## DE LA ÉTICA EN EL BCIE

## TÍTULO I

## CÓDIGO DE ÉTICA

### CAPÍTULO I
### ASPECTOS GENERALES

**Artículo 7-01. Objeto.** El objeto del presente Código es establecer los principios institucionales, valores éticos y estándares de comportamiento que deben observarse en el Banco Centroamericano de Integración Económica, en adelante llamado el Banco, los cuales deberán motivar y servir de guía al comportamiento del personal del Banco.

**Artículo 7-02. Ámbito de aplicación.** Los principios institucionales, valores éticos y estándares de comportamiento serán de aplicación y observancia general a todos los niveles jerárquicos del Banco incluyendo integrantes del Programa de Jóvenes Profesionales y cualquier tipo de becario, practicantes u otros. De igual manera, estos principios, valores y estándares de comportamiento serán requeridos, en lo conducente, para su cumplimiento en la contratación de servicios de consultoría externa, proveedores, contratistas y otros.

**Artículo 7-03. Efectividad de la normativa en el marco de la ética.** El cumplimiento de lo dispuesto en el presente Código será tomado en consideración para el mantenimiento de la relación del personal con el Banco. En aquellos casos en que el Banco se vea afectado en sus intereses, patrimonio u obligaciones contractuales, como producto de la actuación u omisión de un miembro de su personal que conlleve el incumplimiento de los principios institucionales, valores y estándares de comportamiento consagrados en el presente Código, se aplicarán las sanciones contempladas en las normas y procedimientos complementarios a este Código al tenor de lo establecido en el Título II, del presente Libro.

**Artículo 7-04. Definiciones.**
**Acoso:** Aquellas conductas verbales o físicas no solicitadas que interfieran con el ambiente de trabajo o que tenga por finalidad o efecto crear un entorno de trabajo intimidatorio, hostil u ofensivo.

**Acoso laboral:** Aquellas conductas abusivas, consientes y premeditadas, de parte de un superior o de quien haga sus veces, que realizadas en forma sistemática y repetitiva atentan contra la dignidad o la integridad psicológica o física en perjuicio de un subordinado.

**Acoso sexual:** Aquellas conductas que conlleven cualquier tipo de proposición sexual no deseada, solicitud de favores sexuales u otra manifestación verbal o física de naturaleza sexual, explícita o sutil.

**Conflicto de interés:** Toda situación en la cual un miembro del personal del Banco tenga un interés personal (directo o indirecto) en alguna operación o actividad del Banco que influya de manera indebida en su criterio, sus decisiones o acciones en el Banco o sus clientes. Es decir, que los intereses privados de una persona interfieren o pueden entenderse que interfieren con su toma de decisiones y con el cumplimiento de sus funciones oficiales. Se entiende interés personal directo si beneficia al propio miembro del personal e indirecto si las situaciones de conflicto de interés benefician a algunos de los

parientes del miembro del personal (cuarto grado de consanguinidad y segundo de afinidad) o alguna persona con la que el empleado tiene una relación estrecha.

**Dignidad:** Decoro en las personas en la manera de comportarse.

**Discriminación:** Dar trato de inferioridad a un persona o colectividad por motivos de raza, nacionalidad, género, religión, edad o cualquier otra condición personal.

**Integridad:** Conducta recta, proba, intachable.

**Miembros del BCIE:** Son miembros del Banco los socios o países fundadores, los socios o países regionales no fundadores y los socios o países extrarregionales, según lo establecido en el Convenio Constitutivo.

**Miembros del personal:** Conforme con lo establecido en el artículo 16, del Reglamento General de Administración de Recursos Humanos, el cual incluye el personal temporal por contrato laboral (contratistas).

**Niveles jerárquicos:** Todos los niveles contemplados en la organización del Banco, incluyendo Directorio, Presidencia Ejecutiva y Contraloría.

## CAPÍTULO II
## PRINCIPIOS INSTITUCIONALES, VALORES Y ESTÁNDARES DE COMPORTAMIENTO EN EL MARCO DE LA ÉTICA

**Artículo 7-05. Principios institucionales.** Los principios institucionales que el Banco tiene como base para atender de manera apropiada sus objetivos y que deberán contemplarse como guía en todas las actuaciones institucionales del Banco se enuncian a continuación:

**a) El cumplimiento de su objeto y de su marco institucional:**

El Banco actuará diligentemente en cada una de sus operaciones dando fiel cumplimiento a su objeto, al Convenio Constitutivo y a sus normas, reglamentos, resoluciones y acuerdos que regulan el Banco.

El Banco actuará diligentemente en aras de proteger el interés y 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 atienda con objetividad e imparcialidad sus programas de integración económica y de desarrollo económico y social.

**b) Atención al cliente:**

El 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, en un ambiente de cultura de trabajo en equipo, así como de protección de su confidencialidad y privacidad.

**c) El cumplimiento con las fuentes*:***

El Banco honrará sus compromisos con las fuentes de recursos, cumpliendo los términos y condiciones aceptadas en los contratos de préstamos. Asimismo, el Banco debe 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 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 y cultivando una imagen de organismo excepcional en el ámbito internacional.

**d) Valoración de los recursos humanos del Banco:**

El Banco fomentará un clima organizacional propicio para su estabilidad y la realización integral de los miembros de su personal. Asimismo, deberá 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, previniendo de manera efectiva cualquier forma de acoso o discriminación de cualquier naturaleza, incluyendo, pero no limitándose a los de carácter laboral y sexual por parte de los miembros del personal u órganos superiores de dirección.

**e) Cultura de trabajo en equipo y cooperación:**

El Banco, por ser una institución que trabaja por la integración y el desarrollo de los países miembros, fomentará un ambiente laboral que propicie la generación de la cultura del trabajo en equipo, respeto y cooperación entre los miembros de su personal.

**f) Fundamentación de actuaciones:**

Las actuaciones del Banco se llevarán a cabo fundamentadas exclusivamente en criterios técnicos 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 Banco no aceptará de los clientes o las fuentes de recursos condicionamientos de carácter político o que contravengan el objeto del Banco.

**Artículo 7-06. Valores éticos.** Cada miembro del personal del Banco se comportará, en todas sus relaciones y actividades, de conformidad con los valores éticos que se enuncian a continuación:

**a) Probidad:**

Cada miembro del personal del Banco observará un comportamiento legal, ético e íntegro en todas las actividades y operaciones a su cargo, sustentándose en la veracidad, la honradez, la rectitud y la excelencia y actuará con prudencia en todos sus comportamientos, tanto dentro como fuera del Banco.

**b) Transparencia:**

Cada miembro del personal del Banco realizará sus actividades y comunicaciones con claridad, sin duda ni ambigüedad y sin esconder u omitir cualquier tipo de información. Asimismo, actuará con

independencia, evitando, en toda circunstancia, incurrir en riesgos asociados a situaciones que ocasionen conflictos de interés, tanto para sí mismos como para los demás miembros del personal.

**c) Lealtad y confidencialidad:**

Cada miembro del personal del Banco actuará y observará, en toda circunstancia, un comportamiento de compromiso y lealtad o fidelidad hacia la Institución, así como con sus compañeros, promoviendo en todas sus actividades una imagen institucional positiva, evitando comentarios y actuaciones que puedan causar perjuicio al Banco. Las actividades personales deben caracterizarse por la discreción y la confidencialidad debidas en el manejo de la información y demás asuntos de manejo institucional.

**Artículo 7-07. Estándares de comportamiento.** Cada miembro del personal del Banco deberá comportarse tanto en el plano profesional como personal siguiendo las siguientes directrices en el marco de la ética:

**a) Prevención de conflicto de interés:**

Siempre que un miembro del personal del Banco tenga cualquier interés personal directo o indirecto en alguna operación activa o pasiva o asunto sometido a conocimiento del Banco hará público este hecho ante las respectivas instancias de análisis y aprobación y se abstendrá de cualquier gestión, conocimiento o decisión sobre el particular.

Para los efectos del presente artículo, se entiende interés financiero como cualquier derecho a recibir intereses, dividendos, apreciaciones de capital, honorarios u otros pagos o beneficios monetarios.

Lo anterior conforme se desarrolla en las políticas vigentes sobre la materia.

**b) Adecuado uso de privilegios e inmunidades:**

Los miembros del personal deberán hacer uso adecuado de las inmunidades, exenciones y privilegios que el Convenio Constitutivo y otros instrumentos internacionales confieren al Banco ya que los mismos se confieren en interés de este último y no para ventajas personales.

**c) No tolerancia al acoso:**

Los miembros del personal del Banco deben propiciar, en todo momento, un ambiente de trabajo en donde prevalezca la armonía, la dignidad, el decoro y el respeto, por lo que el acoso no tendrá cabida bajo ninguna circunstancia en el ambiente laboral del Banco.

En virtud de lo anterior, corresponde a los miembros del personal del Banco tomar las medidas necesarias para prevenir situaciones que puedan generar cualquier tipo de acoso. Los superiores implementarán las medidas necesarias para prevenir situaciones de acoso, entre ellas, las siguientes:

**i.** Difundir que el comportamiento irrespetuoso y el acoso no serán tolerados.
**ii**. Asegurar que las personas que planteen inquietudes reciban apoyo y no sean objeto de represalias.
**iii.** Cuando sea necesario, llevar las quejas e inquietudes a conocimiento de la Oficina de Ética.

**d) Abstención de ejercer represalias:**

Los miembros del personal del Banco deberán abstenerse directa o indirectamente de ejercer amenazas o acciones que puedan considerarse o interpretarse como represalias en perjuicio de quien haya presentado una denuncia o que coopere en la investigación sobre la misma.

En tal sentido, los miembros del personal del Banco deberán evitar propiciar o llevar a cabo situaciones orientadas a ejercer acciones, medidas o dar a entender con actos o palabras la intención de causar perjuicios como medida de represalia contra la persona, ya sea esta miembro del personal, clientes o proveedores, que denuncie o coopere de buena fe en las investigaciones sobre alguna denuncia.

Ninguna autoridad en el Banco, sin importar su rango, podrá ejercer acción o medida alguna contra quien haya presentado una denuncia ni podrá promover frente a terceros actos o medidas que puedan interpretarse como represalia por la presentación de una denuncia.

**e) No tolerancia a las prácticas prohibidas:**

Los miembros del personal del Banco deben evitar, en todo momento, todo acto de fraude, de corrupción, así como otras prácticas prohibidas, cuyas acciones puedan perjudicar la imagen y la reputación del Banco, además de afectar la confianza de los miembros del personal, de accionistas, de proveedores, de clientes y, en general, el desarrollo de sus operaciones, al tenor de lo establecido en la política que regule la materia.

**f) Cumplimiento de obligaciones financieras:**

Los miembros del personal del Banco deben atender puntualmente y en debida forma las obligaciones financieras contraídas, ya sea a lo interno como a lo externo del Banco, incluyendo el pago de préstamos y tarjetas de crédito, entre otros, a fin de evitar que, por dificultades financieras personales, se generen actos que puedan afectar a la Institución.

**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 relacionados 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.

Para efectos del presente contrato, entiéndase por Prácticas Prohibidas las siguientes:

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 jurídicas que participen como proveedores de dichos bienes y servicios, deberán observar los más altos niveles éticos durante todo el proceso de adquisición o 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 impropiamente 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 rechazará toda propuesta de adjudicación si se determina que el proveedor seleccionado ha promovido o ejecutado estas prácticas y será excluido de los procesos de adquisición del BCIE. Asimismo, el Banco se reserva el derecho de resolver de forma unilateral el contrato sin necesidad de declaración judicial o extrajudicial alguna en caso se llegaré a determinar que el proveedor seleccionado ha promovido o ejecutado estas prácticas.

**C. Declaraciones y Obligaciones de los Proveedores:**

Los proveedores trasladarán 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 los proveedores con sus Relacionados, cuando la misma tenga relación directa o indirecta con la contratación y suministro de bienes y servicios requeridos por el BCIE.

**Declaraciones Particulares de los proveedores:**

Los proveedores declaran 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 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) 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 (a) que se encuentre inhabilitada o declarada inelegible por cualquier otra entidad, (b) o haya sido declarado culpable de un delito vinculado con Prácticas Prohibidas por parte de la autoridad competente.

**Obligaciones de los Proveedores:**

Son obligaciones de los proveedores las siguientes:

**a.** No incurrir en ninguna Práctica Prohibida en suministro de bienes y/o contratación de servicios requeridos por el BCIE con fondos propios o fondos administrados por éste.

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

**c.** Otorgar el acceso irrestricto al BCIE o sus representantes debidamente autorizados a visitar o inspeccionar las instalaciones físicas de los proveedores a cargo de la ejecución de las obras, bienes o servicios que se hubieren contratado con fondos propios del BCIE o administrados por éste. Asimismo, permitirán y facilitarán la realización de entrevistas a sus accionistas, directivos, ejecutivos o empleados de cualquier estatus o relación salarial. De igual forma, permitirán el acceso a los archivos físicos y digitales relacionados con dichas contrataciones, debiendo prestar toda la colaboración y asistencia que fuese necesaria, a efectos que se ejecuten adecuadamente las actividades previstas, a discreción del BCIE.

**d.** 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.

Las Declaraciones y Obligaciones efectuadas por los proveedores 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.

**E. Lista de Contrapartes Prohibidas:**

El BCIE podrá incorporar a los Proveedores 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.

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

BCIE

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL BANCO CENTROAMERICANO DE INTEGRACIÓN ECONÓMICA

**Versión 3**

BCIE

USO INTERNO

# TABLA DE CONTENIDO

# I. INTRODUCCIÓN

Mediante la Resolución No. DI-135/2012, el Directorio ratificó el marco de referencia CobIT como estándar para la gestión y gobierno de la Tecnología de Información del Banco y aprobó la 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.

En respuesta a los cambios en el entorno, las mejores prácticas que regulan la materia y los cambios en el BCIE, se detectó la necesidad de revisar y actualizar esta Política, la cual se ha ajustado a los lineamientos establecidos en el Manual para la Gestión de los Documentos que Integran el Marco Regulatorio del BCIE.

# II. OBJETIVO

El objeto de la presente Política es 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 Aplicación 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 confidencialidad, integridad 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 confidencialidad, integridad 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 Ejecutiva.
- BCIE o Banco: Banco Centroamericano de Integración Económica.
- GEROP: Gerencia de Operaciones y de Tecnología.
- SAAI: Departamento de Servicios Administrativos y de Adquisiciones Institucionales.
- SIATI: Departamento de Seguridad de Información y de Aseguramiento de la Calidad de TI.

## 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, etc.) 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 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 Aplicación de la presente Política.

- **Cuenta Privilegiada:** Las cuentas privilegiadas son aquellas que confieren capacidades extraordinarias no disponibles para las cuentas y usuarios normales. Son identificadores de usuario (Userid) creados por el fabricante de una plataforma tecnológica que posee privilegios de superusuario y los cuales son utilizados regularmente por personal técnico de la Gerencia de Operaciones y Tecnología para 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.
- **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:** Persona o usuario que crea u origina activos de información que deben ser protegidos. Tiene 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, es responsable de mantener un registro actualizado de los activos de información que están bajo su responsabilidad. Por regla general, los responsables de la Información serán los titulares de cada dependencia del Banco, excepto que se nombre a una persona específica para esa función.
- **Riesgo:** Conforme lo definido en la Política para la Gestión Integral de Riesgos del BCIE, el riesgo es el efecto de la incertidumbre sobre los objetivos establecidos (institucionales, procesos, etc.). Se mide en términos de probabilidad e impacto. Los riesgos a los que está expuesto el BCIE se ubican en diferentes categorías y proporcionan un marco de referencia para comprender los diversos orígenes y tipos de riesgos que enfrentan las áreas en sus actividades.
- **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).
- Manual de Aplicación de la Política de Seguridad de la Información del BCIE.
- Reglamento General de Administración de Recursos Humanos.
- Manual de Normas de Conducta.
- Manual de Funcionamiento del Comité de Tecnología de Información.

# 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.
b. Aprobar anualmente los recursos presupuestarios necesarios para mantener un adecuado Sistema de Administración de la Seguridad de la Información y para desarrollar el Plan Operativo Anual de Tecnología de Información.
c. Supervisar el Sistema de Administración de la Seguridad de la Información del Banco.

**2.2.** Corresponde al Comité de Directores de Finanzas y Riesgos analizar y recomendar al Directorio la aprobación de los lineamientos para el adecuado direccionamiento del Sistema de Administración de la Seguridad de la Información que se establecen en la Política de Seguridad de la Información y sus actualizaciones, así como apoyar al Directorio en la supervisión del Sistema de Administración de la Seguridad de la Información del Banco.

**2.3.** Corresponde al Comité de Directores de Presupuesto y Asuntos Organizativos, analizar y recomendar anualmente al Directorio la aprobación de los recursos presupuestarios que a nivel de Tecnología de Información se requieren para mantener un adecuado Sistema de Administración de la Seguridad de Información y para implementar el Plan Operativo Anual de las áreas Tecnológicas del Banco.

**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:

a. Aprobar mediante Resolución de Presidencia el Plan Estratégico de Tecnología de Información del BCIE, asegurando que el mismo contenga las iniciativas necesarias para mantener y fortalecer el Sistema de Administración de la Seguridad de la Información, así como las demás iniciativas tecnológicas requeridas para asegurar la alineación tecnológica y apoyo a la Estrategia Institucional.

b. Elevar a conocimiento y análisis del Comité de Directores de Finanzas y Riesgos, cuando así corresponda y por recomendación del Comité de Tecnología de Información, los cambios requeridos en la Política de Seguridad de la Información, para asegurar que se mantenga su vigencia y efectividad.

c. Elevar a conocimiento y análisis del Comité de Directores de Presupuesto y Asuntos Organizativos y dentro del contexto del anteproyecto de Presupuesto General del Banco; el presupuesto de Tecnología de Información del Banco y los cambios al mismo que pudieren surgir.

d. Aprobar el Manual de Aplicación de la Política 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 Información.

**2.5.** Corresponde al Comité de Tecnología de Información el monitoreo y supervisión del Sistema de Sistema de Administración de la Seguridad de la Información a través de las siguientes funciones:

a. Analizar y recomendar a la Presidencia Ejecutiva la aprobación del Plan Estratégico de Tecnología de Información del BCIE, así como la metodología para su formulación.

b. Analizar y acompañar el Plan Operativo Anual de TI, así como el presupuesto de inversiones de las áreas tecnológicas de la Gerencia de Operaciones y Tecnología.

c. Conocer y analizar con la periodicidad que así defina el Comité los informes de avance y cumplimiento del Plan Estratégico de TI del BCIE, así como del Plan Operativo Anual de Tecnología de Información del BCIE.

d. Analizar y recomendar a la Presidencia Ejecutiva cualquier modificación a la Política de Seguridad de Información y a su Manual de Aplicación.

**2.6.** Corresponde a la Gerencia de Operaciones y Tecnología:

a. Administrar los recursos asignados para gestionar y mantener un adecuado Sistema de Administración de la Seguridad de la Información.

b. Proponer las modificaciones que correspondan a la Política de Seguridad de la Información, su Manual de Aplicación, 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.

d. Desarrollar e implementar los procedimientos, los manuales y las actividades necesarias para incorporar en las operaciones y procesos del Banco lo relacionado con seguridad de la información generada y procesada, la seguridad física y la conservación de registros de archivo físicos y electrónicos.

e. Proponer al Comité de Tecnología de Información, conforme las metodologías y periodicidades definidas en el Manual de Formulación y Monitoreo del Plan Estratégico y el Plan Operativo Anual de la Tecnología de Información del BCIE, las propuestas de Plan Estratégico de Tecnología de Información PETI y de Plan Operativo Anual de Tecnología de Información asegurando que las mismas incluyan iniciativas, proyectos y actividades necesarias para el debido mantenimiento del Sistema de la Seguridad de la Información del Banco.

f. Establecer los controles adecuados para mitigar los riesgos asociados con la seguridad de la información.

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 y al Usuario 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 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 Aplicación 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.** Todo el personal del Banco, así como las demás personas naturales y jurídicas que conforme lo establecido en el alcance de esta Política son sujetos de aplicación a 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 de trabajo con el mismo, salvo aquella información que sea catalogada como pública. La obligación de confidencialidad de la información subsistirá hasta por 7 años después de concluida la relación entre el Banco y la persona. La Oficina de Recursos Humanos deberá asegurar que en los contratos de trabajo se establezca formalmente esta obligación de confidencialidad aplicable cuando el personal se retira del Banco y finaliza su relación laboral.

**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 laboral o 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, trasformación o

consulta y la información legalmente adquirida o cedida de forma voluntaria por alguna contraparte con la que el Banco tiene relaciones.

**Artículo 5.** Aunque se considere la propiedad material, el personal del Banco debe tener en cuenta y está obligado 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 de propiedad del Banco, la Administración Superior, a través de la GEROP, debe asegurar que el Banco cuente 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.** A los jubilados del Banco, a los inversionistas en certificados de depósito bancario que emita el Banco, a los clientes y a los proveedores que realicen transacciones con el Banco por medios electrónicos, se les debe requerir la suscripción de un documento que establezca los acuerdos de uso y de confidencialidad que el Banco defina, según se establezca en el Manual de Aplicación de esta Política. Asimismo, deberán suscribir la aceptación y cumplimiento de la presente Política de Seguridad de la Información, así como del Manual de Aplicación de la misma.

## ACCESO A LOS ACTIVOS DE INFORMACIÓN

**Artículo 8.** La Gerencia de Operaciones y Tecnología es responsable de definir y establecer los activos de información básicos que deben ser otorgados a cada uno de los sujetos obligados a cumplir con esta Política. El acceso que se otorgue a otros activos de información, además de los básicos, debe ser racional en términos de costo y seguridad y debe ser autorizado por los jefes de las áreas responsables de la Información, limitándose exclusivamente a aquellos activos de información necesarios para realizar las funciones oficiales. En este sentido la Gerencia de Operaciones y Tecnología 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 Gerencia de Operaciones y Tecnología debe asegurar la conservación y el monitoreo de bitácoras técnicas y registros de archivo a nivel general y de forma específica, con el objeto de asegurar la confiabilidad de la información, así como dar seguimiento y análisis de actividades o transacciones. En este sentido la plataforma tecnológica del Banco debe tener la capacidad de generar las bitácoras requeridas para el cumplimiento de este lineamiento.

**Artículo 10.** Para efectos técnicos de mantenimiento, respaldo, actualización, soporte u otras actividades análogas, los custodios de la información deben contar con acceso a todos los activos de información, excepto a aquellos cuyo acceso sea expresamente prohibido por el Directorio.

**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, única y exclusivamente con fines de

monitorear el debido cumplimiento de la Política de Seguridad de Información o de prevenir o contener posibles incidentes de seguridad. En casos plenamente justificados o por riesgos reales o potenciales para el BCIE donde los custodios de información u órganos de control del BCIE requieran adelantar investigaciones formales específicas que requieran acceso al contenido de cuentas oficiales de correo, las mismas deberán ser autorizadas por el Presidente Ejecutivo. Si el acceso requerido es a cuentas de correo cuyos responsables de Información formen parte del personal de las Direcciones, del personal de las áreas que reportan al Directorio o del propio Presidente Ejecutivo, los accesos deberán ser autorizados por el Director Coordinador del Directorio. Si el acceso requerido es a cuentas de correo de los directores, los accesos deberán ser autorizados por el Contralor. Si el acceso requerido es a la cuenta del Contralor, el acceso deberá ser autorizado por el Auditor Interno.

**Artículo 12.** Las restricciones de acceso no aplican si la solicitud se realiza para efectos de soporte técnico y proviene del responsable de la Información para acceso a activos bajo su responsabilidad o de la persona a quien se le asignen equipos de usuario final.

**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, sean estos de su propiedad o de propiedad del Banco.

## UTILIZACIÓN Y ADMINISTRACIÓN DEL RECURSO INFORMÁTICO

**Artículo 14.** La Gerencia de Operaciones y Tecnología, 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, se deben establecer los controles necesarios para gestionar y controlar los elementos que forman parte de la infraestructura tecnológica, con el fin de que sean utilizados en un entorno adecuado de seguridad, estándares técnicos y disponibilidad, alineados a las mejores prácticas en ese sentido.

Asimismo, cualquier adquisición, instalación o actualización de los Activos de Información que conforman la plataforma tecnológica del Banco, deberá estar autorizada por la Gerencia de Operaciones y Tecnología a través del Departamento de Seguridad de Información y de Aseguramiento de la Calidad de TI o el Departamento de Tecnología y Comunicaciones, según corresponda y las mismas deben estar en alineación al Plan Estratégico de Tecnología de Información y al Plan Operativo Anual de Tecnología de Información.

**Artículo 15.** Se deben establecer los controles necesarios dentro del Banco que permitan normar y controlar la administración y uso de cuentas privilegiadas y se debe contar con herramientas que permitan llevar la trazabilidad de las acciones realizadas en la plataforma tecnológica por parte del personal técnico del Banco haciendo uso de cuentas privilegiadas.

**Artículo 16.** La administración de los equipos de usuario final, servidores, aplicaciones y en general de toda la infraestructura y plataforma de TI es responsabilidad de la Gerencia de Operaciones y Tecnología. En este sentido, corresponde a la Gerencia de Operaciones y Tecnología proponer para consideración del Comité de Tecnología de Información, los estándares que utilizará el Banco a nivel de plataformas tecnológicas.

**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 USBs, 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. Información Pública:** Es aquella información propiedad del Banco que, de manera unilateral y que, por así convenir a sus intereses y necesidades, el BCIE publique o difunda a la sociedad o al público en general. Esta información puede ser obtenida y ofrecida sin reserva alguna y previo a su publicación en los medios correspondientes, debe ser revisada y aprobada por los responsables de información, según sea cada caso.

**19.2. 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.

**19.3. 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, la Cooperativa/ Caja de Ahorro y Crédito de Empleados del BCIE 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.

**19.4. Información Restringida**. Es aquella información clasificada como confidencial y que, además, por su sensibilidad su acceso está limitado exclusivamente al Directorio, órganos de Control y la Administración Superior (Presidencia y Vicepresidencia).

**19.5. Información No clasificada**: Se refiere específicamente a Información de propiedad del empleado que no contiene ningún tipo de información del Banco.

**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 analizada por la Oficina de Asuntos Jurídicos y aprobada por el Presidente Ejecutivo.

**Artículo 21.** Los gobernadores, los Directores, el Contralor y el Auditor Interno tendrán acceso a toda la información requerida para el cumplimiento de sus funciones vinculadas al 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 Aplicación de la Política de Seguridad de Información.

**Artículo 22.** En el Manual de Aplicación 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.** La Gerencia de Operaciones y Tecnología deberá implementar los mecanismos necesarios para asegurar que todas las dependencias mantengan un inventario de sus principales activos de información en particular aquellos de uso restringido o confidencial. Será responsabilidad de las áreas 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. En caso de que existan activos de información que sean generados por más de un área, por control y previo consenso de las áreas involucradas, se deberá identificar en el inventario de activos de información correspondiente un único responsable de su clasificación.

**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 responsables de la Información al momento de generarla, considerando las cinco 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 Aplicación.

**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.** La administración de la seguridad física y ambiental de las instalaciones del Banco está a cargo de la Gerencia de Operaciones y Tecnología, a través del Departamento de Servicios Administrativos y de Adquisiciones Institucionales (SAAI).

**Artículo 28.** Cualquier cambio relevante en la estructura física de las instalaciones del Banco debe contar con la aprobación de la Gerencia de Operaciones y Tecnología, la que debe validar que se mantenga la seguridad física del Banco.

**Artículo 29.** La Gerencia de Operaciones y Tecnología debe establecer mecanismos de protección, así como procedimientos y actividades de control orientadas a proteger razonablemente los activos propiedad del Banco, a fin de evitar accesos no autorizados, pérdidas, daños o robo. Especialmente, se deberá dar énfasis al establecimiento de controles que permitan restringir el acceso a áreas donde existan terminales de sistemas electrónicos de pago, de negociación de inversiones o de divisas, equipos de comunicación o servidores de procesamiento central. Igualmente, debe establecer procedimientos para la operación y mantenimiento de las instalaciones físicas.

## REVISIONES PERIÓDICAS DE SEGURIDAD

**Artículo 30.** Ante la rapidez que en el contexto tecnológico se generan nuevas amenazas de seguridad de la información, para cada ejercicio anual, el Banco debe realizar 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.

**Artículo 31.** La Gerencia de Operaciones y Tecnología deberá establecer un plan de cierre de las vulnerabilidades identificadas como resultado de las revisiones éticas, para lo cual, de ser necesario se podrá contar con apoyo de firmas, terceros o contratistas especializados que permitan el cierre de las mismas. El seguimiento periódico de estos planes y las acciones mitigantes deberán ser elevadas a conocimiento del Comité de Tecnología de Información.

## CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN

**Artículo 32.** Se deben establecer los documentos normativos que correspondan a fin de controlar la asignación de derechos de acceso a los sistemas y servicios de información.

**Artículo 33.** La Oficina de Recursos Humanos deberá notificar con antelación al Departamento de SIATI todo movimiento de personal asociado a procesos de vinculación, desvinculación, licencias, traslados, ausencias prolongadas o cualquier otro relacionado con la gestión del recurso humano que pudiese requerir una creación, modificación o cancelación de privilegios de acceso de algún usuario, incluyendo la creación o eliminación de áreas o estructuras organizacionales, a fin de que dicha dependencia realice los cambios necesarios en la plataforma tecnológica. Asimismo, dentro del proceso de reclutamiento del Banco, y al menos cada 5 años posterior a la vinculación del personal, se deberán realizar estudios de seguridad que incluyan la verificación de antecedentes al personal que estará asignado a la operación o administración de sistemas electrónicos de pago, a quienes ejerzan la función de custodios de la información del Banco y a demás plazas clave que a consideración de la Administración así lo ameriten.

**Artículo 34.** Se debe asignar 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 Aplicación de esta Política, 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 hacer uso de las herramientas de seguridad tecnológica que implemente la Gerencia de Operaciones y Tecnología y de seguir las prácticas de control que en tal sentido se definan en el Manual de Aplicación de la presente Política.

**Artículo 35.** La Administración debe establecer los horarios en los cuales estarán disponibles los sistemas transaccionales del Banco, incluyendo Sistemas electrónicos de pago, para que los usuarios realicen operaciones. El acceso y uso a los sistemas transaccionales del Banco fuera de las fechas y horarios establecidos deberán ser justificados y autorizados previamente por las áreas dueñas de información en cada caso y por el Departamento de SIATI.

## RETENCIÓN Y CONSERVACIÓN DE REGISTROS DE ARCHIVO

**Artículo 36.** La Información propiedad del Banco debe preservarse para servir de apoyo a futuras actividades y toma de decisiones, de acuerdo con el grado de importancia de la misma.

**Artículo 37.** Se debe mantener en el Banco una adecuada administración, registro, archivo, clasificación, preservación y destrucción de la información física y electrónica del Banco, tomando en cuenta la obsolescencia y limitaciones tecnológicas tanto de los sistemas aplicativos como de la infraestructura tecnológica.

**Artículo 38.** 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 Gerencia de Operaciones y Tecnología.

## USO DE INTERNET Y CORREO ELECTRÓNICO

**Artículo 39.** El acceso a internet es proporcionado a los Usuarios de Información para facilitar 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 Aplicación de esta Política.

**Artículo 40.** 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 Aplicación de esta Política.

**Artículo 41.** El correo electrónico no se usará para el envío de mensajes masivos a todo el personal, salvo aquéllos 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.

**Artículo 42.** 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 43.** 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

**Artículo 44.** La gestión del ciclo de vida de los sistemas aplicativos del Banco es responsabilidad exclusiva de la Gerencia de Operaciones y Tecnología, a través de sus áreas técnicas. En este sentido, cualquier adquisición o implementación interna o externa de aplicativos y de soluciones tecnológicas en general deberá contar con la autorización de las áreas técnicas de dicha Gerencia, quien deberá contar con procedimientos y especificaciones para:

a. Identificación de soluciones automatizadas.
b. Desarrollo y Mantenimiento de Aplicaciones.
c. Administración de cambios.
d. Administración de datos.
e. Administración de configuraciones y de versiones.
f. Administración de la relación con terceros.
g. Documentación técnica y de usuario final.
h. Gestión de proyectos.

**Artículo 45.** El Banco debe contar con una metodología propia y actualizada para la adquisición, desarrollo y mantenimiento de aplicativos, independientemente de que tales labores sean llevadas a cabo internamente o de forma tercerizada.

**Artículo 46.** Para asegurar los procesos de desarrollo e implantación de aplicativos en servidores del Banco, se debe contar con infraestructura de procesamiento separada para tener ambientes de producción, desarrollo y pruebas. Para el caso de procesos de implementación de servicios o aplicativos en la nube o Internet, se deber asegurar que la infraestructura de procesamiento en la nube permita contar con un ambiente productivo separado del ambiente de pruebas y que dichos servicios cuenten con los adecuados niveles de seguridad que permitan salvaguardar la información del Banco ante amenazas y vulnerabilidades de índoles externo o de responsabilidad del proveedor de dichos servicios.

**Artículo 47.** La Gerencia de Operaciones y Tecnología debe asegurar que los procedimientos tecnológicos cuenten con los controles necesarios para permitir la debida segregación de funciones durante la gestión de cambios y la transferencia de software desde el estado de pruebas hacia el estado de producción en un ciclo interactivo. Igualmente, se podrá contar con el apoyo tercerizado de firmas especializadas que permitan asegurar el debido mantenimiento y soporte de la plataforma aplicativa del Banco.

## CONTINUIDAD DEL NEGOCIO

**Artículo 48.** El Banco debe contar con un Plan de Continuidad del Negocio Institucional, basado en una Estrategia de Continuidad, que incluya controles para identificar y reducir riesgos, limitar las consecuencias de los incidentes y asegurar la reanudación oportuna de las operaciones

indispensables para la continuidad del negocio, con el soporte de una plataforma tecnológica alterna. Los lineamientos de dicho Plan deben estar normados en la Política y Manuales establecidos para la Gestión de la continuidad del Negocio.

**Artículo 49.** Se debe mantener un Plan de Recuperación de Desastres de la Plataforma Tecnológica, que permita restablecer las aplicaciones críticas, sistemas de cómputo y comunicaciones en los tiempos requeridos para asegurar la continuidad del negocio.

**Artículo 50.** Anualmente, se deben realizar pruebas del Plan de Continuidad del Negocio y del Plan de Recuperación de Desastres.

**Artículo 51.** Los jefes de las áreas responsables de los procedimientos que se definan como críticos dentro del Plan de Continuidad del Negocio, deberán asegurar el debido respaldo periódico de los registros vitales requeridos para el funcionamiento del Plan, haciendo uso de las herramientas que para tal efecto disponga la Gerencia de Operaciones y Tecnología.

## GESTIÓN DE INCIDENTES DE SEGURIDAD

**Artículo 52.** Los usuarios de información deben reportar al Departamento de Seguridad de Información y de Aseguramiento de la Calidad de TI 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 53.** Mediante el Manual de Aplicación de esta Política, se debe definir el procedimiento 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 54.** La Administración Superior, a través de la Oficina de Relaciones Institucionales 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 55.** 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 56.** A fin de poder detectar y contener oportunamente cualquier ataque cibernético que pudiera atentar contra la disponibilidad de las operaciones y servicios del Banco, el Banco, 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 57.** 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 procedimientos de seguridad de la información.

## SISTEMAS DE DIVULGACIÓN Y COMUNICACIÓN INTERNA DEL BCIE

**Artículo 58.** Se consideran como canales oficiales de comunicación interna el correo electrónico, las aplicaciones tecnológicas contenidas en el sistema de Lotus Notes, 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 59.** La Administración Superior a través de la Oficina de Relaciones Institucionales 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 60.** Se permitirá el uso de redes sociales a los empleados en casos debidamente justificados requeridos para el desarrollo de las actividades del Banco y siempre y cuando dicho servicio a juicio del Departamento de SIATI no represente un riesgo para el Banco ni que el mismo impacte la productividad, operatividad o disminuya la capacidad de los servicios tecnológicos del Banco. En este sentido, se deben contar con mecanismos que permitan balancear las cargas de red o establecer horarios de servicio de tal forma que dichos servicios no impacten la operatividad del Banco. De igual forma, de representar algún riesgo para el Banco o de impactar el rendimiento de la red del Banco, el acceso a sitios específicos de internet podrá ser bloqueada desde la plataforma de seguridad de información del Banco.

**Artículo 61.** La contratación de servicios para la divulgación de información institucional por Internet y redes sociales será responsabilidad exclusiva de la Oficina de Relaciones Institucionales quien 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 62.** La creación y el manejo de las cuentas oficiales del Banco en redes sociales públicas es responsabilidad exclusiva de la Oficina de Relaciones Institucionales, quien 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 63.** El contenido y publicaciones en redes sociales del Banco, así como en los portales web del BCIE deben ser previamente validados por la Oficina de Relaciones Institucionales. En este sentido, en la página web, publicaciones y redes sociales del Banco sólo se publicará información clasificada por los dueños de información como de carácter pública.

**Artículo 64.** La Administración Superior a través de la Oficina de Relaciones Institucionales, 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 poder realizar publicaciones o comentarios en las redes del BCIE.

## IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

**Artículo 65.** 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 66.** 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 67.** 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.

**Artículo 68.** Las acciones disciplinarias por incumplimiento a lo dispuesto en esta Política, en las normas y en los procedimientos complementarios que apruebe la Presidencia Ejecutiva, deben ser tramitadas de acuerdo con lo establecido en el Reglamento General de Administración de Recursos Humanos y en el Manual de Normas de Conducta o en el Código de Ética, según sea el tipo de falta.

**Política para la Prevención de Lavado de Activos del BCIE**

**"RESOLUCIÓN No. DI-40/2016**

**EL DIRECTORIO, CONSIDERANDO:**

Que, de conformidad con el artículo 15 del Convenio Constitutivo del Banco, es facultad del Directorio definir las políticas operativas y administrativas de la Institución.

Que es conveniente actualizar la Política para la Prevención de Lavado de Activos del BCIE contenida en la Resolución No. DI-57/2004, para ajustarla al entorno de mejores prácticas y estándares internacionales en la materia.

Que, con base en el resultado favorable del análisis que el área técnica del Banco ha efectuado, contenido en el documento justificativo denominado "Propuesta de Actualización de la Política para la Prevención de Lavado de Activos del BCIE" y con la opinión favorable del Comité de Directores de Finanzas y Riesgos, contenida en el Acuerdo No. ACFR-10/2015, así como del Comité de Administración de Riesgos y Cumplimiento (CARC), y con la recomendación del Comité de Directores de Auditoría contenida en el Acuerdo No. CA-12/2016, la Presidencia Ejecutiva ha estimado procedente someter a la consideración del Directorio la presente resolución y recomendar su aprobación.

**RESUELVE:**

**PRIMERO:** Aprobar la siguiente**:**

## POLÍTICA PARA LA PREVENCIÓN DE LAVADO DE ACTIVOS DEL BANCO CENTROAMERICANO DE INTEGRACIÓN ECONÓMICA (BCIE)

### CAPÍTULO I

### ASPECTOS GENERALES

**Artículo 1. Objeto.** El objeto de la presente Política es establecer los principios y las normas que serán de aplicación y observancia general en todos los niveles del BCIE para generar una cultura institucional orientada a la administración del riesgo de Lavado de Activos y Financiamiento del Terrorismo (LA-FT). En atención a las recomendaciones internacionales, el BCIE dirige sus esfuerzos para la administración de este riesgo 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, a través de la implementación de un Sistema de Administración del Riesgo de LA-FT que atienda a la naturaleza y demás características particulares del BCIE.

La presente Política representa la parte medular del Sistema de Administración del Riesgo de LA-FT, que se define como el conjunto de políticas, procesos y procedimientos, documentación, 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 en las operaciones del BCIE.

De igual forma, esta Política incorpora elementos para impedir el financiamiento de la proliferación de armas de destrucción masiva.

**Artículo 2. Aplicabilidad de la Política.** La presente Política, en conjunto con la normativa interna, es aplicable a todo el personal del BCIE, así como a aquellas personas, naturales o jurídicas que de alguna manera desarrollen actividades para o encomendadas por el BCIE.

Estas directrices deberán observarse en todas las operaciones activas, pasivas y de adquisición de bienes y/o servicios en las que el BCIE interactúe y sea contraparte directa de otra persona natural o jurídica.

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, que conlleve el incumplimiento de los principios y normas consagrados 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 o en la normativa que resultare aplicable, sin perjuicio de la responsabilidad legal que correspondiere.

## CAPÍTULO II

## PRINCIPIOS BÁSICOS

**Artículo 3. Principios Básicos.** Los principios básicos que regirán la conducta del personal del BCIE frente a la presente Política son los siguientes:

**a)** Cumplimiento de la normativa interna vigente que conforme el Sistema de Administración del Riesgo de LA-FT.

**b)** Observancia de la debida diligencia con respecto al conocimiento de las contrapartes, de acuerdo con la normativa interna vigente en la materia.

**c)** Confidencialidad en relación con la información suministrada por las contrapartes, así como de los registros y de los documentos referentes a las operaciones respectivas, de conformidad con la política del Banco que regula la materia.

**d)** Colaboración requerida para el adecuado funcionamiento del Sistema de Administración del Riesgo de LA-FT y que el cumplimiento de esta Política y demás normativa interna en la materia se anteponga al logro de las metas comerciales.

## CAPÍTULO III

## NORMAS PARA LA APLICACIÓN DE LA POLÍTICA

**Artículo 4. Cumplimiento de la Política.** Todo el personal aplicará rigurosamente la presente Política, de manera tal que se asegure total transparencia en el desarrollo de los negocios y operaciones del BCIE.

**Artículo 5. Adopción de Estándares Internacionales.** Todo el personal actuará respetando los lineamientos que se establezcan en la normativa interna que regula la materia, la cual atenderá, conforme la naturaleza del BCIE, las disposiciones aplicables contenidas en los estándares internacionales emitidos por entidades tales como el Grupo de Acción Financiera (GAFI) y los pronunciamientos del Comité de Basilea, entre otros.

**Artículo 6. Conocimiento de Contrapartes.** Para el adecuado conocimiento de contrapartes se deberá**:**

**a)** Abstenerse de recomendar o, en su caso, de aprobar cualquier operación activa, pasiva o de adquisición de bienes y/o servicios cuando exista duda sobre la idoneidad de las contrapartes con las que el BCIE mantiene relaciones comerciales o de otra naturaleza.

**b)** Establecer requisitos para la vinculación de contrapartes, 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 de acuerdo con la naturaleza de sus contrapartes y negocios, estableciendo procedimientos que faciliten la identificación del beneficiario final.

**d)** Implementar procedimientos de debida diligencia, debida diligencia simplificada y debida diligencia mejorada, de conformidad con el nivel de riesgo de LA-FT de sus contrapartes y atendiendo la naturaleza de los negocios que realiza.

**e)** Establecer mecanismos que impidan promover vínculos con contrapartes que apoyen la construcción, distribución y financiamiento de armas de destrucción masiva.

**f)** Implementar controles para evitar que las operaciones del BCIE se encuentren relacionadas con el financiamiento del terrorismo.

**Artículo 7. Controles de Ingreso y Seguimiento de Contrapartes.** La Administración deberá realizar un permanente seguimiento de las contrapartes involucradas con la debida prudencia, de tal manera que se conozcan razonablemente sus actividades, procedencia de fondos, estructura de gobierno y/o cualquier otro elemento que permita determinar que la contraparte no está vinculada a actividades de LA-FT, considerando su naturaleza y nivel de riesgo de LA-FT asociado.

Se deberán identificar señales de alerta de LA-FT y características catalogadas como de mayor riesgo de LA-FT de conformidad con estándares internacionales, con el propósito de realizar medidas de debida diligencia mejorada. Asimismo, se deberá considerar en el proceso de debida diligencia las listas de entidades y jurisdicciones sujetas a sanciones.

El personal del BCIE tiene el deber de informar de inmediato a sus superiores y al Oficial de Integridad y Cumplimiento cuando se identifiquen operaciones inusuales o sospechosas de contrapartes, de conformidad con lo establecido en la normativa interna.

El personal a cargo de la relación con las contrapartes, denominado responsable primario, y el personal de la Oficina de Integridad y Cumplimiento en el caso de las operaciones analizadas en materia LA-FT por esta dependencia, está obligado a aplicar las medidas de control de ingreso y seguimiento señalados en la normativa interna, utilizando las herramientas disponibles en el BCIE que permitan documentar la debida diligencia realizada.

**Artículo 8. Sistema de Administración del Riesgo de LA-FT.** La Administración deberá adoptar un Sistema de Administración del Riesgo de LA-FT y verificar periódicamente su cumplimiento.

Para este efecto, la Presidencia Ejecutiva conformará un comité para atender los temas relacionados con este sistema. Asimismo, designará un Oficial de Integridad y Cumplimiento a cargo de la Oficina de Integridad y Cumplimiento, informando de tal designación al Directorio del BCIE.

Este sistema deberá considerar las directrices para identificar, medir, controlar y monitorear los riesgos de LA-FT, cautelando la segregación de funciones.

**Artículo 9. Responsabilidades del Oficial de Integridad y Cumplimiento.** El Oficial de Integridad y Cumplimiento coordinará el Sistema de Administración del Riesgo de LA-FT, aplicará y velará por el cumplimiento de la presente Política y su normativa complementaria, establecerá controles antilavado y capacitará al personal en la materia.

**Artículo 10. Consideraciones del Sistema de Administración del Riesgo de LA-FT.**

**a)** El BCIE compromete a todos sus estamentos de gobierno corporativo y, en general, a todo el personal a dar estricto cumplimiento y aplicación de la presente Política, normativa interna y

cualquier otro documento que forme parte del Sistema de Administración del Riesgo de LA-FT.

**b)** El Directorio y la Presidencia Ejecutiva velarán por la existencia de una estructura organizacional adecuada para el eficiente funcionamiento del Sistema de Administración del Riesgo de LA-FT, garantizando el suministro de los recursos necesarios. Asimismo, se deberá contar con una auditoría independiente 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.

**c)** El Directorio y la Presidencia Ejecutiva se comprometen a proporcionar todos los medios necesarios para impartir capacitaciones dirigidas al personal que se considere deban ser capacitados por su exposición al Riesgo de LA-FT, de manera que el modelo se convierta en parte de la cultura organizacional.

Se velará por que el personal de la Oficina de Integridad y Cumplimiento mantenga una preparación y especialización permanente que permita contar con las capacidades y condiciones necesarias para su adecuado desempeño.

Es deber de todo el personal participar en las convocatorias anuales derivadas del programa de capacitación sobre el Riesgo de LA-FT.

**d)** El Directorio, los órganos de control y en general todo el personal del BCIE se compromete a guardar absoluta confidencialidad respecto de la información que se elabore y distribuya en relación al Sistema de Administración del Riesgo de LA-FT.

**Artículo 11. Colaboración con las Autoridades.** 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 relacionadas con la represión y control del delito de lavado de activos.

**Artículo 12. Conservación de los Documentos de Soporte y Registros.** El BCIE dispondrá la conservación de todos los documentos, con la debida seguridad, relacionados con el Riesgo de LA-FT, hasta por un período de siete años.

**Artículo 13. Actualización.** La Administración, a través de la 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.

**SEGUNDO:** Instruir a la Presidencia Ejecutiva para que presente a conocimiento del Directorio el manual correspondiente a la presente Política. Dicha presentación deberá efectuarla en un plazo no mayor a

seis (6) meses, contado a partir de la aprobación de la presente resolución, previo conocimiento del mismo en el Comité de Directores de Auditoría.

**TERCERO:** La presente Política para la Prevención de Lavado de Activos del Banco Centroamericano de Integración Económica (BCIE) entrará en vigencia a partir de la fecha de aprobación por parte de la Presidencia Ejecutiva del manual referido en el resolutivo anterior.

**CUARTO:** Al momento de entrada en vigencia de la Política contenida en la presente resolución, quedará derogada la Resolución No. DI-57/2004 que aprobó la Política para la Prevención de Lavado de Activos del Banco Centroamericano de Integración Económica".

Es conforme con su original, con el que fue debidamente cotejada.