INFORME SOBRE LA GESTIÓN DEL RIESGO OPERATIVO

Al 31 de diciembre de 2023

Elaborado por: **UNIDAD DE RIESGOS**
31/12/2023

Gestión del Riesgo Operativol

En el presente informe se da a conocer las actividades de la gestión del Riesgo Operativo ejecutadas en Banco Ficensa durante el año 2023.

Por definición el Riesgo Operativo es la posibilidad de obtener pérdidas directas o indirectas resultantes de procesos internos inadecuados o fallidos, errores intencionales o no de personas, fallas en los sistemas y ocurrencia de eventos externos adversos. La definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional.

La Gestión del Riesgo Operativo permite minimizar las pérdidas económicas producidas por eventos adversos, mediante el establecimiento anticipado de controles efectivos.

Estrategia de Medición y Mitigación del Riesgo

Para llevar a cabo el proceso de gestión, el Banco dispone de una estructura estratégica y operativa con líneas de autoridad y responsabilidad definidas en la política.

Como estrategia de gestión, se fomenta la cultura del riesgo en toda la organización mediante capacitaciones y mensajes de concientización para lograr que todos los empleados se conviertan en gestores del riesgo, ya que ellos constituyen la primera línea de defensa ante la ocurrencia de eventos de riesgo. Asimismo, se han nombrado Coordinadores de Riesgo Operativo en cada departamento, quienes son los encargados de informar al área de Riesgos los eventos e incidentes que afectan o pudieran afectar a sus áreas y para que se realice la evaluación de la criticidad de cada riesgo, con el fin de que se establezcan los controles necesarios.

Mensualmente el Comité de Riesgos es informado sobre: el estado de los riesgos, los planes de acción correctivos, los eventos de pérdida y las demás actividades. El Comité de Riesgos toma decisiones respecto al tratamiento de los riesgos y finalmente la Junta Directiva es informada, aprueba las políticas, metodologías, límites y emite resoluciones a seguir en aquellos casos que amerite.

Con el fin de lograr el alineamiento entre la gestión del riesgo operativo y la estrategia del Banco, se han incorporado indicadores de gestión dentro del plan estratégico institucional plasmados en la perspectiva de procesos del cuadro de mando.

Se dispone de estadísticas de registros de las pérdidas relacionadas con eventos de riesgo operativo materializados en cada año, procurando que estos se encuentren dentro del apetito de riesgos operativos definido y aprobado por la Junta Directiva.

Perfil del Riesgo Operativo

El perfil de riesgo de la institución se encuentra definido en el Manual de Políticas y Procedimiento de Riesgo Operativo y este indica que, para la definición del apetito del riesgo, la Unidad de Riesgos fijará un monto límite de tolerancia por pérdidas operativas que el Banco está dispuesto asumir, el cual es aprobado por la Junta Directiva. El perfil de riesgos es bastante conservador.

Aceptación de Riesgos

El Modelo implementado en Banco FICENSA para la gestión del Riesgo Operativo permite identificar los riesgos según su criticidad en 5 niveles, siendo los riesgos muy bajos y bajos los que son aceptables, pero aquellos que se ubican en el nivel medio, alto y critico no son aceptables, por lo tanto, se tiene que reducir su criticidad por medio de la implementación de planes de acción correctivos, hasta reducirlos a riesgos aceptables.

Grado de Aceptación	Niveles de Criticidad
Aceptable: Se debe monitorear	Muy Bajo
	Bajo
No Aceptable: Se debe definir un plan de acción correctivo	Medio
	Alto
	Critico

Actividades de Gestión Realizadas y Su resultado

En el 2023 el Banco realizó las actividades de gestión de riesgo operativo establecidas en el Manual de Riesgo Operativo aprobado para tal fin. Se levantó la base de datos con todos los eventos e incidentes de riesgo ocurridos en el año, se ejecutó el

proceso de valoración y monitoreo de eventos e incidentes y se realizó el seguimiento a los planes de acción establecidos para mitigar, trasladar, eliminar o aceptar los riesgos identificados.

Se hizo la revisión anual de las Matrices de Riesgo Operativo según el cronograma establecido, se identificaron nuevos riesgos en los procesos realizados por las áreas, en base a las normativas vigentes y se establecieron controles para cada uno de ellos. Los 29 Macroprocesos de la institución cuentan con su matriz de riesgos operativos.

Se impartieron capacitaciones a los nuevos Coordinadores de Riesgo Operativo, se contrataron los servicios profesionales de los expertos internacionales quienes impartieron capacitaciones a la Junta Directiva y resto del personal en temas de prevención de fraude.

Se adquirió una herramienta para el monitoreo de la Banca Digital con el objetivo de prevenir y mitigar la ocurrencia de fraudes cibernéticos en contra de los usuarios financieros, se fortaleció el área con la contratación de personal experto en prevención de fraude.

Los riesgos legales se identifican junto con los riesgos operativos.
La Política de Riesgo Legal fue revisada y actualizada en el 2023.

Se puso a disposición de los Coordinadores y Gerentes de área las normativas, circulares, leyes y reglamentos emitidos por los entes reguladores para su revisión y análisis de la aplicabilidad e impacto.

Riesgos Identificados en 2023
En 2023 se incorporaron en las Matrices de Riesgo Operativo, nuevos riesgos identificados en los procesos, implementando los controles adecuados para su mitigación.

Eventos de Riesgos por Procesos Identificados en el 2023

Se cuenta con 32 planes de acción nuevos, algunos de ellos consisten en desarrollar programas internos para sustituir procesos manuales por automáticos para reducir errores humanos, se incorporaron nuevos controles en los procesos y en algunos casos se recomendó modificar los procesos.

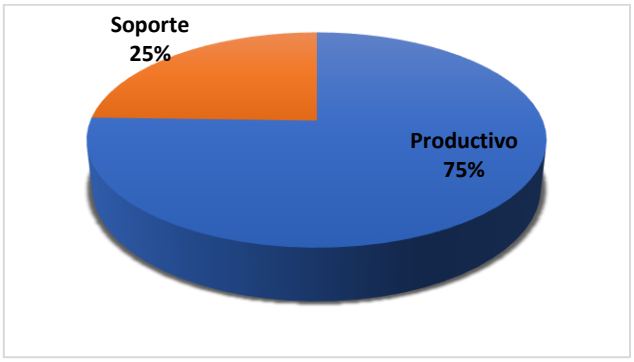
Riesgos con Planes Acción Identificados por Procesos en el 2023

Base de Datos de Eventos de Riesgo Operativo

El Banco cuenta con una base de datos de eventos de pérdidas, los cuales se informan semestralmente a la Comisión Nacional de Bancos y Seguros y se dispone además de otra base de eventos sin generación de pérdidas valorados con el objetivo de mejorar los controles.

En el 2023 el monto de las pérdidas por riesgo operativo ascendió a la suma de L506,564.92 lo que representa el 25.3% del monto límite de tolerancia fijado por Banco FICENSA.

Porcentaje de Pérdidas por Proceso 2023



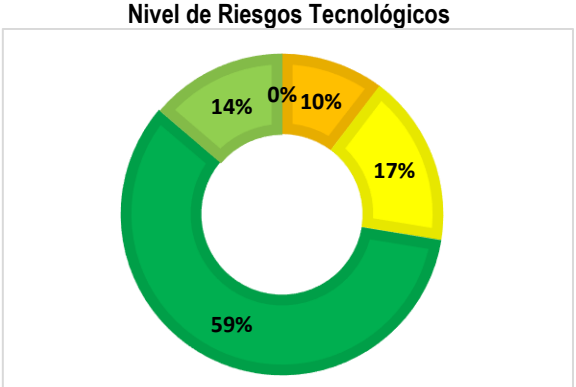
Riesgo Tecnológico

Definido como la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información utilizado en la prestación de servicios con los clientes de la Institución, se traduce en evaluar las vulnerabilidades en sistemas, procedimientos, políticas, procesos y aplicaciones para así identificar los riesgos y administrarlos.

Las amenazas relacionadas con los fraudes se han tratado, robusteciendo las plataformas de seguridad de la información con las que el Banco cuenta. A la vez se implementaron nuevos servicios dentro de la banca en línea adaptándola a nuevas tecnologías, fortaleciéndola y logrando la automatización de controles y monitoreo.
Lo anterior se realizó promoviendo un ambiente de cultura de la seguridad mediante mensajes de concientización y charlas de capacitación, acerca del cuidado ante las amenazas de fraude cibernético.

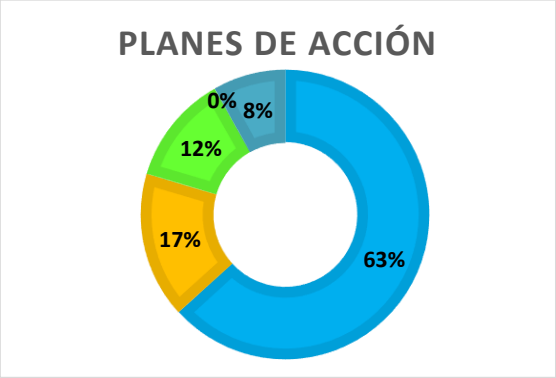
En cuanto al nivel de criticidad de los riesgos tecnológicos, el 73% son de riesgo muy bajo y bajo, 17% de riesgo medio y 10% de riesgo alto. De estos el 22% cuentan con planes de acción en proceso de implementación.

Nivel de Riesgos Tecnológicos



Muy Bajo	Bajo	Medio	Alto	Crítico
14%	59%	17%	10%	0

Parte de la gestión del Riesgo Tecnológico consiste en dar seguimiento mensual al cumplimiento de los planes de acción correctivos que las diferentes áreas llevan a cabo para mitigar los riesgos. A continuación, el estado de los planes de acción al 31 de diciembre de 2023.



Estado de los Planes de acción

Completo	Parcialmente completo	Vigente	Vencido	No aplica
63%	17%	12%	0	8%

Sistema General de Continuidad del Negocio (SGCN)
En materia de Continuidad del Negocio no se han presentado eventos que hayan afectado de manera importante la realización de los negocios.

En vista que el Covid-19 no se ha logrado erradicar por completo, se sigue implementando medidas y cuidados del protocolo de bioseguridad que permite que tanto los colaboradores como los clientes se sientan seguros dentro de la institución.

Respecto al Plan de Recuperación de Desastres, se cumplió con el 100% del plan de pruebas parciales y prueba total simulando caídas en los servidores y enlaces de comunicación, obteniendo resultados satisfactorios y verificando que los equipos y servidores instalados en el data center de contingencia estén disponibles y funcionando correctamente para responder en caso de requerirlos en una contingencia. Los resultados de la prueba total fueron exitosos en un 89%, permitiendo que se realicen los ajustes necesarios.

Se ejecutaron las pruebas de evacuación del personal simulando escenarios adversos que pudieran afectar al personal y a las instalaciones físicas.

El Marco de Gestión de Continuidad del Negocio fue actualizado en el 2023 ya que este es un proceso muy dinámico que amerita constantes cambios.

Se impartieron capacitaciones a los equipos de Gestión de Incidentes en el tema de responsabilidades, asimismo, el Equipo de Respuesta a Emergencias recibió capacitación en temas de primeros auxilios, extinción de incendios, rescate de vidas y evacuación.

Gestión de la Seguridad de la Información y Ciberseguridad
La gestión del riesgo en Seguridad de la Información es un enfoque integral que busca identificar, evaluar y mitigar las amenazas cibernéticas que pueden afectar la confidencialidad, integridad y disponibilidad de los datos. El adecuado sistema de gestión del riesgo cibernético aplicado en Banco FICENSA abarca diversas estrategias y prácticas, entre las que destacan:
Prevención de Intrusiones y Protección del Perímetro:

- Implementación de medidas proactivas para prevenir intrusiones, como firewalls y sistemas de prevención de intrusiones (IPS).
- Configuración adecuada de reglas de seguridad para mitigar vulnerabilidades y reducir el riesgo de ataques.

Monitoreo de Eventos e Identificación de Amenazas:

- Establecimiento de sistemas de monitoreo continuo de eventos para detectar anomalías y posibles amenazas en tiempo real.
- Respuesta inmediata ante incidentes, con procedimientos y equipos preparados para actuar frente a eventos de seguridad.

Administración de Soluciones de Seguridad de Equipos Cliente y Servidores:

- Implementación de software antivirus, antispyware y otras soluciones de seguridad en dispositivos cliente y servidores.
- Actualización constante de las definiciones de amenazas y del software de seguridad para mantener una protección efectiva.

Actualizaciones de Sistemas Operativos y Descubrimiento de Brechas de Seguridad:

- Actualización regular de parches y seguridad en los sistemas operativos para cerrar posibles brechas de seguridad.
- Programación de evaluaciones de vulnerabilidades para identificar posibles riesgos en el entorno informático.

Cumplimiento de Normativas del Regulador y Normas Internacionales (ISO27001, entre otras):

- Adherencia a normativas y estándares específicos relacionados con la seguridad de la información, como ISO 27001.
- Establecimiento de políticas y procedimientos que cumplan con las regulaciones del sector y las leyes de protección de datos.

En resumen, se ha realizado una gestión efectiva del riesgo cibernético con la aplicación de medidas preventivas, el monitoreo constante, la actualización periódica de sistemas y la conformidad con normativas y estándares reconocidos.
Este enfoque holístico contribuye a proteger la infraestructura tecnológica de Banco FICENSA y a preservar la integridad y confidencialidad de la información sensible.