Política de Gestión Integral de Riesgos – *Escuela Didáctica S.A.S. 2026*

Introducción

En un entorno empresarial altamente dinámico, la gestión integral de riesgos se ha convertido en un elemento clave para el éxito, la sostenibilidad y la resiliencia de las organizaciones. Para una empresa tecnológica educativa como *Escuela Didáctica S.A.S.* –dedicada al desarrollo de software, contenidos y plataformas de formación– la gestión de riesgos es fundamental para **anticipar y mitigar amenazas** que puedan afectar la continuidad de sus servicios, la calidad educativa que ofrece, y la confianza de sus usuarios y aliados. Una política clara de gestión de riesgos contribuye a crear una empresa más **resiliente** frente a incertidumbres, capaz de proteger sus activos (financieros, tecnológicos, humanos) y aprovechar oportunidades con mayor seguridad. En resumen, administrar adecuadamente los riesgos **fortalece la capacidad de la empresa para adaptarse y perdurar** ante cambios y eventualidades, asegurando el cumplimiento de sus objetivos estratégicos.

Principios y Marco de Referencia Normativo

La presente política se formula con base en estándares internacionales y nacionales reconocidos en materia de gestión de riesgos. En particular, se adopta el marco de **ISO 31000:2018** (*Gestión del Riesgo – Directrices*), que proporciona principios y directrices globales para identificar, evaluar, tratar y monitorear riesgos de manera sistemática. Asimismo, se cumple con la normativa colombiana vigente aplicable, incluyendo la **Ley 1581 de 2012** (protección de datos personales) y su reglamentación parcial mediante el **Decreto Único 1074 de 2015**, entre otras disposiciones. Estas normas –junto con estándares técnicos locales como la NTC-ISO 31000:2018– establecen un marco de referencia para implementar una gestión integral de riesgos coherente con las mejores prácticas y obligaciones legales en Colombia (por ejemplo, lineamientos de seguridad de la información, continuidad del negocio, gestión financiera responsable y buen gobierno corporativo).

Principios rectores (ISO 31000:2018): La gestión de riesgos de *Escuela Didáctica S.A.S.* se fundamenta en los principios internacionales de ISO 31000, adaptados al contexto de una empresa de tecnología educativa. Entre los **principios clave** se incluyen:

- **Integración:** el manejo de riesgos está **integrado** en todos los niveles organizacionales y procesos de la empresa; forma parte de la planificación estratégica, operativa y financiera cotidiana.
- **Enfoque estructurado:** se aplica un proceso **estructurado y exhaustivo**, que garantiza resultados consistentes y comparables en la identificación y evaluación de riesgos.
- **Adaptación al contexto:** el sistema de gestión de riesgos es **adaptado** a las características específicas de *Escuela Didáctica* (su tamaño, entorno tecnológico-educativo, objetivos y cultura), de modo que resulte pertinente y proporcional a sus contextos interno y externo.
- **Participación inclusiva:** la gestión de riesgos es **inclusiva**, involucrando apropiadamente a las partes interesadas (ej.: directivos, equipos de desarrollo, docentes, clientes institucionales) para aprovechar sus conocimientos y percepciones. Esto genera mayor conciencia y compromiso con la gestión del riesgo informada.
- **Dinamismo:** el proceso es **dinámico** y proactivo; reconoce que los riesgos **evolucionan con el entorno** (tecnológico, regulatorio, del mercado) y, por tanto, se anticipa y reacciona oportunamente a los cambios o eventos emergentes.
- **Información de calidad:** las decisiones se basan en la **mejor información disponible**, combinando datos históricos, análisis actualizados y proyecciones futuras. Se reconocen las posibles limitaciones o incertidumbres en la información, procurando siempre que esta sea oportuna, precisa, clara y accesible.
- **Factores humanos y culturales:** se reconoce la influencia de los **factores humanos y la cultura organizacional** en todos los aspectos de la gestión de riesgos. Se promueve una cultura interna que valore la **prevención** y el pensamiento basado en riesgos en cada proyecto o decisión.
- **Mejora continua:** la gestión de riesgos se asume como un **proceso de mejora continua**, con evaluaciones periódicas y retroalimentación para aprender de la experiencia, adaptarse a nuevos desafíos y optimizar de forma recurrente los procedimientos.

Estos principios aseguran que la **gestión integral de riesgos** no sea una actividad aislada, sino un componente intrínseco de la gestión de *Escuela Didáctica S.A.S.*, creando valor al proteger sus objetivos educativos y empresariales.

Roles y Responsabilidades en la Gestión de Riesgos

Una gestión eficaz de riesgos requiere una definición clara de **roles y responsabilidades** dentro de la organización, de modo que todos conozcan su contribución al sistema de administración de riesgos. *Escuela Didáctica S.A.S.* establece las siguientes responsabilidades:

- **Alta Dirección (Gerencia General y/o Junta Directiva):** Es la responsable de **liderar** la gestión integral de riesgos, definiendo la política y el apetito de riesgo de la empresa. Debe asegurar que la gestión de riesgos esté alineada con la estrategia, los objetivos y la cultura de la organización, asignando los recursos necesarios para su implementación. La alta dirección provee liderazgo y ejemplo, fomentando una cultura proactiva frente al riesgo, y designa **autoridades y responsabilidades claras en todos los niveles** para gestionar los riesgos. También se encarga de la aprobación de los planes de tratamiento de riesgos más significativos y del monitoreo general del sistema de riesgos.
- **Órgano de supervisión / Comité de Riesgos:** Se creará un comité de riesgos o equivalente, su rol es **asesorar y supervisar** el funcionamiento del sistema de gestión de riesgos. Puede incluir miembros de la dirección y líderes de áreas clave. Este órgano verifica que se integren las consideraciones de riesgo en la planeación y en la toma de decisiones estratégicas, revisa periódicamente el mapa de riesgos de la empresa, y asegura que los riesgos relevantes se discutan al más alto nivel. Por ejemplo, la junta directiva debe cerciorarse de que **se consideren los riesgos al establecer los objetivos** corporativos, y que las respuestas a riesgos críticos sean adecuadas.
- **Responsables de Procesos / jefes de Área:** Cada líder de área (desarrollo de software, contenidos educativos, TI, financiero, legal, comercial, etc.) actúa como **"dueño" de los riesgos** en su proceso. Son la **primera línea de defensa** en la identificación y manejo de los riesgos operativos diarios. Deben identificar los riesgos vinculados a sus actividades, evaluarlos y ejecutar las medidas de control o mitigación definidas. Asimismo, reportan a la gerencia sobre los riesgos significativos y el estado de las acciones de manejo. Por ejemplo, el jefe de TI velará por riesgos de seguridad informática; el responsable de contenidos revisará riesgos de calidad pedagógica o propiedad intelectual; el financiero controlará riesgos de liquidez, etc.
- **Responsable de Seguridad de la Información / Protección de Datos:** Dada la naturaleza tecnológica y el manejo de datos personales (estudiantes,

clientes), la empresa designará un encargado (o equipo) para **seguridad de la información y cumplimiento de la Ley 1581**. Este rol (que puede ser el Oficial de Seguridad Informática o el responsable de Protección de Datos Personales) formula e implementa controles específicos para mitigar riesgos tecnológicos y legales asociados a la información: políticas de backup, cifrado, control de accesos, cumplimiento de normas de privacidad, etc., y actúa ante incidentes relacionados.

- **Todos los Colaboradores:** Se fomenta una **cultura de riesgo** en la cual cada empleado entiende que también es parte del sistema de gestión de riesgos. Todos los miembros de la organización **tienen la responsabilidad** de considerar y gestionar los riesgos en sus tareas diarias, siguiendo las políticas y procedimientos establecidos. En la práctica, esto implica que cada colaborador debe: mantener una actitud vigilante para identificar amenazas en su ámbito de trabajo, cumplir con los controles (por ejemplo, políticas de seguridad, calidad, salud ocupacional), reportar oportunamente eventos o condiciones de riesgo a sus superiores, y proponer mejoras cuando detecte debilidades. Una participación activa y consciente de todo el personal fortalece la capacidad de la empresa para manejar riesgos de forma integral.

En síntesis, *Escuela Didáctica S.A.S.* adopta un enfoque de **"tres líneas de defensa"**: (1) las áreas operativas gestionan directamente sus riesgos; (2) la alta dirección y comités supervisan, coordinan y apoyan; (3) eventualmente auditoría interna (o consultores externos) evalúan de forma independiente la eficacia del sistema. Esta estructura asegura que el manejo de riesgos sea **transversal** y esté incorporado en la toma de decisiones a todos los niveles de la empresa.

Procedimiento Pedagógico para la Gestión de Riesgos

El proceso de gestión integral de riesgos de *Escuela Didáctica S.A.S.* se desarrolla en **etapas cíclicas**, acorde con las directrices de ISO 31000. Es un ciclo **iterativo y continuo** que permite la mejora constante. A continuación, se describen de forma *pedagógica* los pasos para **identificar**, **evaluar**, **tratar** y **monitorear** los riesgos empresariales, garantizando la comprensión de todo el personal:

1. **Identificación de Riesgos:** En esta fase se **establece el contexto** y se buscan de manera sistemática las fuentes de riesgo que podrían afectar a la empresa. Se considera el *contexto externo* (p.ej., entorno económico, regulatorio,

tecnológico, condiciones del mercado educativo) y el *contexto interno* (procesos, recursos, cultura organizacional) para tener un panorama completo. Luego, mediante técnicas como **listas de verificación, brainstorming con el equipo, análisis de procesos, revisión de experiencias pasadas e indicadores**, se identifican eventos potenciales que podrían impedir el logro de objetivos. Todos los departamentos contribuyen: por ejemplo, se listan riesgos operativos (fallas de plataforma, errores de contenidos), riesgos financieros (sobrecostos, mora de clientes), riesgos legales (incumplimiento normativo, litigios), tecnológicos (ciberataques, obsolescencia) y reputacionales (insatisfacción de usuarios, mala prensa). Cada riesgo identificado se describe con claridad (causa y posible consecuencia). *Herramienta:* **Matriz de Riesgos Inicial** – se elabora un listado o mapa con todos los riesgos detectados, que será la base para los siguientes pasos.

2. **Evaluación (Análisis y Valoración) de Riesgos:** Una vez identificados, los riesgos se **analizan** y **evalúan** para determinar su nivel de criticidad. En el análisis, se estima para cada riesgo su **probabilidad de ocurrencia** (qué tan frecuente o probable es que ocurra el evento) y el **impacto potencial** (qué tan graves serían las consecuencias si ocurre). *Escuela Didáctica* utiliza escalas cualitativas (p. ej., Probabilidad Baja/Media/Alta; Impacto Bajo/Medio/Alto) apoyadas en criterios predefinidos. Combinando probabilidad e impacto se obtiene un **nivel de riesgo** (por ejemplo, riesgo alto, medio o bajo) que sirve para priorizar. En esta valoración se consideran las condiciones actuales y los controles existentes: es decir, **riesgo inherente** (sin controles) vs. **riesgo residual** (con los controles que ya existen). También se analiza la interdependencia entre riesgos (p. ej., un fallo tecnológico puede derivar en un riesgo reputacional) y se clasifican según su tipo. Los riesgos se **mapean en una matriz** para visualización. *Salida:* **Matriz de Riesgos Valorada** – cada riesgo con su nivel (ej.: crítico, alto, moderado, bajo), lo que permite enfocar esfuerzos en los más significativos.
3. **Tratamiento de Riesgos:** Consiste en definir y aplicar **estrategias de manejo** para cada riesgo según su prioridad. Las opciones típicas de tratamiento incluyen: **evitar** el riesgo (decidir no realizar la actividad riesgosa, si es posible), **mitigar** o reducir el riesgo (implantar controles o acciones que disminuyan su probabilidad o impacto), **transferir** el riesgo (trasladarlo contractualmente a un tercero, por ejemplo mediante seguros o subcontratación, reconociendo que la

responsabilidad última reputacional puede permanecer) y **aceptar** el riesgo (cuando es de nivel bajo o coste de mitigarlo excede el beneficio, se asume y monitorea). Para los riesgos evaluados como *altos o inaceptables*, se elaboran **planes de acción específicos** orientados a reducirlos a niveles aceptables. Dichos planes definen responsables, recursos, plazos e indicadores de seguimiento. Ejemplos: si el riesgo es caída de la plataforma, la medida puede ser implementar servidores redundantes y protocolos de monitoreo; si es riesgo legal por datos personales, acciones como adoptar políticas de seguridad y capacitación en protección de datos. Cada medida apuntará a controlar causas o minimizar consecuencias. Es importante también **formalizar procedimientos**: por ejemplo, planes de continuidad del negocio y respuesta a incidentes para riesgos tecnológicos, protocolos de calidad para riesgos operativos, seguros para riesgos financieros, etc. Todas las acciones definidas quedan documentadas en un **Plan de Tratamiento de Riesgos** y deben integrarse en la planificación de la empresa. (*Nota:* La alta dirección aprueba las respuestas para riesgos críticos, asegurando que se asignen los recursos necesarios para implementarlas).

4. **Monitoreo y Revisión:** La gestión de riesgos no termina con la implementación de controles; por el contrario, exige un **seguimiento continuo**. *Escuela Didáctica* establece mecanismos para **monitorear** periódicamente tanto la evolución de los riesgos como la eficacia de las medidas tomadas. Cada riesgo significativo cuenta con **indicadores de alerta** (KRI – *Key Risk Indicators*), responsables de seguimiento y una frecuencia de revisión (mensual, trimestral, etc., según la naturaleza del riesgo). Por ejemplo, se monitorea el *uptime* de la plataforma (para riesgo de caída), los resultados financieros mensuales (para riesgo de liquidez), los incidentes de seguridad reportados (para riesgo de datos), etc. Además, se realiza una **revisión integral** del sistema de riesgos al menos una vez al año (o cuando ocurra un evento importante) para actualizar la matriz de riesgos, incorporar nuevos riesgos emergentes, evaluar lecciones aprendidas tras eventos ocurridos y verificar si la política y procedimientos siguen siendo adecuados. Este proceso de revisión continua garantiza la **mejora constante** del sistema de gestión de riesgos, adaptándolo a cambios en el entorno interno o externo. Igualmente, se mantienen **registros e informes**: todos los riesgos identificados, evaluaciones, planes e incidentes se documentan de forma organizada (registro de riesgos), y la Gerencia informa

periódicamente a la Junta Directiva o socios sobre el estado de los principales riesgos y las acciones en curso. Una comunicación transparente y oportuna, tanto internamente como hacia las partes interesadas externas cuando corresponda, forma parte esencial del monitoreo (por ejemplo, notificar a los clientes medidas tomadas tras un incidente de seguridad, para preservar la confianza). En resumen, la etapa de monitoreo cierra el ciclo de gestión de riesgos, realimentando el sistema y asegurando que la empresa se **mantenga alerta y preparada** ante la incertidumbre.

Cultura de mejora: Cabe destacar que la gestión de riesgos es un proceso vivo. *Escuela Didáctica S.A.S.* promueve una cultura en la que los riesgos se discuten abiertamente y las prácticas se perfeccionan con el tiempo. A través de capacitaciones, lecciones aprendidas tras incidentes (post-mortem) y auditorías internas, se refuerza el aprendizaje organizacional para enfrentar riesgos futuros con mayor eficacia.

Matriz de Riesgos (Ejemplos Aplicados)

A continuación, se presenta una matriz resumida con **ejemplos de riesgos relevantes** para *Escuela Didáctica S.A.S.*, que ilustra la clasificación por tipo, su descripción, valoración cualitativa (impacto/probabilidad) y algunas medidas de mitigación propuestas. Esta matriz sirve como guía pedagógica, mostrando cómo se documentan y tratan diferentes riesgos en la empresa:

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
Operativo / Tecnológico	**Caída de plataforma educativa:** Interrupción del servicio de la plataforma de *e-learning*, impidiendo a los usuarios acceder a	**Alto** – Afecta el cumplimiento del servicio (clases y evaluaciones se detienen), genera quejas y daña la confianza de usuarios e	**Media** – Puede ocurrir por sobrecarga, fallas de infraestructura o ataques externos en momentos críticos (p. ej. durante exámenes).	Infraestructura **redundante** (servidores de respaldo), **monitoreo 24/7** de desempeño, planes de **contingencia** (p. ej. reprogramar evaluaciones) y

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
	contenidos o evaluaciones.	instituciones aliadas.		comunicación oportuna a usuarios. Mejora de la capacidad y pruebas de estrés periódicas para prevenir caídas.
Legal / Operativo	**Incumplimiento contractual:** Fallo en cumplir a tiempo o con la calidad pactada en un contrato de desarrollo de software o contenido educativo para un cliente.	**Alto** – Puede conllevar penalidades económicas, pérdida del contrato y **dañar la reputación** de la empresa en el mercado (desconfianza de otros clientes).	**Baja** – Se evita con buena gestión de proyectos; aun así, puede ocurrir por mala planificación, sobrecostos imprevistos o factores externos (p. ej. retrasos de terceros).	**Gestión de proyectos rigurosa:** definición clara de alcances y plazos, metodologías ágiles con entregas parciales y feedback del cliente. Cláusulas contractuales realistas, seguimiento cercano a hitos y **comunicación temprana** ante cualquier desvío para negociar ajustes. Planes de contingencia (ej.: redistribuir

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
				recursos, horas extra) para prevenir incumplimientos.
Legal / Tecnológico	**Pérdida de datos personales:** Fuga, robo o acceso no autorizado a datos sensibles de estudiantes, docentes u otros usuarios (brecha de seguridad en bases de datos de la plataforma).	**Alto** – Expone a sanciones legales severas (Ley 1581 de 2012 y regulaciones de datos); la SIC puede imponer multas millonarias y hasta suspender operaciones por violación de datos personales. Además, provoca **pérdida de confianza** de clientes y daños reputacionales duraderos.	**Baja** – Evento grave pero poco frecuente; el riesgo aumenta si no se aplican buenas prácticas de seguridad. (El sector educativo es objetivo de ciberataques, pero con controles adecuados la probabilidad se reduce).	**Seguridad de la información:** Adopción de políticas y medidas de **ciberseguridad** (controles según ISO 27001): cifrado de datos sensibles, gestión estricta de contraseñas, autenticación de múltiples factores en plataformas, copias de seguridad frecuentes. Cumplimiento de estándares y normativa de protección de datos (designar un responsable de datos, obtener consentimientos

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
				, actualizaciones constantes de medidas de seguridad). **Capacitación** al personal y usuarios en buenas prácticas (ej.: prevenir phishing). Además, contar con un **plan de respuesta a incidentes** y protocolos de notificación (para reaccionar rápidamente ante una brecha, minimizando daño y cumpliendo obligaciones legales de reporte).
Tecnológico / Operativo	**Fallos en actualizaciones de software:** Una actualización o cambio en la plataforma	**Medio** – Interrumpe el servicio temporalmente, afectando la experiencia de usuarios	**Media** – Es posible si no se prueban adecuadamente las nuevas versiones antes de su	**Control de calidad (QA) exhaustivo:** implementar un proceso de pruebas robusto antes de

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
	educativa introduce errores graves o provoca la caída parcial del servicio.	(clases o estudios retrasados) y la **imagen de calidad** de la empresa. Puede generar reprocesos y costos adicionales de soporte.	lanzamiento; también por falta de compatibilidad con ciertos dispositivos o navegadores. (La ausencia de actualizaciones oportunas también acumula vulnerabilidades).	desplegar actualizaciones (ambientes de *testing* y *staging* que simulen uso real). Realizar **pilotos** con grupos pequeños de usuarios antes del despliegue general. Contar con la **posibilidad de reversión** rápida (rollback a la versión anterior) si aparece un fallo crítico. Asimismo, aplicar parches y actualizaciones menores de forma continua para no acumular problemas (evitar rezagos que abran brechas de seguridad). Documentar cambios y tener

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
				planes de comunicación para avisar a los usuarios sobre mantenimientos o actualizaciones mayores.
Financiero	**Problemas de liquidez o financieros:** Ejemplo: disminución inesperada de ingresos (p. ej. pérdida de un cliente importante o menor demanda estacional) o incremento imprevisto de costos operativos (p. ej. encarecimiento de servidores en la nube).	**Medio** – Puede limitar la capacidad de invertir en nuevos proyectos, mejoras o incluso dificultar operaciones cotidianas (pago de nómina, proveedores). Si no se gestiona, un problema de liquidez severo compromete la **viabilidad** de la empresa.	**Media** – Depende de factores de mercado y gestión interna; por ejemplo, una startup educativa puede enfrentar ingresos variables. Es un riesgo moderado pero real, especialmente sin diversificación o con **planeación financiera deficiente**.	**Gestión financiera prudente:** elaboración de presupuestos conservadores, seguimiento mensual del *cash flow* y estados financieros. **Diversificación** de fuentes de ingreso (distintos clientes, productos o mercados) para no depender de uno solo. Mantener **reservas o colchón financiero** (ahorros, líneas

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
				de crédito) para emergencias. Contratar **seguros** (cuando aplique, p. ej. seguro de cumplimiento en contratos) y actualizar periódicamente el plan de negocios considerando escenarios adversos. Controles de gastos y ajustes ágiles ante cambios económicos.
Reputacional	**Deterioro de imagen pública:** Por ejemplo, críticas masivas en redes sociales o mala prensa debido a un incidente (como una prolongada caída de la plataforma,	**Alto** – La **confianza de estudiantes, padres, instituciones educativas y aliados** puede verse seriamente erosionada. Un daño reputacional	**Baja** – Incidentes de alto perfil no ocurren con frecuencia, pero *basta un solo evento grave* para desencadenar una crisis de reputación. Además, en la era digital las	**Gestión de la comunicación y calidad:** Mantener **estándares de calidad** elevados en los servicios y contenidos para prevenir errores que deriven en mala imagen.

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
	filtración de datos o contenido inapropiado publicado).	reduce la fidelidad de los clientes actuales, dificulta atraer nuevos usuarios o contratos, e incluso puede alejar inversores y talentos (personal) clave.	noticias negativas se difunden rápidamente, amplificando el impacto.	**Protocolos de comunicación de crisis**: actuar con transparencia y rapidez ante problemas (comunicados oficiales, atención personal a afectados, asumir responsabilidad y explicar soluciones). Monitoreo activo de redes sociales y feedback de usuarios para detectar a tiempo percepciones negativas. Fortalecer la **relación con la comunidad** (usuarios sienten que la empresa escucha y mejora). En caso

Tipo de riesgo	Descripción	Impacto	Probabilidad	Medidas de mitigación
				de crisis reputacional, implementar un plan de recuperación de imagen, incluyendo mejoras demostrables y campañas de reputación corporativa si es necesario.

Nota: La matriz anterior es ilustrativa; la empresa deberá mantener una matriz **viva** y actualizada con todos los riesgos relevantes y sus detalles. Cada riesgo real se evalúa con más precisión cuantitativa cuando sea posible, y se asignan responsables directos. Además, *Escuela Didáctica S.A.S.* revisará y ajustará periódicamente esta matriz, especialmente tras cualquier incidente, cambios significativos en la empresa o el entorno, o nuevas actividades emprendidas (por ejemplo, lanzamiento de una nueva plataforma, entrada a un nuevo mercado), garantizando que la gestión de riesgos permanezca pertinente y efectiva en todo momento.

Conclusión

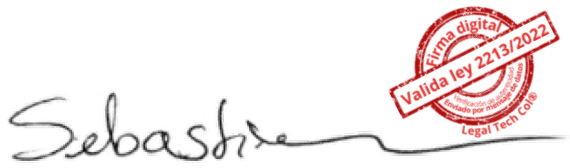
La **Política de Gestión Integral de Riesgos** de *Escuela Didáctica S.A.S.* proporciona un marco estructurado, claro y pedagógico para cultivar una cultura organizacional orientada a la prevención y manejo proactivo de los riesgos. Siguiendo los principios de normas internacionales como ISO 31000:2018 y cumpliendo con la normativa colombiana vigente, la empresa se compromete con la **identificación temprana**, la **evaluación rigurosa**, el **tratamiento efectivo** y el **monitoreo constante** de los riesgos operativos, financieros, legales, tecnológicos y reputacionales que enfrente.

De esta manera, *Escuela Didáctica S.A.S.* busca proteger la continuidad de sus operaciones, la calidad de sus servicios educativos y los datos de sus usuarios, fortaleciendo su resiliencia corporativa y la confianza de todos sus grupos de interés.

En última instancia, una gestión integral de riesgos robusta no solo previene pérdidas, sino que también facilita el logro de objetivos estratégicos, el cumplimiento normativo y la mejora continua, sentando las bases para un crecimiento **sostenible y seguro** de la organización en el largo plazo.

PUBLIQUESE Y CUMPLASE
FECHA: 29/01/2026
DIRECCIÓN: CL 4 8-32
CIUDAD: PEREIRA
DEPARTAMENTO: RISARALDA

Cordialmente,



SEBASTIÁN ROZO CADAVID
Representante Legal
ESCUELA DIDÁCTICA S.A.S
NIT: **901.192.132-5**
E-mail: gerencia@labtica.com

Cuadro de cambios:

Fecha	Versión	Descripción del cambio	Responsable del cambio	Aprobó
29/01/26	1.0	creación		

Luego de su aprobación y dando autenticidad, la presente política corporativa ha sido sometida a un sellado digital de tiempo para su verificación legal y prueba de no modificación.


LEGAL TECH COL®
REVISADO
APROBADO