

|                                                                                   |                                                                                    |                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------|
|  | <p align="center"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página 1 de 7</p> |
| <p><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p>                         |                                                                                    |                                                |

## CONTENIDO

|     |                                     |   |
|-----|-------------------------------------|---|
| 1.  | OBJETIVO .....                      | 2 |
| 2.  | ALCANCE .....                       | 2 |
| 3.  | REFERENCIA NORMATIVA.....           | 2 |
| 4.  | DEFINICIONES.....                   | 3 |
| 5.  | ROLES Y RESPONSABILIDADES.....      | 3 |
| 6.  | DESCRIPCIÓN DE LA POLITICA.....     | 4 |
| 7.  | ACTUALIZACIÓN DE LA POLITICA.....   | 6 |
| 8.  | DIFUSION DE LA POLITICA .....       | 6 |
| 9.  | CONTROL DE REGISTROS ASOCIADOS..... | 6 |
| 10. | ANEXOS .....                        | 6 |
| 11. | HOJA DE CONTROL DE CAMBIOS .....    | 7 |

|                     | Elaborado por:                        | Revisado por:       | Aprobado por:                                 |
|---------------------|---------------------------------------|---------------------|-----------------------------------------------|
| <b>Nombre/Cargo</b> | Gonzalo Gacitúa<br>Encargado del SGSI | Comité de Seguridad | Cristian Wulf<br>Sotomayor<br>Gerente General |
| <b>Fecha</b>        | 23-04-2026                            | 23-04-2026          | 23-04-2026                                    |

|                                                                                   |                                                                                    |                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------|
|  | <p align="center"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página 2 de 7</p> |
| <p><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p>                         |                                                                                    |                                                |

## **1. OBJETIVO**

La información administrada necesita ser protegida de situaciones que atentan contra su disponibilidad, integridad y confidencialidad, amenazas que en definitiva pueden poner en riesgo la continuidad del negocio y exponer a la organización a incumplimientos legales. Para mitigar estos riesgos, surge la necesidad de definir políticas de seguridad de la información al interior de la empresa, a las que deberán adherirse todos los colaboradores, permitiendo de esta forma controlar de una mejor manera el uso de los datos a los que se tiene acceso.

## **2. ALCANCE**

- Todos los colaboradores, independientemente de la relación contractual con la Organización, proveedores de servicios externos, consultores, auditores, contratistas que accedan a las instalaciones de la compañía, ya sea física o remotamente para realizar trabajos y empleen recursos de tecnologías de información.
- Todas las instalaciones, equipamiento (incluyendo equipos portátiles y accesorios móviles) para procesar o almacenar información y redes.
- Todo el software para el procesamiento de datos o transporte de comunicaciones, sin importar el o los medios de almacenamiento o método de procesamiento que se disponga para sus fines.
- La utilización de hardware, software y recursos de terceros que tenga en propiedad o bajo su dominio o licenciamiento o derecho de uso.
- Los ambientes y recintos de PUERTOS DE TALCAHUANO en los cuales se procesa información y alojan redes de comunicaciones.

## **3. REFERENCIA NORMATIVA**

La presente política se define considerando las recomendaciones de las siguientes normativas:

- Norma ISO/IEC 27001:2022 , Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Control A.5.1.

|                                                                                       |                                                                                          |                                                |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------|
|      | <p style="text-align: center;">SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</p> | <p>POL-01<br/>Versión 01<br/>Página 3 de 7</p> |
| <p style="text-align: center;"><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p> |                                                                                          |                                                |

#### 4. DEFINICIONES

**Confidencialidad:** La información debe ser conocida únicamente por aquellas personas que estén autorizadas para acceder información específica del negocio. Esto es necesario para proteger los asuntos reservados como planes estratégicos, información legal, de recursos humanos, información de los colaboradores y cualquier dato sensitivo.

**Integridad:** La información de PUERTOS DE TALCAHUANO solamente puede ser agregada, modificada o eliminada por personas y/o procesos debidamente autorizados. Esto es necesario para garantizar que la información que soporta el negocio sea precisa y completa para que las decisiones que se tomen utilizándola produzcan los resultados que se esperan.

**Disponibilidad:** La información debe estar cuando se necesita en el formato requerido para su procesamiento, para asegurar que los procesos de negocio y las decisiones sean oportunas.

**Propietarios de la Información y otros activos asociados:** Es el dueño del proceso que utiliza o genera dicha información y tiene propiedad sobre otros activos.

**Usuarios de la Información y otros activos asociados:** Es aquella persona, colaborador interno o externo, que con la debida autorización introduce, borra, cambia o lee información de la compañía o utilizar el activo asociado.

Los usuarios sólo deben tener acceso a la información y a los activos a la que cuales autorizados para ver o procesar y las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó permiso.

**Activos de información:** Es cualquier componente que contenga información (sea humano, tecnológico, software, hardware, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

#### 5. ROLES Y RESPONSABILIDADES

**Gerente General / Comité de Seguridad:** Asegurar que las materias abordadas en esta política se ejecutan y se cumplan, identificar cómo se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la presente política detectando y proponiendo mejoras.

|                                                                                       |                                                                                                 |                                                |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------|
|      | <p style="text-align: center;"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página 4 de 7</p> |
| <p style="text-align: center;"><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p> |                                                                                                 |                                                |

**Encargado de SGSI:** Apoyar al Comité de Seguridad en la supervisión de la implementación de la presente política. Recibir y dar respuesta a los incidentes de seguridad de la información asociados a actividades descritas en la presente política.

**Colaboradores:** Dar cumplimiento a la presente política de seguridad de la información y a todas las responsabilidades en materia de seguridad de la información que hayan sido definidas y asignadas.

## 6. DESCRIPCIÓN DE LA POLITICA

Empresa Portuaria Talcahuano San Vicente con el objetivo de administrar, explotar, desarrollar y conservar los terminales de Talcahuano y San Vicente, así como otros bienes que posee a cualquier título.

La empresa se rige por las normas de la iniciativa legal que la creó y por las regulaciones aplicables a las sociedades anónimas. Es fiscalizada por la Comisión para el Mercado Financiero (CMF), por la Contraloría General de la República, el Consejo de Auditoría Interna General de Gobierno y la agencia nacional de ciberseguridad.

Como parte de un sistema portuario cuyas características de integración y competencia no se repiten en otra zona del país, la empresa mantiene inalterable su compromiso por la competitividad del desarrollo portuario de la Región del Biobío, a través de la eficiencia y del impulso a nuevas iniciativas e inversiones que contribuyan a tal objetivo.

Lo anterior se sustenta en el cumplimiento de los siguientes compromisos del Sistema de Gestión de Seguridad de la Información y sus respectivos objetivos, por parte de PUERTOS DE TALCAHUANO:

- Mejorar continuamente la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
  - Implementar anualmente, a lo menos una mejora al sistema de gestión de seguridad de la información.
  - Implementar planes de acción para incidentes de seguridad de la información y no conformidades que resuelvan de raíz los problemas identificados.

|                                                                                   |                                                                                    |                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------|
|  | <p align="center"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página 5 de 7</p> |
| <p align="center"><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p>          |                                                                                    |                                                |

- Cumplir con los requisitos legales y los aplicables a la seguridad de la información, según lo establecido en la norma ISO 27001:2022
  - Mantener en cero las multas o sanciones por incumplimiento legal y contractual relativo a la Seguridad de la Información.
  - Mantener vigente el Sistema de Gestión de la Seguridad de la Información implementado por la norma ISO 27001:2022.
- Proteger la confidencialidad de la información sensible relacionada con la empresa y sus clientes.
  - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la confidencialidad
- Garantizar la integridad de la información de la empresa, que la misma sea precisa y completa.
  - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la integridad
- Asegurar la disponibilidad de la información cuando se necesite, para asegurar la continuidad de los procesos.
  - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la disponibilidad.
- Promover en sus colaboradores el conocimiento de dicha Política de Seguridad de la Información, así como la importancia de su contribución a la eficacia del SGSI.
  - Difundir el Sistema de Seguridad de la Información por medio de la ejecución de un Plan de difusión anual.
  - Capacitar en Seguridad de la Información por medio de la ejecución de un Plan de capacitación anual.

|                                                                                   |                                                                                    |                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------|
|  | <p align="center"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página 6 de 7</p> |
| <p><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p>                         |                                                                                    |                                                |

## **7. ACTUALIZACIÓN DE LA POLITICA.**

Dentro de la mejora continua de las políticas de seguridad de la información, esta política debe ser revisada al menos una vez al año, a partir de la fecha de entrada en vigor.

## **8. DIFUSION DE LA POLITICA**

- La totalidad de las políticas, procedimientos y protocolos deben ser informados a las Jefaturas para que las difundan según el nivel de acceso permitido a cada colaborador.
- El mecanismo formal de comunicación es el correo institucional de la Compañía. Sin embargo, las políticas, procedimientos y protocolos de seguridad de la información se encuentran almacenados en el sitio Sharepoint SGSI PUERTOS DE TALCAHUANO - ISO 27001.

## **9. CONTROL DE REGISTROS ASOCIADOS**

| Nombre del registro | Responsable de Archivo | Modo de Archivo | Tiempo de Archivo |
|---------------------|------------------------|-----------------|-------------------|
|                     |                        |                 |                   |
|                     |                        |                 |                   |

## **10. ANEXOS**

N/A

|                                                                                   |                                                                                    |                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------|
|  | <p align="center"><b>SISTEMA DE GESTIÓN DE<br/>SEGURIDAD DE LA INFORMACIÓN</b></p> | <p>POL-01<br/>Versión 01<br/>Página <b>7</b> de <b>7</b></p> |
| <p align="center"><b>POLITICA DE SEGURIDAD DE LA<br/>INFORMACIÓN</b></p>          |                                                                                    |                                                              |

## 11. HOJA DE CONTROL DE CAMBIOS

| Fecha      | Párrafo | Versión | Cambio realizado         |
|------------|---------|---------|--------------------------|
| 23-04-2026 | Todos   | 01      | Aprobación del documento |
|            |         |         |                          |
|            |         |         |                          |

-----  
**Cristian Wulf Sotomayor**  
**Gerente General**