



## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

En Austral Group S.A.A. (en adelante, Austral), reconocemos que la Seguridad de la Información y la Ciberseguridad son componentes fundamentales para el logro de nuestros objetivos estratégicos y pilares de la estrategia digital de la organización. En este sentido, nos comprometemos a proteger nuestros activos de información y a mantener un entorno tecnológico confiable, garantizando de manera permanente la confidencialidad, integridad y disponibilidad de la información.

### Objetivo y alcance

El objetivo de la presente Política es establecer los principios, compromisos y lineamientos que orientan la gestión de la seguridad de la información y la ciberseguridad en Austral, en concordancia con la estrategia y los objetivos del negocio.

La presente Política es de **cumplimiento obligatorio** para todos los colaboradores, proveedores y terceros que interactúan con los activos de información, sistemas de información, infraestructura tecnológica, redes, servicios digitales y demás recursos de información de Austral, independientemente de su ubicación, modalidad de acceso o forma de prestación de servicio.

### Principios fundamentales

- **Confidencialidad:** La información propia de Austral, así como la información de terceros que se encuentre bajo su control, es protegida contra el acceso, uso, divulgación o revelación no autorizados, independientemente del medio, formato, ubicación o tecnología en la que se encuentre.
- **Integridad:** La información es mantenida de manera exacta, completa y consistente a lo largo de todo su ciclo de vida<sup>1</sup>, asegurando que no sea modificada, alterada o destruida, evitando modificaciones no autorizadas.
- **Disponibilidad:** La información y los servicios asociados se mantienen disponibles y accesibles para usuarios autorizados cuando son legítimamente requeridos de acuerdo con los niveles de servicio y necesidades operativas del negocio.

### Objetivos de Seguridad de la Información y Ciberseguridad

- **Protección de activos de información:** Proteger la información y los recursos tecnológicos de Austral, asegurando su uso adecuado y su protección frente a amenazas internas y externas, de acuerdo con su criticidad y valor para el negocio.

---

<sup>1</sup> El ciclo de vida de la información comprende las etapas desde la creación, almacenamiento, uso, transmisión, archivo y eliminación.



- **Gestión basada en riesgos:** Identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información y ciberseguridad, gestionando amenazas y vulnerabilidades de manera sistemática y priorizando la implementación de controles preventivos, detectivos y correctivos según la criticidad de los activos y el impacto potencial en la operación.
- **Resiliencia operacional y gestión de incidentes:** Fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a eventos e incidentes de ciberseguridad, con el objetivo de preservar la continuidad operativa, la disponibilidad de los servicios y la protección de los activos críticos de información.
- **Cumplimiento normativo y control:** Asegurar el cumplimiento de requisitos legales, regulatorios y contractuales aplicables, así como de las políticas, normas y procedimientos internos que regulan el uso adecuado de la información y los recursos tecnológicos.
- **Cultura de seguridad y concientización:** Promover una cultura de seguridad de la información y ciberseguridad mediante programas de concientización, capacitación y comunicación, fomentando comportamientos responsables y consistentes con los principios establecidos en la presente Política.
- **Entornos digitales y modalidades de trabajos seguros:** Asegurar que la adopción y uso de tecnologías digitales, servicios tecnológicos y modalidades de trabajo remoto o híbrido se realicen de manera segura, implementando controles proporcionales a los riesgos asociados y garantizando la protección de la información.

### **Reporte y gestión de incidentes**

Austral dispone del canal oficial **incidentesti@austral.com.pe** para reportar incidentes de seguridad de la información y ciberseguridad, sospechas de vulneración o anomalías en los sistemas. Este canal permite activar oportunamente las investigaciones y acciones de mitigación correspondientes. La colaboración activa de todos es clave para minimizar impactos y fortalecer continuamente nuestra capacidad de respuesta y mejora en ciberseguridad.

### **Gobierno y supervisión**

Austral cuenta con un **Comité de Ciberseguridad**, conformado por representantes de áreas clave de la organización, responsable del gobierno y de asegurar la supervisión del marco de seguridad de la información y ciberseguridad, supervisar el cumplimiento de esta Política, revisar el panorama de riesgos, evaluar y aprobar medidas de control y promover la cultura de seguridad de la información y ciberseguridad en todos los niveles de la organización. El Comité se reúne periódicamente para revisar incidentes,



**Austral Group** S.A.A.  
Austevoll Seafood Company

tendencias, cambios normativos y nuevas amenazas, asegurando una gestión oportuna, coordinada y alineada con los objetivos del negocio.

Austral reafirma su compromiso con la protección de la información y la ciberseguridad como elementos esenciales para la continuidad del negocio, la confianza de sus partes interesadas y el logro sostenible de sus objetivos estratégicos.

Aprobado por el Comité de Gerencia de Austral Group el 03 de marzo de 2026.