

Política de Seguridad y Privacidad de la Información

Academia de Aprendizaje en el Idioma Inglés WANT2PEAK S.A.S. — Versión 1.0 — Fecha de emisión: 24 de junio de 2026

Responsable:	Academia de Aprendizaje en el Idioma Inglés WANT2PEAK S.A.S.
NIT:	901633442
Domicilio:	Carrera 15 #10-40, Centro Comercial José Luis, Local 501, Barbosa, Antioquia, 051020
Correo de contacto:	want2peak@gmail.com

La Academia de Aprendizaje en el Idioma Inglés WANT2PEAK S.A.S. (en adelante “Want2peak” o “la Institución”) reconoce la información como un activo esencial para la prestación de sus servicios de formación para el Trabajo y el Desarrollo Humano en el idioma inglés. En consecuencia, adopta la presente Política de Seguridad y Privacidad de la Información, en concordancia con su Sistema de Gestión de la Calidad (ISO 9001:2015 y NTC 5555:2011), los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y los referentes de buenas prácticas de la norma ISO/IEC 27001, así como el marco legal colombiano aplicable, incluyendo la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Ley 1273 de 2009 sobre protección de la información y los datos.

1. Objetivo

Establecer los lineamientos, principios y responsabilidades que permitan proteger la confidencialidad, integridad y disponibilidad de la información gestionada por Want2peak, ya sea física o digital, propia, de sus estudiantes, colaboradores, docentes, proveedores o demás partes interesadas, frente a riesgos internos y externos que puedan comprometerla.

2. Alcance

Esta política aplica a todos los procesos académicos y administrativos de Want2peak, a la totalidad de su personal directivo, docente, administrativo, contratistas y proveedores que tengan acceso a información institucional, así como a la infraestructura tecnológica, plataformas digitales de aprendizaje, sitio web, sistemas de información, equipos, redes y medios de almacenamiento físico o digital utilizados por la Institución.

3. Principios de seguridad de la información

- **Confidencialidad:** la información solo es accesible para las personas, procesos o sistemas debidamente autorizados.
- **Integridad:** la información se mantiene exacta, completa y libre de alteraciones no autorizadas durante todo su ciclo de vida.

- **Disponibilidad:** la información y los recursos asociados están accesibles y son utilizables cuando lo requieran las personas o procesos autorizados.
- **Privacidad:** el tratamiento de los datos personales se realiza conforme a la finalidad informada y autorizada por su Titular, en armonía con la Política de Tratamiento de Datos Personales de la Institución.
- **Legalidad:** el manejo de la información se sujeta a la normatividad vigente en materia de protección de datos, derechos de autor y delitos informáticos.
- **Mejora continua:** los controles de seguridad se revisan y ajustan periódicamente conforme a la evolución de los riesgos y la tecnología.

4. Compromisos institucionales

Want2peak se compromete a:

- Proteger la información de sus estudiantes, colaboradores y demás partes interesadas frente a amenazas internas y externas, accidentales o deliberadas.
- Identificar, valorar y tratar los riesgos asociados a la seguridad de la información dentro de sus procesos académicos y administrativos.
- Establecer controles de acceso físico y lógico acordes con la clasificación y criticidad de la información.
- Garantizar la continuidad de los procesos académicos y administrativos ante eventos que puedan afectar la disponibilidad de la información o de la plataforma tecnológica.
- Capacitar y sensibilizar a su personal sobre el uso adecuado, seguro y responsable de la información y los recursos tecnológicos.
- Reportar, gestionar y dar tratamiento oportuno a los incidentes de seguridad de la información.
- Cumplir con la normatividad legal vigente en materia de protección de datos personales, propiedad intelectual y delitos informáticos.

5. Clasificación de la información

Want2peak clasifica la información que administra según su nivel de sensibilidad e impacto, con el fin de definir los controles de protección adecuados:

- **Pública:** información de divulgación general, como contenidos institucionales publicados en el sitio web o redes sociales.
- **Interna o de uso restringido:** información de uso exclusivo del personal de la Institución, como procesos administrativos, académicos o documentos del Sistema de Gestión de la Calidad.
- **Confidencial:** información cuya divulgación no autorizada puede afectar a la Institución o a terceros, como datos personales de estudiantes y colaboradores, contratos o información financiera.

6. Roles y responsabilidades

Dirección / Representante Legal: Aprueba la política, garantiza los recursos necesarios para su implementación y promueve la cultura de seguridad de la información.

Área responsable de TI / Seguridad: Administra los controles técnicos, gestiona los incidentes de seguridad y realiza el seguimiento periódico de los riesgos.

Coordinación de Calidad: Articula la presente política con el Sistema de Gestión de la Calidad y sus procesos de mejora continua.

Personal docente y administrativo: Cumple los lineamientos de esta política, hace uso responsable de los recursos tecnológicos y reporta oportunamente cualquier incidente o vulnerabilidad.

Estudiantes y terceros: Hacen uso adecuado de las plataformas y recursos digitales puestos a su disposición por la Institución.

7. Gestión de incidentes de seguridad

Todo incidente que comprometa la confidencialidad, integridad o disponibilidad de la información —como accesos no autorizados, pérdida o robo de equipos, suplantación de identidad o fallas tecnológicas que afecten la prestación del servicio educativo— deberá ser reportado de manera inmediata a través del correo electrónico want2peak@gmail.com. La Institución adoptará las medidas correctivas necesarias y, cuando corresponda, informará a los Titulares afectados y a las autoridades competentes conforme a la normatividad vigente.

8. Continuidad y respaldo de la información

Want2peak implementa mecanismos de copia de respaldo (backup) y recuperación de información crítica, con el fin de garantizar la continuidad de sus procesos académicos y administrativos ante eventos que afecten la disponibilidad de los sistemas de información o de la infraestructura tecnológica.

9. Uso aceptable de los recursos tecnológicos

Los equipos, plataformas, correo electrónico, redes y demás recursos tecnológicos puestos a disposición del personal, docentes y estudiantes deberán utilizarse exclusivamente para fines académicos y administrativos relacionados con la prestación del servicio educativo, evitando su uso indebido, la instalación de software no autorizado o cualquier conducta que comprometa la seguridad de la información institucional.

10. Relación con la protección de datos personales

Esta política se articula con la Política de Tratamiento de Datos Personales de Want2peak. Mientras esta última define las finalidades, derechos y procedimientos relacionados con el tratamiento de datos personales, la presente Política de Seguridad y Privacidad de la Información establece los controles técnicos, organizacionales y procedimentales orientados a proteger dicha información —y la información institucional en general— frente a riesgos de seguridad.

11. Cumplimiento y consecuencias

El incumplimiento de los lineamientos establecidos en esta política por parte del personal de Want2peak podrá dar lugar a las medidas disciplinarias, contractuales o legales a que haya lugar, conforme al reglamento interno de trabajo y a la normatividad vigente, incluyendo la Ley 1273 de 2009, que tipifica los delitos informáticos en Colombia.

12. Vigencia y actualización

La presente política entra en vigencia a partir de su aprobación y publicación, y será revisada como mínimo una vez al año o cuando se presenten cambios significativos en la normatividad, la tecnología o los riesgos asociados a la información de la Institución, en el marco del ciclo de mejora continua del Sistema de Gestión de la Calidad.

Documento de carácter institucional, elaborado tomando como referencia el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos generales de la norma ISO/IEC 27001. Se recomienda la revisión de un especialista en seguridad de la información y de un asesor jurídico antes de su publicación definitiva.