idea

INGENIERIA Y DESARROLLO
DE ESTUDIOS AMBIENTALES

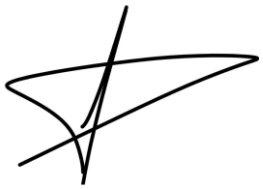
Política de Confidencialidad, Integridad y Protección de Datos

1 DECLARACIÓN DE PRINCIPIOS

IDEA SpA se compromete formalmente con la protección y el uso adecuado de toda la información generada o gestionada en el desarrollo de su giro. La confidencialidad y la integridad de la información son pilares esenciales para la credibilidad de nuestros estudios técnicos y la gestión responsable de los proyectos.

Esta política se alinea con:

1. Código de Ética: Refuerza los principios de Honestidad e Integridad.
2. Manual de Prevención del Delito (MPD): Prohíbe la comisión de Delitos Informáticos y Falsificación de Instrumento Público (Matriz de Riesgo Penal).
3. RIOHS: Complementa lo establecido en el Título Preliminar sobre la Confidencialidad de la Información del Trabajador.



Betzabe Ortega Pavez
Gerente General



Pablo Ugalde Casanova
Gerente Técnico

Santiago, abril del 2025

2 CAPÍTULO I: ALCANCES Y DEFINICIONES

2.1 Artículo 1. ALCANCE

Esta política aplica a:

a) Todos los Trabajadores (independiente de su modalidad contractual o jerarquía).
b) Colaboradores Externos y Colaboradores Empresa (Proveedores y Subconsultores).

2.2 Artículo 2. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL Y SENSIBLE

Cualquier información, dato, registro o material, en formato físico o digital, que no sea de conocimiento público y que, de ser divulgada, manipulada, o destruida sin autorización, pueda causar daño a IDEA SpA, a sus clientes, o a terceros. Incluye, pero no se limita a:

- Información Técnica Sensible: Bases de datos territoriales, cartografía GIS, datos de terreno (líneas de base), Estudios de Impacto Ambiental (EIAs/DIAs) y Adendas en desarrollo.
- Información Financiera: Presupuestos de proyectos, costos operativos, listados de proveedores/subconsultores y condiciones de pago.
- Propiedad Intelectual: Metodologías internas, know-how y software propietarios.
- Información Personal: Datos personales de trabajadores (salvo lo regulado en RIOHS) y clientes.

3 CAPÍTULO II: PRINCIPIOS DE SEGURIDAD Y CUMPLIMIENTO (ALINEACIÓN MPD Y MATRIZ DE RIESGO)

3.1 Artículo 3. DEBER DE CONFIDENCIALIDAD CONTRACTUAL

Todo trabajador y colaborador externo suscribe un Acuerdo de Confidencialidad (NDA) o una cláusula de confidencialidad en su contrato, que prohíbe la divulgación de Información Confidencial durante y después de la relación laboral/contractual.

3.2 Artículo 4. INTEGRIDAD Y TRAZABILIDAD DE DATOS (CONTROL MATRIZ DE RIESGO)

Se prohíbe estrictamente la alteración, manipulación o falsificación de datos de terreno, ambientales, cartográficos o cualquier otro insumo técnico utilizado en los proyectos. Esta acción representa un riesgo de Delito Ambiental/Falsificación de Instrumento Público según la Matriz de Riesgo Penal.

a) **Validación Técnica**: La elaboración de Informes Técnicos y de Due Diligence debe contar con la validación del Gerente Técnico o la Gerente General, según corresponda.

b) **Trazabilidad:** El Coordinador de Proyecto es responsable de asegurar la trazabilidad completa (registro de modificaciones, fecha, autor y versión) de todas las bases de datos GIS y de terreno.

3.3 Artículo 5. SEGURIDAD INFORMÁTICA (PREVENCIÓN DELITO INFORMÁTICO)

El acceso no autorizado a los sistemas de IDEA SpA para obtener, modificar o dañar información es considerado un Delito Informático tipificado en el MPD.

a) **Gestión de Cuentas**: El personal de TI, interno o externo, es responsable de la gestión de accesos y el cifrado de información sensible.
b) **Uso de Contraseñas**: Es obligatorio el uso de contraseñas seguras y su cambio periódico.
c) **Dispositivos**: Se prohíbe el almacenamiento de Información Confidencial en dispositivos personales (USB, discos duros externos) que no cumplan con las medidas de seguridad corporativas.

4 CAPÍTULO III: RESPONSABILIDADES POR PERFIL DE CARGO (ORGANIGRAMA)

4.1 Artículo 6. ROLES CRÍTICOS Y EXPOSICIÓN A RIESGOS

Cargo	Rol y Exposición al Riesgo	Responsabilidad Específica en Confidencialidad
Gerente General (Betzabé Ortega)	Máxima exposición a Información Técnica Sensible. Riesgo de Falsificación.	Supervisar el cumplimiento global de la política y gestionar las denuncias de infracción.
Gerente Técnico	Máxima exposición a Información Técnica Sensible. Riesgo de Falsificación.	Asegurar el proceso de Validación Técnica de los entregables y la integridad de los datos de proyecto.
Coordinadores de Proyecto	Custodia de bases de datos GIS/Terreno. Riesgo de manipulación/divulgación de datos. Gestión directa de la relación con Clientes/Subconsultores. Acceso a toda la información del proyecto.	Seguir instrucciones de implementación y monitoreo del sistema de Trazabilidad GIS/Terreno y el uso adecuado de la información por su equipo. Administrar, según instrucciones de Gerencia, el acceso a la información del proyecto (carpetas, claves) solo al personal autorizado y asegurar la firma de NDA por subconsultores.
Coordinadores de Proyecto	Gestión directa de la relación con Clientes/Subconsultores. Acceso a toda la información del proyecto.	Administrar, según instrucciones de Gerencia, el acceso a la información del proyecto (carpetas, claves) solo al personal autorizado y asegurar la firma de NDA por subconsultores.
Jefe Gis y Territorio / Ing. Control y Gestión de Proyectos	Acceso a información de costos, presupuestos y Due Diligence de proveedores.	Asegurar , según instrucciones de Gerencia, que la información financiera y de control interno (HH, OC) se maneje bajo estricta reserva.

Cargo	Rol y Exposición al Riesgo	Responsabilidad Específica en Confidencialidad
Finanzas y Contabilidad	Custodia de información financiera y contractual sensible.	Garantizar la protección de los datos bancarios, pagos y cláusulas contractuales de IDEA SpA y terceros, aun bajo modalidad externa.

5 CAPÍTULO IV: SANCIONES Y DENUNCIA

5.1 Artículo 7. SANCIONES

El incumplimiento de esta política, incluyendo la divulgación no autorizada, la manipulación de datos o el acceso indebido a sistemas, constituye una falta grave.

a) **Sanción Laboral:** Amonestación, suspensión o despido, de acuerdo con el RIOHS.
b) **Sanción Penal:** La empresa colaborará con las autoridades en la persecución de los delitos de Falsificación de Instrumento, Delitos Informáticos o Trata de Personas, cuando aplique.

5.2 Artículo 8. CANAL DE DENUNCIAS

Cualquier sospecha o evidencia de incumplimiento debe ser reportada de forma inmediata a la Gerencia General o al Canal de Denuncias Éticas del MPD, garantizando la confidencialidad de la denuncia y la no represalia.

6 HISTORIAL DE LA POLÍTICA

Fecha de Elaboración V 1.1:	29 abril 2025	Autor: Andrés Rojas/Abogado
Fecha de primera revisión :	5 de mayo 2025	Nombre: Betzabé Ortega/ Gerente General
Fecha de segunda revisión:	7 de julio 2025	Nombre: Pablo Ugalde /Gerente Técnico
Fecha de aprobación:	8 de Septiembre 2025	Nombre: Betzabé Ortega/ Gerente General.
Fecha de entrada vigencia:	1 de octubre 2025	