying", "predicate", "precedent" because they are prior to the money laundering crime and "serious" because of the penalty to be imposed and the importance and seriousness of the crime. They are considered as such, according to the FATF: swindling; terrorism, including Terrorism Financing; trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children; illicit trafficking in narcotic drugs and psychotropic substances; illicit arms trafficking; illicit trafficking in stolen goods and other goods; corruption and bribery; fraud; counterfeiting currency; counterfeiting and piracy of products; environmental crimes; murder, grievous bodily injury; kidnapping, illegal restraint and hostage-taking; robbery or theft; smuggling; (including in relation to customs and excise duties and taxes); tax crimes (related to direct taxes and indirect taxes); extortion; forgery; piracy; and insider trading and market manipulation. The above list is not exhaustive, but rather enunciative and must consider the regulations of each jurisdiction in which the Bank operates.

- **Financing the Proliferation of Weapons of Mass Destruction (FPADM):** is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transport, transfer, deposit or dual use of weapons or other objects for illegitimate purposes in contravention of national laws or international obligations, when the latter is applicable.
- **Terrorism Financing (FT):** An internationally recognized crime committed by any person who, by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used, or in the knowledge that they are to be used in whole or in part, for the financing of terrorist acts and of terrorists and terrorist organizations.
- **Risk Management:** Coordinated activities to direct and control the organization in relation to risk.
- **Asset Laundering (LA):** It is the procedure carried out to conceal the origin of funds or assets generated through the commission of one or more source, underlying, predicate, precedent or serious crimes. Its purpose is to conceal or cover up that the funds or assets obtained through illicit activities appear as the product of licit activities and circulate without problem in the economic and financial system. Money laundering is also known as money laundering, money laundering or money laundering.
- **Sanctions Lists:** Records issued or disclosed by any Sanctioning Body under the cover of laws and regulations on economic, financial or trade sanctions, embargoes or originating from restrictive measures administered, enacted or enforced by any Sanctioning Body, among these: United Nations (UN) Security Council Consolidated Sanctions List, Consolidated List of persons, groups and entities subject to European Union (EU) financial sanctions, World Bank (WB) List of Ineligible Entities and Individuals, Foreign Assets Control Office (OFAC) Consolidated List, and "HM Treasury Sanctions List of the Financial Sanctions Implementation Office (OFSI) and any others that are of observance for CABEI in its financial activities. Said lists shall be consolidated by OFIC and submitted to the Committee defined in section "b", subsection "iii" of Article 4.
- **Sanctioning Body:** Refers to, but is not limited to, the United Nations, the European Union, the United Kingdom, the World Bank, and governments and official institutions or agencies of observance for CABEI in its financial activities.
- **Other Financial Crimes:** These are criminal conducts typified in the criminal regulations of the jurisdictions in which the Bank operates and that threaten the security of the legal traffic, operations, assets and the sound and efficient management of financial entities, which are typified in an enunciative but not limiting manner, provided that they have a direct relationship with the LA/FT/FPADM risk.
- **Prohibited Practice:** Any fraudulent, corrupt, coercive, collusive, or obstructive practice as defined in CABEI's Anti-Fraud, Anti-Corruption and Other Prohibited Practices Policy.

- **Related Parties:** Individuals or legal entities that participate or provide services to the Counterparties in projects or operations, whether as coordinators, supervisors, contractors, subcontractors, consultants, suppliers, grant recipients (and all their employees, representatives and agents), as well as any other type of similar relationship.
- **Primary Responsible Parties:** Any person who establishes a relationship or has contact with a CABEI Counterparty. Without distinction of position, whether personnel under CABEI's employer's responsibility, personnel under CABEI's employer's responsibility or personnel with whom CABEI has no employer's responsibility, personnel under CABEI's employer's responsibility and personnel with whom CABEI has no employer's responsibility, the person who maintains direct and constant contact with the Counterparty shall be considered the Primary Responsible Party.
- **Integral Risk Management System:** It is the LA/FT/FPADM, Integrity and Sanctions Risk Management System.

VI. RELATED DOCUMENTATION

- CABEI's Anti-Fraud, Anti-Corruption and Other Prohibited Practices Policy.
- Regulation of the Ring Fence Mechanism for Activities and Operations Related to the Republic of Cuba or its Nationals.
- Integrated Risk Management Policy.

VII. DEVELOPMENT

1. RISK MANAGEMENT AND BASIC PRINCIPLES

Article 1. The Bank shall ensure the management of the following types of risks in its operations:

- **Risk of Money Laundering, Terrorism Financing and Proliferation of Weapons of Mass Destruction (LA/FT/FPADM):** It is the probability of loss, damage or exposure that may be suffered by an entity that, by the nature of its operations, is likely to be used directly or indirectly as a vehicle for money laundering, the channeling of resources to carry out terrorist activities and/or activities aimed at Financing the Proliferation of Weapons of Mass Destruction (FPADM). This risk inherently involves reputational, legal, operational and contagion aspects.
- **Integrity Risk:** This is the management of the risks of fraud, corruption, and other prohibited practices. These practices may expose the entity to disrepute, bad image, negative publicity, true or not, regarding the institution and its business practices, causing loss of customers, decrease in revenues or legal proceedings.

- c. **Sanctions Risk:** May be defined as the risk of legal action, regulatory action, financial loss, material, or reputational damage that an entity may suffer as a result of the imposition of an economic sanction established by a Sanctioning Body.

For the management of this type of risks, the Bank and its personnel must act under the following basic principles:

- a. **Regulatory Compliance:** Compliance with current internal regulations on LA/FT/FPADM, Integrity and Sanctions and any other applicable regulations.
- b. **Due Diligence:** Observance of due diligence with respect to the knowledge of the Counterparties, in accordance with the internal regulations in force regarding LA/FT/FPADM, Integrity, Sanctions and Other Financial Crimes, which have a direct relationship with the LA/FT/FPADM risk.
- c. **Compliance Culture:** The Bank will promote a culture of compliance with international best practices in the areas of LA/FT/FPADM, Integrity and Sanctions to demonstrate CABEI's commitment to responsible business conduct and adequate risk management.
- d. **Confidentiality:** The information kept and administered by the Integrity and Compliance Office, as well as the information provided by the Counterparties, the records and documents referring to the respective operations that are sent to said office for the fulfillment of its functions, will be classified in the "non-public" categories in accordance with the Information Security Policy, remaining at the discretion of the Head of the Integrity and Compliance Office of the classification as restricted or sensitive information.
- e. **Collaboration:** The collaboration of all CABEI personnel and its Counterparties is essential for the proper functioning of the LA/FT/FPADM, Integrity and Sanctions Risk Management System and that the compliance with this Policy and other internal regulations on the matter takes precedence over the achievement of business goals.

Article 3. For the adequate management of this type of risk, the Bank shall establish a LA/FT/FPADM, Integrity and Sanctions Risk Management System considering international standards as a reference in each matter, issued by entities such as the Financial Action Task Force (FATF) -of which the Bank participates as Observer in the regional groups GAFILAT and GAFIC-, the pronouncements of the Basel Committee, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the Sarbanes-Oxley Act, the Economic Cooperation and Development Organization (OECD), the Association of Certified Fraud Examiners (ACFE), the Global Forum on Transparency and Information Exchange for Tax Purposes, the United Nations Convention against Corruption, the Vienna Convention, the COBIT Framework and ISO31,000, among others.

All personnel, Counterparties and their Related Parties shall act in compliance with the guidelines established in the internal regulations governing the LA/FT/FPDAM, Integrity and Sanctions Risk Management System.

2. RESPONSIBLES FOR POLICY MANAGEMENT

Article 4. The following actors and responsibilities are established for the implementation and execution of this policy:

a. The Board of Directors and Senior Management:

- i. The Board of Directors, through this policy's approval, sets the institutional tone regarding the relevance and importance of the risk management described therein.
- ii. The Board of Directors and Senior Management will ensure that OFIC's personnel maintain a level of preparation and specialization that allows them to have the necessary skills and conditions for their adequate performance.
- iii. The Board of Directors and Senior Management are committed to provide all the necessary means to provide training on LA/FT/FPDAM, Integrity and Sanctions prevention to the staff, so that the model becomes part of the institutional culture, empowering the staff and integrating this culture into the daily activities of the organization.
- iv. The Board of Directors and Senior Management support and recognize the authority and independence of the Risk Manager and the Head of the Integrity and Compliance Office and their staff, to propose policies and procedures to effectively control the LA/FT/FPDAM, Integrity and Sanctions risks faced by CABEI.

b. Senior Management:

- i. The Senior Management shall ensure the existence of an adequate organizational structure for the efficient functioning of the Integrity and Compliance Office within the Risk Management and for the adequate Management of LA/FT/FPDAM, Integrity and Sanctions Risks, including the human resources dedicated to said function, in accordance with the required experience, professionalization of personnel, information technologies that support the function, and other resources in accordance with the volume of the operations, markets in which it operates, and other factors that affect CABEI's risk profile.

- ii. Establish lines of reporting and communication to the Board of Directors, through the Risk Management, on matters related to LA/FT/FPDAM, Integrity and Sanctions risks, including the issuance of reports on these.
- iii. Maintain a risk management and compliance committee to address issues related to LA/FT/FPDAM risk management.
- iv. Designate the Head of the Integrity and Compliance Office, who shall act as the Bank's Integrity and Compliance Officer.
- v. Promote appropriate means for reporting situations in which non-compliance with regulations and/or illegal acts regarding LA/FT/FPDAM, Integrity and Sanctions by CABEI, its personnel or Counterparties is detected.
- vi. Ensure through the different units that coordinated efforts are made to protect CABEI from the effects of actions derived from the materialization of a LA/FT/FPDAM, Integrity and Sanctions or Other Financial Crime risk that has a direct relationship with the LA/FT/FPDAM risk.
- vii. Instruct the different areas to remedy any gaps identified in internal or independent reviews.

c. Risk Management, through its Integrity and Compliance Office:

- i. The Head of the Integrity and Compliance Office, in his role as Integrity and Compliance Officer, and his staff are responsible for coordinating the LA/FT/FPDAM, Integrity and Sanctions Risk Management System, applying and ensuring compliance with this Policy and its complementary regulations, establishing controls to manage these risks.
- ii. Manage the process of identification, assessment, follow-up and control of risks related to LA/FT/FPDAM in CABEI, through the implementation of risk management tools, as well as the design, development, implementation, monitoring, updating, dissemination and training of the regulatory framework and procedures in force throughout the organization in accordance with best practices that allow the prevention and mitigation of these risks.
- iii. Coordinate its resources in order to effectively carry out its own and specialized analyses for the adequate "Know Your Customer" in CABEI's operations and sanction mitigation activities. Likewise, advise and support the Primary Responsible Parties in the application of the defined regulatory guidelines.
- iv. Establish and keep the principles and rules that will be applied and generally observed at all levels of the organization related to compliance, integrity and

RISK MANAGEMENT POLICY FOR MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION OF WEAPONS OF MASS DESTRUCTION, INTEGRITY AND SANCTIONS.

sanctions updated, and attend to operations that present elements of risk and, if necessary, submit them to the respective body for consideration.

- v. Evaluate compliance, integrity and sanctions management in the different areas and follow up on action plans that they propose, and the recommendations made.
- vi. Promote the prevention and detection of LA/FT/FPDAM risk elements, prohibited practices and sanctions, through the communication and training program, the development and updating of the regulatory framework, advice and due diligence, the administration of the different means of complaints, among others.
- vii. Coordinate investigation and sanction processes for prohibited practices, with the support of the Integrity Committee and based on the principles of due process.
- viii. Manage and maintain the sanctions compliance program, coordinating the Ring Fence's special attention processes and the necessary controls for potential operations and transactions with sanctioned countries, entities and/or individuals, with the purpose of safeguarding negative impacts on CABEI derived from regulations imposed by sanctioning entities.
- ix. Monitor updates from sanctioning bodies and establish or update policies and procedures that could have implications on CABEI operations. Escalate to the respective instances the risks of sanctions present in CABEI's operations. Develop, implement and monitor training on sanctions in accordance with the needs of the personnel, in order to permeate the risks of sanctions in the Institution. Coordinate the implementation of corrective actions to the sanctions program.
- x. Coordinate and assist in the various internal or independent reviews of the compliance, integrity and/or sanctions program.
- xi. Lead inquiries and due diligence from resource sources on the special schemes and procedures on sanctions, LA/FT/FPDAM controls, and its integrity system.
- xii. Represent the Bank before external entities (national and international) in matters of LA/FT/FPDAM, integrity and sanctions prevention.

d. Primary Responsible Party:

- i. Apply the entry and follow-up due diligence measures and document the controls and guidelines set forth in current regulations in a timely manner, using the tools available at CABEI.

- ii. Manage, with the support of the Head of the Integrity and Compliance Office, the LA/FT/FPDAM, integrity and sanctions in the counterparties and operations under his/her responsibility.
- iii. Participate in calls for specialized training derived from the training program on LA/FT/FPDAM, Integrity, Sanctions Risk and Other Financial Crimes that have a direct relationship with the LA/FT/FPDAM risk.
- iv. Perform a permanent follow-up of the Counterparties involved, complying with the entry and follow-up controls established in the internal regulations, as well as when some warning signs are identified during the course of the relationship. In order to comply with the above, and if necessary, the Counterparties and their Related Parties are responsible for responding to the requests made by the Primary Responsible Party in due time and form.

e. About the Counterparties:

- i. Comply in due time and form with the requirements of CABEI regulations related to the prevention of LA/FT/FPDAM, Integrity, Sanctions and Other Financial Crimes.
- ii. Communicate any changes in its shareholding structure, organizational structure, board members, mergers, acquisitions and any significant information according to the risk profile of the Counterparty.
- iii. In applicable cases, ensure that the funds provided for the execution of the projects do not come from or are not linked to LA/FT/FPDAM or any other illicit activity.
- iv. Safeguard the suitability of the Related Parties financed with CABEI resources and other resources. This includes compliance with recognized international best practices in this area, as well as searches made in the Sanctions Lists.
- v. Comply in due time and form with the presentation of the Related Parties' documentation, in case CABEI requires it.
- vi. Depending on its nature and in accordance with the applicable legal framework, adopt or maintain a program to prevent LA/FT/FPDAM, Integrity and Sanctions risks, as applicable.
- vii. Report any warning signals or Red Flags identified during the execution of the operation through the CABEI Reporting Channel.
- viii. Comply with all provisions set forth in this Policy, related regulations and established contractual provisions.

f. Internal Audit:

- i. The role of the Bank's Internal Audit is to seek mechanisms to verify the application and effectiveness of the policies of the LA/FT/FPADM, Integrity and Sanctions Risk Management System.

3. LA/FT/FPDAM, INTEGRITY, AND SANCTIONS RISK MANAGEMENT SYSTEM

Article 5. The LA/FT/FPDAM, Integrity and Sanctions Risk Management System is composed of the set of policies, manuals, instructions and due diligence procedures, documentation, risk assessment methodologies, organizational structure, control bodies, technological infrastructure, information dissemination and training mechanisms established and to be established to promote the risk management culture and prevent the occurrence of LA/FT/FPDAM, prohibited practices and sanctions in CABEI's relationships or operations.

Article 6. Risk management shall consider the guidelines for identifying, measuring, controlling, and monitoring LA/FT/FPDAM, Integrity and Sanctions risks, ensuring the segregation of duties.

Article 7. For the adequate knowledge of the Counterparties and their Related Parties, due diligence shall be performed considering the following:

- a. Apply the guidelines indicated in this Policy, in a comprehensive manner, to all Counterparties and their Related Parties with which the Bank maintains or intends to maintain any type of relationship.
- b. Establish requirements for Counterparty relationships and their Related Parties, rejecting the establishment or renewal of a relationship that does not comply with the requirements of the internal regulations.
- c. Determine the level of LA/FT/FPDAM, Integrity and Sanctions risk according to the nature of its Counterparties and business in accordance with the requirements established in the internal regulations.
- d. Establish procedures that allow the identification of the final beneficiary, in accordance with the requirements established in the internal regulations.
- e. Implement simplified due diligence, normal due diligence and enhanced due diligence procedures, in accordance with the level of LA/FT/FPDAM, Integrity and Sanctions risk of its Counterparties and considering the nature of the business it conducts.
- f. Consider Sanctions Lists and jurisdictions in the due diligence process that are subject to sanctions. Additionally, controls should cover transaction filtering and sanctions list management, including additions to lists and filtering of Counterparty databases.

- g. Establish mechanisms to prevent the promotion of links with Counterparts that support the construction, distribution, and financing of weapons of mass destruction.
- h. Implement controls to prevent CABEI operations from being related to the Terrorism Financing.
- i. Develop mechanisms, from a preventive approach, to identify, implement and maintain anti-fraud, anti-corruption and other prohibited practices controls in CABEI's operations.
- j. Implement controls and take isolation or other applicable measures when risks of sanctions are identified in the Counterparties and their Related Parties.

If, as a result of the due diligence carried out, doubts arise about the suitability of a Counterparty and/or its Related Parties, the Integrity and Compliance Office, the responsible for the operation or the corresponding instance, must refrain from recommending or, where appropriate, approving any active, passive, donation operation, sponsorships or acquisition of goods and / or services.

4. LA/FT/FPADM RISK CONSIDERATIONS

Article 8. Prior to the issuance of new products, the use of new commercial practices, including new channels; the modification of the characteristics of a product; the incursion into a new market; the opening of operations in new jurisdictions, an analysis shall be performed by the Integrity and Compliance Office in conjunction with the area responsible for the same to define its risk level and determine whether it requires special due diligence guidelines according to the applicable characteristics.

Article 9. CABEI shall provide for the conservation of all documents, with due security, related to the LA/FT/FPDAM Risk, for a period of up to seven years.

Article 10. There shall be an independent review every two years, which shall ensure that there are sufficient and necessary controls to prevent CABEI from being used as a vehicle to channel resources derived from criminal activities or to finance terrorist acts or weapons of mass destruction.

5. INTEGRITY RISK CONSIDERATIONS

Article 11. The Board of Directors and Senior Management are committed to combating prohibited practices in their operations, and therefore have acquired a zero-tolerance policy to the commission of these practices.

Article 12. The complementary mechanisms and guidelines to manage integrity risk are set forth in the Anti-Fraud, Anti-Corruption and Other Prohibited Practices Policy and other regulations in force.

6. PENALTY RISK CONSIDERATIONS

Article 13. CABEI shall act in observance of the different economic and financial sanctions in the jurisdictions in which businesses are conducted, including business conducted in or through foreign financial institutions (correspondents).

Article 14. CABEI shall carry out a sanctions risk evaluation every two years, which reflects in an integral and adequate manner the possible risks to which CABEI is exposed, taking into consideration the following factors that, in an enunciative but not limiting manner, may have points of contact or links to the external part of the organization: clients, products, services, intermediaries, Counterparties, transactions and geographic location. Likewise, through its risk management methodology, it shall identify, analyze and manage any sanction risk identified, a process that will serve as a basis for updating policies, procedures, controls and training needs to mitigate this risk.

Article 15. The internal controls shall allow CABEI to prevent, identify, prohibit, escalate and report to the competent personnel, the transactions and activities that may be prohibited, as well as to establish the mitigating measures in the applicable cases. The different areas of CABEI must manage the risk of sanctions that are identified as being exposed as a result of their functions. Likewise, the areas shall manage the storage of the records related to these controls.

Article 16. CABEI will not promote relations or carry out operations of any type, directly or indirectly, in countries subject to exhaustive sanctions by the sanctioning organisms, except when said country is a CABEI member, for which it must be evaluated, the specialized attention mechanism must be defined, and the pertinent measures must be taken. Indirect activities include, but are not limited to, purchases of goods, products or services from third party intermediaries, originating in or destined for the listed jurisdictions, or with banks or financial institutions associated with these transactions. Regarding the Republic of Cuba, the established in the Ring Fence Mechanism for Activities and Operations Related to the Republic of Cuba or its Nationals Regulations shall prevail.

Article 17. CABEI shall monitor any emerging risk in jurisdictions that expose the Bank to the risk of sanctions and shall establish the necessary mitigating measures to limit the identified exposure.

Article 18. The funds that may eventually have to be received as payments from individuals, institutions¹ and entities² on sanctioning agencies' sanction lists must be handled properly, separately, without being mixed with the rest of the Bank's flows.

¹ Includes entities 50% or more owned or controlled (directly or indirectly) by one or more sanctioned individuals or entities, or an individual or entity acting on behalf of sanctioned parties.

² Ships, vessels, aircraft.

Article 19. CABEI will not establish relationships of any nature with individuals, institutions, or entities that are on sanctioning agencies' sanction lists. In existing relationships in which a risk of sanctions arises, isolation, mitigation or termination measures shall be applied as necessary.

Article 20. In the event that a Counterparty or Related Party is identified in resolutions of the United Nations Security Council relating to the prevention and suppression of terrorism and the Terrorism Financing and the financing of the proliferation of weapons of mass destruction, there will be an immediate freeze, that is, the retention of funds or respective disbursements within a period of twenty-four hours.

Article 21. All personnel must comply with the provisions and guidelines defined to avoid the risk of sanctions and must refrain from taking actions to evade the limitations derived from sanctions, either in transfer messages and cross-border transactions, as well as the deletion, reissuance and/or alteration of relevant information of sanctions.

Article 22. CABEI's personnel subject to the sanctioning regulations are prohibited from participating, authorizing, or approving, financing to a sanctioned Counterparty, nor may they facilitate or direct another member of the personnel to intervene or approve an operation with the sanctioned Counterparty.

7. OTHER PROVISIONS

Article 23. It is the responsibility of CABEI's personnel at all levels and estates to understand, comply with and apply this policy, internal regulations and any other document that forms part of the LA/FT/FPADM, Integrity and Sanctions Risk Management System, as well as to receive adequate advice when there are doubts or consultations on its application. Likewise, it is the duty of all personnel to participate in the annual calls derived from the training program on LA/FT/FPDAM Risk, Integrity, Sanctions and Other Financial Crimes that have a direct relationship with LA/FT/FPDAM risk.

Article 24. CABEI's personnel have the duty to immediately inform their superiors, the Integrity and Compliance Office and/or through the available means of reporting when unusual or suspicious aspects are identified in the Bank's activities or operations, in accordance with the provisions of the internal regulations.

Article 25. CABEI shall provide, in accordance with its Constitutive Agreement and in accordance with the regulations governing its activity in this matter, collaboration to the competent authorities that so require.

Article 26. CABEI, with the advice of the Integrity and Compliance Office, shall ensure that the contracts of all active operations of the Bank, as well as the contracts with its suppliers of goods and services, shall contain the necessary contractual provisions to mitigate, prevent and counteract the risk of LA/FT/FPDAM, Integrity and Sanctions. CABEI will ensure that the contracts for all active operations of the Bank, as well as the contracts with its suppliers of goods and services, shall contain the contractual provisions necessary to mitigate, prevent and

RISK MANAGEMENT POLICY FOR MONEY LAUNDERING, TERRORISM
FINANCING, PROLIFERATION OF WEAPONS OF MASS DESTRUCTION,
INTEGRITY AND SANCTIONS.

counteract the risk of LA/FT/FPDAM, Integrity and Sanctions, being the responsibility of the Integrity and Compliance Office, the design of the relevant clauses that allow said purpose.

Article 27. Senior Management, through Risk Management and its Integrity and Compliance Office, shall ensure the timely updating of this Policy, in accordance with the progress of best practices and international standards in this area.