

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 1 de 6

Política de Seguridad con Proveedores

Hanseatic Global Terminals Latin America S.A.

12 2023

Information & Communication Technologies

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 2 de 6

1. Resumen 3

2. Objetivos..... 3

3. Alcance 3

4. Glosario 3

5. Principios..... 4

6. Roles y Responsabilidades 5

7. Cumplimiento de Política 6

7.1. Excepción..... 6

7.2. Incumplimiento 6

8. Estándares Relacionados, Normativas y Procedimientos 6

9. Control de Versiones 6

10. Control de Cambios 6

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 3 de 6

1. Resumen

Hanseatic Global Terminals Latin America reconoce la importancia crítica de la seguridad de la Información en nuestro entorno operacional. En respuesta a las crecientes amenazas de seguridad de la información en el ciberespacio, estamos comprometidos por salvaguardar la integridad, confidencialidad y disponibilidad de nuestros activos de información. Este enunciado orienta a nuestros proveedores, instándolos a adoptar medidas proactivas que reflejen nuestro compromiso con la seguridad de la información y contribuir a preservar la continuidad del negocio.

2. Objetivos

Determinar los requisitos esenciales para asegurar la integridad y protección de la información y activos de Hanseatic Global Terminals Latin America y Filiales durante la contratación de servicios con terceros como durante la ejecución del contrato.

3. Alcance

Esta política aplica a todo el personal permanente de Hanseatic Global Terminals Latin America ("Hanseatic Global Terminals Latin America" o la "Compañía") y a sus empresas filiales, así como a cualquier tercero que maneje información de la Compañía y Filiales.

Las disposiciones se aplican en tareas que incluyen el diseño, desarrollo o funcionamiento de sistemas de información, mantenimiento de los sistemas, accesos remotos a la información y usuarios externos que requieran acceso a los sistemas o datos de Hanseatic Global Terminals Latin America y/o Filiales.

Se recomienda su adopción por parte de las empresas coligadas en las cuales Hanseatic Global Terminals Latin America no tenga participación mayoritaria ni control administrativo.

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.

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 4 de 6

5. Principios

- 5.1. Todo tercero debe suscribir una cláusula de confidencialidad y un acuerdo de no divulgación antes de obtener acceso a la información interna o confidencial de Hanseatic Global Terminals Latin America y/o Filiales.
- 5.2. Hanseatic Global Terminals Latin America y Filiales se reserva el derecho de auditar a sus proveedores, notificándoles con al menos 60 días de antelación para llevar a cabo la auditoría y verificar el cumplimiento de sus normativas internas.
- 5.3. Todo tercero está obligado a mantener un proceso de gestión de vulnerabilidades y de parches de seguridad en sus activos de información.
- 5.4. Se establece que todo tercero que gestionan servicios críticos debe realizar un escaneo de vulnerabilidades al menos semestralmente en su infraestructura, demostrando que cualquier brecha de seguridad está mitigada o cuenta con controles complementarios que reduzcan el nivel de riesgo.
- 5.5. Todo tercero que gestione información interna o confidencial, especialmente aquellos que proveen servicios críticos, se compromete a mantener actualizadas y activas las firmas de antivirus en su granja de servidores para la detección y eliminación de malware.
- 5.6. Para todo desarrollo, se debe de incorporar la capacidad de registro de logs de auditoría con el fin de obtener evidencia en caso de eventos operacionales, incidentes, actividades, acceso a información o sistemas, alertas, mensajes de consola y errores de sistema.
- 5.7. Todo tercero es responsable de los actos y omisiones de su personal. Por lo tanto, cualquier individuo con acceso a los activos de información de Hanseatic Global Terminals Latin America y/o Filiales, acceso a las instalaciones o información confidencial, debe recibir entrenamiento y participar de un programa de concientización en temas de seguridad de la información.
- 5.8. La complejidad de las contraseñas debe seguir la Política de Contraseñas publicado por Hanseatic Global Terminals Latin America, para mitigar amenazas relacionadas con el uso de contraseñas débiles.
- 5.9. Para cualquier transferencia de información entre Hanseatic Global Terminals Latin America y/o Filiales y un tercero a través de un canal de comunicación, se exige un cifrado robusto, evitando cifrados débiles como RC4 y 3DES.
- 5.10. La propiedad de software desarrollado para Hanseatic Global Terminals Latin America y/o Filiales debe quedar definida en el contrato con terceros.
- 5.11. a) La Vicepresidencia de Tecnologías de la Información y Comunicaciones lleva a cabo una evaluación anual de sus proveedores de servicios, con el objetivo de identificar aquellos clasificados como proveedores críticos, a los cuales se les implementará un proceso especial que incluirá el envío de un checklist de ciberseguridad con una periodicidad programada, para medir su nivel de cumplimiento con los estándares y políticas de seguridad de la información establecidos, garantizando así un monitoreo proactivo de la ciberseguridad.
b) Para las Filiales, la evaluación de sus proveedores de servicio es responsabilidad de la Gerencia de Tecnologías de la Información o del área interna encargada, quienes deben informar a la Information Security & Cybersecurity Manager sobre los resultados obtenidos.
- 5.12. Los proveedores de servicios deben de contar con un proceso formal y sistemático de gestión de incidentes que aborde de manera efectiva cualquier interrupción o impacto que pueda afectar la provisión de productos, servicios o actividades.
- 5.13. Se requiere que el proveedor contratado que gestione información interna o confidencial, especialmente aquellos que proveen servicios críticos, debe poseer certificaciones

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 5 de 6

independientes reconocidas a nivel internacional, en términos de gestión de seguridad de la información, continuidad del negocio y calidad del servicio.

- 5.14. Los datos, plataformas tecnológicas y aplicaciones utilizadas en la externalización de los servicios deben estar alojados en sitios de procesamiento específicos. En el caso de procesamiento en el extranjero, se requiere que estos se ubiquen en una jurisdicción definida y conocida. Además de la jurisdicción, es necesario tener información detallada de la ciudad donde operan los centros de datos.
- 5.15. a) La Information Security & Cybersecurity Manager verifica que el proveedor cuenta con adecuados mecanismos de seguridad, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la confidencialidad e integridad de los datos del negocio.
b) Para las Filiales, la responsabilidad de verificar el cumplimiento de los proveedores recae en la Gerencia de Tecnologías de la Información o área interna encargada, la cual debe informar a la Information Security & Cybersecurity Manager sobre el estado de cumplimiento de sus proveedores.
- 5.16. Todo tercero que utilice equipos no corporativos para el manejo de información interna de Hanseatic Global Terminals Latin America y Filiales, deben adherirse a los requerimientos técnicos establecidos por la Vicepresidencia de Tecnologías de la Información y Comunicaciones.

6. Roles y Responsabilidades

- **Vicepresidencia de Tecnologías de la Información y Comunicaciones:**
 - Garantizar la realización del proceso de evaluación de proveedores.
 - Mantener actualizada la lista de proveedores de tecnología.
- **Information Security & Cybersecurity Manager:**
 - Definir los requisitos de seguridad de la información para los proveedores.
 - Coordinar con la Vicepresidencia de Tecnologías de la Información y Comunicaciones que las directrices de seguridad de la información sean aplicadas por los proveedores.
 - Liderar evaluación anual de los proveedores de servicio, asegurando el cumplimiento de los estándares de seguridad de la información.
- **Proveedor o Tercero:**
 - Cumplir con las directrices de seguridad de la información establecidas por Hanseatic Global Terminals Latin America.
 - Colaborar en el proceso de evaluación llevadas a cabo por la Vicepresidencia de Tecnologías de la Información y Comunicaciones, proporcionando la información necesaria.

Para Filiales:

- **Gerencia de Tecnologías de la Información o área interna encargada:**
 - Garantizar la realización del proceso de evaluación de proveedores.
 - Mantener actualizada la lista de proveedores de tecnología.
 - Validar que las directrices de seguridad de la información sean aplicadas por los proveedores.

POLÍTICA DE SEGURIDAD CON PROVEEDORES		Versión	1.2
Ref.	POL-011	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 6 de 6

- Reportar a la Information Security & Cybersecurity Manager los resultados y acciones relacionadas con la evaluación de proveedores.

7. Cumplimiento de Política

7.1. Excepción

No existe excepción a la presente política.

7.2. 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.

8. Estándares Relacionados, Normativas y Procedimientos

- POL-001 Política General de Seguridad de la Información
- POL-003 Política de Contraseñas
- POL-008 Política de Desarrollo Seguro
- POL-010 Política de Gestión de Vulnerabilidades
- POL-016 Política Gestión de Incidentes
- MZ-003 Matriz de Evaluación Servicio Proveedores

9. Control de Versiones

Versión	Modificación		Descripción de Modificación
	Fecha	Nombre	
1.0	Dic-2023	Creación	Creación documento
1.1	Mar-2025	Modificación	Alcance. Se añade ítem 4. Glosario
1.2	Oct-2025	Modificación	Conversión del documento a formato HGT.

10. 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	