



POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS (ERM)

Riesgos corporativos, de sostenibilidad, de la cadena de distribución y APL, y de integridad

Guatemala · El Salvador · Honduras · Nicaragua · Costa Rica · Panamá · República Dominicana · Colombia

Código PO-GC-02 · Versión 1.3 · 6 de octubre de 2026

Política regional única · Documento público · Pendiente de aprobación por el Comité de Riesgos

Marco ISO 31000 · Metodología PMBOK · Próxima etapa COSO ERM

Contenido

Contenido	2
Control del documento	4
1. Declaración de compromiso	6
2. Objetivo	6
3. Alcance.....	6
4. Marco de referencia	7
5. Definiciones.....	7
6. Principios.....	8
7. Enfoque integrado ERM.....	8
8. Gobierno y responsabilidades	9
8.1 Modelo de las Tres Líneas	9
8.2 Responsabilidades	9
9. Taxonomía de riesgos.....	11
10. Proceso de gestión de riesgos.....	12
11. Metodología de valoración	13
11.1 Escala de probabilidad	13
11.2 Escala de impacto	13
11.3 Mapa de calor y niveles de riesgo.....	13
11.4 Evaluación de controles y riesgo residual	14
11.5 Análisis cuantitativo	14
12. Estrategias de respuesta	14
13. Matrices de riesgos por departamento	15
13.1 Reglas	15
13.2 Fuentes que se integran en la matriz corporativa	15
14. Apetito, tolerancia, umbrales y escalamiento	15
14.1 Declaración de Apetito de Riesgo (RAS)	15
14.2 Umbrales y KRIs.....	16
14.3 Escalamiento	16
14.4 Herramientas: Smart Tools y tablero.....	16
15. Riesgos de sostenibilidad: ambientales, sociales y climáticos	17
16. Riesgos de la cadena de distribución y de American Pallet & Logistics (APL)	18
17. Riesgos de integridad y cumplimiento	18
18. Continuidad del negocio.....	19
19. Riesgos de proyectos y del portafolio	19
20. Monitoreo, reporte e indicadores	19
21. Auditoría Interna.....	20
22. Cultura, capacitación y comunicación.....	20

23. Ruta de implementación y próximos pasos	20
23.1 Próximos pasos de madurez	21
24. Documentos relacionados	21
25. Incumplimiento	21
26. Disposiciones finales.....	22
Anexo A. Formato único de la matriz de riesgos del departamento	23
Anexo B. Técnicas recomendadas	23
Anexo C. Mapa de calor	23
Anexo D. Modelo de Declaración de Apetito de Riesgo	24
Anexo E. Equivalencia entre PMBOK, ISO 31000 y COSO ERM	24

Para actualizar el índice en Word: clic derecho sobre él → Actualizar campo.

Control del documento

Código	Versión	Fecha de emisión	Próxima revisión
PO-GC-02	1.3	06/10/2026	06/10/2027

Versión	Fecha	Descripción
1.0	30/09/2026	Primera emisión. Establece el Sistema de Gestión Integral de Riesgos (ERM) del Grupo Rent a Pallet, con matrices de riesgo por departamento, integración de los riesgos ambientales, sociales y climáticos del SGAS, de los riesgos de la cadena de distribución y de American Pallet & Logistics (APL), y de los riesgos de integridad y cumplimiento. Adopta el ciclo de gestión de riesgos del PMBOK como metodología operativa, la norma ISO 31000 como marco y COSO ERM como siguiente etapa de madurez.
1.1	01/10/2026	Se alinea con la operatividad definitiva del Canal de Ética y con el paquete de integridad vigente: los riesgos de seguridad y salud ocupacional pasan del Especialista Regional de Sostenibilidad al Coordinador Regional de Seguridad Industrial y Salud Ocupacional; se precisa que el escalamiento de un riesgo de integridad distingue entre el Comité de Ética y Conducta (conducta, constituido en octubre de 2026) y el Comité de Auditoría (fraude, corrupción, LA/FT/FPADM), que recibe además el informe trimestral del Canal de Ética; el "Comité de ESG y RES" se renombra Comité ESG/RES y de Bono Verde; se agregan referencias al Procedimiento de Debida Diligencia de Terceros (PR-CU-04) y al Procedimiento de Quejas y Denuncias (PR-CU-08).
1.2	01/10/2026	Se incorporan ocho precisiones identificadas al revisar el documento de trabajo previo del Grupo: (1) la Declaración de Apetito de Riesgo (RAS) se aprueba antes de fijar los covenants financieros del Term Sheet de cualquier emisión, para negociarlos contra el apetito propio del Grupo; (2) se preserva el circuito de aprobación propio del SGAS (factibilidad de Finanzas Regional y aprobación final del Director General), distinto del Comité de Riesgos, por ser el circuito ya validado con BID Invest; (3) se precisa la distinción contractual entre el SGAS (sistema) y el PAAS (instrumento del contrato de préstamo con BID Invest, de divulgación pública, cuyo incumplimiento persistente puede derivar en el retiro del apoyo financiero); (4) el cargo que opera el programa ambiental y social es el Coordinador de Calidad (antes referido como "Coordinador de Sistemas de Gestión"), y el control documental de las matrices de riesgo pasa a la Analista de Gobierno Corporativo; (5) se agrega ISO 37002 como referencia del Canal de Ética; (6) se agregan ISO 28000 e ISO 20400 para la cadena de suministro, y el Operador Económico Autorizado (OEA/AEO) para los riesgos de APL; (7) se agregan CITES y el Reglamento Europeo de Deforestación (EUDR) en el origen de la madera; (8) se agregan dos indicadores: nivel de madurez de la gestión de riesgos y porcentaje de pruebas de continuidad del negocio ejecutadas, y la regla de que ninguna matriz se consolida en Smart Tools sin validar antes sus campos mínimos.
1.3	06/10/2026	Alineación con el paquete vigente. Se agrega el sistema de gestión de los riesgos de fraude, soborno, corrupción y LA/FT/FPADM (documento de uso interno) como aplicación de esta política a la categoría de integridad y cumplimiento (capítulos 8.2, 13.2, 14.3, 17, 20 y 24). Se confirma que "crítico" equivale a los niveles alto y extremo, de 16 a 25 (capítulo 11.3). El Oficial de Cumplimiento Regional forma parte del Departamento de Gobierno Corporativo; la secretaría de los comités de Auditoría, Riesgos y Compensaciones pasa de la Coordinación a la Analista de Gobierno Corporativo; el Comité ESG/RES y de Bono Verde es un comité único; el Comité de Ética y Conducta se constituye en octubre de 2026; el Auditor Interno inicia el 19 de octubre de 2026 y el Comité de Auditoría propone su plan, que aprueba la Junta; el Director General integra los comités con voz y sin voto. Aprobación y apetito de riesgo: esta política y la Declaración de Apetito de Riesgo las aprueba el Comité de Riesgos (antes, la Junta Directiva), que informa a la Junta; firman: elabora Gobierno Corporativo, revisa el Director General y aprueba Josef Sauter Atmetlla, Presidente del Comité de Riesgos.

Clasificación: documento público. **Dueño del documento:** Coordinación de Gobierno Corporativo, función F06 Gestión de Riesgos (ERM) y Continuidad del Negocio. **Gestión:** trabajo en equipo de todos los departamentos, bajo la supervisión del Comité de Riesgos. **Aprobación:** elabora la Coordinación de Gobierno Corporativo; revisa el Director General; **aprueba el Comité de Riesgos**, a través de su Presidente, Josef Sauter Atmetlla, director externo. El Comité de Riesgos aprueba también la Declaración de Apetito de Riesgo (capítulo 14.1) e informa a la Junta Directiva, que recibe el informe anual del sistema.

Aprobaciones

Elaborado por	Revisado por	Aprobado por el Comité de Riesgos
<hr/> Catalina Nicholls Coordinadora de Gobierno Corporativo Fecha: ____/____/____	<hr/> Carlos Luis Monge Director General (CEO) Fecha: ____/____/____	<hr/> Josef Sauter Atmetlla Director externo · Presidente del Comité de Riesgos Fecha: ____/____/____

1. Declaración de compromiso

En el Grupo Rent a Pallet **gestionar el riesgo es trabajo de todos**. Cada departamento conoce mejor que nadie los riesgos de su proceso, y por eso es dueño de su matriz de riesgos, de sus controles y de sus planes de respuesta. El Comité de Riesgos, con la Dirección General, fija cuánto riesgo estamos dispuestos a asumir e informa a la Junta Directiva; la Coordinación de Gobierno Corporativo integra una sola visión del Grupo; y la Auditoría Interna verifica, con independencia, que el sistema funcione. Gestionamos el riesgo para proteger lo que tenemos, cumplir lo que prometemos a clientes, inversionistas y tenedores de bonos, y aprovechar las oportunidades con decisiones informadas.

2. Objetivo

- Establecer el marco, los principios, los roles y la metodología única con la que el Grupo **identifica, analiza, evalúa, responde, monitorea y comunica** sus riesgos y oportunidades.
- Integrar en una **matriz corporativa de riesgos** las matrices elaboradas por cada departamento, los riesgos ambientales, sociales y climáticos del SGAS, los de la cadena de distribución y APL, y los de integridad y cumplimiento, con una sola escala de valoración.
- Vincular la gestión de riesgos con los **objetivos estratégicos**, el presupuesto, los proyectos y la continuidad del negocio.
- Dar a la Junta Directiva, a los comités, a BID Invest, a las calificadoras y a los inversionistas información de riesgos confiable, oportuna y verificable.

3. Alcance

Esta es una **política única** para todo el Grupo. Aplica a las **12 sociedades**, incluidas el emisor de valores —Costa Rican Pallet & Pooling Co., Corp.— y las sociedades tenedoras en Panamá, y a las sociedades operativas de los ocho países:

País	Sociedad operativa	Aplicación
Costa Rica	RENT A PALLET S.A.	Política regional
Guatemala	LOGÍSTICA RAP, S.A.	Política regional
El Salvador	RENT A PALLET EL SALVADOR, S.A. DE C.V.	Política regional
Honduras	LOGÍSTICA RAP S.A.	Política regional
Nicaragua	TRÉBOL SOCIEDAD ANÓNIMA	Política regional
Panamá	RENT A PALLET PANAMÁ S.A.	Política regional
República Dominicana	CRP&P RENT A PALLET S.A.S.	Política regional
Colombia	COLOMBIANA DE ESTIBAS S.A. (COLESTIBAS)	Política regional, articulada con el SAGRILIFT y el PTEE
Costa Rica, Guatemala y El Salvador	Sociedades de American Pallet & Logistics (APL)	Política regional, en lo relativo a la cadena de distribución

Cubre todos los departamentos, procesos, plantas, proyectos, productos y relaciones con terceros, y todos los tipos de riesgo de la taxonomía del capítulo 9, tanto **amenazas** (riesgos negativos) como **oportunidades** (riesgos positivos).

4. Marco de referencia

Referente	Cómo lo usa el Grupo
ERM – Gestión Integral de Riesgos Empresariales	Enfoque general: el riesgo se gestiona de forma integrada en toda la organización y vinculado a la estrategia, no por silos.
PMBOK / PMI – Gestión de riesgos	Metodología operativa actual. Ciclo de siete pasos: planificar, identificar, análisis cualitativo, análisis cuantitativo, planificar respuestas, implementar respuestas y monitorear (capítulo 10).
ISO 31000:2018 – Gestión del riesgo	Marco de referencia adoptado: principios, marco y proceso. La norma no es certificable; el Grupo declara su alineación.
IEC 31010 – Técnicas de evaluación del riesgo	Selección de técnicas: lluvia de ideas, árbol de problemas, escalera de por qué, análisis de causa raíz, bow-tie, análisis de escenarios.
COSO ERM 2017 – Integrando con la estrategia y el desempeño	Siguiente etapa de madurez (capítulo 23): apetito vinculado a la estrategia, desempeño y cultura.
COSO 2013 – Control Interno	Diseño y evaluación de los controles, incluido el riesgo de fraude (Principio 8).
IIA – Modelo de las Tres Líneas	Distribución de roles entre dueños del riesgo, funciones de segunda línea y Auditoría Interna (capítulo 8).
ISO 22301 – Continuidad del negocio	Análisis de impacto al negocio y planes de continuidad (capítulo 18).
Normas de Desempeño de IFC (ND1) e ISO 14001 / 45001	Identificación de riesgos e impactos ambientales, sociales y de seguridad y salud del SGAS (capítulo 15).
NIIF S2 y recomendaciones del TCFD	Riesgos físicos y de transición del cambio climático.
ISO 37301, ISO 37001 e ISO 37002	Riesgos de cumplimiento, de soborno y del sistema de gestión del Canal de Ética (capítulos 12 y 17).
ISO 28000 e ISO 20400	Seguridad de la cadena de suministro y compras sostenibles (capítulo 16).
Programa de Operador Económico Autorizado (OEA/AEO) de cada país	Referencia de control para los riesgos aduaneros y de comercio exterior de APL (capítulo 16).
CITES y Reglamento Europeo de Deforestación (EUDR)	Trazabilidad y legalidad de la madera, en especial ante clientes o inversionistas europeos (capítulo 15).
ISO 14064 e ISO 21502	Complementan el GHG Protocol en la verificación de inventarios de gases de efecto invernadero, y aportan un marco adicional para los riesgos de proyectos (capítulo 19).

5. Definiciones

Término	Definición
Riesgo	Efecto de la incertidumbre sobre los objetivos. Puede ser negativo (amenaza) o positivo (oportunidad).
ERM	Gestión integral de riesgos empresariales: cultura, capacidades y prácticas integradas con la estrategia para gestionar el riesgo en toda la organización.
Dueño del riesgo	Jefatura o gerencia con la autoridad y la responsabilidad de gestionar un riesgo y sus controles.
Matriz de riesgos del departamento	Registro de riesgos de un área, con su valoración, controles, costos y plan de respuesta (Anexo A).

Término	Definición
Matriz corporativa de riesgos	Consolidación de todas las matrices del Grupo bajo una sola escala, a cargo de la Coordinación de Gobierno Corporativo.
Riesgo inherente	Nivel de riesgo antes de considerar los controles.
Riesgo residual	Nivel de riesgo después de aplicar los controles existentes.
Riesgo crítico	Riesgo de nivel alto o extremo (puntaje de 16 a 25). El Reglamento del Comité de Auditoría (GC-RC-01, Art. 23) usa “críticos o extremos” con este mismo alcance.
Apetito de riesgo	Cantidad y tipo de riesgo que el Grupo está dispuesto a aceptar para lograr sus objetivos. Se expresa en la Declaración de Apetito de Riesgo (RAS).
Tolerancia y umbral	Variación aceptable alrededor del apetito para un riesgo o categoría, expresada como límite medible.
Indicador clave de riesgo (KRI)	Métrica que alerta de forma anticipada sobre el aumento de un riesgo.
Valor monetario esperado (VME)	Probabilidad del riesgo multiplicada por su impacto en dinero. Base del análisis cuantitativo.
Reserva de contingencia	Recursos previstos para responder a riesgos identificados que se materialicen.
Plan de contingencia	Acciones predefinidas que se activan si el riesgo ocurre o si se dispara su señal de alerta.
Riesgo emergente	Riesgo nuevo o en evolución, todavía difícil de cuantificar.
Jerarquía de mitigación	Para riesgos ambientales y sociales: evitar, luego reducir y, solo al final, compensar (P-SGAS-05).

6. Principios

Siguiendo la norma ISO 31000, la gestión de riesgos en el Grupo es:

Principio	Qué significa en RAP
Integrada	Forma parte de la planeación estratégica, el presupuesto, los proyectos y la operación diaria; no es un ejercicio aparte.
Estructurada y exhaustiva	Todos los departamentos usan la misma metodología, la misma escala y el mismo formato de matriz.
Adaptada	Se ajusta al tamaño, la operación y el contexto de cada país y sociedad.
Inclusiva	Participan los dueños del riesgo, los puntos focales de planta, los comités y, cuando corresponde, las partes interesadas externas.
Dinámica	Se actualiza ante cambios del entorno, nuevos proyectos, incidentes o hallazgos; el monitoreo retroalimenta la identificación de nuevos riesgos.
Basada en la mejor información disponible	Usa datos históricos, costos reales, indicadores y opinión experta, reconociendo sus limitaciones.
Consciente de factores humanos y culturales	Considera el comportamiento de las personas y promueve que se hable de riesgos sin temor.
De mejora continua	Se aprende de los incidentes, de las auditorías y de los errores.
Trabajo en equipo	Ningún departamento gestiona sus riesgos en solitario, y ninguna función concentra toda la responsabilidad.

7. Enfoque integrado ERM

El Grupo combina tres marcos que se complementan y que se adoptan de forma gradual:

Marco	Para qué lo usamos	Estado
PMBOK	Cómo se hace: el ciclo operativo de siete pasos con el que cada departamento construye y actualiza su matriz, con análisis cuantitativo de costos y planes de contingencia.	En uso. Paso actual: 5, planificación de respuestas.
ISO 31000	El marco: principios, liderazgo, integración, diseño, implementación, evaluación y mejora del sistema.	Adoptado con esta política.
COSO ERM	La madurez: vincular el apetito de riesgo con la estrategia, el desempeño y la cultura, y reportar el riesgo como parte de la gestión del negocio.	Próxima etapa (2027).

La equivalencia entre los tres marcos se presenta en el Anexo E, para que cada departamento sepa que el trabajo hecho bajo la metodología de proyectos sigue siendo válido al avanzar hacia ISO 31000 y COSO ERM.

8. Gobierno y responsabilidades

8.1 Modelo de las Tres Líneas

Línea	Quién	Qué le corresponde
Órgano de gobierno	Junta Directiva, Comité de Riesgos y Comité de Auditoría	El Comité de Riesgos aprueba la política y el apetito de riesgo; la Junta Directiva y el Comité de Auditoría supervisan el sistema y reciben los informes.
Primera línea	Todos los departamentos y gerencias de país: Operaciones, Logística, Producción, Comercial, Compras, Finanzas, Tesorería, Desarrollo Humano, Tecnología, Calidad, Coordinador Regional de Seguridad Industrial y Salud Ocupacional, Protección de Activos, APL y el propio Departamento de Gobierno Corporativo en sus procesos	Son dueños de sus riesgos : elaboran y actualizan su matriz con costos, operan los controles, ejecutan los planes de respuesta y reportan cada mes.
Segunda línea	Departamento de Gobierno Corporativo (F06), que incluye al Oficial de Cumplimiento Regional; Especialista Regional de Sostenibilidad, Medio Ambiente y Social; Seguridad de la Información	Diseñan la metodología, asesoran, consolidan, monitorean y reportan. No ejecutan la operación que supervisan.
Tercera línea	Auditoría Interna	Aseguramiento independiente sobre el diseño y la eficacia del sistema, incluido el trabajo de la segunda línea.

8.2 Responsabilidades

Instancia	Responsabilidades
Junta Directiva	Conoce al menos una vez al año el perfil de riesgos del Grupo, la Declaración de Apetito de Riesgo aprobada por el Comité de Riesgos y los riesgos extremos; asigna recursos; recibe el informe anual del sistema.
Comité de Riesgos	Aprueba esta política y aprueba la Declaración de Apetito de Riesgo y los umbrales, e informa de ello a la Junta Directiva; aprueba la metodología, la taxonomía y la matriz corporativa; revisa cada trimestre el mapa de calor, los riesgos altos y extremos y el avance de los planes de respuesta; aprueba el tratamiento de los riesgos ambientales, sociales y climáticos; aprueba las calibraciones del sistema de riesgos de integridad; acordó la ruta de implementación del capítulo 23; informa de inmediato al Comité de Auditoría los riesgos altos y extremos de integridad y sesiona con él al menos una vez al año sobre la matriz completa (GC-RC-01, Art. 23).

Instancia	Responsabilidades
Comité de Auditoría	Supervisa la eficacia del sistema de control interno y de gestión de riesgos; propone a la Junta el plan y el presupuesto de Auditoría Interna basados en riesgos y supervisa su ejecución; conoce y resuelve directamente los riesgos e incidentes de información financiera, fraude, corrupción, soborno y LA/FT/FPADM y supervisa el sistema de gestión de esos riesgos; recibe el informe trimestral integrado de riesgos de integridad, que incluye el informe agregado del Canal de Ética (PR-CU-08), conforme al Reglamento del Comité de Auditoría (GC-RC-01).
Comité ESG/RES y de Bono Verde	Comité único que ve todos los temas ambientales, sociales, de ESG y RES y supervisa el Bono Verde. Da seguimiento a los riesgos ambientales, sociales y climáticos y al PAAS, y los reporta al Comité de Riesgos. Su Secretaría Técnica está siempre a cargo del Especialista Regional de Sostenibilidad, Medio Ambiente y Social.
Comité de Ética y Conducta	Órgano permanente del Canal de Ética, que se constituye en octubre de 2026. Resuelve los casos de conducta; los de fraude, corrupción, soborno y LA/FT/FPADM los resuelve el Comité de Auditoría.
Director General (CEO)	Promueve la cultura de riesgos; asigna dueños y recursos; aprueba los planes de respuesta y los presupuestos de mitigación; decide sobre riesgos extremos junto con el Comité de Riesgos. Integra los comités de la Junta con voz y sin voto.
Coordinación de Gobierno Corporativo (F06)	Dueña de la metodología y de la matriz corporativa. Consolida las matrices de los departamentos; opera Smart Tools y el tablero; prepara los informes a los comités; coordina la continuidad del negocio y la actualización de esta política.
Analista de Gobierno Corporativo	Responsable del control documental de las matrices de riesgo: recibe cada matriz departamental, verifica que contenga los campos mínimos del formato único (Anexo A, capítulo 13.1) y solo entonces la consolida en Smart Tools; mantiene el registro mensual y el historial de versiones. Asume la secretaría de los comités de Auditoría, Riesgos y Compensaciones, hoy a cargo de la Coordinación [fecha del traslado por confirmar]. Registra y enruta los casos del Canal de Ética que revelen riesgos, con número de caso y clave de seguimiento (PR-CU-08), sin investigarlos.
Oficial de Cumplimiento Regional (Departamento de Gobierno Corporativo)	Dueño del sistema de gestión de los riesgos de fraude, soborno, corrupción y LA/FT/FPADM. Identifica, evalúa y monitorea los riesgos de cumplimiento, integridad, terceros (con apoyo del PR-CU-04), protección de datos y uso de IA; los entrega a la Coordinación para su consolidación; reporta funcionalmente al Comité de Auditoría.
Especialista Regional de Sostenibilidad, Medio Ambiente y Social	Gestiona de punta a punta los riesgos ambientales, sociales y climáticos y de la cadena de madera, conforme a la ND1 y al P-SGAS-05, y los entrega a la Coordinación. Ejerce siempre la Secretaría Técnica del Comité ESG/RES y de Bono Verde. No es dueño de la matriz corporativa. No gestiona los riesgos de seguridad y salud ocupacional , que son responsabilidad exclusiva del Coordinador Regional de Seguridad Industrial y Salud Ocupacional.
Coordinador de Calidad	Opera el Programa de Gestión de Riesgos Ambientales y Sociales (P-SGAS-05): conduce el proceso técnico de diez pasos (identificación de causa raíz, objetivos e indicadores, jerarquía evitar–reducir–compensar, cronograma y recursos) y consolida el Plan de Acción Ambiental y Social (R-SGAS-05). Antes conocido como “Coordinador de Sistemas de Gestión”. Trabaja de la mano del Especialista Regional, que entrega el resultado consolidado a la Coordinación de Gobierno Corporativo.
Coordinador Regional de Seguridad Industrial y Salud Ocupacional	Identifica, evalúa y monitorea los riesgos de seguridad y salud ocupacional de colaboradores propios, de contratistas y de visitantes en todas las plantas y sedes, con sus propios indicadores (accidentabilidad, incidentes, días perdidos), y los entrega a la Coordinación de Gobierno Corporativo para su consolidación en la matriz corporativa. Es la autoridad técnica exclusiva en esta materia.

Instancia	Responsabilidades
Auditor Interno	Evalúa de forma independiente el sistema al menos una vez al año; basa su plan en la matriz corporativa; no diseña ni opera controles ni elabora matrices, para preservar su independencia. Inicia funciones el 19 de octubre de 2026.
Finanzas Regional	Valida los costos e impactos económicos de las matrices, la reserva de contingencia y los umbrales financieros; transfiere riesgos mediante seguros.
Tecnología de la Información	Mantiene Smart Tools y el tablero; gestiona los riesgos tecnológicos y de ciberseguridad.
PMO (F11)	Aplica esta metodología a los proyectos del portafolio y escala a la matriz corporativa los riesgos de proyecto que afecten al Grupo.
Gerencias de país y puntos focales de planta	Aplican la política localmente, alimentan las matrices y ejecutan los planes en su país.
Todos los colaboradores	Identifican y reportan riesgos, incidentes y cuasi incidentes, y cumplen los controles de su puesto.

9. Taxonomía de riesgos

Todas las matrices clasifican cada riesgo en una de estas categorías, para poder consolidarlos y compararlos:

Categoría	Ejemplos en RAP
Estratégicos	Expansión a nuevos mercados, competencia, concentración de clientes, cambios tecnológicos del sector, cumplimiento de los objetivos estratégicos.
Financieros y de mercado de capitales	Liquidez, tipo de cambio, tasas de interés, crédito de clientes, incumplimiento de covenants de la emisión de bonos, calificación de riesgo, obligaciones del emisor.
Operativos	Producción y reparación de tarimas, disponibilidad de madera, mantenimiento, calidad, inventarios, dependencia de proveedores críticos.
Cadena de distribución y APL	Pérdida y retención de tarimas en clientes, recuperación del activo, transporte y fletes, operadores logísticos, trazabilidad del pooling, riesgos de las sociedades de American Pallet & Logistics (capítulo 16).
Ambientales	Permisos y licencias, residuos peligrosos, aguas residuales, químicos, ruido, emisiones, origen legal de la madera, biodiversidad.
Sociales y laborales	Condiciones laborales, trabajo infantil y forzoso en la cadena, acoso y violencia de género, comunidades vecinas, derechos humanos.
Seguridad y salud ocupacional	Accidentabilidad, incidentes, días perdidos, condiciones de planta, equipo de protección personal, siniestralidad de contratistas, gestionados por el Coordinador Regional de Seguridad Industrial y Salud Ocupacional.
Climáticos	Físicos (inundaciones, huracanes, sequías, calor) y de transición (precio del carbono, regulación, exigencias de clientes e inversionistas).
Cumplimiento e integridad	Corrupción, soborno, fraude, LA/FT/FPADM, conflictos de interés, partes relacionadas, sanciones, protección de datos, obligaciones regulatorias en los ocho países.
Tecnológicos y de información	Ciberseguridad, disponibilidad de sistemas (SAP, Smart Tools), fuga de información, uso de inteligencia artificial.
Personas y talento	Rotación en cargos clave, sucesión, clima organizacional, dependencia de personas críticas.
Reputacionales	Afectación de la marca ante clientes, comunidades, inversionistas o medios, como consecuencia de otros riesgos.
Proyectos	Riesgos de alcance, costo, plazo y calidad de los proyectos del portafolio (capítulo 19).

10. Proceso de gestión de riesgos

El Grupo aplica el ciclo de gestión de riesgos del PMBOK, alineado con el proceso de la norma ISO 31000 (Anexo E). **El monitoreo retroalimenta la identificación de nuevos riesgos.** A la fecha de esta política, los departamentos se encuentran en el paso 5, planificación de respuestas.



#	Paso	Qué se hace	Responsable
1	Planificar	Definir roles, método, escalas, calendario y presupuesto de la gestión de riesgos del área.	Dueño del riesgo con la Coordinación de GC
2	Identificar	Identificar los riesgos y oportunidades de cada proceso, con su causa, evento y consecuencia, mediante lluvia de ideas, entrevistas, listas de verificación, lecciones aprendidas y análisis de causa raíz (árbol de problemas, escalera de por qué).	Cada departamento, con sus puntos focales
3	Análisis cualitativo	Calificar probabilidad e impacto en escala 1–5 (capítulo 11), obtener el riesgo inherente, evaluar los controles y obtener el riesgo residual.	Dueño del riesgo
4	Análisis cuantitativo	Estimar en dinero el impacto de los riesgos altos y extremos y su valor monetario esperado; costear los controles y las respuestas; proponer la reserva de contingencia.	Dueño del riesgo con Finanzas
5	Planificar respuestas	Elegir la estrategia de respuesta (capítulo 12), definir el plan de acción y el plan de contingencia, con responsable, fecha, costo e indicador.	Dueño del riesgo; aprueba el CEO según nivel
6	Implementar respuestas	Ejecutar los planes aprobados y registrar la evidencia. Cierra el vacío entre definir la respuesta y verificar si se ejecutó.	Dueño del riesgo
7	Monitorear	Registro mensual del estado de cada riesgo, sus KRIs y sus planes; identificación de riesgos nuevos y emergentes; reporte a los comités.	Dueño del riesgo; consolida la Coordinación de GC

Durante todo el ciclo se aplica la **comunicación y consulta** con las partes involucradas y el **registro** de cada decisión, conforme a la norma ISO 31000.

11. Metodología de valoración

11.1 Escala de probabilidad

Nivel	Descriptor	Criterio
5	Casi seguro	Ocurre o se espera que ocurra más de una vez al año; > 80 % de probabilidad en el horizonte evaluado.
4	Probable	Ha ocurrido en el Grupo en los últimos dos años o es probable que ocurra en el año; 51 %–80 %.
3	Posible	Ha ocurrido alguna vez en el Grupo o en el sector; 21 %–50 %.
2	Improbable	Podría ocurrir, pero no hay antecedentes recientes; 5 %–20 %.
1	Raro	Solo en circunstancias excepcionales; < 5 %.

11.2 Escala de impacto

El impacto se califica en la dimensión más afectada. Los montos financieros los fija Finanzas y los aprueba el Comité de Riesgos junto con la Declaración de Apetito de Riesgo.

Dimensión	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
Financiero (USD)	< []	[] – []	[] – []	[] – []	> [] o afecta covenants
Operación	Sin interrupción	Interrupción < 1 día en una planta	1–3 días en una planta	> 3 días o varias plantas	Paralización de un país o del Grupo
Legal y regulatorio	Observación sin sanción	Requerimiento de autoridad	Multa menor o hallazgo formal	Sanción relevante o suspensión de permiso	Cierre, responsabilidad penal o pérdida de licencia
Reputación	Sin trascendencia	Queja aislada	Cobertura local o de un cliente clave	Cobertura nacional o de inversionistas	Cobertura regional o internacional sostenida
Personas y SST	Primeros auxilios	Lesión sin incapacidad	Lesión con incapacidad	Lesión grave o permanente	Fatalidad
Ambiental y social	Efecto nulo, contenido en sitio	Efecto menor reversible	Efecto moderado o queja comunitaria	Daño significativo o conflicto con la comunidad	Daño grave irreversible

11.3 Mapa de calor y niveles de riesgo

Nivel de riesgo = probabilidad × impacto. Es la misma escala de la matriz regional de riesgos climáticos, de la Política LA/FT/FPADM (PO-CU-01), de la Política Antifraude (PO-CU-02) y del sistema de gestión de los riesgos de integridad, para que todos los riesgos del Grupo sean comparables.

Probabilidad \ Impacto	Insig. (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Posible (3)	3	6	9	12	15
Improbable (2)	2	4	6	8	10
Raro (1)	1	2	3	4	5

Nivel	Puntaje	Tratamiento mínimo
Extremo	21–25	Respuesta inmediata; plan aprobado por el CEO; informe al Comité de Riesgos en 48 horas.
Alto	16–20	Plan de respuesta obligatorio con análisis cuantitativo; seguimiento mensual; informe al Comité de Riesgos.

Nivel	Puntaje	Tratamiento mínimo
Moderado	11–15	Plan de respuesta con responsable y fecha; seguimiento por la gerencia del área.
Menor	6–10	Controles existentes y monitoreo periódico.
Bajo	1–5	Se acepta y se monitorea en la revisión anual.

Riesgos críticos. A efectos del escalamiento de este documento y del Reglamento del Comité de Auditoría (GC-RC-01, Art. 23), un riesgo es **crítico** cuando su nivel es **alto o extremo** (16 a 25).

11.4 Evaluación de controles y riesgo residual

Efectividad del control	Reducción del puntaje	Criterio
Fuerte	Hasta 3 niveles de probabilidad o impacto	Control documentado, automatizado o con evidencia, ejecutado siempre y probado.
Adecuado	Hasta 2 niveles	Control documentado, manual, ejecutado con regularidad.
Débil	1 nivel	Control informal o ejecutado ocasionalmente.
Inexistente	Ninguna	No hay control o no funciona.

11.5 Análisis cuantitativo

- Obligatorio para los riesgos **altos y extremos**; recomendado para los moderados.
- **Valor monetario esperado (VME)** = probabilidad (%) × impacto estimado (USD).
- Cada matriz registra el **costo del control actual** y el **costo de la respuesta propuesta**, para comparar costo y beneficio antes de aprobar.
- La suma de los VME de los riesgos aceptados orienta la **reserva de contingencia** que Finanzas propone en el presupuesto anual.
- Para riesgos complejos se pueden usar árboles de decisión, análisis de sensibilidad o simulación.

12. Estrategias de respuesta

Tipo de riesgo	Estrategias	Ejemplo en RAP
Amenazas	Evitar (eliminar la causa) · Mitigar (reducir probabilidad o impacto) · Transferir (seguros, contratos) · Aceptar (activa o pasivamente, con reserva) · Escalar (fuera de la autoridad del área)	Transferir el riesgo de incendio en planta con la póliza de propiedad; mitigar la pérdida de tarimas con conteos y cláusulas contractuales.
Oportunidades	Explotar · Mejorar · Compartir · Aceptar · Escalar	Aprovechar la valorización de residuos de madera; compartir con un aliado el desarrollo de una nueva línea.
Ambientales y sociales	Jerarquía de mitigación: evitar, luego reducir y, solo al final, compensar (P-SGAS-05 y R-SGAS-05)	Sustituir un químico peligroso antes de reducir su exposición.

- Todo plan de respuesta de un riesgo alto o extremo incluye un **plan de contingencia** con su señal de activación.
- La aceptación de un riesgo alto o extremo solo la puede decidir el CEO con el Comité de Riesgos, y queda documentada.
- Se identifican los **riesgos secundarios** que la propia respuesta genere.

13. Matrices de riesgos por departamento

Cada departamento es dueño de su matriz. La matriz es la base del sistema: sin matrices por área no hay matriz corporativa.

13.1 Reglas

- Todos los departamentos y gerencias de país elaboran su matriz en el **formato único** (Anexo A), con **costos por área**.
- Cada riesgo tiene un **dueño con nombre y cargo**; no se asignan riesgos a áreas genéricas.
- La matriz se actualiza **cada mes** en Smart Tools y se revisa completa **cada año**, o antes ante un cambio relevante, un incidente o un nuevo proyecto.
- Los riesgos que involucren a más de un área se identifican una sola vez, con un dueño principal y áreas de apoyo.
- Los riesgos altos y extremos pasan automáticamente a la matriz corporativa.

13.2 Fuentes que se integran en la matriz corporativa

Fuente	Responsable	Instrumento
Matrices de los departamentos y países	Dueños del riesgo	Formato del Anexo A en Smart Tools
Riesgos ambientales, sociales y climáticos	Especialista Regional de Sostenibilidad, Medio Ambiente y Social	P-SIG-01, P-SGAS-05 y R-SGAS-05; matriz regional de riesgos de cambio climático (NIIF S2)
Riesgos de seguridad y salud ocupacional	Coordinador Regional de Seguridad Industrial y Salud Ocupacional	Programa de SSO por país, registro de accidentabilidad e incidentes
Riesgos de cumplimiento e integridad	Oficial de Cumplimiento Regional	Matrices LA/FT/FPADM, antifraude y anticorrupción, integradas en el sistema de gestión de los riesgos de fraude, soborno, corrupción y LA/FT/FPADM (uso interno); en Colombia, matrices SAGRILAFT y PTEE
Riesgos de la cadena de distribución y APL	Operaciones, Logística y APL	Matriz de la cadena de distribución (capítulo 16)
Riesgos de proyectos	PMO (F11)	Registro de riesgos de cada proyecto
Hallazgos de auditoría e incidentes	Auditoría Interna, dueños del riesgo	Informes y registro de incidentes
Casos del Canal de Ética	Analista de Gobierno Corporativo	Estadística y causa raíz de los casos, con número de caso y clave de seguimiento (PR-CU-08)

14. Apetito, tolerancia, umbrales y escalamiento

14.1 Declaración de Apetito de Riesgo (RAS)

La aprueba el **Comité de Riesgos** cada año, junto con la revisión del plan estratégico y del presupuesto, e informa de ello a la Junta Directiva. Expresa, por categoría, cuánto riesgo acepta el Grupo: **cero tolerancia** a riesgos de integridad, de seguridad de las personas y de incumplimiento legal; apetito **bajo** en riesgos financieros que afecten los covenants; apetito **moderado** en riesgos operativos y comerciales asociados al crecimiento (Anexo D).

Secuencia obligatoria frente a la emisión de bonos

La RAS se calibra una vez que Smart Tools consolide el panorama real de riesgos y costos de todos los departamentos, para que parta de datos operativos y no de una estimación previa. Aun así, **la RAS debe quedar aprobada por el Comité de Riesgos antes de que se fijen los covenants financieros del Term Sheet** de cualquier emisión de bonos u otro instrumento de deuda. De esta forma, los covenants se negocian contra el apetito de riesgo propio del Grupo, y no al revés. Ningún equipo negociador acuerda covenants financieros sin la RAS vigente.

14.2 Umbrales y KRIs

Cada categoría tiene límites medibles y KRIs con tres zonas: verde (dentro del apetito), amarilla (alerta) y roja (fuera de tolerancia). Ejemplos: índice de pérdida de tarimas, días de cartera, margen frente al límite de covenants, accidentes con incapacidad, permisos por vencer en 90 días, proveedores críticos sin debida diligencia, disponibilidad de sistemas críticos.

14.3 Escalamiento

Situación	Se informa a	Plazo
Riesgo extremo o KRI en zona roja	CEO y Presidente del Comité de Riesgos	48 horas
Riesgo que afecta covenants o la información al mercado	CEO, Comité de Auditoría y Coordinación de GC	Inmediato
Riesgo alto nuevo o que sube de nivel	Comité de Riesgos	Siguiente sesión
Riesgo alto o extremo de integridad (fraude, soborno, corrupción, LA/FT/FPADM)	Comité de Auditoría directamente, con copia al Comité de Riesgos, conforme al sistema de gestión de esos riesgos y al GC-RC-01 (Art. 23)	Inmediato
Riesgo de conducta, convivencia o integridad no asociado a fraude	Oficial de Cumplimiento Regional y Comité de Ética y Conducta (desde oct. 2026; antes, Desarrollo Humano con Legal y aprobación del CEO)	Inmediato, por el Canal de Ética
Riesgo de fraude, corrupción o LA/FT/FPADM	Oficial de Cumplimiento Regional y Comité de Auditoría	Inmediato, por el Canal de Ética
Riesgo moderado	Gerencia del área	Registro mensual

14.4 Herramientas: Smart Tools y tablero

- **Smart Tools**, la plataforma web desarrollada internamente por Tecnología, es el repositorio único de las matrices: registro, dueños, controles, planes, costos y evidencias, con control de acceso y trazabilidad.
- **Ningún departamento carga su matriz directamente en Smart Tools.** Primero la completa en el formato único (Anexo A); la Analista de Gobierno Corporativo valida que contenga los campos mínimos del capítulo 13.1 y solo entonces la consolida, para que todas las matrices del Grupo sean comparables entre sí.
- El **tablero (dashboard)** muestra el mapa de calor del Grupo, por país, departamento y categoría, los KRIs, la evolución mensual y el avance de los planes.
- Hasta que Smart Tools esté en operación, las matrices se mantienen en el formato Excel único del Anexo A, custodiado por la Coordinación de Gobierno Corporativo.

15. Riesgos de sostenibilidad: ambientales, sociales y climáticos

- Se identifican y evalúan planta por planta, proceso por proceso y país por país, conforme a la **Norma de Desempeño 1 de IFC** y a los procedimientos P-SIG-01 y P-SGAS-05, con análisis de causa raíz e incorporación expresa de la **dimensión de género**.
- Se tratan con la **jerarquía de mitigación** —evitar, reducir, compensar— y se documentan en el Programa de Gestión de Riesgos Ambientales y Sociales (R-SGAS-05), con acción, indicador, fecha, responsable, recursos y procedimiento.
- Se valoran con la **misma escala 5x5** del capítulo 11 y se integran en la matriz corporativa, como exige la Política de Sostenibilidad y Responsabilidad Empresarial (PO-GC-01).
- Incluyen los **riesgos climáticos** físicos y de transición de la matriz regional elaborada bajo NIIF S2 y TCFD, revisada cada año y ante cualquier evento climático mayor.
- Incluyen los riesgos de **permisos y licencias** y de los compromisos que impone cada resolución, y los de la **cadena de madera** (origen legal, FSC, NIMF-15).
- Los riesgos de **seguridad y salud** de colaboradores y contratistas los gestiona el Coordinador Regional de Seguridad Industrial y Salud Ocupacional, conforme al capítulo 8.2, y se integran igualmente en la matriz corporativa.
- El **Comité ESG/RES y de Bono Verde** da seguimiento a estos riesgos y al PAAS, y los reporta al Comité de Riesgos, que conoce el panorama integral sin sustituir el circuito de aprobación propio de este programa.
- Los compromisos con BID Invest (PAAS e ICAS) que estén en riesgo se tratan como riesgo alto por su consecuencia contractual y financiera.

SGAS y PAAS: qué es cada uno

El **SGAS** (Sistema de Gestión Ambiental y Social) es el sistema de gestión en sí, exigido conforme a las ocho Normas de Desempeño de IFC. El **PAAS** (Plan de Acción Ambiental y Social, registro R-SGAS-05) es, además, **el instrumento contractual específico acordado con BID Invest, que forma parte integral del contrato de préstamo**: su incumplimiento persistente puede derivar en el retiro del apoyo financiero, y se divulga públicamente en el sitio de BID Invest junto con el resumen de la revisión ambiental y social del proyecto. Por su carácter contractual, el PAAS conserva un circuito de aprobación propio (ver recuadro siguiente), distinto del trámite ordinario de otros riesgos del Grupo.

Circuito de aprobación del Programa de Gestión de Riesgos Ambientales y Sociales (P-SGAS-05)

Este programa lo opera el **Coordinador de Calidad** (antes referido como “Coordinador de Sistemas de Gestión”), de la mano del Especialista Regional de Sostenibilidad. Sus planes de acción se aprueban mediante un circuito **propio y distinto** al del resto de riesgos del Grupo: evaluación de factibilidad financiera por **Finanzas Regional** y aprobación final del **Director General**, sin pasar por el Comité de Riesgos como instancia aprobatoria. El Grupo preserva este circuito porque es el que ya validó la banca multilateral; cada país incluye en su presupuesto anual, antes de la planeación del presupuesto corporativo, el monto estimado para sus planes de acción ambientales y sociales. Para efectos de visibilidad integral, los riesgos priorizados en este programa, con su costo de impacto y de solución, se trasladan también a la matriz corporativa (capítulo 13), sin que ello sustituya este circuito de aprobación.

16. Riesgos de la cadena de distribución y de American Pallet & Logistics (APL)

El modelo de pooling depende de que el activo circule y regrese. Por eso los riesgos de la cadena de distribución tienen una matriz propia, a cargo de Operaciones, Logística y APL, que se integra en la matriz corporativa.

Riesgo	Ejemplos y controles esperados
Pérdida, retención o uso no autorizado de tarimas	Conteos en puntos de venta, conciliación de saldos con clientes, cláusulas de reposición, guías de uso correcto.
Recuperación del activo	Índices de retorno por cliente y país, rutas de recolección, cobro de tarimas no devueltas.
Transporte y operadores logísticos	Siniestralidad de transportistas, fletes, disponibilidad de flota, acuerdos de seguridad en la cadena de suministro (contrabando, estupefacientes).
Trazabilidad y sistemas	Exactitud del registro de movimientos, disponibilidad de Smart Tools y SAP, integración con APL.
Clientes y concentración	Dependencia de grandes cadenas, crédito, cambios contractuales.
Fronteras y aduanas	Demoras, requisitos fitosanitarios NIMF-15, pagos de facilitación (prohibidos por la PO-DH-17).
Terceros de la cadena	Debida diligencia de transportistas, distribuidores y operadores conforme a la PO-CU-04 y al Procedimiento de Debida Diligencia de Terceros (PR-CU-04).
Riesgos propios de APL	Riesgos operativos, financieros, legales y de integridad de las sociedades de APL en Costa Rica, Guatemala y El Salvador, y operaciones con partes relacionadas conforme a la PO-CU-03. Riesgos aduaneros, cambiarios y de comercio exterior propios de la operación transfronteriza, con el Programa de Operador Económico Autorizado (OEA/AEO) de cada país como referencia de control cuando aplique.

La gestión de estos riesgos se apoya en **ISO 28000** (seguridad de la cadena de suministro) e **ISO 20400** (compras sostenibles), y en la trazabilidad y legalidad de la madera frente a **CITES** y, cuando corresponda por la presencia de clientes o inversionistas europeos, el **Reglamento Europeo de Deforestación (EUDR)**, en coordinación con el capítulo 8.2 de la Política de Integridad para Terceros (PO-CU-04).

17. Riesgos de integridad y cumplimiento

- El **Oficial de Cumplimiento Regional**, del Departamento de Gobierno Corporativo, identifica, evalúa y monitorea estos riesgos con la misma escala, y los entrega a la Coordinación para su consolidación. Lo hace mediante el **sistema de gestión de los riesgos de fraude, soborno, corrupción y LA/FT/FPADM** (documento de uso interno), que es la aplicación de esta política a esta categoría: define los esquemas de riesgo, los controles clave, las pruebas de eficacia, los indicadores y el informe trimestral.
- Incluyen corrupción y soborno (PO-DH-17), LA/FT/FPADM (PO-CU-01), fraude (PO-CU-02), conflictos de interés y partes relacionadas (PO-CU-03), terceros (PO-CU-04, PR-CU-04), regalos, contribuciones y donaciones (PO-CU-05 a PO-CU-07), derechos humanos y acoso (PO-DH-19, PO-DH-20), protección de datos, uso de IA y obligaciones regulatorias y del emisor en los ocho países.
- Su apetito es **cero tolerancia**; ningún riesgo de integridad se acepta sin plan de respuesta.
- Los riesgos **altos y extremos** de esta categoría se escalan de forma directa e inmediata al Comité de Auditoría (capítulo 14.3), sin esperar a la sesión conjunta anual con el Comité de Riesgos.

- Los casos del Canal de Ética (PR-CU-08) y sus causas raíz alimentan la identificación de nuevos riesgos (PO-CU-08). Los de conducta los conoce el Comité de Ética y Conducta; los de fraude, corrupción, soborno y LA/FT/FPADM, el Comité de Auditoría.
- En Colombia se integran las matrices del SAGRILAFT y del PTEE de COLESTIBAS.

18. Continuidad del negocio

- La Coordinación de Gobierno Corporativo (F06) coordina el **análisis de impacto al negocio** de los procesos críticos: producción y reparación, distribución y recuperación, sistemas, tesorería y cumplimiento del emisor.
- Para los riesgos extremos que puedan interrumpir la operación se establecen **planes de continuidad** y de recuperación, alineados con ISO 22301.
- Se integran con los planes de preparación y respuesta ante emergencias de cada planta (P-SGAS-06 e IM-PL-002) y con el plan de recuperación de Tecnología.
- Los planes se prueban al menos una vez al año mediante simulacros o ejercicios de mesa.

19. Riesgos de proyectos y del portafolio

- Todo proyecto del portafolio (F11) tiene su registro de riesgos, elaborado con el mismo ciclo PMBOK y la misma escala.
- Los proyectos estratégicos —emisión de bonos, expansión, nuevas plantas, sistemas— se evalúan antes de su aprobación y en cada fase.
- La PMO escala a la matriz corporativa los riesgos de proyecto que afecten los objetivos del Grupo.

20. Monitoreo, reporte e indicadores

Frecuencia	Qué se reporta	A quién
Mensual	Registro de cada matriz en Smart Tools: estado de riesgos, KRIs, planes y riesgos nuevos	Coordinación de Gobierno Corporativo
Trimestral	Mapa de calor del Grupo, riesgos altos y extremos, KRIs fuera de umbral, avance de planes y riesgos emergentes	Comité de Riesgos
Trimestral	Informe integrado de riesgos de integridad: riesgos de información financiera, fraude, soborno, corrupción y LA/FT/FPADM, eficacia de controles, indicadores e informe agregado del Canal de Ética	Comité de Auditoría
Semestral	Riesgos ambientales, sociales y climáticos y avance del PAAS	Comité ESG/RES y de Bono Verde, y Comité de Riesgos
Anual	Perfil de riesgos del Grupo, cumplimiento del apetito, eficacia del sistema y actualización de la RAS aprobada por el Comité de Riesgos	Junta Directiva

Indicadores del sistema: porcentaje de departamentos con matriz vigente y costeadas; riesgos altos y extremos con plan aprobado; planes ejecutados en plazo; KRIs dentro de umbral; riesgos materializados que no estaban identificados; hallazgos de auditoría sobre el sistema cerrados en plazo; **nivel de madurez de la gestión de riesgos** (evaluado cada año frente a esta política); y **porcentaje de pruebas de continuidad del negocio ejecutadas** frente a las programadas (capítulo 18).

21. Auditoría Interna

- Evalúa de forma independiente, al menos una vez al año, el diseño y la eficacia del sistema de gestión de riesgos y de sus controles, incluido el sistema de gestión de los riesgos de integridad.
- Elabora su plan anual con base en la matriz corporativa de riesgos; **lo propone el Comité de Auditoría y lo aprueba la Junta Directiva**, que también aprueba su presupuesto (GC-RJ-01, Art. 8).
- No elabora matrices ni diseña u opera controles, para preservar su independencia; puede asesorar sin asumir responsabilidades de gestión.
- Coordina con la segunda línea un esquema de aseguramiento combinado que evite duplicidades, conforme al capítulo 7 de la Política y Estatuto de Auditoría Interna (PO-GC-03).

22. Cultura, capacitación y comunicación

- Capacitación anual en la metodología a dueños de riesgo, puntos focales y gerencias; inducción para nuevos jefes, conforme al módulo 11 del Programa de Capacitación en Ética e Integridad (PG-CU-01).
- Formación a la Junta Directiva y a los comités sobre el perfil de riesgos del Grupo.
- Los riesgos se discuten sin temor: reportar un riesgo o un error a tiempo es una conducta esperada, no un motivo de sanción.
- La gestión de riesgos se incorpora en los objetivos de desempeño de las jefaturas.

23. Ruta de implementación y próximos pasos

El Comité de Riesgos acordó la siguiente secuencia. Esta política formaliza el paso 6, aunque los pasos se ejecutan de forma coordinada:



#	Paso	Entregable	Estado
1	Matrices	Matriz de riesgos de cada departamento, con costos por área	En curso
2	Smart Tools	Carga de las matrices en la plataforma web	Pendiente
3	Dashboard	Tablero con mapa de calor y KRIs	Pendiente
4	Apetito	Declaración de Apetito de Riesgo aprobada por el Comité de Riesgos	Pendiente
5	Umbral	Límites y KRIs por categoría	Pendiente
6	Política	Esta política, aprobada por el Comité de Riesgos	En aprobación
7	Implementar	Ejecución de los planes de mitigación	Pendiente

#	Paso	Entregable	Estado
8	Monitoreo	Registro mensual y reportes a los comités	Pendiente

23.1 Próximos pasos de madurez

Horizonte	Acción
2026–2027	Completar las matrices de todos los departamentos y países; aprobar la RAS y los umbrales; operar Smart Tools y el tablero; integrar la matriz de la cadena de distribución y APL; poner en marcha el sistema de gestión de los riesgos de integridad.
2027	Alinear formalmente el sistema con ISO 31000 mediante una autoevaluación; primera revisión del sistema por el Auditor Interno (que inicia el 19 de octubre de 2026); primer ejercicio de continuidad del negocio.
2027–2028	Adoptar COSO ERM 2017: apetito vinculado a cada objetivo estratégico, riesgo en la evaluación del desempeño y reporte integrado de riesgo, desempeño y sostenibilidad.
Continuo	Evaluación externa de madurez del sistema cada dos o tres años.

24. Documentos relacionados

- Código de Ética y Conducta (GC-CE-01); Política y Código de Gobierno Corporativo (GC-CG-01); Programa Regional de Integridad, Ética y Cumplimiento (PG-CU-00); Reglamento de la Junta Directiva (GC-RJ-01).
- Política de Sostenibilidad y Responsabilidad Empresarial (PO-GC-01); Política y Estatuto de Auditoría Interna (PO-GC-03).
- PO-SIG-01 Política de Sistemas Integrados de Gestión; P-SIG-01 Identificación y Evaluación de Riesgos e Impactos; P-SGAS-05 y R-SGAS-05 Programa de Gestión de Riesgos Ambientales y Sociales; P-SGAS-06 e IM-PL-002 Planes de emergencia.
- Matriz regional de riesgos de cambio climático y Matriz de Certificados y Otros Regionales.
- PO-DH-17 Anticorrupción y Antisoborno; PO-CU-01 LA/FT/FPADM; PO-CU-02 Antifraude; PO-CU-03 Conflictos de Interés y Partes Relacionadas; PO-CU-04 Integridad para Terceros; Procedimiento de Debida Diligencia de Terceros (PR-CU-04); PO-CU-08 Protección al Denunciante; Procedimiento de Quejas y Denuncias (PR-CU-08); Garantías al Denunciante (GC-DP-05); Política de Derechos Humanos (PO-DH-19); Política de Prevención del Acoso, la Discriminación y la Violencia en el Trabajo (PO-DH-20).
- Reglamentos del Comité de Riesgos (GC-RC-03) y del Comité de Auditoría (GC-RC-01).
- **Sistema de gestión de los riesgos de fraude, soborno, corrupción y LA/FT/FPADM** (documento de uso interno), que aplica esta política a la categoría de cumplimiento e integridad.
- Procedimiento de gestión de riesgos, Declaración de Apetito de Riesgo y plan de continuidad del negocio (en elaboración).

25. Incumplimiento

No elaborar o actualizar la matriz del área, ocultar un riesgo o un incidente, no ejecutar un plan de respuesta aprobado o alterar la información de riesgos son faltas que se atienden conforme al Código de Ética, a las Sanciones por Incumplimiento (GC-DP-06), al régimen disciplinario (PO-DH-24) y al reglamento interno de trabajo de cada país.

26. Disposiciones finales

- **Vigencia:** desde su aprobación por el Comité de Riesgos. La Junta Directiva es informada y recibe el informe anual del sistema.
- **Revisión:** al menos una vez al año, y antes ante un cambio estratégico, regulatorio o un riesgo materializado relevante. La coordina la Coordinación de Gobierno Corporativo con el Comité de Riesgos.
- **Publicación:** español e inglés, PDF abierto, sitio web corporativo → Gobierno Corporativo → Gestión de riesgos, e intranet.

Anexo A. Formato único de la matriz de riesgos del departamento

Campo	Contenido
Identificación	Código del riesgo, país, sociedad, departamento, proceso, fecha de identificación
Descripción	Causa → evento → consecuencia; tipo (amenaza u oportunidad); categoría de la taxonomía
Objetivo afectado	Objetivo estratégico u operativo que se vería afectado
Dueño	Nombre y cargo del dueño del riesgo; áreas de apoyo
Riesgo inherente	Probabilidad (1–5), impacto (1–5), dimensión del impacto y puntaje
Controles existentes	Descripción, tipo (preventivo o detectivo), efectividad y costo actual
Riesgo residual	Probabilidad, impacto y puntaje después de controles; nivel
Análisis cuantitativo	Impacto estimado en USD, VME, costo de la respuesta (altos y extremos)
Respuesta	Estrategia, acciones, responsable, fecha, costo, indicador y plan de contingencia con su señal de activación
KRI	Indicador, umbral verde / amarillo / rojo y valor del mes
Seguimiento	Estado del plan, evidencia, fecha de la última revisión y tendencia del riesgo

Anexo B. Técnicas recomendadas

Paso	Técnicas
Identificar	Lluvia de ideas, entrevistas, listas de verificación, revisión de incidentes y auditorías, lecciones aprendidas, análisis de supuestos, análisis FODA
Causa raíz	Árbol de problemas y escalera de por qué (P-SGAS-05), diagrama de Ishikawa, bow-tie
Análisis cualitativo	Matriz de probabilidad e impacto, evaluación de la calidad de los datos
Análisis cuantitativo	Valor monetario esperado, árbol de decisión, análisis de sensibilidad, simulación de Monte Carlo
Respuesta	Análisis costo-beneficio, análisis de alternativas, planes de contingencia
Monitoreo	KRIs, tablero, auditorías de riesgos, análisis de tendencias

Anexo C. Mapa de calor

Probabilidad \ Impacto	Insig. (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Posible (3)	3	6	9	12	15
Improbable (2)	2	4	6	8	10
Raro (1)	1	2	3	4	5

Verde: bajo (1–5) · Amarillo: menor (6–10) · Naranja: moderado (11–15) · Rojo: alto (16–20) · Rojo oscuro: extremo (21–25). Son riesgos críticos los de nivel alto y extremo.

Anexo D. Modelo de Declaración de Apetito de Riesgo

Categoría	Apetito	Criterio (a validar por el Comité de Riesgos)
Integridad, corrupción, fraude, LA/FT	Cero	No se acepta ningún riesgo residual sin plan de respuesta.
Seguridad y salud de las personas	Cero	Ninguna meta justifica exponer a las personas; fatalidades y lesiones graves fuera de tolerancia.
Cumplimiento legal y regulatorio	Cero	Permisos vigentes y obligaciones en plazo; sin tolerancia a incumplimientos conocidos.
Ambiental y social	Bajo	Sin daños significativos ni conflictos con comunidades; PAAS en plazo.
Financiero y covenants	Bajo	Margen mínimo de [] % frente a los límites de covenants; liquidez de [] meses.
Reputacional	Bajo	Sin afectaciones nacionales o regionales sostenidas.
Operativo y cadena de distribución	Moderado	Índice de pérdida de tarimas $\leq$ [] %; interrupciones < [] días.
Estratégico y crecimiento	Moderado	Nuevos mercados y proyectos con caso de negocio y evaluación de riesgos aprobados.
Tecnológico	Bajo	Disponibilidad de sistemas críticos $\geq$ [] %; sin fugas de información.

Anexo E. Equivalencia entre PMBOK, ISO 31000 y COSO ERM

PMBOK (en uso)	ISO 31000 (adoptada)	COSO ERM 2017 (próxima etapa)
1. Planificar la gestión de riesgos	Alcance, contexto y criterios	Gobierno y cultura · Estrategia y objetivos
2. Identificar	Identificación del riesgo	Desempeño: identificar el riesgo
3. Análisis cualitativo	Análisis y valoración del riesgo	Desempeño: evaluar la severidad y priorizar
4. Análisis cuantitativo	Análisis del riesgo	Desempeño: evaluar la severidad
5. Planificar respuestas	Tratamiento del riesgo	Desempeño: implementar respuestas
6. Implementar respuestas	Tratamiento del riesgo	Desempeño: implementar respuestas
7. Monitorear	Seguimiento, revisión, registro e informe	Revisión y ajuste · Información, comunicación y reporte
Transversal	Comunicación y consulta · Liderazgo y compromiso	Gobierno y cultura