



INFORME SOBRE LA GESTION DEL RIESGO OPERATIVO

Al 31 de diciembre de 2020

Elaborado por:
UNIDAD DE RIESGOS
31/12/2020

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 2020.

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.

La Junta Directiva 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 crítico 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 |
| | Crítico |

Actividades de Gestión realizadas y su resultado

En el 2020 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 ejecuto 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 realizó la revisión anual de las matrices de riesgo operativo según el cronograma establecido, se identificaron nuevos riesgos en los procesos realizados por las áreas y se establecieron controles para cada uno de ellos

Se continua 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 revisa y actualizada en el presente año

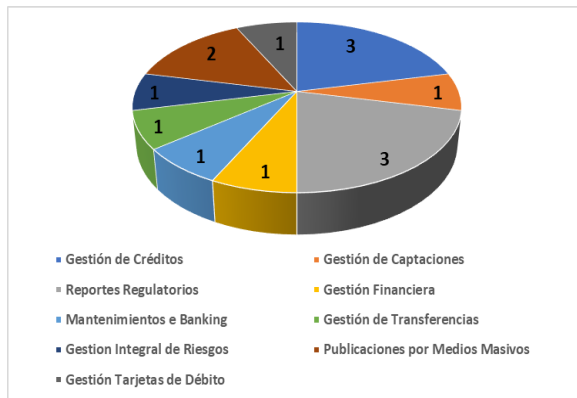
Para fortalecer la cultura de gestión se impartieron a nivel nacional 7 capacitaciones durante el año 2020.

Riesgos Identificados en 2020

En 2020 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.

De riesgos identificados 14 requirieron planes de acción.

Riesgos Identificados 2020 Con Planes de Acción



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 2020 el monto de las pérdidas por riesgo operativo ascendió a la suma de L.590,383.03, estos eventos se presentaron en los procesos de Tarjetas de Débito, Impuestos, Cuentas Inactivas y otros.

Riesgo Tecnológico

En el año en que la digitalización, el teletrabajo y la transformación digital fueron requeridos en el mundo de los negocios, Banco FICENSA ha demostrado su resiliencia ante los cambios drásticos del entorno, producto de la pandemia por COVID-19. Cada cambio trae consigo una serie de riesgos que se deben gestionar y optimizar de forma que estos no se interpongan ante los nuevos proyectos y necesidades del negocio. Entre los riesgos que el Banco identificó y logró tratar se encuentran los relacionados al teletrabajo como por ejemplo los accesos a información sensible desde fuera del banco y el uso del equipo corporativo para fines personales; se logró robustecer 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. También durante el año fueron adquiridos nuevos equipos de comunicación y red, eliminando los puntos de falla que puedan afectar la continuidad de los servicios.

Se identificaron 31 riesgos tecnológicos, de los cuales 15 presentan riesgos bajos y 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 |
|----------|------|-------|------|---------|
| 1 | 14 | 12 | 4 | 0 |

Continuidad del Negocio

El 2020 fue un año atípico debido al surgimiento de una pandemia y de dos tormentas tropicales devastadoras que afectaron a la economía hondureña.

Banco FICENSA activo el sistema de gestión de continuidad del negocio, mediante la implementación de la estrategia del teletrabajo, con excelentes resultados ya que las operaciones nunca se detuvieron y el servicio al cliente se mantuvo en los niveles predefinidos.

En atención a la pandemia Covid-19, se creó un Protocolo de Bioseguridad que permitió que tanto los colaboradores como los clientes se sintieran seguros dentro de las instalaciones, asimismo, se aplicaron las medidas establecidas por el Gobierno y la Secretaría de Salud.

A lo largo del 2020 se actualizó el Marco del Sistema de Gestión de Continuidad del Negocio SGCN en todos sus componentes: Política de Continuidad del Negocio, Plan de Continuidad del Negocio, Plan de Gestión de Crisis, Plan de Recuperación de Desastres, Análisis de Impacto en el Negocios, Plan de Respuesta a Emergencias y Evaluación de Riesgos de Continuidad del Negocio.

Seguridad de la Información

Banco Ficensa en materia de Ciberseguridad por medio del área de Seguridad de la Información desarrolló mecanismos de apoyo al negocio durante la pandemia por COVID-19, bajo la responsabilidad de la administración de plataformas de Office 365 en la nube, de manera preliminar días antes de comenzar la nueva metodología de teletrabajo, se configuraron y se realizaron pruebas piloto con un grupo de colaboradores que permitiera el uso de soluciones como Teams y Sharepoint para mejorar la experiencia del usuario final, con el fin de mantener sus operaciones desde su hogar, también fueron configurados los accesos VPN para conexión remota de los colaboradores desde las redes domésticas hacia la red institucional de manera segura. Se capacitó al personal sobre como establecer las medidas de ciberseguridad en una red residencial interconectada a la red institucional por medio del equipo asignado a cada colaborador en teletrabajo. Para mejorar la comunicación en línea, el área de Seguridad de la Información desarrolló el portal institucional Ficensa People, con el fin de mejorar la capacidad de tener información corporativa y así facilitar la comunicación entre el Banco y sus colaboradores, permitiendo así desarrollar la capacitación normativa sobre Seguridad de la Información y con esta ser pioneros en establecer el nuevo mecanismo de aprendizaje para colaboradores, haciendo uso de videos y exámenes en línea desde el portal Ficensa People y obteniendo con esto una reducción en costos y tiempo relacionados en

capacitaciones. Seguridad de la Información lideró el proyecto de confirmación de transferencias internacionales por medio del canal Swift, el cual era obligatorio para mantener el servicio y el cual se cumplió en tiempo. Durante la pandemia y la metodología de teletrabajo se lograron reducir los incidentes de seguridad en equipos, redes y los relacionados con colaboradores, donde Seguridad de la Información mantuvo los niveles de monitoreo constante y sobre todo verificando el correcto manejo de la información por parte de los colaboradores de Banco Ficensa.