PRIMER BANCO
DE LOS TRABAJADORES

Informe de Gestión Integral de Riesgos 2024

PRIMER BANCO
DE LOS TRABAJADORES

INFORME DE GESTION INTEGRAL DE RIESGOS
CORRESPONDIENTE AL EJERCICIO ECONOMICO 2023

I.- Introducción

Las "Normas Técnicas para la Gestión Integral de Riesgo de las Entidades Financieras" (NRP-20) y las "Normas Técnicas de Gobierno Corporativo" (NRP-17), establecen que el Gobierno Corporativo es el sistema por el cual las sociedades son administradas y controladas; y su estructura debe contemplar las atribuciones y obligaciones de las que participan en su administración, supervisión y control, los Accionistas, la Junta Directiva, miembros de la Alta Gerencia, Comités y Unidades de Control; y debe proporcionar un marco adecuado de transparencia de la institución y la protección de los intereses de los depositantes y usuarios; así como, las partes interesadas de las entidades. Lo que conlleva a que nuestra Junta Directiva ejerza una permanente labor de dirección y supervisión en el manejo, control y mitigación de los riesgos del Banco. Por lo que, como dichas atribuciones son llevadas por: Comités de Junta Directiva, Comités de apoyo y Gerencia de Riesgos en forma conjunta con las Gerencias Financiera y Gerencia de Activos de Riesgos, y su verificación por la Auditoría Interna; velando por una adecuada gestión de los riesgos garantizándose que la toma de decisiones sea congruente con el apetito de riesgo del Banco. Por lo que la Junta Directiva recibe informes actualizados sobre los riesgos del Banco, aprueba las Políticas, Límites y Estrategias de Riesgo a seguir, participando activamente tanto en la aprobación como en el seguimiento de estos.

La Gestión de Riesgos como parte esencial de la visión estratégica de PRIMER BANCO DELOS TRABAJADORES, y es aplicada en todas las áreas, por ello, la Gestión Integral de Riesgos se apoya en una estructura de gobierno organizada, procesos, herramientas de gestión y la cultura de prevención de riesgos; de igual forma, se han implementado metodologías que incluyen la identificación, medición, control y mitigación, monitoreo y comunicación, permitiendo a través del proceso de gestión; tomar decisiones y asumir dentro de un nivel prudencial, riesgos que se encuentran inherentes en la operatividad reduciendo las posibilidades de ocurrencias e impactos negativos.

En cumplimiento de lo establecido en el Art. 21 de las Normas Técnicas para la Gestión Integral de Riesgo de las Entidades Financieras NRP-20, se presenta el informe para el período correspondiente al ejercicio económico 2024.

II.- Estructura Organizativa

Dentro de las acciones desarrolladas para la gestión Integral de riesgos, se ha establecido una estructura responsable de impulsar la cultura de la administración de riesgos; y que establece lineamientos que se implementan en el Banco con el objeto de llevar a cabo la identificación, medición, monitoreo, límites de riesgo, control y divulgación.

1.- Comité de Auditoría

Tiene como objetivo principal asistir a la Junta Directiva en el cumplimiento de sus responsabilidades de diseño, actualización permanente y adecuado funcionamiento del Sistema de Control Interno del Primer Banco de los Trabajadores y del cumplimiento de leyes, regulaciones y normativas aplicables.

2.- Comité de Riesgos

Tiene como asignación dar seguimiento de la gestión integral de riesgos; mediante una adecuada coordinación con las áreas operativas para apoyar las labores realizadas por la Gerencia de Riesgos, y es el enlace entre esta y la Junta Directiva. El Mandato del Comité de Riesgos forma parte del Código de Gobierno Corporativo del Banco.

3.- Comité de lavado de dinero y de activos, financiamiento del terrorismo y financiación de la proliferación de armas de destrucción masiva - LDA/FT/FPADM

Tiene como asignación comunicar de manera oportuna a la Junta Directiva los informes de control interno y las transacciones catalogadas como sospechosas a fin de reportar a los entes reguladores y fiscalizadores. Esta función no resta la debida independencia que posee el Gerente de Cumplimiento de reportar transacciones identificadas como sospechosas.

4.- Comité Gerencial Ampliado

El Comité Gerencial Ampliado tiene como finalidad decidir sobre temas relacionados con el planeamiento estratégico, presupuesto, sistemas de información, procesos, mejora continua, asuntos administrativos y de gestión en general, bajo los parámetros establecidos en las políticas y estrategias de la institución.

5.- Comité de Tecnología y Comunicaciones

El Comité de Tecnología y Comunicaciones tiene por objeto ser una instancia asesora y de coordinación de temas de Tecnología de la Información y de Comunicaciones informáticas, de Riesgos Tecnológicos y su gestión.

6.- Comité de Recuperación de Créditos

El Comité de Recuperación de Crédito tiene como finalidad analizar, discutir y aprobar/denegar solicitudes de clientes con problemas de morosidad o dificultades para cumplir con las obligaciones crediticias adquiridas con la institución.

III.- Gestión por Tipo de Riesgos

1.- Riesgo de Crédito

Según la norma NPB4-49 define Riesgo de Crédito como la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida esta última como un prestatario o un emisor de deuda.

Se identifica con la probabilidad de que el acreditado no cumpla con los compromisos de pago y otras obligaciones pactadas, también por la concentración de financiamiento en un grupo de empresas o en ramas de actividad que son más vulnerables que otras, a variaciones económicas. La disminución de este tipo de riesgo se logra mediante la aplicación de un objetivo análisis de crédito, una cuidadosa investigación de las referencias del solicitante de crédito, de las garantías correspondientes, de un monitoreo permanente del servicio de la deuda y de la posición financiera del acreditado; así como, de una eficiente labor de cobranza.

El Proceso en la toma de decisiones comienza con la evaluación del riesgo de crédito de la contraparte. Entre los factores considerados en la evaluación son la solvencia actual y proyectada del cliente, resultados financieros, la experiencia en la industria en la cual opera el solicitante y/o deudor, tendencias económicas, políticas y la capacidad de repago del cliente. Dependiendo del segmento de mercado (Créditos de Consumo, Créditos para Empresas, Créditos para Vivienda) así es el análisis por aplicar.

Para la gestión del Riesgo de Crédito el Banco cuenta con las herramientas siguientes:
- Políticas, manuales y procedimientos para el otorgamiento de préstamos, y
- Comités de Crédito, para el análisis de las operaciones a financiar con límites escalonados según los montos de financiamientos.
- Herramientas de Medición a través de la aplicación adquirida por el Banco, denominada Risk Assistant.

2.- Riesgo de Mercado

Según lo define la norma NRP-20, Riesgo de Mercado, como la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados financieros de la entidad y se subdividen en Riesgo de Tasa de Interés, Riesgo de Precio y Riesgo por Tipo de Cambio.

Para la gestión del Riesgo de Mercado el Banco cuenta con las herramientas siguientes:
- Política de Manejo de Inversiones, y
- Herramientas de Medición a través de la aplicación adquirida por el Banco, denominada Risk Assistant.

3.- Riesgo de Liquidez

Según las Normas Técnicas para la Gestión del Riesgo de Liquidez - NRP-05, es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas.

En este contexto la Gerencia Financiera y de Administración realiza anualmente un Plan de Contingencia de Liquidez, que establece un marco que determinan las acciones apropiadas ante el acontecimiento de una crisis de liquidez, sin perder de vista las normativas coadyuvantes al mantenimiento de los índices tales como las normas Norma NRP-05 Normas Técnicas para la Gestión del Riesgo de Liquidez,

Para la gestión del Riesgo de Liquidez el Primer Banco cuenta con las herramientas siguientes:
- Política de Manejo de Inversiones,
- Plan de Contingencia de Liquidez,
- Plan de Recuperación Financiera y
- Herramientas de Medición a través de la aplicación adquirida por el Banco, denominada Risk Assistant, en la cual se monitorean brechas de liquidez en espacios temporales a fin de tomar medidas de acción de ser necesario.

4.- Riesgo Operacional

Según la norma NRP-42 define como Riesgo Operativo a la posibilidad de incurrir en pérdidas debido a fallas en los procesos, de las personas, en los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal que consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros.

Riesgo operativo se define a las posibles pérdidas para el Banco por errores o fallas en el desarrollo de las actividades administrativas y operativas del negocio, o por deficiencias o fallas en los sistemas informáticos, recursos humanos o por la posible ocurrencia de sucesos inesperados, relacionados con la infraestructura operativa y tecnológica interna y externa.

El riesgo operacional está siendo gestionado dentro de un sistema de control interno, por lo que el Banco cuenta con los procedimientos y controles para gestionar y mitigar las actividades relacionadas entre otros con:
- Administración de Recursos Humanos y Capacitación,
- Documentación de procesos, políticas, procedimientos y controles significativos,
- Sistemas de Información Gerencial,
- Desarrollo y Mantenimiento de Tecnología.

5.- Riesgo Reputacional

Según la norma NRP-20 define como Riesgo Reputacional a la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros.

Está relacionado con la publicidad o imagen negativa del Banco, sea ésta verdadera o falsa, lo cual puede originarse de todos los aspectos de la actividad bancaria, entre ellas, las prácticas de negocios de la institución, la forma y manejo de las operaciones, la conducta de nuestros empleados, atención a clientes, por la no atención de las regulaciones internas y regulatorias debidamente establecidas, así como de las instrucciones de los supervisores, que en definitiva terminarán afectando la imagen de la institución, y consecuentemente podría incidir en la cartera de clientes existentes y generar altos costos para el Banco.

6.- Riesgo Legal

Definido como la posibilidad de pérdida en que incurre una entidad al ser sancionada, multada u obligada a indemnizar daños como resultado de incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

La administración de riesgo legal cuya implementación como parte de un enfoque integral que tiene como componentes principales de mitigación los siguientes elementos:
- Políticas generales y específicas sobre la administración del riesgo legal.
- Estructura organizacional adecuada para la administración del riesgo legal.
- Procesos, procedimientos y sistemas de control.
- Metodologías, modelos de contratos depositados en la Superintendencia del Sistema Financiero, y sistemas de información.

7.- Riesgo Tecnológico

Definido como la perdida potencial por daños, interrupción, alteración, o fallas derivadas del uso o dependencia del hardware, software, sistemas, aplicaciones, comunicaciones, y cualquier otro canal de distribución de información que una entidad tiene para prestar sus servicios; así como la aplicación de lo contenido en la norma NRP-23 Normas técnicas para la gestión de la seguridad de la información.

En la administración del Riesgo Tecnológico, el Banco cuenta con la Auditoria de Sistemas que vela por el cumplimiento de las políticas y normas de seguridad tecnológica mediante el monitoreo de la matriz de eventos de riesgos relacionados con la temática.

8.- Riesgo de lavado de dinero y de activos, financiamiento del terrorismo y financiación de la proliferación de armas de destrucción masiva - LDA/FT/FPADM.

Riesgo de lavado de dinero y de activos y de financiamiento al terrorismo. La gestión del riesgo de lavado de dinero y de activos y de financiamiento al terrorismo está delegada en la Oficialía de Cumplimiento con dependencia directa de la Junta Directiva, la cual ejerce funciones de prevención de dichos riesgos, cumpliendo además con las facultades establecidas en la Ley aplicable, en el Instructivo de la Unidad de Investigación Financiera (UIF) y con las responsabilidades establecidas en la NRP-36 "Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva" emitida por el Banco Central de Reserva de El Salvador

9.- Riesgo Ambiental y Social

Riesgo Ambiental y social; posibilidad de incurrir en pérdidas generadas por los impactos ambientales y sociales negativos ocasionados por el otorgamiento de créditos para el financiamiento de actividades, obras o proyectos.

Para la gestión del Riesgo Ambiental y Social Primer Banco cuenta con procedimiento debidamente establecido, que incluye entre otros el cumplimiento del marco regulatorio nacional como lo es la NRP-53 Normas Técnicas para la Gestión de Riesgos Ambientales y Sociales, con enfoque en los riesgos indirectos asociados con la cartera de crédito.

Metodología: Primer Banco viene desarrollando y fortaleciendo su modelo de gestión Ambiental y Social desde el 2023, con mejoras continuas al sistema de gestión de Riesgos Ambientales y Sociales, así también, se cuenta con una Política de Riesgo Ambiental y Social, y su Reglamento; documentos que fueron aprobados el 23 de diciembre de 2024, y que tiene como objetivo, brindar los lineamientos bajo los cuáles el Primer Banco controla y mitiga el Riesgo Ambiental y Social de su cartera.

10.- Continuidad del Negocio.

La Metodología empleada para la Gestión de Continuidad del Negocio se basa en las etapas definidas en la Política de Gestión de Continuidad del Negocio y el Plan de Continuidad del Negocio, siendo la siguiente:

a) Entendimiento de la Organización. Es la etapa mediante la cual el Primer Banco entiende sus procesos críticos, previa elaboración de los planes de contingencias, así mismo se establece una instancia para la toma de decisiones ante las situaciones de crisis, para lo cual se utiliza:

- Análisis de Impacto del Negocio (BIA)
- Organización del Comité de Crisis.

b) Selección de la Estrategia de Continuidad. A partir del análisis del BIA se identifican las diferentes estrategias de continuidad, seleccionando las más adecuada para el Primer Banco, analizando las variables de criticidad del proceso a proteger, el costo de la estrategia y el tiempo de recuperación.

c) Desarrollo e Implementación de Continuidad. Las estrategias seleccionadas son documentadas, en los siguientes planes:

- Plan de Emergencia y Evacuación
- Plan de Gestión de Crisis.
- Plan de Recuperación Informático ante Desastres.
- Plan de Continuidad del Negocio.

Todos los planes deben en tener en cuenta las etapas de evaluación, activación y retorno a la normalidad.

d) Pruebas y actualización. Consiste en probar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del Plan de Continuidad del Negocio, siendo la oportunidad de identificar y prevenir problemas y fallas respecto al Plan de Continuidad del Negocio definido, de manera que puedan ser atendidas, preparando al negocio para la emergencia real.

Las pruebas deben incluir guion de pruebas, paso a pasa de la planeación, paso a paso de la ejecución, paso a paso del retorno, acta de reunión.

e) Integrar la Gestión de Continuidad del Negocio a la Cultura Organizacional. Como parte de esta esta etapa se encuentra el registro de los incidentes o eventos a través de la herramienta de riesgo, los cuales afectan la operatividad o desarrollo de los procesos críticos del Primer Banco, además de efectuar jornadas de capacitación, envío de boletines informativos y evaluaciones periódicas para medir el grado de gestión y conocimiento de la continuidad del negocio.

11.- Seguridad de la Información.

La Metodología empleada para la Gestión de la Seguridad de la Información esta definida en el Programa de Seguridad de la Información, basado en el ciclo de mejoramiento continuo, siendo lo siguiente:

a) Políticas de Seguridad y Ciberseguridad. Como parte fundamental de la Gestión de Seguridad de la Información se define el establecimiento de Políticas de Seguridad de la Información y su revisión periódica.

b) Organización de Seguridad de la Información. Se establece un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro del Primer Banco nombrando a un responsable.

c) Seguridad Relativa a los Recursos Humanos. Se define un marco de gestión para asegurar que los empleados contratados bajo cualquier modalidad jurídica entiendan sus responsabilidades en materia de seguridad de la información

d) Gestión de Activos de Información. Los activos de información son identificados, clasificados y protegidos, de manera que se garantice razonablemente la confidencialidad, integridad y disponibilidad de los mismos; por lo cual los activos de información son clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad de cumplen y rotulados en función a ello, con el objeto de señalar como ha de ser tratada y protegida. Para esta etapa se utiliza:
Inventario de activos de información, la cual que contiene los registros del resultado del proceso de identificación, valoración, clasificación y tratamiento de los activos de información del Primer Banco.

e) Control de Acceso a la Información. Se definen las directrices de limitación de acceso a la información y a instalaciones de procesamiento de la información, así mismo los controles para la prevención de acceso no autorizado a sistemas y aplicaciones.

f) Seguridad Física y del Entorno. Se definen las directrices de prevención de acceso físico no autorizado, daños e interferencia a las instalaciones de la Organización, protección del equipamiento de procesamiento de información del Primer Banco ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

g) Seguridad de las Operaciones. Se procura garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones

h) Seguridad de las Comunicaciones. Se establecen los aspectos mínimos para asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

i) Relación con Proveedores. Se definen directrices para la relación con proveedores en cuanto a los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC del Primer Banco.

j) Gestión de Incidentes de Seguridad de la Información. Se establecen funciones y procedimientos de manejo de incidentes basados en la Metodología de la Gestión del Riesgo Operacional garantizando una respuesta rápida y sistemática a los incidentes relativos a seguridad de la Información

k) Seguridad de la Información para la Gestión de la Continuidad del Negocio. Se establece una Política de Gestión de Continuidad del Negocio para minimizar los efectos de las posibles interrupciones de las actividades normales de la organización y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

l) Cumplimiento Legal, Contractual y Normativo. Se establecen directrices para evitar incumplimientos de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

Conclusión

Como institución financiera, el Primer Banco debe gestionar los riesgos inherentes a la naturaleza de sus operaciones, servicios y productos. Entre los riesgos más críticos se presentan el Lavado de Activos y el Financiamiento al Terrorismo. Para combatirlos, el Banco debe de adoptar las tecnologías, metodologías y buenas prácticas recomendadas y/o exigidas por el regulador.

Políticas, manuales y procedimientos para la Gestión Integral de Riesgos

En concordancia con el compromiso a los requerimientos regulatorios, se actualizan las políticas, lineamientos, manuales, procedimientos y formularios para la Gestión Integral de los Riesgos.

Como parte del compromiso con la mejora continua, para la gestión Integral de Riesgos se continuará orientando esfuerzos a los siguientes temas:

- Implementación de cambios normativos. El Primer Banco dará prioridad al cumplimiento regulatorio, por lo cual los esfuerzos serán orientados para la implementación de cambios en

la normativa Integral de Riesgos, así como también a los planes de trabajo que se definan para los requerimientos de implementación de las nuevas normativas de Seguridad de la Información y Continuidad del Negocio.

- Fortalecimiento de cultura de alertas de Indicadores de Riesgos Relevantes. Conscientes de la relevancia que tiene las decisiones tomadas por el personal ante las alertas que generen los riesgos relevantes, se continuará fortaleciendo la cultura de prevención por medio de planes y controles.

El presente informe anual de Gestión Integral de Riesgos 2024 fue aprobado por Junta Directiva en Punto No. 5 del Acta No. 1807-25, de sesión celebrada en fecha 6 de marzo de dos mil veinticinco.