INFORME SOBRE LA GESTION DEL RIESGO OPERATIVO

Al 31 de diciembre de 2018

Elaborado por:
UNIDAD DE RIESGOS
31/12/2018

Gestión del Riesgo Operativo

La finalidad del presente informe es dar a conocer las actividades que Banco Ficensa ha efectuado durante el año 2018 respecto a la Gestión del Riesgo Operativo.

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.

Estrategia de Medición y Mitigación del Riesgo

Con la gestión del riesgo operativo se busca minimizar las pérdidas que puedan producir eventos adversos, mediante el establecimiento de controles efectivos.

El sistema de gestión consiste en el establecimiento de una metodología para identificar, evaluar, monitorear y controlar el riesgo operativo, así como disponer de un registro y clasificación de las pérdidas relacionadas con eventos de riesgo operativo.

Además de contar con una metodología para cumplir con el ciclo del riesgo también se dispone de una estructura de personal con líneas claras de autoridad, responsabilidad e información y la necesidad de fomentar la cultura propositiva del riesgo operativo en toda la institución y con el personal nuevo que ingresa a la organización.

El Manual de Gestión del Riesgo Operativo y la Norma de Gestión del Riesgo Operativo constituyen el marco de actuación.

En vista que el riesgo operativo abarca a toda la organización, la estrategia para administrar este riesgo consiste en la vinculación de todas las áreas del banco en la gestión. En ese sentido, se han nombrado Coordinadores de Riesgo Operativo en las diferentes áreas, quienes se encargan de reportar a la Unidad de Riesgos la ocurrencia de todos los eventos de pérdida, así como de incidentes que se hayan presentado en sus áreas. Al mismo tiempo este personal es responsable de coordinar las actividades que contribuyan a la mitigación de los riesgos en su ámbito de acción laboral a través de planes de acción correctivos, una vez que se hayan evaluado los riesgos residuales.

Se fomenta la cultura de gestión del riesgo a través de las capacitaciones periódicas recibidas en riesgo operativo al personal existente y nuevo.

El personal responsable de cada proceso está ejecutando los planes de acción correctivos cuyo seguimiento se realiza por medio de indicadores de avance, presentados y discutidos en el Comité de Riesgos y los mismos son informados a la Junta Directiva.

El apoyo de la Junta Directiva y Alta Gerencia en el proceso de gestión se ve reflejado en la aprobación de los recursos humanos y materiales presupuestados y en la definición de objetivos dentro del plan estratégico institucional, siendo una de las perspectivas de dicho plan la gestión de riesgos.

Actividades de Gestión realizadas y su resultado

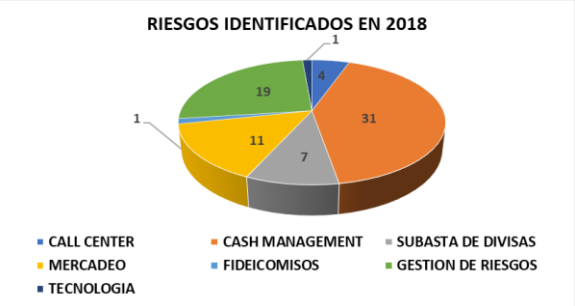
En el 2018 se modificó la política principalmente en lo relacionado al límite de tolerancia que se refiere a las pérdidas por eventos de riesgo operativo que el banco está dispuesto a asumir, el cual forma parte de la estrategia corporativa y que se dará participación a las áreas de control del banco en la evaluación de la efectividad de los controles.

En el 2018 el banco continuo con 28 procesos y cada uno cuenta con su matriz de riesgos operativos.

Respecto al riesgo legal los riesgos se identifican junto con los riesgos operativos. En 2018 se implementó el sistema de lectura y seguimiento de las nuevas normas emitidas por la Comisión Nacional de Bancos y Seguros y Banco Central de Honduras asignando las acciones a realizar para su cumplimiento al área correspondiente. La política de riesgo legal fue revisada sin modificaciones.

Riesgos Identificados en 2018

De acuerdo con la metodología establecida para la gestión del Riesgo Operativo, la cual consiste en identificar riesgos ya sea a través de los coordinadores de riesgo operativo o de hallazgos de auditoria interna y externa, durante el 2018 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.



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 acciones correctivas hasta lograr niveles más bajos.

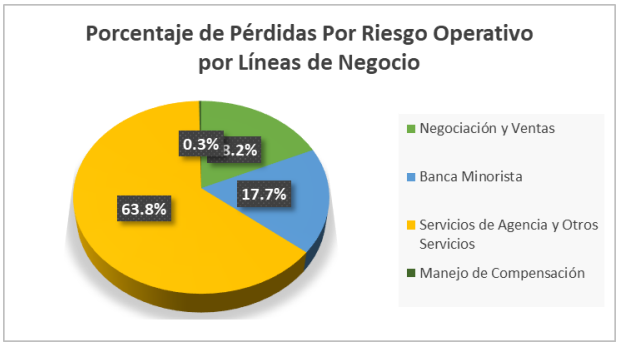
Nivel de Aceptación	Nivel de Riesgo
Aceptable: Se debe monitorear	Muy Bajo
	Bajo
No Aceptable: Se debe definir un Plan de Acción	Medio
	Alto
	Critico

Siguiendo la metodología y con base en el apetito del riesgo que Banco Ficensa ha establecido, para los riesgos identificados y que no sean aceptados de acuerdo con el nivel de tolerancia, se han determinado una serie de planes de acción correctivos buscando minimizar la probabilidad de la ocurrencia del riesgo y esperando que los resultados sean la creación de resiliencia organizacional, el fortalecimiento de la seguridad de la información, la protección de los colaboradores y clientes así como la conservación de la buena reputación del Banco.

Base de datos de eventos de riesgo

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

En el 2018 las pérdidas por riesgo operativo fueron el orden de L626,155.20 corresponden a las áreas de Finanzas y Tesorería y Banca de Personas, principalmente por eventos externos y penalizaciones.



Perfil del Riesgo Operativo

El perfil de riesgo de la institución se encuentra definido en el Manual de Políticas y Procedimientos de Riesgo Operativo y este indica que, para la definición del apetito del riesgo, la Unidad de Riesgos fijará un monto límite de tolerancia, que se refiere al monto de las pérdidas por eventos de riesgo operativo que el banco está dispuesto asumir, el cual es aprobado por la junta directiva y forma parte de la estrategia corporativa. Adicionalmente se ha determinado los parámetros de aceptabilidad de riesgos operativos, los cuales son los criterios que permiten determinar si un nivel de riesgo residual específico se ubica dentro de la categoría de nivel de riesgo aceptable o no.

Riesgo Tecnológico

Durante el 2018 se reportaron 14 eventos de riesgo correspondientes al proceso de Tecnología de Información y Comunicaciones, de los cuales se derivaron planes de acción correctivos orientados a establecer controles de calidad previo al lanzamiento de modificaciones y desarrollos en los sistemas de información, blindar los sistemas expuestos a fraude interno y externo, mantener la continuidad del negocio y reducir el riesgo de error humano al ejecutar actividades dentro del área de Tecnologías de Información. En el mes de octubre el banco logro poner en producción el nuevo Core Bancario, proceso que se llevó a cabo con el acompañamiento de consultores externos con buen suceso.

Continuidad del Negocio

En cuanto a la Gestión de Continuidad del Negocio, se logró la actualización de los documentos que son la base de la gestión, como ser, la Evaluación de Riesgos de Continuidad, el Análisis de Impacto en el Negocio y el Plan de Gestión de Crisis, permitiéndole a la institución establecer acciones preventivas y correctivas de acuerdo con la prioridad de los riesgos identificados y con el reconocimiento de los procesos más críticos del Banco. Y siendo el recurso humano una de las prioridades para la institución, se buscó fortalecer la cultura de seguridad, mediante la realización de ejercicios de evacuación y capacitación en temas de fenómenos naturales y recomendaciones a seguir en caso de presentarse alguno.

Gestión de la Seguridad de la Información

En materia de seguridad de la información las principales actividades realizadas durante el 2018 son las siguientes: control total de accesos de los principales sistemas en producción, optimización de mecanismos de seguridad en la infraestructura de transferencias nacionales e internacionales, definición de roles y responsabilidades para los diferentes puestos en el nuevo Core bancario recién implementado, cifrado de discos del total de equipos móviles de la institución, migración e implementación segura de las herramientas de office 365, certificación de la seguridad en la implementación de la nueva banca electrónica y la implementación de un nuevo Sistema de Gestión para Eventos de Seguridad de la Información.