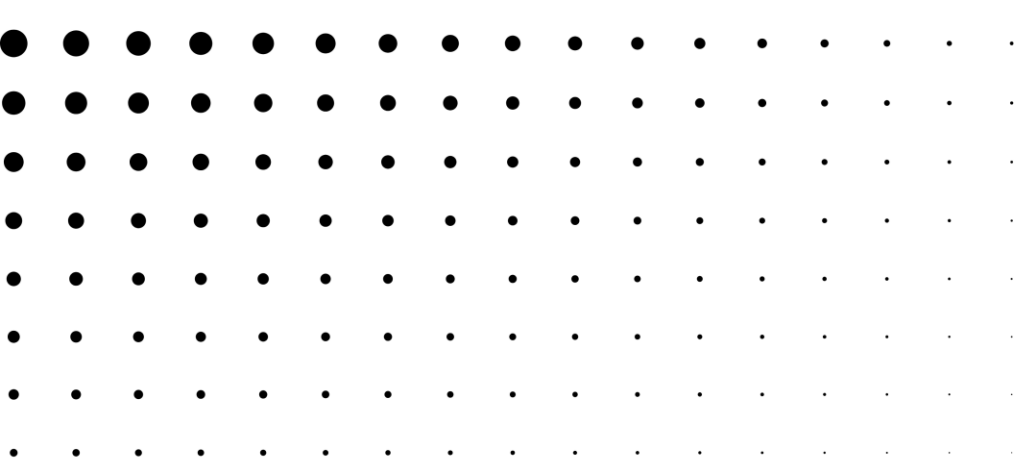
ANDINO
Global

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aprobada por el Consejo de Administración — Versión 2025

1. Objeto y finalidad

La presente Política de Seguridad de la Información tiene por objeto establecer los principios, normas y responsabilidades que aseguran la protección, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (CIADT) de la información gestionada por Andino Inversiones Global S.A. y su grupo de sociedades. Su finalidad es garantizar el cumplimiento normativo, la continuidad del negocio y la confianza de clientes, accionistas, empleados y terceros.

2. Ámbito de aplicación

Esta política aplica a toda la información, sistemas, procesos, infraestructuras, empleados, directivos, contratistas y terceros que tengan acceso a datos o recursos tecnológicos del Grupo Andino, incluyendo sus filiales en otros países. Es de cumplimiento obligatorio para todos los usuarios que manejen información corporativa, personal o confidencial.

3. Marco normativo y de referencia

- Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD).
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS).
- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27035:2023 – Gestión de incidentes de seguridad.
- Código Penal español (artículos 197 y 31 bis) – delitos informáticos y responsabilidad penal de la persona jurídica.
- Recomendaciones del CCN-CERT, ENISA y AEPD.
- Legislación aplicable en Perú (Ley N° 29733) y México (LFPDPPP).

4. Principios rectores

• Confidencialidad: la información solo será accesible a las personas autorizadas.
• Integridad: la información será exacta, completa y estará protegida contra modificaciones no autorizadas.
• Disponibilidad: la información y los sistemas estarán accesibles cuando sean necesarios.
• Autenticidad y trazabilidad: las identidades y accesos serán verificables y auditables.
• Legalidad: cumplimiento de las leyes y regulaciones aplicables.
• Responsabilidad compartida: cada usuario es responsable del uso seguro de la información.
• Mejora continua: el sistema se revisará periódicamente para incorporar avances tecnológicos y normativos.

5. Clasificación de la información

Toda la información del Grupo se clasificará conforme a su nivel de sensibilidad y riesgo asociado:

- Información confidencial: datos personales, financieros, estratégicos o legales.
- Información interna: documentación de uso interno, procedimientos y comunicaciones internas.
- Información pública: aquella destinada a difusión externa y sin restricciones de acceso.
- Cada categoría determinará las medidas de protección, control de acceso y almacenamiento aplicables.

6. Roles y responsabilidades

• Consejo de Administración: aprueba la política y supervisa su cumplimiento.

• Comité de Seguridad y Cumplimiento: coordina la aplicación del Sistema de Gestión de Seguridad de la Información (SGSI).

• Delegado de Protección de Datos (DPD): supervisa el cumplimiento del RGPD y las notificaciones a la AEPD.

• Departamento de Sistemas: implementa las medidas técnicas y controles de acceso.

• Todos los empleados y colaboradores: deben cumplir las normas de seguridad y reportar incidentes.

7. Controles de seguridad

El Grupo Andino implementará medidas técnicas y organizativas basadas en ISO/IEC 27001 y ENS:

- Control de accesos lógicos y físicos.
- Autenticación multifactor y contraseñas robustas.
- Cifrado de datos sensibles y comunicaciones seguras (SSL/TLS, VPN).
- Copias de seguridad cifradas y pruebas periódicas de restauración.
- Políticas de uso de correo electrónico, internet, dispositivos móviles y almacenamiento en la nube.
- Registro y monitorización de accesos, auditorías y trazabilidad de operaciones.

8. Gestión de incidentes de seguridad

Todo incidente de seguridad (pérdida, acceso no autorizado, malware, fuga de información, etc.) deberá ser comunicado de inmediato al Comité de Seguridad a través del canal habilitado. El procedimiento de respuesta seguirá las fases de identificación, contención, erradicación, recuperación y notificación.

Cuando el incidente afecte a datos personales, se notificará al Delegado de Protección de Datos (DPD) y, en su caso, a la AEPD en un plazo máximo de 72 horas.

9. Formación y concienciación

El Grupo desarrollará programas anuales de formación obligatoria sobre seguridad de la información, protección de datos y ciberseguridad. Asimismo, se promoverán campañas de sensibilización periódicas para reforzar las buenas prácticas y el cumplimiento de esta política.

10. Supervisión, auditoría y mejora continua

El Comité de Seguridad y Cumplimiento realizará auditorías periódicas para evaluar la eficacia del sistema, los controles implementados y los incidentes registrados. Los resultados se documentarán en un informe anual, integrado en el Sistema de Gestión de Cumplimiento y en el Estado de Información No Financiera (EINF). Las lecciones aprendidas se utilizarán para actualizar esta política y fortalecer el modelo de seguridad.

11. Aplicación internacional

Las filiales del Grupo Andino en otros países fuera de la Unión Europea adaptarán esta política a sus respectivos marcos normativos de protección de datos y ciberseguridad. Cada filial deberá:

- Cumplir las leyes nacionales de protección de datos (Ley N° 29733 en Perú y LFPDPPP en México).
- Implementar controles de acceso, copias de seguridad y gestión de incidentes locales.
- Designar un responsable de seguridad de la información o equivalente.
- Coordinar la notificación de incidentes con la matriz española y mantener coherencia con el SGSI del Grupo.
- Participar en las auditorías globales y reportes ESG del Grupo Andino.

12. Aprobación y entrada en vigor

La presente Política de Seguridad de la Información ha sido aprobada por el Consejo de Administración de Andino Inversiones Global S.A. y entra en vigor en la fecha de su aprobación. Es de cumplimiento obligatorio para todas las entidades del Grupo y será difundida por los canales corporativos internos.