PADTEC HOLDING S.A.

POLÍTICA DE GESTIÓN DE RIESGOS CORPORATIVOS

1. Objectivo

Esta Política Corporativa de Gestión de Riesgos ("Política") De Padtec Holding S.A. ("Compañía" o "Padtec") Tiene como objetivo estipular los lineamientos, principios, roles y responsabilidades en la gestión de riesgos corporativos, así como el desarrollo, difusión e implementación de la cultura de gestión de Riesgos, orientando los procesos de identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de los Riesgos mapeados, con el objetivo de promover la mejora continua de los procesos de la Compañía y obtener mejores resultados.

Esta Política contempla también a las sociedades controladas y coligadas de la Compañía, especialmente a Padtec S.A.

2. Cobertura

Esta Política se aplica a todos los macroprocesos, operaciones comerciales y áreas de la Compañía, y su cumplimiento por parte de la Administración, los miembros del Comité de Auditoría y todos los colaboradores es obligatorio.

3. Definiciones

"Administración" - Junta Directiva y Junta Ejecutiva de la Compañía.

"Análisis de Riesgo" **-** es el proceso de comprender la naturaleza de cierto riesgo y determinar la Probabilidad de que se materialice, lo que da como resultado cuánto estaría expuesta la Compañía a ese riesgo en particular.

"Apetito de Riesgo" - es el nivel de exposición al riesgo que la Compañía está dispuesta a aceptar para lograr sus objetivos dentro de los límites establecidos por la Administración.

"Evaluación de Riesgos" - es el proceso de comparar los resultados obtenidos en el Análisis de Riesgos con los criterios establecidos por la Administración, de acuerdo con esta Política, para determinar si el Riesgo y/o su magnitud son aceptables o tolerables por la Compañía.

"Compañía" - es Padtec Holding S.A. y sus subsidiarias, especialmente Padtec SA

"Controles" - son las acciones que realiza la Compañía con el objetivo de reducir los riesgos inherentes a las actividades que desarrollan las unidades de negocio y otras áreas, pudiendo ser periódicas o continuas. Estas acciones ayudarán a los respectivos órganos de la Compañía y sus colaboradores, según sea el caso, a monitorear los niveles de exposición de cada uno de estos Riesgos.

"Evento" - es la ocurrencia o cambio en un conjunto específico de circunstancias que resultan en la materialización de un Riesgo.

"Fuente de Riesgo" - son los elementos que, individualmente o en combinación, tienen el potencial intrínseco de dar origen a un Riesgo determinado.

"Gestión de Riesgos" - es el conjunto de actividades coordinadas y estructuradas con el fin de alinear el Apetito de Riesgo con el ciclo de toma de decisiones estratégicas en la búsqueda de la mitigación de Riesgos y optimización de los resultados a alcanzar por la Compañía.

"Plan de Acción" - es la forma organizada, según una determinada metodología previamente definida por las áreas de Controles Internos y Auditoría Interna, según sea el caso, en la que se describen las metas y objetivos, así como las actividades que se deben realizar para el tratamiento de un determinado Riesgo, ya sea para evitarlo, aceptarlo, reducirlo, eliminarlo o transferirlo.

"Probabilidad": indica la posibilidad de que ocurra un evento determinado. Puede expresarse en términos cuantitativos, como: porcentaje, frecuencia de ocurrencia u otra métrica numérica, o en términos cualitativos, como: alto, medio, bajo.

"Propietario del riesgo": tiene la definición en el "Paso 2" del ítem 7 de esta Política.

"Riesgo (s)" - son los factores y/o eventos que pueden causar impactos negativos, comprometiendo la capacidad de la Compañía para lograr sus objetivos estratégicos y la creación y protección efectiva de su valor.

"Tratamiento del Riesgo" - es el proceso de modificación del Riesgo, que puede ser la acción de (i) evitar el Riesgo al decidir no iniciar o descontinuar la actividad que da lugar al Riesgo; (ii) asumir o incrementar el Riesgo, con el fin de buscar una oportunidad para la Compañía; (iii) eliminación de la Fuente de Riesgo; (iv) el cambio en la probabilidad; (v) cambiar las consecuencias esperadas; (vi) compartir el Riesgo

con otras partes; y/o (vii) la retención del Riesgo debido a una elección consciente de la Compañía.

4. Funciones y Responsabilidades

FUNCIÓN	RESPONSABILIDADES
Consejo de Administración	• Establecer las directrices generales de Riesgos alineadas al contexto del negocio y del ciclo de planeamiento estratégico de la Compañía; • Establecer, por medio de la capacidad y tolerancia de la Compañía, los límites aceptables de Propensión de Riesgos; • Evaluar, deliberar y aprobar la matriz de riesgos estratégicos y priorizados, alineados a la Propensión de Riesgos de la Compañía; • Definir y revisar los criterios y estrategias de la Gestión de Riesgos; • Evaluar, anualmente, la suficiencia de la estructura y del presupuesto del área de Auditoría Interna para el desempeño de sus funciones, conforme a la recomendación del Comité de Auditoría; • Evaluar y deliberar sobre los informes realizados por la Auditoría Interna, por medio del Comité Estatutario de Auditoría y Riesgo; • Revisar y aprobar las definiciones generales de las estrategias de la Gestión de Riesgos; • Garantizar para el Comité Estatutario de Auditoría y Riesgo la autonomía operativa y aprobación del presupuesto propio destinado a cubrir los gastos con su funcionamiento – que será incluido en los valores del presupuesto general anual de la Compañía; • Aprobar y modificar la presente Política, sus evoluciones y revisiones futuras.
Comité Estatutario de Auditoría y Riesgo	• Acompañar las actividades del área de Auditoría Interna y del área de Controles Internos de la Compañía; • Evaluar y monitorear las exposiciones a los Riesgos de la Compañía; • Proponer para el Consejo de Administración las definiciones y directrices para componer el modelo de Gestión de Riesgos de la Compañía; • Proponer para el Consejo de Administración los niveles de tolerancia a la exposición de los Riesgos; • Acompañar y apoyar el proceso de Gestión de Riesgos en la definición de los Riesgos priorizados alineados al contexto del negocio y las directrices del Consejo de Administración; • Supervisar las actividades de Gestión de Riesgos siguiendo el cumplimiento de las legislaciones vigentes y de las políticas, normas y procedimientos internos de la Compañía; • Evaluar, monitorear e informar periódicamente al Consejo de Administración sobre los Riesgos priorizados identificados por las revisiones de los Propietarios de los Riesgos en el proceso de Gestión de Riesgos, auxiliando en la evaluación de los planes de acción y elaboración de las recomendaciones; • Evaluar, aprobar y acompañar la ejecución del tratamiento y monitoreo de los Riesgos; • Evaluar, aprobar y recomendar para la Administración la corrección o perfeccionamiento de las políticas internas de la Compañía; • Evaluar las informaciones trimestrales, estados intermedios y estados financieros anuales de la Compañía; • Entregar para el Consejo de Administración, para su deliberación, los informes realizados por la Auditoría Interna; • Realizar recomendaciones, anualmente, para el Consejo de Administración, sobre la suficiencia de la estructura y del presupuesto del área de Auditoría Interna.
Dirección	• Promover la integración y la cultura de Riesgos en la Compañía y en los ciclos de gestión y de planeamiento estratégico; • Garantizar la implantación de un modelo eficiente de Gestión de Riesgos, alineado a los objetivos y metas de la Compañía. Aplicar las directrices generales establecidas por el Consejo de Administración

	para atribuir el nivel de Propensión a los Riesgos aceptable para la Compañía; • Acompañar los Riesgos administrados en cada etapa del proceso y garantizar la efectividad de las medidas de Control; • Participar de los rituales de validación y priorización de los Riesgos de la Compañía junto con el Comité Estatutario de Auditoría y Riesgo; • Evaluar y monitorear el Tratamiento de los Riesgos alineado a la ejecución del planeamiento estratégico de la Compañía; • Evaluar, tempestivamente, la eficacia y la aplicabilidad de las directrices de esta Política; • Evaluar y apoyar las adecuaciones de la estructura destinada al proceso de gestión de Riesgos, considerando los recursos humanos, financieros y tecnológicos; y • Monitorear, evaluar y supervisar las actividades de la 1ª y de la 2ª Línea de Defensa.
Área de Compliance	• Orientar el análisis de los Riesgos de terceros, de modo a mitigar los posibles Riesgos de corrupción, fraude, conflictos de interés y medios de comunicación negativos, garantizando el cumplimiento de las leyes y reglamentos de anticorrupción vigentes, de acuerdo con la matriz de Riesgos priorizados; • Monitorear los análisis de Riesgos realizados con base en el nivel de clasificación de los Riesgos; • Auxiliar en la elaboración y adecuación de las normas, políticas y procedimientos de tal forma para reducir la exposición a los Riesgos del negocio; y • Diseminar la cultura de Compliance, por medio de las capacitaciones y comunicaciones, garantizando el cumplimiento de las leyes y reglamentos existentes, del Código de Ética y Conducta y de las demás normas y procedimientos internos, buscando mitigar los Riesgos identificados.
Área de Controles Internos	• Auxiliar a las demás áreas de la Compañía en la implementación de las mejorías de los Controles y procesos; • Apoyar a las demás áreas de la Compañía en la implementación de los Planes de Acción y en la remediación de los puntos identificados en el proceso de la Gestión de Riesgos; • Participación en las auditorías interna y externa; y • Auxiliar a las demás áreas en las mejorías de los Controles y procesos.
Área de Gestión de Riesgos	• Garantizar la operatividad de la Gestión de Riesgos; • Realizar el mapeo de los Riesgos; y • Auxiliar a las demás áreas de la Compañía en la identificación y evaluación de los Riesgos.
Líderes de las áreas de apoyo y de negocio (back office y front office)	• Identificar, clasificar y gerenciar los Riesgos de las respectivas áreas de acuerdo con las estrategias de mitigación, en conjunto con el área de Controles Internos; • Indicar a un profesional que responderá como facilitador de la Gestión de Riesgo junto al área de Controles Internos; • Prestar cuentas de los niveles de exposición, de los Planes de Acción y de los indicadores que describen el nivel de los Riesgos para los que fuera responsable; • Poseer un conocimiento técnico de los procesos en el cual los Riesgos se encuentran identificados; • Ser el responsable por la actualización de las informaciones del mapeo y tratamiento de los Riesgos de su unidad de negocio; • Mantener las informaciones actualizadas tempestivamente, respetando el calendario de planeamiento del ciclo de la Gestión de Riesgos; y • Monitorear el estado de los Planes de Acción junto con los responsables por la implementación de los dispositivos de Control.
Área de Auditoría Interna	• Evaluar la calidad y la efectividad de los procesos de gerenciamiento de Riesgos, Control y gobernanza corporativa de la Compañía; • Identificar y apuntar oportunidades de mejorías en los procesos de Controles Internos y de Gestión de Riesgo; • Reportar periódicamente para el Comité Estatutario de Auditoría y Riesgo y para sus clientes auditados los resultados de las evaluaciones

	independientes, imparciales y tempestivas sobre la efectividad de la Gestión de Riesgos en la Compañía; • Elaborar el planeamiento y garantizar la operatividad de la Gestión de Riesgos; • Elaborar y realizar el plan de Auditoría Interna, por sector de la Compañía, de acuerdo con los riesgos previamente mapeados y priorizados; • Evaluar la eficiencia de los Controles Internos, con la medición del potencial impacto y probabilidad de una eventual falla de los Controles; • Evaluar y proponer estrategias de Control; y • Apoyar a las áreas para la implantación de mejorías de los Controles y procesos internos. • Revisión y apoyo en la elaboración de las normas, políticas y manuales de procedimiento vinculados a los procesos que estuvieran siendo auditados; • Realizar el acompañamiento y control del *follow-up* de los principales puntos reportados en las Auditorías internas.
Todos los colaboradores de la Compañía	• Garantizar la operatividad de la Gestión de Riesgos, formando parte del proceso de identificación, evaluación y mensuración, e implementando las acciones preventivas y correctivas; y • Participar de las capacitaciones que permitan la diseminación, de forma consciente, de la cultura de Gestión de Riesgos.

La estructura del gerenciamiento de Riesgos de la Compañía será conducida por las siguientes áreas/responsables, además de contar con la participación efectiva de los miembros del Comité Estatutario de Auditoría y Riesgo, de la Dirección y del Consejo de Administración:

- Compliance: esta función será desempeñada por la Dirección Jurídica y Secretaría General, cuyo(a) ocupante será el(la) Compliance Officer de la Compañía, subordinado al Consejo de Administración;
- Auditoría Interna: esta función será desempeñada por el área de Auditoría Interna reportándose directamente a la Presidencia y al Comité Estatutario de Auditoría y Riesgo;
- Controles Internos: esta función será desempeñada por el área de Controles Internos, reportándose a la gerencia de Tecnología de la Información/Calidad Corporativa, que por su vez está subordinada a la Dirección Financiera.
- Gestión de Riesgos: esta función será desempeñada por el área de Planeamiento Estratégico reportándose al responsable por el área de Contraloría, que por su vez está subordinada a la Dirección Financiera.

5. Lineamientos y Líneas de Defensa de la Compañía

Esta Política tiene como directriz general el compromiso con la propuesta de valor de la Compañía, que, en línea con las demás políticas corporativas y el Código de Ética y Conducta, busca crear una cultura de Gestión de Riesgos eficiente e integrada,

involucrando a la Administración y a todos los colaboradores en el proceso de identificación, evaluación y mitigación de los Riesgos identificados.

La Gestión de Riesgos forma parte de la estructura de gobierno corporativo de la Compañía, integra el proceso de toma de decisiones y contribuye a la ejecución de su estrategia. Los riesgos se identifican y tratan con el fin de asegurar el cumplimiento de las metas establecidas para cada ciclo de planificación estratégica.

Para ello, la estructura de Gestión de Riesgos considera el desempeño conjunto de los órganos de gobierno corporativo y de gestión, de acuerdo con el concepto de las tres líneas de defensa, de acuerdo con las competencias que se describen a continuación:

- **1ra línea de defensa (Liderazgo - *front y back offices*)**

→ Incluye la Gestión Operativa, representada por los directores, gerentes y demás empleados de las unidades de negocio que operan en las operaciones y tareas del día a día.

→ Los colaboradores que laboran en la 1ra Línea de Defensa tienen propiedad sobre los Riesgos y son responsables de implementar acciones correctivas con el fin de resolver deficiencias en el Control y procesos, mitigando los Riesgos relacionados con las actividades que realizan.

→ Estos empleados juegan un papel fundamental en el apoyo a la 2da Línea de Defensa en el proceso de identificación del mapeo de riesgos, así como en el proceso de implementación de los Planes de Acción definidos por el área de Gestión de Riesgos y Controles Internos o por el área de Auditoría Interna.

→ Los Gerentes son responsables de la gestión de los Riesgos inherentes a los procesos bajo su responsabilidad desde la identificación, evaluación, seguimiento y tratamiento de estos Riesgos, con la participación de las demás áreas a involucrarse, de acuerdo con la división de competencias prevista en esta Política.

→ Informar a la 2da Línea de Defensa (área de Gestión de Riesgos, Controles Internos y Compliance) sobre los riesgos inherentes a las actividades que realiza la 1ra Línea de Defensa que aún no están cubiertos por Controles que mitiguen su probabilidad de ocurrencia y/o impacto.

→ Implementación y seguimiento de Planes de Acción para abordar las deficiencias identificadas en los respectivos procesos.

- Informe de la ocurrencia de materialización de riesgos a la 2da Línea de Defensa (área de Gestión de Riesgos, Controles Internos y Compliance) de forma inmediata para tratamiento y elaboración de Planes de Actuación.

- **2da Línea de Defensa (áreas de Gestión de Riesgos, Controles Internos y Cumplimiento)**

- La 2da Línea de Defensa tiene carácter preventivo en relación a Riesgos, con énfasis en controles internos y *cumplimiento* de las leyes y reglamentos aplicables a la Compañía, así como en relación con los aspectos de control, con el seguimiento de los riesgos financieros y las cuestiones de información financiera.
- Debe orientar, monitorear y evaluar el cumplimiento de los estándares y políticas definidas y apoyar a la 1ra Línea de Defensa para lograr los objetivos establecidos por la Compañía.
- Debe asesorar a la 1ra Línea de Defensa en los aspectos de controles internos, procedimientos, estándares y políticas de gestión de soporte, definir roles y responsabilidades, identificar cambios en el Apetito de Riesgo de la Compañía, asistir en la construcción de procesos, Controles y procedimientos.
- Facilitación, comunicación y seguimiento de las prácticas de Gestión de Riesgos y asistencia en la identificación de Riesgos de acuerdo al Apetito de Riesgo establecido por la Administración.
- Evaluación de la vulnerabilidad del entorno de Controles de los procesos de la Compañía mediante pruebas de efectividad.
- Seguimiento de la implementación de los Planes de Acción para las fallas identificadas.
- Elaboración del planeamiento de la Gestión de Riesgos.

- **3ra Línea de Defensa (área de Auditoría Interna)**

- Proporciona a los órganos de gobierno y dirección de la Compañía evaluaciones estructuradas de los Riesgos mapeados, con base en los eventos y consecuencias relacionadas, de manera independiente y objetiva dentro de la Compañía.
- De forma detectivesca, proporciona evaluaciones del *estado* de la gobernanza, controles internos estructurados y cómo este escenario impacta los objetivos de la Compañía, teniendo en su alcance la evaluación de la eficiencia y efectividad de la operación, salvaguardando los activos, confiabilidad de la información,

integridad de los procesos, cumplimiento de leyes, regulaciones, políticas y procedimientos, análisis de los procesos de las áreas de negocio y soporte de la Compañía.

- Elaboración y operacionalización del plan de auditoría interna, por área de la Compañía, de acuerdo a los riesgos previamente mapeados y priorizados.
- Evaluación de la eficiencia de los controles internos, con la medición del potencial impacto y probabilidad de una eventual falla de los Controles. A los controles deficientes deben ser vinculadas las deficiencias de los Controles, siéndoles recomendado a los gestores de las áreas responsables la creación de Planes de Acción para la mitigación de los respectivos riesgos.
- Identificación de las Ausencias de Controles internos, con recomendación para los gestores de las áreas responsables de la creación de los planes de acción, que resulten en la elaboración de los controles internos para la mitigación de los respectivos riesgos.
- Identificación de los apuntamientos generales sobre los procesos auditados, con recomendación para los gestores de las áreas responsables de la creación de los planes de acción para la mitigación de los respectivos riesgos.
- Acompañamiento de los Planes de Acción sobre las deficiencias, ausencias de controles internos y apuntamientos generales, identificados por la Auditoría Interna.

A continuación, se detalla el modelo de tres líneas de Defensa que operan en la Compañía:

6. Categorización de Riesgos

Los Riesgos a los que está expuesta la Compañía se categorizan con el fin de estandarizar interna y externamente las referencias a los distintos Riesgos que puedan impactar sus actividades. La categorización de Riesgos facilita el proceso de división organizado de acuerdo a las respectivas naturalezas, también debido a los segmentos en los que opera la Compañía que se ven afectados por los Eventos de diferente manera.

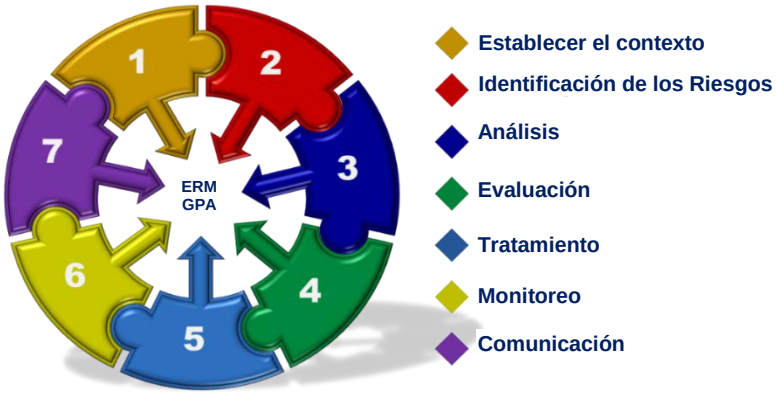
En este sentido, la Compañía categoriza a los Riesgos de la siguiente forma:

CATEGORÍA DE LOS RIESGOS	DESCRIPCIÓN DE LA CATEGORÍA DE LOS RISCOS
ESTRATÉGICO	Riesgos asociados a la toma de decisiones por parte de la Administración de la Compañía cuya materialización puede generar la pérdida substancial del valor económico, del capital o de participación en el mercado de la Compañía, como consecuencia del planeamiento y/o decisiones erróneas, usualmente relacionados a las estrategias del negocio/participación en el mercado, inversiones, sucesión, innovación y competición. Son, por lo tanto, Riesgos que pueden perjudicar al núcleo del modelo de negocios de la Compañía. Desafían la lógica de las elecciones estratégicas, amenazan a la competitividad y perjudican la capacidad de alcanzar o mantener un desempeño excepcional.
OPERATIVO	Son Riesgos derivados de las fallas de los procesos y Controles, falta de consistencia y adecuación de los sistemas de información, bien como oriundos de errores o fraudes que perjudican o imposibilitan el ejercicio de las actividades de la Compañía. Los riesgos operativos generalmente conllevan a la reducción, degradación o interrupción, total o parcial, de las actividades de la Compañía, con un posible impacto negativo de reputación y financiero además de una potencial generación de pasivos contractuales, reglamentarios y ambientales. Además, también se incluyen los riesgos financieros que pueden afectar de forma adversa a las finanzas de la Compañía, asociados a la exposición de las operaciones financieras y relacionados a las variaciones de los valores de sus activos y pasivos, incumplimiento de las obligaciones financieras de contrapartes, alto costo o incapacidad para cumplir las obligaciones financieras, ineficiencia en la asignación del capital y fallas en los informes y reportes financieros.

7. Proceso de Gestión de Riesgos

El proceso de Gestión de Riesgos de la Compañía se definió con base en los lineamientos de COSO - *Comité de Organizaciones Patrocinadoras de la Comisión Treadway* e ISO 31000: 2018 - Principios y Directrices de Gestión de Riesgos.

En este contexto, el proceso de Gestión de Riesgos es um proceso continuo y parte integral del desarrollo de las actividades de la Compañía, incorporado a la cultura y prácticas organizacionales y adaptado a los procesos de negocio, que consta de los siguientes pasos posteriores y dependientes:



<u>Paso 1</u>: Establecer el contexto

Fase inicial del proceso continuo de Gestión de Riesgos, que articula los objetivos estratégicos de la Compañía con los parámetros externos e internos que se tendrán en cuenta, estableciendo el alcance y los criterios de Riesgo para el resto del proceso.

Busca comprender el escenario y contexto empresarial considerando factores vinculados a la planificación estratégica a corto y largo plazo de la Compañía, en línea con el entorno en el que se insertan estos objetivos.

Es un paso fundamental para asegurar que el proceso de Gestión de Riesgos esté alineado con los ciclos de gestión y planificación estratégica de la Compañía para alinear sus niveles aceptables de Apetito por el Riesgo.

Para establecer los escenarios que deben sustentar esta etapa, se consideran los factores influyentes tanto del Contexto Externo como del Contexto Interno.

Contexto Externo

El Contexto Externo es el entorno externo en el que la Compañía busca lograr sus objetivos. Incluye, pero no se limita a: (a) entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; (b) factores y tendencias clave que tienen un impacto en los objetivos de la organización; y (c) relaciones con grupos de interés externos y sus percepciones y valores.

Generalmente, la Compañía no puede intervenir directamente en el Contexto Externo, teniendo una acción predominantemente reactiva. Sin embargo, siguiendo los lineamientos de esta Política, la Compañía debe buscar mitigar cualquier impacto de los Eventos materializados en el Contexto Externo.

Contexto Interno

Consiste en el ambiente interno de la Compañía, basado en la cultura organizacional, procesos, estructura y estrategias de la Compañía, en los siguientes niveles, pero no limitado a: (a) cultura; (b) reglas, lineamientos y modelos adoptados por la Compañía; (c) gobernanza, estructura organizativa, funciones y responsabilidades; (d) políticas, objetivos y estrategias implementadas para lograrlos; (e) capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías); (f) sistemas de información, flujos de información y procesos de toma de decisiones (formales e informales); (g) relaciones con los grupos de interés internos, y sus percepciones y valores; y (h) relaciones contractuales.

La atención a los Contextos Internos y Externos puede ayudar a asegurar que la Gestión de Riesgos sea adecuada a las circunstancias, la Compañía y los Riesgos que realmente impactan en relación al alcance real de sus objetivos estratégicos.

Paso 2: Identificación de los Riesgos

El enfoque de identificación de Riesgos es *top-dpwn*, a partir de entrevistas con los principales ejecutivos de las unidades de negocio, teniendo en cuenta los principales procesos de los que son responsables.

El producto generado en este paso es una lista completa de Riesgos basada en eventos que pueden identificar vulnerabilidades y amenazas que ponen en riesgo el logro de los objetivos estratégicos de la Compañía.

En esta etapa también se debe definir el titular y el responsable de cada uno de los Riesgos identificados (Dueño del Riesgo), así como una descripción que guiará las próximas etapas del mapeo.

Aún en esta etapa, se mapean todos los Riesgos asociados a las actividades de la Compañía, estén o no bajo su Control.

Paso 3: Análisis de los Riesgos

A partir de la conclusión de la Etapa 2, los Riesgos identificados son analizados de forma detallada, con el objetivo de obtener una mayor claridad y respaldo cualitativo y cuantitativo que generen variables que auxiliarán en la clasificación de los Riesgos para que la Compañía pueda actuar de forma más asertiva en su priorización y en la elaboración de los Planes de Acción.

En esta etapa, son definidos, entre otros, las causas o factores de Riesgos, bien como sus posibles efectos en el caso de la materialización de un determinado Evento. Además también, la Compañía realiza la clasificación de los factores agravantes de cada uno de los Riesgos identificados para asegurar la asertividad de sus Controles.

De esta forma, son levantadas las informaciones con el objetivo de la obtención de los datos que pudieran describir la probabilidad, impactos, y la clasificación de los Riesgos identificados, generándose así una matriz cualitativa para describir de forma ejecutiva el universo de Riesgos con base en sus clasificaciones. Dentro de la matriz cualitativa, los Riesgos son clasificados de acuerdo con los siguientes criterios:

IMPACTO	ASPECTOS CUALITATIVOS	PROBABILIDAD	ASPECTOS CUALITATIVOS
ALTO	- Impacto superior al 5% del ingreso líquido anual, comprometiendo la sustentabilidad financiera de la empresa; - Interrupción total o significativa de las operaciones, afectando la cadena productiva y la entrega de productos o servicios en el mercado; - Incumplimiento grave de las normas reglamentarias, pudiendo generar penalizaciones severas, multas elevadas o restricciones para la operación; - Exposición negativa significativa en los medios de comunicación, pérdida de	**ALTA**	- El evento ya sucedió en un pasado reciente o sucede con frecuencia. - Hay fallas significativas en los controles internos existentes o ausencia de controles preventivos. - No existen procesos, políticas y procedimientos formalizados y actualizados; - Evidencias de un historial de fraudes, errores o no conformidades relacionadas al riesgo en cuestión.

IMPACTO	ASPECTOS CUALITATIVOS	PROBABILIDAD	ASPECTOS CUALITATIVOS
	confianza de los clientes y stakeholders, comprometiendo la credibilidad de la empresa.		
MEDIO	- Impacto entre el 1% y 5% del ingreso líquido anual, causando ajustes financieros relevantes, pero sin comprometer a la operación de forma irreversible. - Interrupción parcial de las operaciones, con impacto gestionable dentro de plazos razonables; - No conformidades que resultan en sanciones moderadas o exigen adecuaciones relevantes para evitar impactos futuros; - Exposición moderada, con impacto en la percepción del mercado, pero factible de mitigación con acciones estratégicas	MODERADA	- El evento ya sucedió en el pasado, pero sin una recurrencia frecuente. - Existen controles internos implementados, pero con fallas u oportunidades de mejorías. - Existen procesos, políticas y procedimientos formalizados, sin embargo están desactualizados. - El riesgo puede ser activado por factores internos o externos bajo determinadas condiciones
BAJO	- Impacto inferior al 1% del ingreso líquido anual, con reflejos financieros mínimos y absorbidos por las operaciones normales de la empresa; - Pequeña disrupción operacional, sin impacto relevante en la entrega o calidad de los productos y servicios; - Pagos de multas u otras penalizaciones de pequeña relevancia; - Impacto puntual y de corta duración, sin consecuencias relevantes para la imagen corporativa.	BAJA	- El evento nunca ocurrió o hay raros registros de ocurrencia; - Controles internos son robustos, testeados y considerados efectivos; - El riesgo depende de circunstancias excepcionales para que ocurra. - - No existen procesos, políticas y procedimientos formalizados; - El historial de auditorías y revisiones no indica fallas o problemas relevantes.

Después de la definición del impacto y probabilidad del Riesgo, se genera automáticamente su clasificación, que puede ser BAJO, MEDIO o ALTO. Conforme a la matriz descripta abajo:

PROBABILIDADE				
	ALTA	MÉDIA	ALTA	ALTA
	MÉDIA	BAIXA	MÉDIA	ALTA
	BAIXA	BAIXA	BAIXA	MÉDIA
		BAIXO	MÉDIO	ALTO
		IMPACTO		

Campinas
Rua Doutor Ricardo Benetton Martins, 1.000
Parque II do Polo de Alta Tecnologia
Campinas • SP • CEP 13.086-510

+55 19 2104-9700
+55 19 2104-9703
padtec@padtec.com.br

A continuación, se deben atribuir los grupos. En un análisis de Riesgos, grupos de Riesgos son categorías que agrupan tipos semejantes de amenazas que pueden impactar al negocio de diferentes formas. Esta categorización ayuda en la identificación, evaluación y gerenciamiento de los Riesgos de forma organizada, permitiendo que la Compañía adopte las medidas eficaces para mitigar o controlar estos Riesgos.

En la Compañía los grupos de Riesgos están divididos en:

Acceso: Se refiere a los Riesgos asociados a la gestión de permisos y control del acceso a la información, sistemas e instalaciones. Sirve para proteger datos sensibles y garantizar la seguridad de la infraestructura tecnológica y física de la Compañía y de sus negocios. Es importante destacar que la Compañía posee una Política de Privacidad y Protección de Datos Personales que atiende y cumple con todos los requisitos de la Ley General de Protección de Datos Personales (LGPD), Ley nº 13.709, de 14 de agosto de 2018.

Administrativo: Contempla los Riesgos relacionados a las fallas o ineficiencias en los procesos administrativos y gerenciales, como problemas de comunicación, gestión inadecuada de recursos humanos y decisiones de gestión deficientes. Esencial para garantizar la operación eficiente y la conformidad interna.

Aduanero: Abarca los Riesgos asociados a los procesos de importación y exportación, incluyendo el cumplimiento de las reglamentaciones aduaneras y el cobro de las multas. En el caso de que estos Riesgos no fueran debidamente mitigados, pueden ocasionar problemas operativos, legales y perjuicios financieros. La falla en la gestión de estos Riesgos de forma eficaz puede comprometer los costos y tiempos de entrega de los productos de la Compañía para los clientes finales y la manutención del Certificado de Operador Económico Autorizado (OEA), esencial para la continuidad de sus operaciones de comercio exterior. Para asegurar la conformidad con las legislaciones vigentes y la preservación del Certificado OEA, los Riesgos Aduaneros son rigurosamente monitoreados por el gestor designado y están sujetos a las auditorías frecuentes conducidas por el área de Auditoría Interna.

Ambiental: Incluye los Riesgos relacionados a los impactos ambientales y a la sostenibilidad, como desastres naturales, contaminación y modificaciones reglamentarias ambientales. Sirve para mitigar las consecuencias negativas y mantener la conformidad con las leyes ambientales y con la actuación de la Compañía ante la sociedad.

Cibernético: Se refiere a las amenazas de seguridad digital, como los ataques de *hackers*, fuga de datos y *malwares*. Fundamental para proteger la integridad y la confidencialidad de los datos de la Compañía y de su público relacionado cuando son compartidos con la Compañía.

Cliente: Riesgos relacionados al comportamiento y expectativas de los clientes y potenciales clientes, incluyendo los cambios en la demanda, insatisfacción y pérdida de clientes. Importante para mantener la fidelidad, recurrencia de los ingresos y la reputación de la marca.

Comercial: Involucra a los Riesgos asociados con las estrategias comerciales y de mercado, como fallas en el diseño de productos y servicios, campañas de marketing, definición de precios inadecuada y cambios en la competencia. Impacta el ingreso y la posición de la Compañía en el mercado.

Contable: Se refiere a los Riesgos relacionados a la precisión de los estados financieros y conformidad con las normas contables. Importante para evitar errores financieros y mantener la confianza de los inversionistas, accionistas y acreedores financieros.

Desarrollo: Riesgos asociados a los proyectos de desarrollo de productos o servicios, como fallas de innovación, atrasos, tecnologías obsoletas y exceso de costos. Ayuda para garantizar la competitividad y la eficiencia de los productos y servicios ofrecidos por la Compañía.

Stock: Riesgos relacionados a la gestión del inventario, como exceso, falta de productos u obsolescencia. Esencial para la continuidad de la operación, atendimiento a las demandas de los clientes y optimización de los costos.

Financiero: Contempla los Riesgos de naturaleza financiera, como fluctuaciones cambiarias, tasas de intereses, falta de pago de clientes, liquidez de recursos financieros y acceso al crédito. Importante para garantizar la salud financiera y la estabilidad de la Compañía.

Fiscal: Riesgos relacionados a la conformidad tributaria y las alteraciones de las leyes fiscales. Sirve para evitar penalizaciones, mantener la conformidad con las obligaciones fiscales y minimizar el impacto de las provisiones contables.

Proveedores: Se refiere a los Riesgos relacionados a la dependencia y desempeño de los proveedores, como fallas en la entrega, calidad insatisfactoria y problemas

logísticos. Importante para la continuidad de la cadena de producción de la Compañía.

Infraestructura: Se refiere a los Riesgos asociados al mantenimiento y operación de las instalaciones y equipamientos, como averías y desastres estructurales. Esencial para la operación ininterrumpida de la Compañía.

Legal: Incluye los Riesgos jurídicos, como litigios, no conformidad con legislaciones y modificaciones reglamentarias. Sirve para proteger a la Compañía de las penalizaciones legales, mantener su conformidad y minimizar el impacto de las provisiones contables.

Logístico: Riesgos relacionados al movimiento y transporte de productos, como atrasos, extravíos y fallas en rutas. Impacta directamente la eficiencia de la cadena de producción de la Compañía.

Manufactura: Se refiere a los Riesgos en el proceso de producción, como fallas técnicas, desperdicio e ineficiencia. Importante para mantener la cualidad y la eficiencia de todas las etapas de la producción.

Personas: Contempla los Riesgos relacionados a la gestión de recursos humanos, como alta rotación, falta de capacitación y conflictos internos. Esencial para la retención de colaborados y manutención de la productividad de la Compañía.

Planeamiento: Riesgos relacionados al planeamiento estratégico y operativo, como fallas en las proyecciones y planes inadecuados. Sirve para garantizar la ejecución de las estrategias alineadas a los objetivos de la Compañía.

Productos: Se refiere a los Riesgos asociados a la calidad, seguridad y aceptación de los productos. Importante para la satisfacción del cliente y conformidad con los estándares del mercado.

Calidad: Contempla a los Riesgos de las fallas para mantener los estándares de la calidad en los procesos y productos. Impacta a la cadena de producción de la Compañía y la manutención de la fidelidad del cliente.

Servicios: Relativo a los Riesgos en la prestación de servicios, como fallas en el desarrollo, en la entrega y atención al cliente. Esencial para mantener la confianza y satisfacción del cliente.

Suministros: Riesgos asociados a la adquisición y gestión de las materias primas y recursos necesarios para la cadena de producción de la Compañía. Sirve para mantener la eficiencia y evitar interrupciones en la producción.

Tecnología: Contempla los Riesgos relacionados al uso e implementación de nuevas tecnologías, como fallas de software y obsolescencia. Importante para la innovación y competitividad de la Compañía.

De esta manera, el análisis de Riesgos requiere poder desarrollar la comprensión de los Riesgos mapeados en la Etapa 2. A partir de esta comprensión, se llega a la Etapa 4 de Evaluación de Riesgos y a la toma de decisiones sobre cuales tratamientos serán adoptados, bien como sobre cuales estrategias y métodos son los más adecuados para su gerenciamiento.

Paso 4: Evaluación de los Riesgos

Los riesgos mapeados y analizados se evalúan de acuerdo con sus potenciales impactos de materialización con el fin de alcanzar los objetivos de la Compañía.

En este sentido, la Administración de la Compañía, los Dueños de Riesgo y los líderes de procesos evalúan de manera conjunta los Eventos desde la perspectiva de Probabilidad, Frecuencia e Impactos. En el proceso de evaluación de riesgos se buscan variables que combinen métodos cualitativos y cuantitativos. Así, se consideran variables, entre otras, para la clasificación de impactos que ayuden en la mejor clasificación de Riesgos, utilizando el gradiente alto, medio y bajo para cada variable.

Finalmente, combinando todas las variables de evaluación, se define la criticidad de los Riesgos identificados, lo que permite la construcción de un mapa de priorización, partiendo de los Riesgos con mayor exposición a aquellos con menor exposición.

Este mapa ayuda a la Compañía a obtener un mayor grado de alineación de la planificación estratégica con el nivel aceptable de Apetito de Riesgo de la Compañía.

En este sentido, el Paso 4 es crucial para ayudar a la Administración de la Compañía en la toma de decisiones sobre los riesgos que deben o no ser priorizados.

Además, anualmente se realiza una evaluación general de los Riesgos de la Compañía, liderada por la Junta Directiva, con la participación del Consejo Ejecutivo y los miembros del Comité de Auditoría, mediante reuniones y entrevistas, cuyo

objetivo es realizar el diagnóstico de la estructura de la Compañía, identificar los Riesgos, definir la priorización en el tratamiento de los Riesgos identificados, elaborar un nuevo mapa de Riesgos, definir la estrategia de gestión de Riesgos y, en consecuencia, los recursos humanos y financieros necesarios para operativizar la estructura de Gestión de Riesgos de la Compañía.

No obstante, a pesar de la periodicidad de la evaluación general descrita anteriormente, el mapa de Riesgos está sujeto a ajustes en cualquier momento (exclusión, modificación y adición de Riesgos y prioridades), si se observan cambios en la realidad de la Compañía que justifiquen dicha adaptabilidad.

Paso 5: Tratamiento de Riesgos

La fase de Tratamiento de Riesgos implica identificar los dispositivos de Control existentes dentro del proceso para analizar la efectividad de estos Controles como medidas preventivas y como factores que reducen el grado de exposición (Factor Mitigante), para llegar al Riesgo Residual.

Para procesos que requieran un mayor grado de efectividad de los Controles o que no cuenten con factores de mitigación efectivos, el Riesgo será tratado por el área de Gestión de Riesgos y Controles Internos en conjunto con el área responsable de la 1ra Línea de Defensa de este Riesgo, a través de la implementación de uno o más Planes de Acción que tengan como objetivo mitigar la exposición al Riesgo y/o los impactos en caso de materialización de un Evento asociado al mismo.

Para cada Plan de Acción se asignan los responsables y los cronogramas de implementación para asegurar la efectividad y eficiencia de los Planes y así reducir el nivel de Riesgo Residual.

En este proceso, para cada acción de Tratamiento de Riesgos, se debe asignar una respuesta al Riesgo, que puede ser:

- → Aceptar (nada que hacer): no realice ninguna acción para reducir la Probabilidad o el impacto del Riesgo. Esta alternativa debe aplicarse cuando el costo de manejo/mitigación no compensa, si se compara con el impacto asumido, dentro del nivel aceptable de Apetito de Riesgo definido por la Compañía. En este caso, el Riesgo debe ser monitoreado de manera continua, a fin de garantizar un nuevo tratamiento adecuado si se produce un cambio en la situación que pueda incrementar el impacto y/o probabilidad del Riesgo, generando un cambio en su criticidad.
- → Eliminar: adoptar acciones que alteren o eliminen un proceso o proyecto, protegiendo los objetivos de negocio de los impactos de un Riesgo determinado.
- → Mitigar (control interno): definir controles internos para mitigar los riesgos y/o reducir la probabilidad de que el Riesgo se materialice y/o su impacto si ocurre. Esta alternativa deberá aplicarse cuando la reducción de la Probabilidad o del impacto sea suficiente para hacer asumible el riesgo, de acuerdo con el Apetito de Riesgo de la Compañía.

Al optar por una determinada acción en el proceso de tratamiento del riesgo, los ejecutivos y gestores responsables deben analizar el costo beneficio de la acción, considerando los costos involucrados, esfuerzo e implementación, asi como estudiar los beneficios que surgen de la acción en el ambito financiero, legal y reputacional, entre otros. El plan de tratamiento debe identificar el orden de prioridad en el que se debe implementar cada tratamiento.

Luego de determinar junto con las áreas responsables y/o afectadas las estrategias de tratamiento a adoptar, el Plan de Acción será documentado y comunicado a las áreas involucradas, para asegurar la implementación oportuna de las medidas determinadas.

El área de Gestión de Riesgos y Controles Internos apoyará a las áreas en la elaboración de Planes de Acción para corregir las fallas de control identificadas en la causa raíz y mitigar los Riesgos identificados.

Paso 6: Supervisión

Los procesos de seguimiento de la Compañía tienen como objetivo asegurar que los Controles de Riesgos sean efectivos y eficientes en su implementación, con el logro

de los resultados previstos y las estrategias diseñadas por la Administración y las Líneas de Defensa.

A través del proceso de monitoreo, es posible obtener información que pueda orientar mejor las fases de Evaluación de Riesgos, análisis de Eventos, cambios, tendencias, aciertos y fracasos, detección de cambios en los Contextos Internos y Externos, e identificación de Riesgos emergentes. Los resultados del seguimiento deben ser registrados e informados a los responsables de Gestión de Riesgos, Controles Internos y Compliance de la Compañía.

En este escenario, el monitoreo de Riesgos se constituye en un ciclo dinámico y continuo, siendo fundamental para garantizar de manera oportuna, preventiva y reactiva acciones que ayuden a minimizar impactos en caso de materialización de Riesgos.

El seguimiento debe ser realizado por la 1ra Línea de Defensa, buscando evaluar continuamente la efectividad de sus controles y la mejora en la gestión de sus Riesgos. El área de Gestión de Riesgos y Controles Internos (2da Línea de Defensa) apoyará a las áreas de negocio en el seguimiento de riesgos, con el objetivo de contribuir al logro de los objetivos y metas de la Compañía.

Así, los empleados involucrados en cada área deben tener la capacidad y competencia para identificar, evaluar, priorizar, monitorear y gestionar los Riesgos de su responsabilidad, considerando todos los cambios dentro del entorno interno y externo de la Compañía, para que puedan obtener un mayor grado de control de sus procesos y, en consecuencia, para que puedan alcanzar los objetivos establecidos durante la Gestión de Riesgos.

El proceso de supervisión también está vinculado a la implementación de los Planes de Acción, que serán elaborados y puestos en práctica por las unidades de negocio de acuerdo con las responsabilidades y periodicidad definidas por los titulares de los Riesgos y por las áreas de Auditoría Interna y Gestión de Riesgos y el personal interno de la Compañía de Controles.

Sistema Prisma - GRC

El Sistema Prisma - GRC contiene la descripción detallada de todos los procesos de la Compañía, incluyendo los Riesgos asociados, los Controles internos previamente testeados por el área de Auditoría Interna, bien como las Ausencias y Deficiencias de Controles identificadas y las auditorías internas realizadas.

Todos los colaboradores de la Compañía poseen el acceso al Sistema Prisma – GRC para la consulta de los procesos, Riesgos y controles internos vinculados, que se encuentran minuciosamente documentados en la plataforma.

Los gestores responsables por cada área específica tienen, adicionalmente, el acceso a las informaciones referentes a las Ausencias y Deficiencias de los controles internos, así como a los registros de las Auditorías internas realizadas.

<u>Paso 7</u>: Comunicación

Los riesgos deben ser comunicados de manera clara y objetiva, con toda la información relevante posible, a todos los afectados y/o responsables y, principalmente, a los responsables de determinar e implementar las medidas para su tratamiento.

Asimismo, una vez determinadas las medidas a adoptar para hacer frente a los Riesgos, deberán ser comunicadas de forma precisa y rápida a las áreas encargadas de implementar las medidas determinadas.

8. Vigencia y Revisión de la Política

Esta Política fue aprobada por el Consejo de Administración de la Compañía en la reunión realizada el 23 de febrero de 2021 y modificada mediante adenda en la reunión realizada el 25 de marzo de 2025, debiendo ser revisada siempre que hubiera su necesidad, y permanecerá vigente por plazo indefinido.

9. Referencias

- ABNT NBR ISO 31.000 / 2009: Gestão de Riscos – Princípios e diretrizes.
- As três linhas de defesa no gerenciamento eficaz de riscos e controles, IAA (*The Institute of Internal Auditors*) 2013.
- Código de Ética e Conduta da Companhia.
- COSO – ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*.
- Guia de Orientação para Gerenciamento de Riscos Corporativos IBGC (Instituto Brasileiro de Governança Corporativa) 2007.