

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 1 de 8

Política General de Seguridad de la Información

Hanseatic Global Terminals Latin America S.A.

12 2023

Information & Communication Technologies

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 2 de 8

- 1. **Resumen..... 3**
- 2. **Objetivos..... 3**
 - 2.1. Objetivo General 3
 - 2.2. Objetivos Específicos..... 3
- 3. **Alcance 3**
- 4. **Glosario 4**
- 5. **Principios..... 4**
- 6. **Roles y Responsabilidades..... 5**
- 7. **Integración de Normativas/políticas subordinadas en el Gobierno de Seguridad de la Información..... 5**
- 8. **Cumplimiento de la Política 7**
 - 8.1. Excepción..... 7
 - 8.2. Incumplimiento 7
- 9. **Estándares Relacionados, Normativas y Procedimientos 7**
- 10. **Control de Versiones 7**
- 11. **Control de Cambios 8**

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 3 de 8

1. Resumen

En un entorno empresarial en constante evolución, las tecnologías de la Información desempeñan un papel esencial, donde la protección de la información se convierte en una prioridad. Hanseatic Global Terminals Latin America reconoce la importancia de resguardar sus sistemas y datos contra amenazas de ciberseguridad y ha establecido una Política General de Seguridad de la Información.

Por medio del presente documento, se dan a conocer a todos los colaboradores de Hanseatic Global Terminals Latin America los lineamientos base para el resguardo de la información y documentación referente al negocio.

2. Objetivos

2.1. Objetivo General

Hanseatic Global Terminals Latin America establece su Política General de Seguridad de la Información para proporcionar directrices claras que orienten a la empresa y defina las responsabilidades en materia de Seguridad de la Información.

2.2. Objetivos Específicos

- Crear un marco referencial sólido que asegure una protección efectiva de los activos tecnológicos de Hanseatic Global Terminals Latin America.
- Definir las directrices corporativas que regulen el uso adecuado de los recursos informáticos de Hanseatic Global Terminals Latin America, así como las medidas necesarias para protegerlos.
- Fomentar la conciencia de Seguridad de la Información en todos los colaboradores, tanto internos como externos, y promover la comprensión de sus responsabilidades individuales asociadas a sus roles.
- Detallar las medidas esenciales de Seguridad de la Información que Hanseatic Global Terminals Latin America debe implementar para proteger sus activos de información contra posibles amenazas que puedan afectar la Confidencialidad, Integridad y Disponibilidad y Desempeño de la información.
- Proporcionar a todos los colaboradores herramientas que les permitan tomar decisiones adecuadas relacionadas con los mecanismos y soluciones de Seguridad de la Información.
- Garantizar la seguridad del activo de información tecnológico, abordando tanto las amenazas identificadas como la remediación de sus vulnerabilidades.
- Alinear la presente política con las leyes y regulaciones vigentes relacionadas con la protección de la información

3. Alcance

Esta política es aplicable a todos los activos de información tecnológica de Hanseatic Global Terminals Latin America y cubre a todo su personal permanente ("Hanseatic Global Terminals Latin America" o la "Compañía"), así como a sus empresas filiales.

Se recomienda que las empresas coligadas en las que Hanseatic Global Terminals Latin America no tenga participación mayoritaria ni control administrativo también adopten esta política.

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 4 de 8

4. Glosario

Las definiciones y términos incluidos en este documento están consignados en el registro centralizado 'REG-0004 Glosario de Términos', el cual se encuentra accesible en el Sharepoint corporativo.

5. Principios

- 5.1. Hanseatic Global Terminals Latin America establece la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de asegurar la existencia y ejecución de controles periódicos, minimizando los riesgos de Seguridad de la Información y Ciberseguridad, protegiendo los activos de información contra amenazas.
- 5.2. Se crea el Comité de Ciberseguridad, conformado por representantes de la Vicepresidencia de Tecnologías de la Información y Comunicaciones, con la responsabilidad de aprobar políticas y normas para la administración y gestión adecuada del riesgo de seguridad de la Información.
- 5.3. El Directorio y los Gerentes de área brindan su respaldo al proceso de administración y gestión del riesgo de seguridad de la información, proporcionando directrices claras, recursos, prioridades y promoviendo una cultura de seguridad.
- 5.4. El Information Security & Cybersecurity Manager es responsable de difundir políticas, reglamentos y procedimientos de Seguridad de la Información a todos los colaboradores, proveedores y terceros, asegurando la comprensión y el cumplimiento de responsabilidades. En el caso de Filiales, el Gerente de Tecnologías de la Información o encargado del área de Tecnologías de la Información es el encargado de la difusión de las Políticas, reglamentos y procedimientos de Seguridad de la Información a los colaboradores.
- 5.5. El Information Security & Cybersecurity Manager supervisa el cumplimiento de los requisitos normativos relacionados con seguridad de la información y aplica controles a través de revisiones periódicas para mejorar la efectividad del SGSI.
- 5.6. a) Todos los Colaboradores, Proveedores y Terceros deben reportar a la Information Security & Cybersecurity Manager cualquier incumplimiento de las políticas, normas y procedimientos de seguridad de la información.
b) Para las Filiales, la Gerencia de Tecnologías de la Información o el área interna de Tecnologías de la Información correspondiente de cada entidad asumirá la responsabilidad de gestionar los reportes de incumplimiento. Posteriormente, informarán a la Information Security & Cybersecurity Manager.
- 5.7. La Vicepresidencia de Tecnologías de la Información y Comunicaciones son responsables de garantizar la Confidencialidad, Integridad y Disponibilidad de los activos tecnológicos, así como de contribuir a la continuidad de las operaciones.
- 5.8. Cada colaborador de Hanseatic Global Terminals Latin America y Filiales es responsable de la información que maneja en su equipo de trabajo, en consonancia con las políticas y estándares emitidos por la Vicepresidencia Tecnologías de la Información y Comunicaciones de Hanseatic Global Terminals Latin America.
- 5.9. Se debe garantizar que todo el personal reciba capacitación en materia de seguridad de la información, adaptada a sus necesidades y roles dentro de la empresa.
- 5.10. Los colaboradores tienen la obligación de reportar de manera oportuna y adecuada cualquier incidente que ponga en riesgo la información.

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 5 de 8

6. Roles y Responsabilidades

- **Vicepresidencia de Tecnologías de la Información y Comunicaciones:** El SVP Information & Communication Technologies responde al Gerente General de la empresa por la existencia y cumplimiento de las medidas orientadas a mantener un nivel de seguridad de la información acorde con las necesidades de Hanseatic Global Terminals Latin America y filiales.
- **Comité de Ciberseguridad:**
 - a) Responsables de revisar y aprobar políticas y procedimientos de Seguridad de la Información que guíen las buenas prácticas a los Colaboradores y al negocio.
 - b) Contribuir en la planificación estratégica de seguridad de la información, alineándola con los objetivos del negocio y las necesidades actuales.
 - c) Fomentar una cultura de seguridad de la información, promoviendo la concienciación y la formación en seguridad de la información en todos los niveles del negocio.
 - d) Actúa como principal impulsor para el desarrollo y la implementación de iniciativas relacionadas con la seguridad de la información en el negocio, garantizando que esta se integre de manera transparente en las operaciones y estrategias.
 - e) Mantenerse informado acerca de las tendencias, normas, y métodos de seguridad que permitan detectar nuevos riesgos en materia de seguridad de información.
- **Information Security & Cybersecurity Manager:** Es el principal responsable en la definición de los criterios de seguridad de la información de la empresa, para lo cual deberá analizar permanentemente el nivel de riesgo existente, proponiendo soluciones costo-efectivas. Una vez autorizada la implementación de las medidas, deberá coordinar su materialización oportuna y correcta.

Para Filiales:

- **Gerente de Tecnologías de la Información o Encargado de área:** Colabora estrechamente con la Information Security & Cybersecurity Manager para garantizar el cumplimiento de las políticas establecidas. Informa y gestiona toda irregularidad de seguridad de la información, y vela por el cumplimiento de las medidas orientadas a mantener un nivel de seguridad acorde a las necesidades del negocio

7. Integración de Normativas/políticas subordinadas en el Gobierno de Seguridad de la Información

La Política General de Seguridad de la Información de Hanseatic Global Terminals Latin America, establece los principios fundamentales que guían una gestión efectiva de la seguridad en todas las operaciones y procesos relacionados con la información. Dado el aumento de la complejidad y diversidad de los riesgos en el entorno actual, esta política actúa como guía base para preservar los Activos de Información del negocio.

Al implementar estas directrices en conjunto, Hanseatic Global Terminals Latin America refuerza su compromiso con la seguridad en todos sus aspectos y con la gestión eficaz de la información. Cada una de estas directrices, junto con la Política General de Seguridad de la Información, conforma un marco robusto que fortalece la postura de seguridad en el negocio, asegurando la Confidencialidad, Integridad y Disponibilidad de la información en todos los niveles.

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 6 de 8

- **Política de Escritorio Limpio:** esta política establece las directrices para mantener un entorno de trabajo seguro y organizado, abordando tanto aspectos físicos como digitales. Esto incluye medidas como asegurar las estaciones de trabajo y dispositivos cuando estos no se encuentren en uso, gestionar adecuadamente las impresiones y proteger la información confidencial.
- **Política de Control de Acceso Lógico:** Define como se gestionará el acceso a los sistemas y aplicaciones. Establece los procedimientos para asignar, revisar y revocar permisos, garantizando que solo las personas autorizadas puedan acceder a información crítica.
- **Política de Uso de Software:** Establece las directrices para la adquisición, instalación y uso de software en los sistemas del negocio. Busca asegurar que todo software utilizado cumpla con requisitos de seguridad y licencias, minimizando riesgos y amenazas.
- **Política de Continuidad del Negocio:** Describe las directrices para la implementación de estrategias para mantener las operaciones en situaciones de crisis, incluyendo la preparación para desastres y la recuperación de sistemas, asegurando la resiliencia ante eventos adversos.
- **Política de Gestión de Activos de la Información:** Se centra en identificar y proteger Activos de Información. Desde equipos hasta datos, estableciendo directrices para el seguimiento y resguardo de los activos, minimizando pérdidas y riesgos.
- **Política de Gestión de Vulnerabilidades:** Establece como identificar, evaluar y corregir las vulnerabilidades en sistemas y aplicativos del negocio. Se busca prevenir posibles ataques y asegurar la integridad del sistema.
- **Política de Trabajo Remoto:** Esta política se enfoca en las medidas de seguridad necesarias para asegurar la realización segura y eficiente del trabajo remoto. Contiene pautas sobre el acceso a redes seguras, la protección de dispositivos utilizados en entornos remotos y la sensibilización sobre los riesgos asociados.
- **Política de Entorno en la Nube:** Define como se evaluarán y adoptarán servicios en la nube de manera segura. Se establecen requisitos de privacidad, cumplimiento y seguridad para garantizar la protección de datos en entornos cloud.
- **Política de Seguridad con Proveedores:** Establece requisitos de seguridad que deben cumplir los proveedores externos que tengan acceso a la información del negocio, garantizando la protección de datos confidenciales.
- **Política de Respaldo, Custodia y Recuperación de Información:** Detalla cómo se realizarán los respaldos de información crítica y cómo se custodiará adecuadamente la información, garantizando la recuperación y evitando fuga de datos.
- **Política de Destrucción de Información:** Describe como se llevará a cabo la destrucción adecuada de la información sensible, asegurando la confidencialidad y evitando fugas.
- **Política de Desarrollo Seguro:** Estas directrices establecen la implementación de prácticas de seguridad desde las fases tempranas del desarrollo de aplicaciones y sistemas, garantizando la protección del producto final contra vulnerabilidades y riesgos.
- **Política de Contraseñas:** Define los criterios para la creación de contraseñas sólidas y seguras, reduciendo la probabilidad de accesos no autorizados y resguardando la información del negocio.

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 7 de 8

- **Política de Administración de Redes:** Establece directrices para garantizar la integridad, confidencialidad y disponibilidad de los recursos tecnológicos, manteniendo una infraestructura de red robusta y segura.
- **Política de Gestión de Incidentes de Seguridad de la Información:** Garantiza una gestión eficiente y sistemática de los incidentes de seguridad de la información, abarcando la detección, respuesta y notificación de eventos de seguridad y vulnerabilidades.

8. Cumplimiento de la Política

8.1. Excepción

Cualquier solicitud de excepción a esta política debe estar debidamente fundamentada por el solicitante y contar con la autorización del Information Security & Cybersecurity Manager, SVP Information & Communication Technologies y la Jefatura directa correspondiente.

8.2. Incumplimiento

El desconocimiento de las políticas por parte de los trabajadores, proveedores o terceros no los exime de la posible imposición de medidas legales y administrativas según corresponda.

9. Estándares Relacionados, Normativas y Procedimientos

- POL-002 Política de Escritorio Limpio
- POL-003 Política de Contraseñas
- POL-004 Política de Gestión de Activos de Información Tecnológica
- POL-005 Política de Control de Acceso
- POL-006 Política de Uso de Software
- POL-007 Política de Administración de Redes
- POL-008 Política de Desarrollo Seguro
- POL-009 Política de Trabajo Remoto
- POL-010 Política de Gestión de Vulnerabilidades
- POL-011 Política de Seguridad con Proveedores
- POL-012 Política de Respaldo, Custodia y Restauración de Información
- POL-013 Política de Destrucción de Información
- POL-014 Política de Entorno en la Nube
- POL-015 Política de Continuidad del Negocio
- POL-016 Política de Gestión de Incidentes de Seguridad de la Información

10. Control de Versiones

Versión	Modificación		Descripción de Modificación
	Fecha	Nombre	
1.0	Dic-2023	Creación	Creación documento
1.1	Mar-2025	Modificación	Se añade POL-016 en ítem 7 y 9. Se elimina ítem Responsabilidades de usuarios y se mueve a las políticas subordinadas.
1.2	Oct-2025	Modificación	Se cambia documento a formato HGT.

POLÍTICA GENERAL DE SEGURIDAD INFORMACIÓN		Versión	1.2
Ref.	POL-001	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 8 de 8

11. Control de Cambios

Autor	Cargo	Fecha de Revisión	Aprueba
Daniela Romero	Information Security & Cybersecurity Manager	Octubre-2025	

Aprobador	Cargo	Firma
Claudio Aguilera	SVP Information & Communication Technologies	
Guillermo Henriquez	IT Operation Manager	
Gerardo Pacheco	IT Systems & PMO Manager	
Rolando Anzola	Business Intelligence & Analytics Manager	