INFORME SOBRE LA GESTION DEL RIESGO OPERATIVO

Al 31 de diciembre de 2019

Elaborado por:
UNIDAD DE RIESGOS
31/12/2019

Gestión del Riesgo Operativo

En el presente informe se da a conocer las actividades de la gestión del Riesgo Operativo que Banco Ficensa ha efectuado durante el año 2019.

Riesgo Operativo es la posibilidad de obtener pérdidas directas o indirectas resultantes de procesos internos inadecuados o fallidos, errores intencionales o no de personas y 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, donde los coordinadores de riesgo de cada área informan a la Unidad de Riesgos acerca de los eventos que afectan y que pudieran afectar a la institución, 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.

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.

En vista que en la gestión de este riesgo participa toda la organización, la Unidad de Riesgos fomenta la cultura de gestión mediante capacitaciones impartidas y mensajes de concientización.

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

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

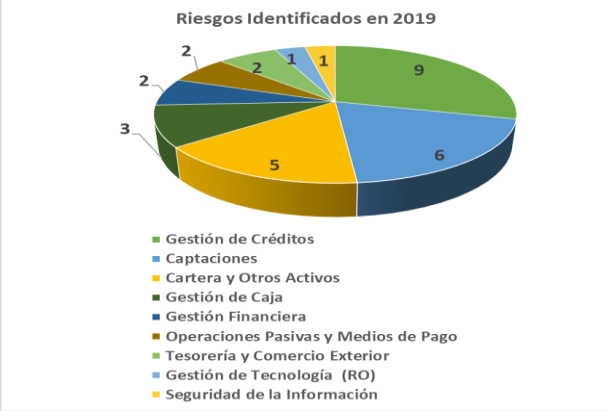
En el 2019 se modificó la Política de Gestión del Riesgo Operativo en lo relacionado a las responsabilidades adquiridas por los Coordinadores de Riesgo Operativo y los Gerentes de Área, con el propósito de que exista una mayor claridad en el papel que cada uno de ellos representa durante la administración del riesgo.

En el 2019 el banco continuo con 28 Macroprocesos y cada uno cuenta con su matriz de riesgos operativos.
Respecto al riesgo legal los riesgos se identifican junto con los riesgos operativos. La política de riesgo legal fue revisada sin modificaciones.

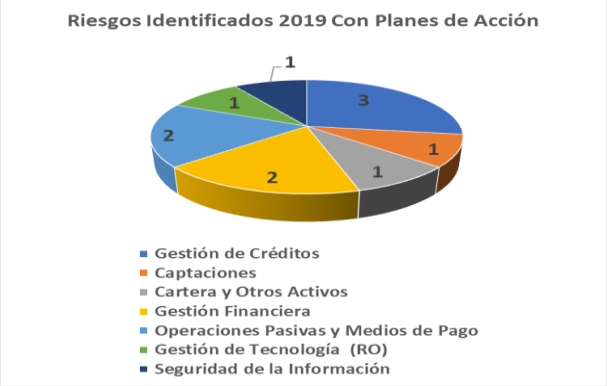
Para fortalecer la cultura de gestión se impartieron a nivel nacional 9 capacitaciones durante el año 2019.

Riesgos Identificados en 2019

En 2019 se incorporaron en las matrices de riesgo operativo nuevos riesgos, para los cuales, gracias al trabajo de los distintos responsables de los procesos, se implementaron los controles adecuados para su mitigación.



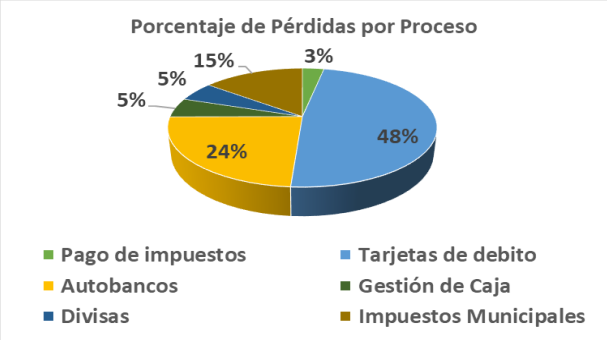
Se requirieron 11 planes de acción nuevos, algunos de ellos consisten en desarrollar programas internos para sustituir procesos automáticos en vez de manuales para reducir errores humanos, se incorporaron nuevos controles en los procesos y en algunos casos se recomendó modificar políticas.



Base de datos de Eventos de Riesgo Operativo

El banco cuenta con una base de datos de eventos de pérdidas, los cuales se informan anualmente 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 2019 el monto de las pérdidas por riesgo operativo ascendió a la suma de L386,828.76, el cual se considera relativamente insignificante; siendo en los procesos de Tarjetas de Débito y Autobancos donde se presentó el mayor porcentaje de concentración de dicho monto.

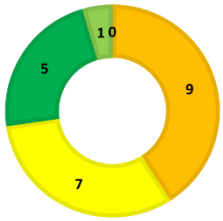


Riesgo Tecnológico

Con el objetivo de mejorar la gestión de los riesgos tecnológicos, en el 2019 se contrató los servicios de una consultoría para la revisión y actualización de la metodología de Riesgo Tecnológico tomando como base las mejores prácticas a nivel internacional establecidas por la Organización Internacional de Normalización (ISO) y la Asociación de Auditoría y Control de Sistemas de Información (ISACA). Como resultado de ello, se revisaron y ajustaron los criterios para la evaluación de impacto y probabilidad en el cálculo de los riesgos inherentes y en la efectividad de los controles para el cálculo del riesgo residual. Asimismo, se logró fortalecer la cultura de riesgo en los equipos de trabajo, obteniendo así un mayor nivel de conciencia y conocimiento de los impactos y consecuencias de cada riesgo, facilitando también su tratamiento y monitoreo.

Se identificaron 22 riesgos tecnológicos, de los cuales 15 presentan riesgos muy bajos y 16 de ellos cuentan con planes de acción en proceso de implementación.

Nivel de Riesgos Tecnológicos



Muy Bajo	Bajo	Medio	Alto	Crítico
5	10	7	9	0

Estado de los Planes de acción

Completos	Vigentes	Vencidos	No necesita plan	Total
5	16	0	1	22

Continuidad del Negocio

Las actividades desarrolladas durante el sistema de gestión de continuidad del negocio durante el 2019 se enfocaron en fortalecer el conocimiento de los miembros del equipo de gestión de crisis en temas de manejo efectivo de las emergencias, logrando identificar sus causas, sus fases, el mejor uso de las comunicaciones, el manejo efectivo del personal durante la situación de crisis, así como otras mejores prácticas para una adecuada gestión. También se reforzaron las funciones del equipo de respuesta a emergencias quienes tienen el objetivo de liderar y dirigir a los colaboradores durante un evento disruptivo, obteniendo una adecuada distribución de roles y responsabilidades entre los miembros del equipo y los cuerpos de socorro. Respecto al tema de la continuidad de los servicios críticos que el banco ha identificado, se realizaron inversiones importantes en infraestructura de tecnología de la información y comunicaciones que vinieron a afianzar el Plan de Recuperación de Desastres definido.

Gestión de la Seguridad de la Información

Banco Ficensa en materia de Ciberseguridad por medio del área de Seguridad de la Información, realizó inversiones significativas en soluciones tecnológicas de prevención y protección, se implementó un Security Information and Event Manager (SIEM) para monitoreo de eventos de las plataformas tecnológicas de seguridad, infraestructura, base de datos y telecomunicaciones. Se implementó además una segunda capa de protección al correo electrónico institucional en la nube, al igual que la implementación de un Firewall de servidor para monitoreo y control de accesos hacia las plataformas iSeries de IBM. Se cumplió con los lineamientos de seguridad establecidos por Swift para el año 2019, así como la mejora en la estructura del Directorio Activo y ordenamiento de este que ha permitido una unificación de autenticación de usuarios de

diversos sistemas en producción, también se realizaron análisis y remediaciones de posibles vulnerabilidades sobre las plataformas iSeries, al igual que el establecimiento de los primeros lineamientos preparatorios para la ejecución del proyecto de Clasificación de la Información que se comenzará a desarrollar a partir del año 2020.