Guía práctica para la implementación de la norma ISO 31000 en startups Fintech en Colombia

Luisa Fernanda Cano Salgado
Fabián Andrés Ortiz Medina

Universitaria Agustiniana - Uniagustiniana
Facultad de Ingeniería
Programa de Ingeniería Industrial
Bogotá D.C.
2025

Índice de Contenido

Introducción 4
Objetivo de la Guía 4
Alcance 5
Marco Normativo 5
Fundamentos de ISO 31000 5
Orientaciones Prácticas 7
Desarrollo de la Metodología Adaptada 8
Fases de la Metodología 8
Instrucciones de uso 8
Información General de la Empresa 9
Aplicación de la metodología 10
Paso 1: Diagnóstico Inicial y Análisis Contextual 10
Paso 2: Identificación y Evaluación de Riesgos 16

Paso 3: Diseño e Implementación de Controles 20
Paso 4: Seguimiento, Monitoreo y Comunicación 24
Paso 5: Mejora Continua 28
Recomendaciones Finales 31
Pasos adicionales 32
Conclusiones 33
Referencias 34
Anexo 35

Introducción

El ecosistema Fintech en Colombia ha crecido rápidamente, promoviendo la digitalización financiera e inclusión, pero también enfrentando riesgos emergentes como la ciberseguridad, cumplimiento normativo, fraude y lavado de activos. Las startups Fintech, altamente digitalizadas y regulatoriamente vulnerables, requieren herramientas efectivas de gestión de riesgos. La norma ISO 31000:2018 ofrece un marco internacional para identificar, evaluar y tratar riesgos de manera estructurada, siendo clave para mejorar la sostenibilidad, competitividad y confianza en el sector.

Objetivo de la Guía

Esta guía tiene como objetivo principal facilitar la implementación de la norma ISO 31000 en las empresas Fintech de Colombia, adaptando sus lineamientos a las particularidades y necesidades del sector. Para alcanzar este propósito general, se plantean los siguientes objetivos específicos:

- Integrar la gestión de riesgos en todos los niveles y procesos de la startup Fintech, promoviendo una cultura organizacional orientada a la prevención y mitigación de riesgos en la toma de decisiones.
- Fortalecer la toma de decisiones basada en la gestión de riesgos, de modo que se optimicen los recursos disponibles y se aumente la eficiencia operativa de la empresa.
- Promover la mejora continua en los procesos de gestión de riesgos, permitiendo que la organización se adapte proactivamente a

los cambios del entorno y aproveche oportunidades de crecimiento sostenible.

Alcance

Aplicable a startups Fintech colombianas, independientemente de su tamaño o modelo de negocio. Se enfoca en riesgos estratégicos, operativos, tecnológicos, legales, financieros y reputacionales. Es especialmente útil para Fintech no vigiladas por la Superintendencia Financiera.

Marco Normativo

La guía se basa en la NTC-ISO 31000:2018, complementada por regulaciones locales sobre ciberseguridad, protección de datos (Ley 1581 de 2012) y prevención de lavados de activo y financiación de terrorismo. Aunque la ISO no es obligatoria, su adopción alinea a las Fintech con buenas prácticas internacionales.

Fundamentos de ISO 31000

Esta guía metodológica se fundamente a partir de estructura que propone la ISO 31000:2018 que se compone de los siguientes tres componentes:

Principios**:** son en total ocho principios que aseguran que la gestión de riesgos cree valor, esté integrada, basada en información fiable, inclusiva, adaptable y orientada a la mejora continua.

Marco de referencia**:** que establece que las organizaciones deben incluir en su sistema de gestión de riesgos liderazgo, integración en procesos, asignación de roles, recursos, y mejora continua.

Proceso de gestión del riesgo**:** Comprende establecer el contexto, identificación, análisis, evaluación y tratamiento del riesgo, acompañado por comunicación, monitoreo y revisión, esta es la principal base para desarrollar esta guía metodología, discriminados así:

1. Establecimiento del contexto**:** Definir el entorno externo (regulación, mercado, tecnología) e interno (estructura, capacidades) mediante herramientas como PESTEL y FODA.
2. Política y apetito de riesgo**:** Crear una política de riesgos que defina roles, responsabilidades y niveles de aceptación del riesgo.
3. Identificación del riesgo**:** Reconocer riesgos tecnológicos, normativos, financieros, operativos, reputacionales y emergentes.
4. Análisis del riesgo: Evaluar probabilidad e impacto usando escalas cualitativas o semi-cuantitativas y considerar controles existentes.
5. Evaluación del riesgo**:** Priorizar riesgos según su aceptabilidad y urgencia de tratamiento.
6. Tratamiento del riesgo: Aplicar estrategias como evitar, mitigar, aceptar o transferir riesgos, y elaborar planes de acción.
7. Monitoreo y revisión**:** Establecer KPIs, ciclos de revisión y reportes a la dirección para asegurar mejora continua.
8. Comunicación y consulta: Involucrar a todas las partes interesadas mediante canales efectivos, fomentando una cultura de

transparencia.

Orientaciones Prácticas

- Promover una cultura de riesgo desde los fundadores.
- Usar herramientas ligeras como hojas de cálculo para documentación.
- Enfocarse en riesgos críticos con planes de contingencia.
- Apalancar tecnología para mitigar y monitorear riesgos.
- Operar con orden y prepararse para regulaciones futuras.
- Capacitar al equipo y hacer simulacros.
- Medir el avance con checklists y retroalimentar los incidentes.
- Esta guía acompaña una herramienta en Excel (ver anexo) que permite autoevaluar el nivel de madurez en gestión de riesgos y planificar mejoras, ayudando a las Fintech colombianas a implementar ISO 31000 de forma efectiva y adaptada a su realidad emprendedora.

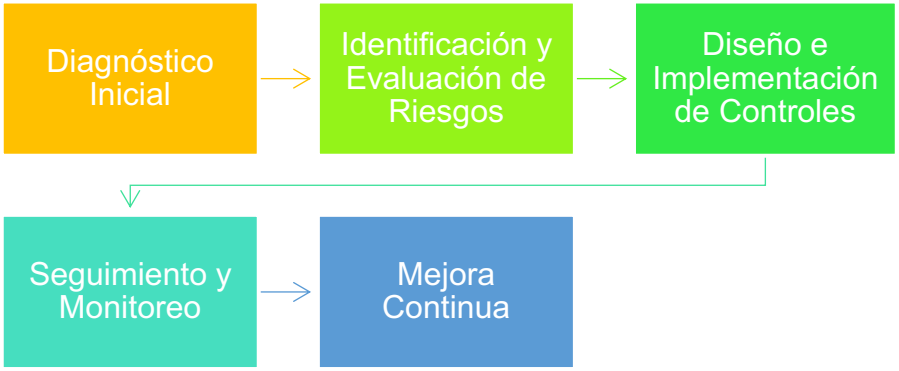
Desarrollo de la Metodología Adaptada

Fases de la Metodología

La metodología adaptada para la implementación de la norma ISO 31000 en las Fintech colombianas se estructura en cinco fases clave (ver figura 1) que fueron resumidas de las 8 actividades originales de la parte del proceso establecida en la norma cada una con objetivos claros, actividades específicas y resultados esperados que aseguran una gestión de riesgos efectiva, práctica y alineada con la realidad del sector.

Figura 1

Fases de la Metodología Adaptada



Fuente: Elaboración propia (2025)

Instrucciones de uso

1. Complete cada sección con la información de su empresa y situación actual.

2. Actualice el formato periódicamente, especialmente después de incidentes, auditorías, cambios regulatorios o revisiones internas.
3. Utilice los campos de observaciones para registrar detalles relevantes y facilitar la mejora continua.
4. Comparta este formato con todo el equipo y fomente la participación activa en la gestión de riesgos.
5. Adjunte documentos de soporte (políticas, manuales, reportes de incidentes, etc.) en anexos digitales o físicos.

Información General de la Empresa

- Nombre de la Fintech:
- Fecha de constitución:
- Vertical Fintech (crédito, pagos, Regtech, etc.):
- Número de empleados:
- Responsable de gestión de riesgos:
- Equipo de trabajo involucrado:
- Versión del formato:
- Fecha de inicio de implementación:

Aplicación de la metodología

Paso 1: Diagnóstico Inicial y Análisis Contextual

Objetivo: Evaluar el estado actual de la gestión de riesgos en la Fintech y comprender el contexto interno y externo para orientar la implementación.

Actividades requeridas:

- Realizar revisión documental de políticas, procedimientos y controles existentes.
- Aplicar entrevistas y encuestas con actores clave (directivos, equipos operativos, cumplimiento).
- Analizar el contexto interno y externo mediante herramientas como FODA y PESTEL.
- Identificar preliminarmente riesgos críticos y áreas vulnerables.

Resultados esperados:

- Informe diagnóstico que refleje el nivel de madurez en gestión de riesgos.
- Lista preliminar de riesgos y brechas en controles.
- Recomendaciones iniciales para priorizar esfuerzos y definir el plan de trabajo.

Herramientas sugeridas:

Lista de chequeo de cultura de riesgos (Sí/No) (ver tabla 1), Matriz FODA (ver tabla 2), Matriz PESTEL (ver tabla 3).

Para iniciar el primer paso de la implementación de una gestión de riesgos basada en la norma ISO 31000, usted debe evaluar la cultura de riesgos existente en su organización.

Esto lo puede realizar mediante la aplicación de una encuesta dirigida a las partes interesadas relevantes, tales como empleados, operarios, clientes, proveedores, entre otros actores que usted considere pertinentes

Una vez identificados los grupos clave, usted podrá realizar una encuesta con las preguntas, registradas en la Tabla 1, emplear el formato en Excel disponible (Anexo A) o solicitar el diligenciamiento del formato lista de verificación presentada en la Tabla 1.

Dado que es necesario calcular un porcentaje ponderado de los resultados obtenidos, se recomienda utilizar un formato que facilite el procesamiento de la información. Por esta razón, se sugiere preferiblemente el uso de la encuesta, ya que está diseñada para generar resultados automáticos con mayor eficiencia.

Tabla 1

Lista de Chequeo de Cultura de Riesgos

Ítem	Sí	No	Parcial	Observaciones / Acciones Requeridas
¿El equipo conoce los principales riesgos Fintech?				
¿Existen procedimientos para reportar incidentes?				
¿Se han realizado capacitaciones en gestión de riesgos?				
¿Se cuenta con documentación sobre controles y políticas?				

Ítem	Sí	No	Parcial	Observaciones / Acciones Requeridas
¿La alta dirección participa en la gestión de riesgos?				
¿Existen canales para comunicar riesgos?				
¿Se revisan los riesgos al menos trimestralmente?				

Fuente: Elaboración propia (2025)

Una vez tenga recopilada la información es necesario que evalué los porcentajes de repuesta Si/No y tenga en cuenta las siguiente, si mas de cuatro de las preguntas tienen un porcentaje de respuesta “NO” por encima del 50% es necesario que tome en cuenta las siguientes recomendaciones:

- Realizar talleres introductorios para todo el equipo con respecto al tema de los riesgos en Fintech y la norma ISO 31000
- Asegurar que los líderes demuestren un compromiso visible con la gestión de riesgos.
- Desarrollar una política clara sobre cómo se gestionarán los riesgos y difundirla en toda la organización.
- Incorporar el análisis de riesgos en la planificación estratégica, proyectos, operaciones y toma de decisiones.
- Involucrar a los empleados en todos los niveles y partes interesadas en el proceso de gestión de riesgos.
- Crear canales para que se compartan riesgos identificados, lecciones aprendidas y controles eficaces.
- Medir la madurez de la cultura de riesgos, identificar brechas y realizar ajustes periódicos.

Una vez aplicadas las recomendaciones anteriores, el siguiente paso es evaluar el contexto interno de su organización. Para ello, se sugiere realizar un análisis de fortalezas, oportunidades, debilidades y amenazas (FODA), que le permitirá identificar los factores internos y externos que influyen en la gestión del riesgo. Puede utilizar la plantilla presentada en la Tabla 2 para organizar esta información de manera estructurada y facilitar su interpretación.

Tabla 2

Plantilla Análisis FODA

Fortalezas	**Oportunidades**
Debilidades	**Amenazas**

Fuente: Elaboración propia (2025)

Como recomendación, después de realizar el análisis FODA, resulta útil complementar el ejercicio estableciendo una correlación entre las fortalezas y oportunidades (FO), las debilidades y oportunidades (DO), las fortalezas y amenazas (FA), y las debilidades y amenazas (DA).

Este cruce permite identificar estrategias que potencien los factores positivos y minimicen los riesgos asociados a las debilidades o

amenazas. Por ejemplo, las estrategias FO buscan aprovechar al máximo las capacidades internas para responder a las oportunidades del entorno, mientras que las estrategias DA están orientadas a reducir vulnerabilidades frente a riesgos potenciales

Posterior al análisis de correlación estratégica del FODA, también es necesario evaluar el contexto externo de la organización. Para ello, se recomienda diligenciar de manera detallada el análisis PESTEL, el cual se presenta en la Tabla 3. Esta herramienta permite identificar factores del entorno Político, Económico, Social, Tecnológico, Ambiental y Legal que pueden influir positiva o negativamente en la gestión de riesgos de la organización.

Tabla 1.

Plantilla Análisis PESTEL

Factor	Descripción	Riesgos Asociados	Oportunidades
Político			
Económico			
Social			
Tecnológico			
Ecológico			
Legal			

Fuente: Elaboración propia (2025)

Al finalizar este paso usted tendrá unos resultados claves para facilitar la toma de decisiones informadas, anticiparse a los cambios en en el entorno y alinear las estrategias de gestión de riesgos

Paso 2: Identificación y Evaluación de Riesgos

Objetivo: Detectar y analizar los riesgos específicos que afectan a la Fintech, evaluando su probabilidad e impacto para priorizar su tratamiento.

Actividades:

- Facilitar talleres participativos con equipos multidisciplinarios para identificar riesgos en procesos clave.
- Aplicar matrices de riesgo para clasificar riesgos según probabilidad e impacto.
- Realizar evaluación cualitativa y cuantitativa considerando factores técnicos, regulatorios y operativos.
- Documentar y validar resultados con responsables de áreas.

Resultados esperados:

- Registro formal y actualizado de riesgos priorizados.
- Matriz de riesgos con niveles de criticidad definidos.
- Base sólida para diseñar controles efectivos y asignar recursos.

Recomendaciones adicionales:

Se plantea el realizar mapas de procesos claves, como pagos, onboarding, gestión de datos, entre otros procesos. También realizar sesiones de lluvia de ideas que permitan identificar riesgos en cada proceso, como, por ejemplo, se propone analizar los riesgos de fraude en pagos digitales, ataques de phishing y el incumplimiento de las normativas de datos.

Herramienta sugerida:

Matriz de identificación y evaluación de riesgos (ver tabla 4)

Una vez definido el contexto organizacional, el siguiente paso en la implementación de una gestión de riesgos es la identificación y evaluación de los riesgos.

En esta etapa, el objetivo es reconocer de manera estructurada todos aquellos eventos, condiciones o factores que podrían afectar el logro de los objetivos estratégicos, operativos, financieros o de cumplimiento de la organización.

A través de este proceso, usted podrá clasificar los riesgos según su naturaleza, origen y nivel de impacto, así como establecer prioridades para su tratamiento. En la Tabla 4 se propone una plantilla de identificación y evaluación de riesgos, en la que usted puede identificar riesgos a partir de las fuentes de información internas y externas analizadas en el paso 1 y a su vez evaluarlos según criterios de probabilidad y consecuencias.

Tabla 4

Plantilla de Matriz de Identificación y Evaluación de Riesgos

Proceso / Área	Riesgo Identificado	Descripción Detallada	Causa Principal	Consecuencia Potencial	Probabilidad (Baja/Media/ Alta)	Impacto (Bajo/ Medio/ Alto)	Nivel de Prioridad	Responsable	Fecha de Identificación	Estado Actual	Observaciones

Fuente: Elaboración propia (2025)

Para términos de esta guía se propone establecer la siguiente escala de valoración:

Probabilidad:

- Baja (1): Ocurre raramente, 1 vez en más de 3 años o nunca
- Media (2): Puede ocurrir ocasionalmente, 1-2 vez al año
- Alta (3): Probable o frecuente, 1 o más veces al mes o trimestre

Impacto:

- Valor económico de materialización del riesgo

Nivel de Prioridad:

- Bajo: Hasta $1.000.000 COP
- Medio: $1.000.001 – $5.000.000 COP
- Alto: Más de $5.000.000 COP

No obstante, usted también puede considerar otras alternativas como:

Probabilidad:

- Según experiencia interna: Basada en eventos ocurridos anteriormente en la organización.
- Según percepción de expertos o personal clave: A través de encuestas o entrevistas.
- Usando datos estadísticos o históricos: Si están disponibles (por ejemplo, reportes de incidentes, bases de datos).

Impacto:

- Según el tiempo de interrupción de procesos (por ejemplo: horas/días de inactividad).
- Según el daño a la reputación (por ejemplo: quejas de clientes o afectación en redes sociales).
- Según pérdidas no monetarias (como afectación en la moral del equipo, cumplimiento legal, calidad del servicio, etc.).

Usted también puede establecer la escalara de valoración a su criterio y adicionalmente se recomienda establecer esta plantilla en una hoja de Excel que realice de los respectivos resultaos de automáticamente (ver anexo A) de manera que la dinámica de priorización sea más ágil.

Paso 3: Diseño e Implementación de Controles

Objetivo: Desarrollar e implementar múltiples estrategias y controles de mitigación de riesgos priorizados, que se alineen con los recursos y capacidades de las Fintech

Actividades:

- Diseño de políticas, controles y procedimientos específicos para cada uno de los riesgos identificados.
- Integrar controles tecnológicos y operativos, por ejemplo, sistemas de monitoreo, autenticación multifactorial.
- Capacitar y sensibilizar al personal en la aplicación y seguimiento de controles.
- Implementar pilotos y ajustar controles basados en retroalimentación y resultados.

Resultados esperados:

- Controles implementados y operativos en áreas críticas.
- Personal capacitado y comprometido con la gestión de riesgos.
- Documentación actualizada y accesible para consulta y auditoría.

Recomendaciones adicionales:

Se propone la asignación de escalas de probabilidad e impacto bajo, medio, alto para cada riesgo, al igual que hacer uso de una matriz de riesgos para visualizar las prioridades. Por ejemplo, un ciberataque puede tener alta probabilidad y alto impacto, y un error menor, como en el área de atención al cliente, tiene bajo impacto.

Herramienta sugerida:

Matriz de impacto/probabilidad (ver Tabla 5) y Plantilla de Plan de Acción (ver Tabla 6)

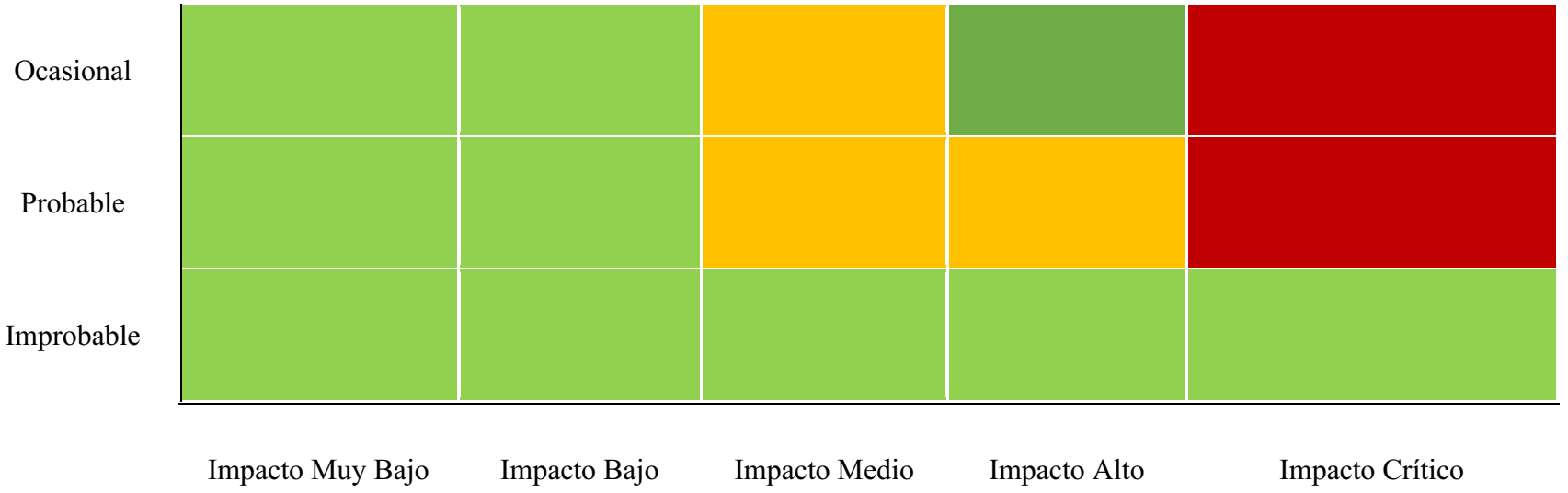
Una vez finalizado el paso 2, usted puede priorizar los riesgos más críticos mediante la valoración combinada del impacto y la probabilidad. Para ello, se recomienda multiplicar ambos valores y asignar un color de alerta según el resultado, lo que facilitará la visualización de los riesgos más relevantes.

Por ejemplo, un ciberataque podría tener una alta probabilidad y un alto impacto, ubicándose así en la zona de riesgo alto (color rojo)**.** En contraste, un error menor en atención al cliente podría presentar una baja probabilidad y un bajo impacto, clasificándose como un riesgo bajo (color verde**)**. Esta clasificación visual le permitirá enfocar los esfuerzos de control en los riesgos que realmente pueden comprometer los objetivos de la organización para ello, puede basarse en la plantilla propuesta en la Tabla 5

Tabla 5

Plantilla de Matriz de impacto/probabilidad





Fuente: Elaboración propia (2025)

Una vez priorizados los riesgos, se recomienda diligenciar la plantilla propuesta en la Tabla 6, la cual le permitirá definir planes de acción concretos para reducir la probabilidad de ocurrencia y el impacto en caso de materialización de los riesgos identificados.

Esta plantilla facilita el diseño de estrategias de tratamiento del riesgo, permitiéndole establecer responsables, plazos y recursos necesarios para la implementación de medidas preventivas, correctivas o de mitigación. Además, le servirá como una herramienta de seguimiento para monitorear el avance y la efectividad de las acciones tomadas

Tabla 6

Plantilla de Plan de Acción

esgo Prioritario	Control Propuesto	Descripción del Control	Responsable de Implementación	Fecha de Inicio	Fecha de Finalización	Recursos Necesarios	Estado (Pendiente/ En Proceso/ Implementado)	Evidencia de Implementación	Observaciones / Aju

Fuente: Elaboración propia (2025)

Paso 4: Seguimiento, Monitoreo y Comunicación

Objetivo: Supervisar continuamente la efectividad de los controles implementados y la evolución del perfil de riesgos, asegurando la detección temprana de desviaciones y facilitando la comunicación interna y externa.

Actividades:

- Definir indicadores clave de riesgo (KRI) y de desempeño (KPI) para monitoreo.
- Utilizar software o herramientas digitales para seguimiento en tiempo real.
- Realizar auditorías internas periódicas y revisar incidentes reportados.
- Elaborar reportes regulares para la alta dirección y partes interesadas.
- Mantener canales de comunicación claros y efectivos para consulta y retroalimentación.

Resultados esperados:

- Informes de seguimiento con análisis de tendencias, alertas y recomendaciones.
- Identificación oportuna de nuevos riesgos o fallas en controles.
- Mejora en la toma de decisiones basada en datos confiables y oportunos.
- Fortalecimiento de la cultura organizacional en gestión de riesgos.

Recomendaciones adicionales:

Se deben definir controles específicos en el área de tecnología, operatividad y en el área formativa, al igual que asignar responsables y plazos establecidos para cada una de las acciones. Por ejemplo, implementar una autenticación de dos pasos, capacitar al personal en prevención de fraudes o actualizar políticas de privacidad de la organización.

Herramienta sugerida:

Plan de acción de controles (ver tabla 6) y plantilla de KPI (ver tabla 7)

Tabla 7

Plantilla de Seguimiento de Indicadores de Éxito (KPI)

Indicador	Definición	Meta / Valor Esperado	Frecuencia de Medición	Valor Actual	Responsable	Acciones de Mejora	Fecha de Última Revisión	Observaciones

Fuente: Elaboración propia (2025)

KPI sugeridos:

- Número de riesgos identificados y gestionados
- Porcentaje de controles implementados
- Incidentes críticos reportados y resueltos
- Cumplimiento normativo
- Personal capacitado
- Actualización de la matriz de riesgos

Estos indicadores deben ser monitoreados y reportados periódicamente, permitiendo identificar avances, áreas de mejora y demostrar el compromiso de la startup con la gestión de riesgos ante inversionistas, clientes y reguladores

Indicadores de Éxito (KPI) sugeridos

Para medir el éxito de la implementación de la gestión de riesgos en startups Fintech, se proponen los siguientes indicadores clave:

1. Número de riesgos identificados y gestionados:

Meta: Al menos el 80% de los riesgos críticos identificados y con controles implementados en los primeros seis meses.

2. Porcentaje de controles implementados vs. planificados:

Meta: Implementar al menos el 90% de los controles definidos en el plan de acción.

3. Incidentes críticos reportados y resueltos:

Meta: Reducir incidentes críticos en un 50% durante el primer año.

4. Cumplimiento normativo:

Meta: Cero sanciones regulatorias o advertencias formales en el primer año.

5. Capacitación del personal:

Meta: Al menos el 90% del personal capacitado en gestión de riesgos y controles básicos.

6. Actualización de la matriz de riesgos:

Meta: Actualización trimestral o después de cada incidente relevante.

Paso 5: Mejora Continua

Objetivo: Garantizar la actualización y optimización constante del sistema de gestión de riesgos para adaptarse a cambios tecnológicos, regulatorios y del entorno.

Actividades:

- Evaluar periódicamente la metodología y resultados obtenidos.
- Incorporar lecciones aprendidas y mejores prácticas.
- Actualizar políticas, procedimientos y controles según nuevas necesidades.
- Promover la capacitación continua y la sensibilización permanente.

Resultados esperados:

- Sistema de gestión de riesgos dinámico, resiliente y alineado con los objetivos estratégicos.
- Mayor capacidad de adaptación y respuesta ante nuevos desafíos.
- Cultura organizacional consolidada en torno a la gestión de riesgos.

Recomendaciones adicionales:

Se sugiere el establecimiento de reuniones periódicas para la revisión de los riesgos, bien sea de manera mensual o trimestral. También registrar los diversos incidentes y acciones correctivas de los mismos, como, por ejemplo, hacer un análisis de los incidentes de seguridad, actualizar la matriz de riesgos existentes en la organización y ajustar los diversos controles de acuerdo a los resultados obtenidos.

Herramienta sugerida:

Registro de incidentes (ver tabla 8), seguimiento de acciones (ver tabla 9), informe de revisión (ver tabla 10), plan de actualización y mejora continua (tabla 11)

Tabla 2

Plantilla Seguimiento de Acciones

Fecha de Seguimiento	Control Revisado	Resultado de la Revisión	Incidentes Detectados	Acciones Correctivas	Responsable	Estado

Fuente: Elaboración propia (2025)

Tabla 3

Plantilla de Registro de Incidentes y Lecciones Aprendidas

Fecha del Incidente	Área / Proceso Afectado	Descripción del Incidente	Riesgo Relacionado	Acción Correctiva Tomada	Responsable	Fecha de Resolución	Estado (Abierto/ Cerrado)	Impacto Real	Lecciones Aprendidas / Mejoras Propuestas

Fuente: Elaboración propia (2025)

Tabla 10

Plantilla de Evaluación Periódica de la Metodología

Fecha de Revisión	Aspectos Evaluados	Hallazgos Principales	Acciones de Mejora	Responsable	Fecha de Próxima Revisión

Nota. plantilla de efectividad para el seguimiento de control de riesgos. Fuente: Elaboración propia (2025)

Tabla 4

Plantilla de Plan de Actualización y mejora continua

Nuevos riesgos identificados:	
Controles a fortalecer:	
Necesidades de capacitación:	
Cambios regulatorios recientes:	
Otras observaciones relevantes:	

Fuente: Elaboración propia (2025)

Recomendaciones Finales

1. Se debe fomentar una capacitación continua. Esto se logrará a través de la inversión en la formación básica de todo el equipo en el área de la gestión de riesgos, la ciberseguridad y el cumplimiento normativo, haciendo uso de recursos gratuitos o alianzas con gremios Fintech e incluso con instituciones educativas de nivel superior.
2. Se deben enfocar los esfuerzos en los riesgos de mayor impacto, es decir, priorizar los mismos, implementando controles efectivos, aunque simples, y escalando la gestión de acuerdo al crecimiento del startup.
3. Se deben aprovechar las herramientas accesibles. Esto se logra a través del uso de plataformas digitales gratuitas o de bajo costo, tales como Notion, Trello y Google Sheets, para permitir así la documentación y el seguimiento de los riesgos, lo que facilitará la colaboración y la actualización constante de la información dentro de la empresa.
4. Se debe incentivar en todo momento la promoción de una cultura de riesgos, así como la comunicación abierta sobre el tema, los errores y las lecciones que se han aprendido, evitando la cultura de culpa y haciendo una promoción activa de la participación de todos los miembros del equipo de la empresa.
5. Se propone realizar un seguimiento periódico y constante de los KPI que se han definido para poder ajustar las metas y los controles de acuerdo a los resultados y los cambios observados en el entorno.
6. Buscar asesoría externa: Cuando sea posible, recurrir a expertos o consultores en gestión de riesgos para validar la metodología y fortalecer los procesos internos.

7. Actualizar la guía periódicamente: Revisar y mejorar la guía metodológica al menos una vez al año o después de incidentes relevantes, incorporando nuevas mejores prácticas y aprendizajes del sector.

Pasos adicionales

- Utilizar herramientas digitales gratuitas (Google Sheets, Trello, Notion) para registrar y hacer seguimiento de riesgos.
- Fomentar la comunicación abierta sobre riesgos y errores.
- Buscar alianzas con gremios Fintech o consultores para asesoría puntual.

NOTA IMPORTANTE: Este formato propuesto puede ser adaptado y digitalizado en hojas de cálculo, sistemas internos o software de gestión de riesgos según las necesidades de cada Startup Fintech.

Conclusiones

Aún con los diversos beneficios y ventajas que se tienen a través de la implementación de la metodología propuesta, siempre será importante reconocer las limitaciones o desafíos que pueden surgir durante su implementación.

Muchas startups pueden contar con presupuestos y equipos reducidos o limitados, lo que podría dificultar la implementación de los controles complejos o adquirir herramientas tecnológicas avanzadas.

1. La ausencia de un personal capacitado o especializado en la gestión de riesgos podría generar una curva de aprendizaje inicial, lo que ameritaría una capacitación constante del mismo.
2. El marco normativo para las Fintech en Colombia se encuentra siempre en constante evolución, lo que exigiría actualizar de manera permanente los controles y los procedimientos de la empresa.
3. Se debe fomentar una cultura de gestión de riesgos en equipos pequeños y multidisciplinarios, lo cual requiere que se tenga liderazgo, aplicar comunicación efectiva y fomentar la participación activa de todos los miembros.
4. Pueden existir dificultades en cuanto al acceso a los datos internos y externos, lo que puede limitar la identificación y la evaluación precisa de los riesgos que se presenten en la empresa.

Referencias

Manual de servicios financieros digitales. (s.f.). *FindevGateway*. https://www.findevgateway.org/sites/default/files/publications/files/es_ifc_risk_handbook_spanish_final.pdf

Norma ISO 31000:2018 en español. (2018). *Rama Judicial*. https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf

Pirani (s.f.). Estrategias para la gestión de riesgos emergentes según la norma ISO 31050. Recuperado de https://www.piranirisk.com/academy/pirani-explains/strategies-for-handling-emerging-risks-in-line-with-iso-31050

Pirani. (2021, 1 de septiembre). Matriz de riesgos: qué es, ejemplos y cómo crearla fácil. https://www.piranirisk.com/es/blog/matriz-de-riesgos-que-es-ejemplos-y-como-crearla-facil