

OBJETIVO

El propósito de este informe es presentar a los grupos de interés los resultados de la gestión de riesgos de Banco Ficensa al 31 de diciembre de 2025.

A continuación, se describe la forma en que el Banco gestiona los riesgos desde el punto de vista de la Gobernanza:

GESTIÓN DE RIESGOS

La Gestión de Riesgos garantiza en primera instancia el cuidado de los depósitos, la inyección de los recursos económicos requeridos por a las empresas y personas en calidad de préstamos, actividades que requieren un adecuado nivel de seguridad y por último el alcanzar una rentabilidad razonable para los accionistas.

GOBIERNO DE RIESGOS

La Junta Directiva del Banco es el órgano responsable de asegurar la implementación de la gestión de riesgos a través de una adecuada estructura estratégica y operativa, cultura de riesgos, marco de políticas y una declaración del apetito por el riesgo que este dentro de las capacidades y límites de tolerancia considerando el entorno competitivo y regulatorio y los objetivos estratégicos de Banco.

La Junta Directiva aprueba las políticas y metodologías para la gestión de riesgos, así como sus actualizaciones, asegurando que las mismas sean aplicadas e incluyan el análisis de escenarios y pruebas de estrés y planes de contingencia.

La Junta Directiva aprueba la constitución del Comité de Riesgos que es su enlace para que fluya la información a dicho órgano a través del Presidente de dicho comité, quien es el encargado de elevar todos los aspectos relacionados con la gestión de riesgos que requieren aprobación o conocimiento de la Junta Directiva.

La Unidad de Riesgos de manera independiente del resto de las áreas de la organización es la responsable de la conducción del proceso de identificación, medición, valoración, monitoreo e información de las exposiciones de riesgo asumidos en todos los procesos del Banco, actividad que se ejecuta en base a las normas de la Comisión Nacional de Bancos y Seguros y estándares aceptables. Esta área también es responsable del diseño y actualización de las metodologías, políticas y procesos de gestión de riesgos, como también de la realización de los diferentes escenarios de estrés y pruebas de simulación para identificar que tan resiliente es la institución ante situaciones adversas.

ACTIVIDADES Y LOGROS OBTENIDOS AL 31 DE DICIEMBRE 2025 EN MATERIA DE GESTIÓN DE RIESGOS**Riesgo de Crédito e Inversión**

El Riesgo de Crédito e Inversión es la pérdida potencial por el incumplimiento de las obligaciones que tienen las contrapartes en operaciones de crédito e inversiones.

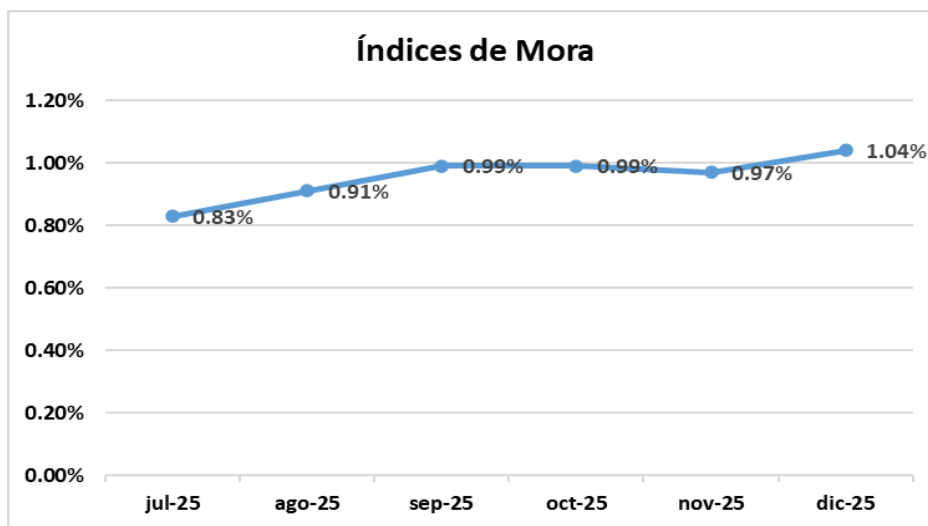
Monitoreo del Riesgo de Crédito

El monitoreo del riesgo de crédito se realiza por medio de un sistema de alertas que mide el grado de acercamiento de los indicadores a los límites aprobados por la Junta Directiva, de manera que se puedan tomar decisiones que contribuyan a mitigar los riesgos de manera anticipada y evitar desviaciones a los límites.

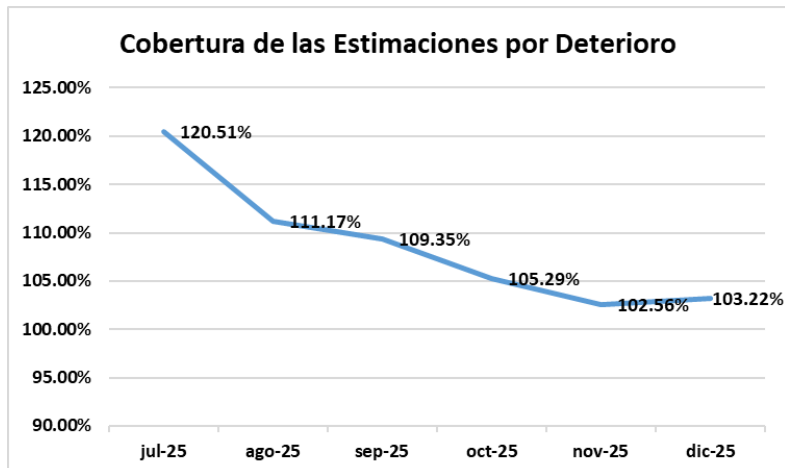
Resultados obtenidos

Para el segundo semestre del período 2025, Banco FICENSA continuó mostrando indicadores sólidos en la administración de riesgo de crédito, monitoreando los indicadores de mora, partes relacionadas, exposición en moneda extranjera, exposición de capital y reservas, índice de cobertura de reserva y mora, actividad económica, los cuales permanecieron de acuerdo con los límites establecidos y apetito por el riesgo, sin reportar excesos o desviaciones en los límites máximos o mínimos.

Los niveles de riesgo de crédito se mantienen en el rango bajo durante el periodo analizado, en general, la cartera conserva una adecuada calidad crediticia, sin señales de deterioro significativo.



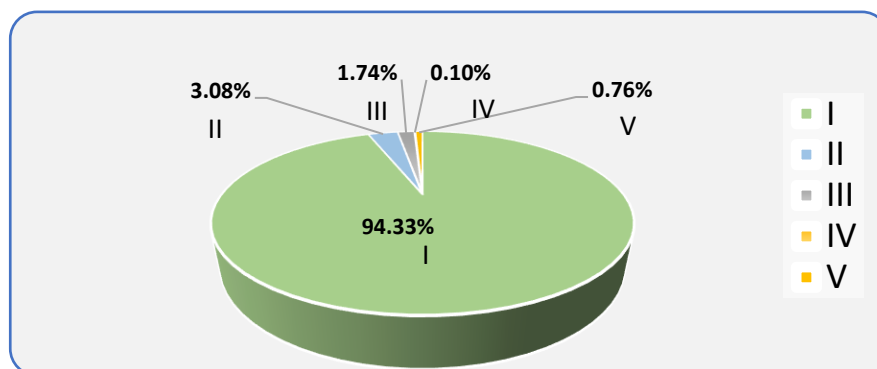
El Banco mantiene estimaciones suficientes para créditos dudosos; no obstante, de julio a diciembre de 2025 se observa una disminución gradual en la cobertura.



La calidad de la cartera crediticia se ha mantenido en condiciones óptimas reflejado en la composición de la cartera de créditos por categoría de riesgos, manteniéndose en condiciones saludables. A continuación, se muestra su distribución por categoría:

Composición de la Cartera Clasificada

Al 31 de diciembre 2025



Al 31 de diciembre 2025 el 97.41 % de los créditos están en categorías I y II, lo que demuestra una sólida calidad de cartera y un bajo nivel de riesgo crediticio.

Inversiones

El Banco cuenta con políticas y procedimientos para la gestión del Riesgo de las Inversiones en Valores y en Acciones.

Las inversiones en valores se miden a costo amortizado y a valor razonable dependiendo del tipo.

Las inversiones en acciones se realizan bajo una metodología muy similar a la aplicada a los créditos corporativos.

Todas las inversiones se encuentran dentro de los niveles de riesgo aceptables.

GESTIÓN DEL RIESGO DE LIQUIDEZ

Riesgo de Liquidez es la pérdida potencial que se podría tener por la imposibilidad de renovar pasivos o de contratar otros en condiciones normales para el Banco; por la venta anticipada o forzosa de activos a descuentos inusuales para hacer frente a sus obligaciones, o bien, por el hecho de que una posición no pueda ser oportunamente enajenada, adquirida o cubierta mediante el establecimiento de una posición contraria equivalente.

Se cuenta con una herramienta para la gestión del Riesgo de Liquidez.

El Comité de Activos y Pasivos tiene como función principal la de conocer y tomar decisiones relacionadas con la gestión y optimización del balance, la liquidez estructural e individual y los resultados de la rentabilidad.

El Comité de Riesgos es el responsable de recomendar los límites y dar seguimiento a los indicadores de alerta temprana buscando que se tomen decisiones en caso de sobrepasarse dichos límites o tomar acciones en caso de que se activen las alertas.

El monitoreo de la liquidez diariamente se realiza por el área de Tesorería responsable de administrar la liquidez, así como sus fuentes de fondeo, el área de Riesgo Financiero es la encargada de efectuar la medición y análisis de los indicadores de límites establecidos.

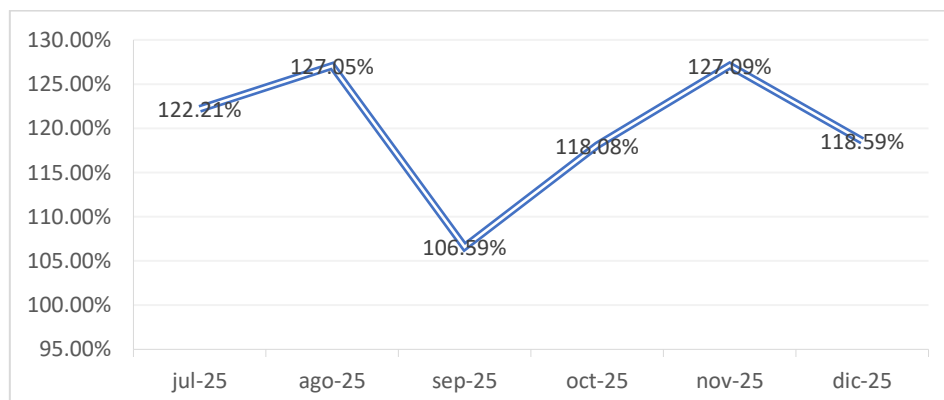
Los indicadores que se monitorean mensualmente se encuentran bajo los límites fijados, apegándose al apetito por el riesgo.

RCL (Ratio de Cobertura de Liquidez)

El Banco posee un nivel de activos líquidos de alta calidad no comprometidos convertibles fácilmente en efectivo y que sirven para cubrir las necesidades de liquidez, en un horizonte de treinta (30) días bajo un escenario de tensión de liquidez.

El indicador RCL diario registrado a lo largo del segundo semestre de 2025 fue superior al límite de 100% establecido para ambas monedas (nacional y extranjera) como también el combinado. Este indicador es monitoreado diariamente por parte de la Unidad de Gestión de Riesgos.

Ratio de Cobertura de Liquidez Combinado



Indicadores de Alerta Temprana

Mensualmente se dio seguimiento a las alertas tempranas relacionadas con concentraciones de activos y pasivos, cancelaciones anticipadas y no renovaciones de depósitos a plazo fijo, la volatilidad de los depósitos, la calidad del crédito, el margen financiero y su suficiencia y la posición de encaje.

Todos estos indicadores de alerta han estado dentro de los límites establecidos.

GESTIÓN DEL RIESGO DE MERCADO

El Riesgo de Mercado es la posibilidad de que el Banco tenga pérdidas derivadas del incremento no esperado en el monto de las obligaciones con acreedores externos o pérdidas en el valor de los activos, a causa de variaciones en los parámetros que sirven de referencia o afecten el precio de los instrumentos financieros.

Riesgo de Tasas de Interés

Posibilidad de tener pérdidas en el estado de resultados o reducción del valor económico del Banco, porque no exista correspondencia en los períodos de ajuste de las tasas activas y las tasas pasivas, dados los movimientos de estas en el mercado.

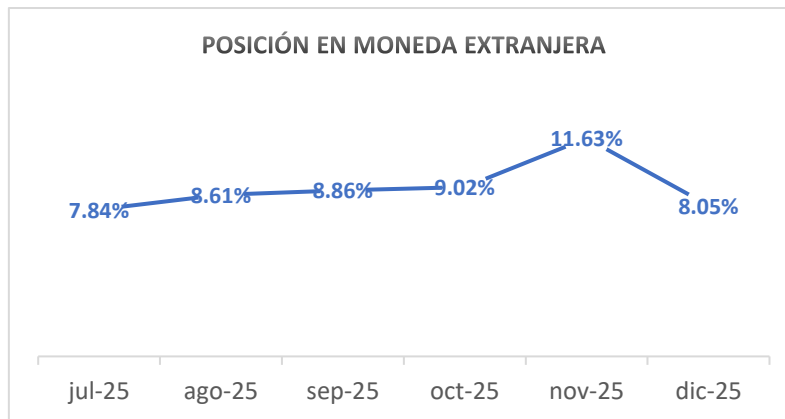
El Banco utiliza la metodología para la gestión del riesgo de tasas de interés denominada Análisis de Brechas de reprecio a Corto y Largo Plazo, con el fin de determinar los impactos de los movimientos en las tasas de interés en el Margen Financiero del Banco y en su Valor Patrimonial.

Los resultados de aplicar esta metodología reflejaron que, en caso de reducir las tasas de interés, el impacto en el margen financiero y en el valor patrimonial se mantienen dentro de los límites aprobados por la Junta Directiva.

Riesgo de Tipo de Cambio

Es la posibilidad de ocurrencia de pérdidas derivadas de variaciones en los tipos de cambio correspondientes a instrumentos en los cuales el Banco mantiene una posición larga dentro y fuera del balance. El riesgo estructural de tipo de cambio se refiere a la potencial pérdida que asume el Banco ante variaciones en la cotización del lempira frente al dólar sabiendo que existe una brecha entre los vencimientos de sus operaciones activas y pasivas en dicha moneda.

El seguimiento del riesgo de tipo de cambio se lleva a cabo a través de la Posición o Calce en Moneda Extranjera. Históricamente el Banco ha mantenido una posición larga, es decir, que los activos en moneda extranjera son mayores que los pasivos en dicha moneda, siendo el límite de esa brecha hasta el 20% del capital y reservas. Las posiciones se muestran en el siguiente gráfico:



Riesgo de Precios

Posibilidad de tener pérdidas por disminuciones en el precio en el mercado de acciones y otros instrumentos de renta variable que posea el Banco.

Debido a que en el mercado hondureño no se dispone de un sistema de cotización para Inversiones en títulos de deuda pública y privada, la valorización de estas inversiones se realiza aplicando los métodos de costo amortizado para los instrumentos de renta fija, costo histórico para las acciones y para el resto de las inversiones se utiliza el método de valor razonable.

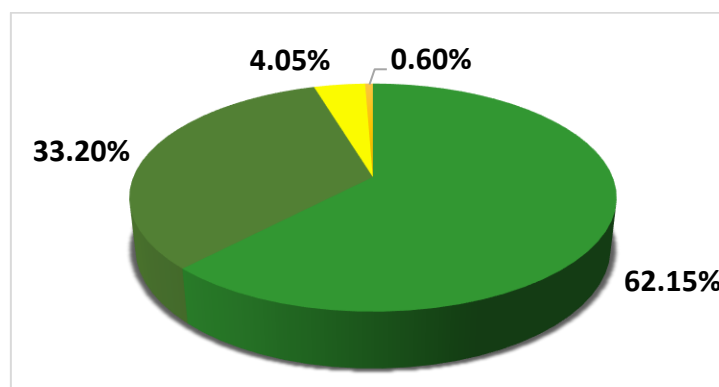
Índice de Adecuación de Capital (IAC)

Banco FICENSA mantiene un nivel de adecuación de capital por arriba de lo requerido, administrando y monitoreando este indicador mensualmente para asegurar el cumplimiento regulatorio y del apetito por el riesgo.

GESTIÓN DEL RIESGO OPERATIVO

El Riesgo Operativo, es el riesgo de pérdidas que resultan de aplicar procesos internos fallidos o inadecuados, errores de personas, fallas en sistemas y ocurrencia de eventos externos. La definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional.

Criticidad de los Riesgos Operativos



Como estrategia de gestión, se fomenta la cultura del riesgo en toda la organización para lograr que todos los empleados se conviertan en gestores de 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 se encargan de informar a la Unidad de Riesgos acerca de los eventos que afectan y que pudieran afectar a la institución, para que sean evaluados en base a una metodología que abarca criterios de impacto y probabilidad dando como resultado niveles de criticidad de riesgo inherente, para después proceder al análisis de la efectividad de los controles existentes hasta llegar a determinar el riesgo residual.

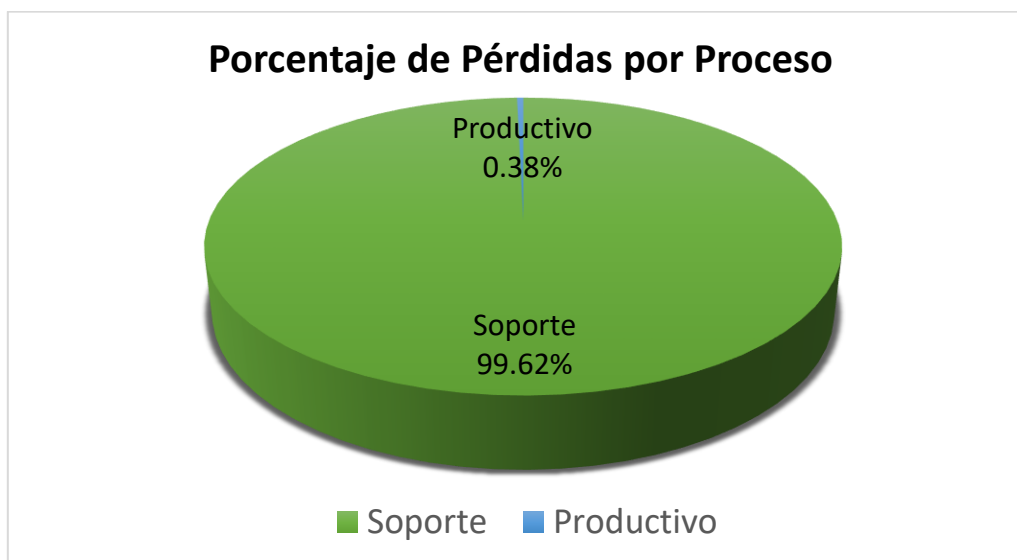
Para los riesgos residuales cuya criticidad es considerada de nivel medio, alto y crítico, se definen planes de acción a las diferentes áreas vinculadas al riesgo. A estos planes se les da seguimiento hasta su culminación logrando reducir la criticidad a niveles aceptables. El área de Riesgos procede a evaluar los riesgos inherentes y residuales bajo el criterio del Subcomité de Riesgo Operativo.

El Comité de Riesgos es informado con una frecuencia mensual y en este órgano se toman decisiones respecto al tratamiento de los riesgos.

La Junta Directiva es informada mensualmente acerca del estado de los riesgos operativos.

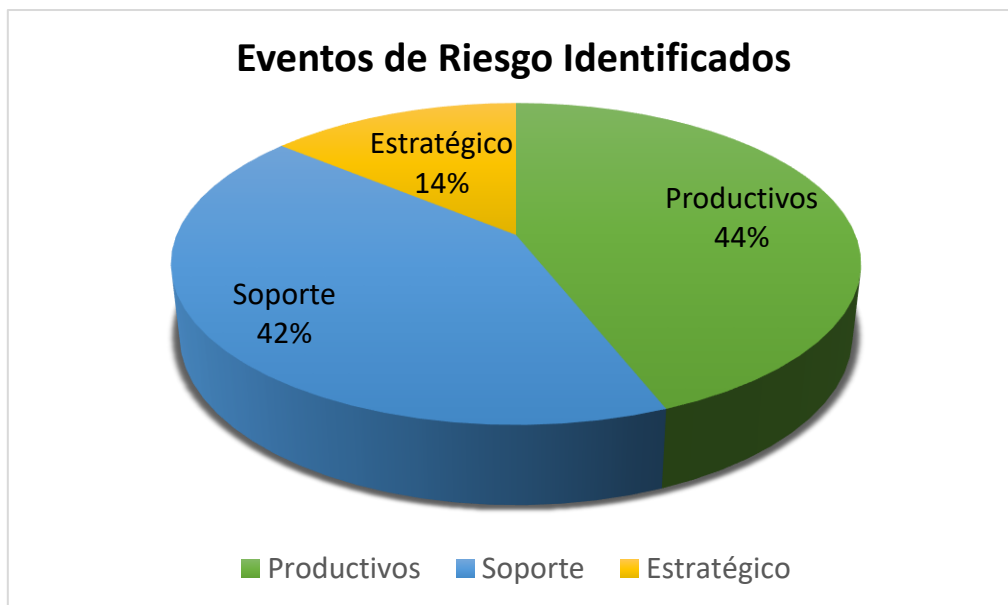
La Junta Directiva ha aprobado el apetito de riesgos por pérdida máxima acumulada que el Banco está dispuesto a asumir por riesgos operativos.

El monto de las pérdidas por riesgo operativo al 31 de diciembre 2025 ascendió a la suma de L.11.1M sobrepasando el monto límite de tolerancia fijado por Banco FICENSA.



Entre las actividades más relevantes realizadas en la gestión del riesgo operativo están:

- La revisión anual de las matrices de riesgo operativo según el cronograma establecido.
- Se identificaron y evaluaron nuevos riesgos en los procesos realizados por las áreas, se establecieron controles para cada uno de ellos y se dio seguimiento a los planes de acción establecidos para mitigar, trasladar, eliminar o aceptar los riesgos identificados.



A diciembre de 2025 se impartieron capacitaciones a los nuevos Coordinadores de Riesgo Operativo y al personal nuevo 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 para asegurar a los clientes transacciones confiables en el uso de nuestros productos.

Se realizó 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.

GESTIÓN DEL RIESGO LEGAL

Aunque el Riesgo Legal forma parte del Riesgo Operativo, el Banco cuenta con la política propia para la gestión de este riesgo y la metodología adoptada establece los lineamientos a seguir para gestionar los riesgos de documentación, regulatorios o normativos y de incapacidad de cumplimiento de las contrapartes.

Los riesgos legales se identifican y valoran al mismo tiempo con los riesgos operativos y bajo la misma metodología.

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.

GESTION DEL 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.

La metodología de Gestión del Riesgo Tecnológico es similar a la del riesgo operativo, pero con criterios de impacto y criticidad muy particulares dado el carácter técnico de este riesgo.

La metodología contempla el cálculo de los riesgos inherentes y residuales y se definen los planes de acción respectivos. Las decisiones de inversión y el seguimiento de los proyectos de tecnología se realizan en el seno del Comité de Tecnología y Seguridad de la Información. El Comité de Riesgos y la Junta Directiva son mensualmente informados acerca de la gestión de este riesgo.

Se incorpora la gestión de riesgos de la tercerización significativa de procesamiento de datos y los proveedores que la brindan.

Como parte de la estrategia de Riesgo tecnológico se realizó el fortalecimiento de la cultura de riesgo en las áreas de tecnología y seguridad de la información; incorporando capacitaciones enfocadas a las responsabilidades y promoviendo la participación activa en la identificación temprana de los riesgos.

Criticidad de los Riesgos Tecnológicos

Los Riesgos Tecnológicos al segundo semestre de 2025 son en total 70 y de estos el 80% son muy bajos y bajos; el resto son medios y altos.

Muy Bajo	Bajo	Medio	Alto	Crítico
14%	66%	19%	1	0

Los riesgos medios y el riesgo alto cuentan con planes de acción remediales.

GESTION DE LA CONTINUIDAD DEL NEGOCIO

El sistema de Continuidad del Negocio es el conjunto de actividades realizadas para asegurar que todos los procesos críticos del negocio estarán disponibles para los clientes, proveedores, y otras entidades que deben acceder a ellos, en caso de un evento crítico de interrupción. Para ello se dispone de los planes de pruebas a realizar.

A diciembre 2025 no se ha registrado ningún evento de riesgo significativo que afecte la continuidad del negocio.

Actividades realizadas:

Se actualizó el Marco de Gestión de Continuidad del Negocio y se concientizó impartieron capacitaciones a la Junta Directiva, a los equipos de gestión de crisis, al equipo de respuesta a emergencia y a todos los colaboradores en materia de

Continuidad del Negocio promoviendo mayor participación, responsabilidades y una cultura orientada a la prevención y preparación ante cualquier situación de crisis.

Plan de Recuperación de Desastres

A diciembre 2025 la Gestión de Continuidad del Negocio fue parte del fortalecimiento de la resiliencia operativa del Banco. Se ejecutaron pruebas y ejercicios 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.

GESTION DE LA SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

1) Consolidación del Liderazgo en el CSIRT Financiero AHIBA

Banco Ficensa mantuvo su posicionamiento como referente nacional en ciberseguridad, reafirmando los resultados obtenidos ante el CSIRT Financiero de la Asociación Hondureña de Instituciones Bancarias (AHIBA), gracias a la continuidad y fortalecimiento de sus controles de mitigación, prevención y respuesta ante riesgos cibernéticos.

2) Sostenimiento de una Calificación Sobresaliente en Ciberseguridad

Se preservó un alto nivel de desempeño en el score de ciberseguridad evaluado mediante la plataforma Security Scorecard, evidenciando la efectividad de los controles técnicos, operativos y de gobierno implementados, así como la consistencia en la gestión del riesgo tecnológico.

3) Fortalecimiento de la Protección de Canales Digitales

La solución de Firewall de Aplicación Web (WAF) implementada en el semestre anterior continuó operando de forma efectiva, reforzando la protección de los servicios web y móviles del banco frente a ataques dirigidos, vulnerabilidades de aplicaciones y amenazas a los canales digitales.

4) Salida a Producción del Centro de Operaciones de Seguridad (SOC)

Durante el segundo semestre de 2025 se concretó la salida a producción del Centro de Operaciones de Seguridad (SOC), estableciendo capacidades de monitoreo continuo 24/7, correlación de eventos y supervisión centralizada de la infraestructura tecnológica.

Este hito representa un avance significativo en la capacidad institucional para detectar, analizar y gestionar eventos de seguridad de forma oportuna y estructurada.

5) Implementación de Capacidades Formales de Incident Response

Como parte del SOC en producción, se integraron capacidades formales de respuesta a incidentes, con procedimientos definidos, roles y responsabilidades claras, y flujos de escalamiento establecidos.

Esto fortalece la resiliencia operativa del banco y reduce de forma significativa el impacto potencial de incidentes de ciberseguridad sobre la operación, los servicios críticos y la reputación institucional.

6) Monitoreo en Tiempo Real de Bases de Datos de Producción

Se implementó el monitoreo en tiempo real de bases de datos en ambiente productivo, ampliando la visibilidad sobre accesos, actividades y comportamientos anómalos en activos críticos de información, y reduciendo el riesgo de incidentes asociados a uso indebido, errores operativos o amenazas internas y externas.

7) Avance en la Estrategia de Defensa Proactiva mediante XDR

Durante este período se inició el proceso de implementación de una solución de Extended Detection and Response (XDR), orientada a integrar y correlacionar eventos provenientes de endpoints, servidores, red y otros componentes críticos.

Esta iniciativa permitirá fortalecer las capacidades de detección temprana, análisis avanzado y respuesta proactiva ante amenazas complejas y persistentes, complementando las funciones del SOC.

8) Evolución del Sistema de Gestión de Seguridad de la Información (SGSI)

Se mantuvo el proceso de actualización del SGSI para su alineación con la norma ISO/IEC 27001:2022, fortaleciendo el marco de gobierno, gestión de riesgos y controles, como paso previo a un eventual proceso formal de certificación.

9) Operación Estable y Sin Incidentes Relevantes

Durante el segundo semestre de 2025, no se registraron incidentes de Seguridad de la Información o Ciberseguridad que generaran impactos negativos en la operación, los servicios críticos, la situación financiera o la imagen institucional del banco.

10) Evolución e implementación de la Malla de Ciberseguridad

Durante el segundo semestre de 2025 se dio inicio a la implementación progresiva de una malla de ciberseguridad, basada en la arquitectura Security Fabric de una marca reconocida mundialmente en infraestructura de telecomunicaciones y ciberseguridad, orientada a integrar de forma coherente y orquestada los distintos controles de seguridad de la Institución.

Esta malla permite mejorar la visibilidad transversal, la correlación de eventos y la automatización de respuestas ante amenazas, fortaleciendo la defensa en profundidad y reduciendo el riesgo operativo asociado a ataques avanzados y movimientos laterales dentro de la red.

Los avances alcanzados durante el segundo semestre de 2025 reflejan la madurez progresiva del modelo de gestión integral del riesgo tecnológico y cibernético de Banco Ficensa, sustentado en la consolidación del SOC 24/7, la incorporación de capacidades de Incident Response, el monitoreo en tiempo real de activos críticos y el avance en la estrategia XDR.

Este enfoque integral fortalece la resiliencia operativa, reduce el riesgo residual y reafirma el compromiso institucional con la protección de la información, la continuidad del negocio y la confianza de clientes, reguladores y partes interesadas.

GESTION DEL RIESGO ESTRATEGICO

El Riesgo Estratégico es la probabilidad de pérdida como resultado de la imposibilidad de implementar apropiadamente los planes de negocio, las estrategias, las decisiones de mercado, la asignación de recursos y su incapacidad para adaptarse a los cambios en el entorno de los negocios. Asimismo, emerge de la pérdida de participación en el mercado y/o disminuciones en los ingresos que pueden afectar la situación financiera del Banco.

En el segundo semestre se dio seguimiento a los riesgos estratégicos identificados mediante la Metodología de identificación realizando una matriz de contraste entre cada componente del FODA.

En las actividades de control del riesgo estratégico participan todas las gerencias de banco cada una desde su ámbito de acción.

GESTION DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO (LAFT)

Este riesgo es la posibilidad de pérdida o daño que puede sufrir un banco por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.

Para la gestión de este riesgo se ha cumplido con el 100% de las revisiones y acciones de prevención contenidas en el Plan de Trabajo Anual, dentro de las cuales está el mantenimiento de una cultura institucional que se logra mediante la capacitación constante a todo el personal; se atendió el 100% de las alertas generadas por el monitoreo de las transacciones de los clientes y se documentaron cuando fue necesario; y, también se actualizó el Programa de Cumplimiento y procesos operativos de acuerdo a la realidad del mercado, pero sin desatender el trato personalizado y ágil para nuestros clientes.

En el análisis institucional de riesgo que se elabora de forma periódica se obtuvo resultados satisfactorios y dentro del apetito de riesgo definido en la Políticas Internas.

El Comité de Cumplimiento está activo y ha cumplido con todas las reuniones programadas para este año, y a su vez este Comité ha reportado los resultados a la Junta Directiva.

Por otro lado, para evitar el riesgo de contagio se emprenden acciones de debida diligencia con los proveedores y alianzas, así como de otros sujetos obligados, ya sea por su relación como acreedores financieros o clientes del banco.

Con el ente regulador se ha cumplido en tiempo y forma con la entrega de reportes regulatorios y requerimientos de información.

La gestión de prevención del riesgo LAFT fue evaluada por la CNBS, KPMG y los auditores internos y no se encontraron hallazgos por parte de ellos.

GESTION DEL RIESGO AMBIENTAL Y SOCIAL

Durante el período 2025 se dio seguimiento a la integración del riesgo ambiental y social dentro de los procesos de crédito y gestión de riesgos, en cumplimiento de las políticas internas, el marco regulatorio y los estándares internacionales aplicables.

La gestión se ejecutó en base a:

- De acuerdo con la Norma de Riesgo Ambiental y Social CNBS N°028/2020.
- Política Ambiental y Social institucional.
- Metodología de Evaluación de Riesgo Ambiental y Social (RAS) para clientes y actividades económicas.
- Clasificación de riesgo basada en los factores: impacto potencial, sensibilidad del entorno, gestión del cliente y cumplimiento normativo.
- Listas de exclusión y criterios sectoriales.
- Procedimientos de debida diligencia para casos de alto riesgo.
- Capacitaciones impartidas al personal de negocios y riesgos.

Clasificación de la Cartera Empresarial por Categoría de Riesgo Ambiental y Social al 31 de diciembre 2025:

SECTOR ECONÓMICO	CATEGORÍA AS	% RIESGO AS
Generación de Energía (Térmica y Renovable)	Alto	9.83%
Producción Farmacéutica y Biotecnológica	Alto	
Producción Química -Otros	Alto	
Productos de Madera	Alto	
Producción de compuestos Inorgánicos	Alto	
Obras de Ingeniería Civil a Mediana y Baja Escala	Medio	20.41%
Otros Actividades Agrícolas	Medio	
Papel, Cartón y Derivados	Medio	
Procesamiento de Aceites Vegetal/Animal	Medio	
Procesamiento de Alimentos y Bebidas	Medio	
Procesamiento de Carne	Medio	
Producción Anual de Cosechas	Medio	
Textiles	Medio	
Actividades de Comercio	Bajo	69.76%
Otras actividades a baja escala	Bajo	
Servicios Financieros	Bajo	

Asuntos e impactos relevantes sobre riesgos Ambientales y Social

Al 31 de diciembre 2025 no se han presentado asuntos relevantes sobre riesgos ambientales y sociales con relación a la cartera de clientes Empresariales.

Resultados de las quejas atendidas por sus clientes, presentadas por las partes interesadas o afectadas de un proyecto de inversión

No se presentaron quejas de clientes relacionadas a riesgos ambientales y sociales durante el periodo 2025.

Autoevaluación del Sistema de Administración de Riesgo Ambiental y Social (ARAS)

La autoevaluación del Sistema de Administración de Riesgo Ambiental y Social (SARAS) permitió identificar fortalezas clave, como el compromiso del Directorio y la Alta Dirección, el apetito institucional por robustecer la gestión RAS sin embargo, también se evidenciaron áreas de mejora, con avances claros en la implementación del SARAS, impulsando la mejora continua para fortalecer los procesos, la documentación y las capacidades técnicas que aseguren un manejo integral y efectivo de estos riesgos.