INFORME SOBRE LA GESTIÓN DEL RIESGO OPERATIVO

Al 31 de diciembre de 2025

Elaborado por: UNIDAD DE RIESGOS
12/01/2026

Gestión del Riesgo Operativo
En el presente informe se da a conocer las actividades de la gestión del Riesgo Operativo ejecutadas en Banco FICENSA durante el año 2025.

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 2025 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 26 Macroprocesos de la institución cuentan con su matriz de riesgos operativos.

Se impartieron capacitaciones a los nuevos Coordinadores de Riesgo Operativo y al personal en temas relacionados con riesgo operativo y legal, se realizó el Primer Encuentro sobre Riesgo Operativo: Retos y Soluciones dirigido a la Alta Gerencia, Jefes y Supervisores de departamento con personal experto de la CNBS.

Banco FICENSA ha realizado inversiones importantes en la adquisición de herramientas de prevención de fraude de última generación y fortaleció la estructura para asegurar a los clientes transacciones confiables en el uso de nuestros productos.

Se realizo la contratación de una consultoría de profesionales expertos internacionales para brindar apoyo durante la implementación de la herramienta tecnológica adquirida, aportando criterio de experto en la definición de la estrategia funcional y optimizar el Modelo de Gestión de Fraude a partir de incorporar tecnología y mejores prácticas de mercado. Adicionalmente el experto impartió capacitaciones a la Junta Directiva y resto del personal en temas de prevención de fraude.

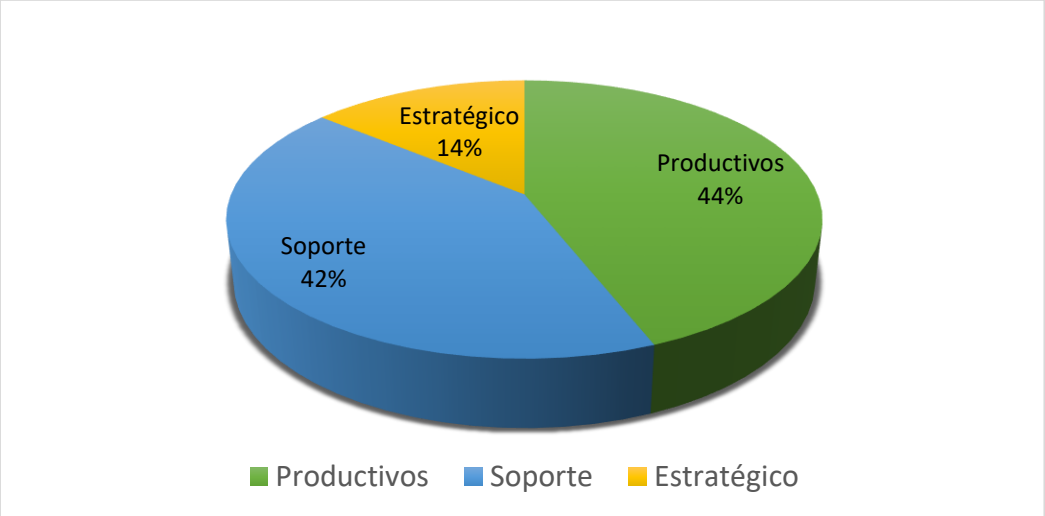
Los riesgos legales se identifican junto con los riesgos operativos.
La Política para la Gestión del Riesgo Operativo y Legal fue revisada y actualizada en el 2025.

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 2025

En 2025 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 2025



Se cuenta con 29 planes de acción vigentes, 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 Vigentes 2025

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.

Al 31 de diciembre 2025 el monto de las pérdidas por riesgo operativo ascendió a la suma de L11.1M.

Porcentaje de Pérdidas por Proceso 2025

Tipo de Proceso	Monto
Soporte	11.0M
Productivo	0.04M

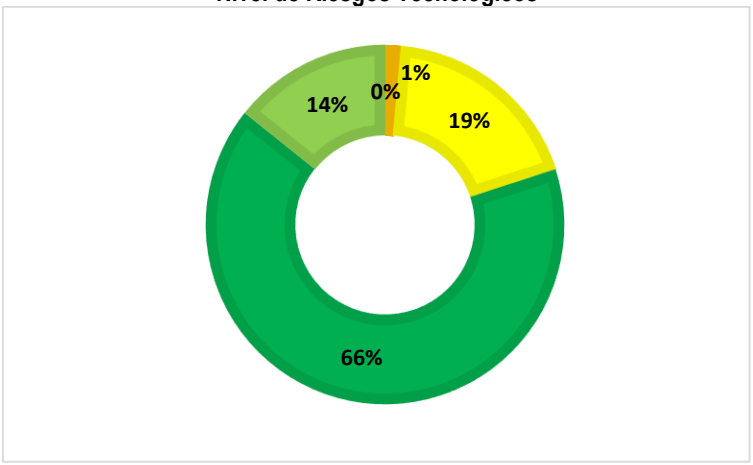
Análisis de Productos y Servicios:
En el 2025 se realizó el Análisis Integral de Riesgos a un (1) productos y/o servicio requerido por el área de Mercadeo con el acompañamiento del Depto. De Riesgo Operativo y Cumplimiento Regulatorio incluyendo Prevención de Fraude, Depto. De Riesgos Financieros, Seguridad de la Información, Analista de Riesgo Tecnológico y Asesor Legal.

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 se han tratado y robustecido los controles. A la vez se implementaron nuevos servicios adaptando a nuevas tecnologías, fortaleciendo y logrando la automatización de controles y monitoreo.
Lo anterior se realizó promoviendo un ambiente de cultura de riesgos mediante capacitaciones acerca de la gestión, responsabilidades y promoviendo la participación en la identificación temprana de los riesgos.

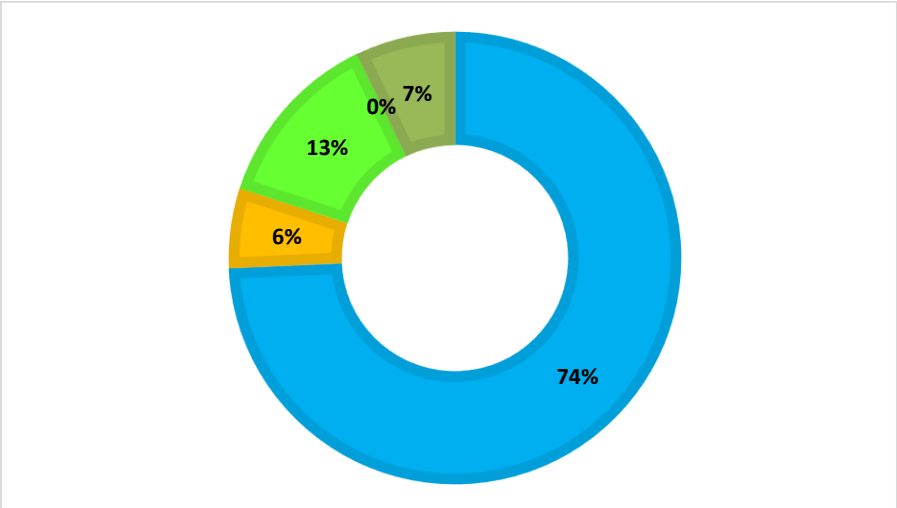
En cuanto al nivel de criticidad de los riesgos tecnológicos, el 80% son de riesgo muy bajo y bajo, 19% de riesgo medio y 1% de riesgo alto. De estos el 20% cuentan con planes de acción en proceso de implementación.

Nivel de Riesgos Tecnológicos



Muy Bajo	Bajo	Medio	Alto	Crítico
14%	66%	19%	1%	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 2025.



Estado de los Planes de acción

Completo	Parcialmente completo	Vigente	Vencido	No aplica
74%	6%	13%	0	7%

Sistema General de Continuidad del Negocio (SGCN)
En materia de Continuidad del Negocio no se han presentado eventos que hayan afectado de manera significativa la continuidad de las operaciones.

Respecto al Plan de Recuperación de Desastres, se cumplió con el 100% del plan de pruebas individuales y prueba total simulando caídas en los servidores y enlaces de comunicación, lo que permitió validar la efectividad de los planes, identificar brechas y fortalecer los mecanismos de respuesta ante incidentes. Las lecciones aprendidas fueron incorporadas contribuyendo a una mejora continua. Los resultados de la prueba total fueron satisfactorios en un 80%, 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.

Los planes que son parte de la Gestión de Continuidad del Negocio fueron actualizados durante 2025 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. Se completo la concientización a los colaboradores confirmando su participación en materia de continuidad del negocio, promoviendo mayor participación, responsabilidades y una cultura orientada a la prevención y preparación ante una situación de crisis.

Gestión de la Seguridad de la Información y Ciberseguridad
La gestión del riesgo operativo en Seguridad de la Información en Banco FICENSA se concibe como un proceso integral, continuo y evolutivo, orientado a identificar, evaluar, tratar y monitorear los riesgos cibernéticos que puedan afectar la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos críticos de la Institución.
Durante el 2025, dicho enfoque se ha fortalecido significativamente mediante la incorporación de nuevas capacidades tecnológicas y operativas, que complementan y potencian los controles ya existentes, consolidando un modelo de gestión del riesgo más preventivo, detectivo y reactivo.

I. Prevención de Intrusiones y Protección del Perímetro Tecnológico

Se mantiene la aplicación de medidas proactivas orientadas a la prevención de accesos no autorizados y ataques cibernéticos, mediante el uso de firewalls, sistemas de prevención de intrusiones (IPS), sistemas de Firewalls de Aplicaciones (WAF) y configuraciones avanzadas de seguridad.
Estas medidas se han reforzado con el proceso de implementación de una solución XDR (Extended Detection and Response) la mejor posicionada en el mercado para este tipo de tecnología, la cual permitirá ampliar la visibilidad y correlación de eventos de seguridad a través de endpoints, servidores, red y cargas de trabajo, reduciendo el tiempo de detección y contención de amenazas avanzadas.

II. Monitoreo Continuo de Eventos e Identificación de Amenazas

La Institución cuenta con mecanismos de monitoreo continuo para la detección temprana de anomalías y eventos de seguridad. Durante este período, se dio un paso relevante con la salida a producción de un Centro de Operaciones de Seguridad (SOC), operando con monitoreo en tiempo real 24/7, lo que fortalece la capacidad de vigilancia permanente sobre los activos críticos.
Adicionalmente, se implementó el monitoreo en tiempo real de las bases de datos de producción, permitiendo identificar actividades inusuales, accesos indebidos o comportamientos anómalos que puedan representar riesgos operativos o de seguridad de la información.

III. Gestión de Incidentes y Respuesta Operativa

Como parte de la madurez del modelo de seguridad, el SOC en producción incorpora capacidades formales de Incident Response, con procedimientos definidos, roles asignados y tiempos de respuesta establecidos.
Esto permite una respuesta oportuna y coordinada ante incidentes de seguridad, minimizando impactos operativos, financieros y reputacionales para la Institución.

IV. Administración de Soluciones de Seguridad en Equipos Cliente y Servidores

Se mantiene la administración centralizada de soluciones de seguridad para estaciones de trabajo y servidores, incluyendo antivirus, antimalware y otros mecanismos de protección.
Estas soluciones son actualizadas de forma constante, asegurando que las definiciones de amenazas y los componentes de seguridad se mantengan alineados con el panorama de riesgos cibernéticos vigente y con las capacidades que, progresivamente, serán integradas al ecosistema XDR.

V. Gestión de Actualizaciones, Vulnerabilidades y Brechas de Seguridad

La gestión de parches de seguridad y actualizaciones de sistemas operativos continúa siendo un componente clave para la reducción del riesgo operativo.
Asimismo, se realizan evaluaciones periódicas de vulnerabilidades, cuyos resultados alimentan los planes de mitigación y fortalecimiento de controles técnicos y administrativos en el entorno tecnológico.

VI. Cumplimiento Normativo y Alineación con Estándares Internacionales

La gestión del riesgo operativo en Seguridad de la Información se mantiene alineada con las disposiciones del regulador y con estándares internacionales reconocidos, tales como ISO/IEC 27001, entre otros.
Para ello, se dispone de políticas, procedimientos y controles que respaldan el cumplimiento regulatorio y promueven una cultura de seguridad transversal en la Institución.

VII. Conclusión

En conclusión, durante el último semestre de 2025, Banco FICENSA ha consolidado una gestión efectiva y progresivamente madura del riesgo cibernético, fortalecida por la incorporación de nuevas capacidades estratégicas como el SOC 24/7, el monitoreo en tiempo real de bases de datos productivas y la implementación en curso de una solución XDR.
Este enfoque integral contribuye de manera directa a la reducción del riesgo operativo, al fortalecimiento de la resiliencia tecnológica y a la protección de la información sensible, asegurando la continuidad de los servicios y la confianza de los clientes, reguladores y demás partes interesadas.