

POLÍTICA DE ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 1 de 6

Política de Escritorio Limpio

Hanseatic Global Terminals Latin America S.A.

12 2023

Information & Communication Technologies

POLÍTICA DE ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	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 5

7.1. Excepción 5

7.2. Incumplimiento 5

8. Estándares Relacionados, Normativas y Procedimientos 5

9. Control de Versiones 6

10. Control de Cambios 6

POLÍTICA DE ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 3 de 6

1. Resumen

La Política de Escritorio Limpio se establece con el propósito de garantizar la seguridad de cualquier información sensible, ya sea en formato digital o físico. Se enfoca en mantener la confidencialidad e integridad de los datos, previniendo posibles riesgos como filtraciones o accesos no autorizados. Todos los Colaboradores son responsables de cumplir con esta política para mantener un entorno de trabajo seguro y protegido.

2. Objetivos

Respaldar activamente la reducción de riesgos asociados al robo de información, posibles fraudes y prevenir la ocurrencia de brechas de seguridad al evitar la exposición de información sensible en espacios de trabajo desatendidos, promoviendo el mantenimiento seguro de los puestos de trabajo.

3. Alcance

Este alcance aplica a todo el personal permanente de Hanseatic Global Terminals Latin America ("Hanseatic Global Terminals Latin America" o la "Compañía"), así como a sus empresas filiales, proveedores y terceros que se encuentren en sus dependencias. Se extiende a todos aquellos que, de una u otra manera, interactúen con el entorno de trabajo, garantizando el cumplimiento de las medidas de seguridad establecidas.

Asimismo, se recomienda la adopción de esta política 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 ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 4 de 6

5. Principios

- 5.1. Al abandonar un espacio de trabajo sin supervisión, es esencial bloquear la sesión en las estaciones de trabajo y laptops para prevenir el acceso no autorizado y salvaguardar la integridad de los datos.
- 5.2. Para garantizar la Seguridad de la Información, los muebles y escritorios deben permanecer cerrados con llave cuando se encuentren desatendidos.
- 5.3. Los equipos de trabajo asignados deben asegurarse mediante un candado de seguridad al escritorio o almacenarse en una cajonera al dejar desatendido el puesto de trabajo.
- 5.4. Cualquier impresión que contenga información sensible debe ser retirada inmediatamente después de su uso.
- 5.5. Todas las impresiones que no sean retiradas serán destruidas al final de la jornada laboral para evitar divulgación no autorizada de la información.
- 5.6. Los escritorios deben mantenerse despejados, sin documentos ni credenciales de acceso a aplicativos del negocio a la vista, para mantener la confidencialidad.
- 5.7. Al finalizar cada reunión, se debe dejar las salas libres de información y materiales para mantener la privacidad y confidencialidad.
- 5.8. Todos los documentos y medios físicos que contengan información sensible deben de ser eliminados de manera segura mediante trituración o destrucción certificada cuando ya no sean necesarios.
- 5.9. Las pantallas de las estaciones de trabajo y dispositivos deben estar orientados de manera que no se vean visibles por personas no autorizadas, garantizando así la privacidad de la información.
- 5.10. En caso de escritorios compartidos, cada usuario es responsable de dejar el espacio libre de documentos y datos sensibles al finalizar su jornada.
- 5.11. Las contraseñas y credenciales de acceso deben ser almacenadas de forma segura y no deben quedar a la vista en ningún momento, incluso cuando se esté utilizando el puesto de trabajo.
- 5.12. Los dispositivos portátiles de uso corporativo como smartphones y tablets deben estar protegidos mediante contraseñas o autenticación biométrica para evitar accesos no autorizados.
- 5.13. Los visitantes deben ser acompañados y supervisados en todo momento, y se les debe informar sobre la Política de Escritorios Limpios si ingresan a las áreas de trabajo
- 5.14. Cuando los dispositivos de hardware y equipos ya no sean utilizados, deben ser desactivados y almacenados de manera segura o desechados siguiendo los procedimientos establecidos.
- 5.15. Se llevarán a cabo programas de capacitación y concientización para todos los Colaboradores, Proveedores y Terceros involucrados, para asegurar la comprensión y el cumplimiento de la Política de Escritorios Limpios.
- 5.16. Cualquier incidente de vulneración o incumplimiento de esta política debe ser reportado a la Information Security & Cybersecurity Manager de manera inmediata para su gestión y resolución, o bien, la Gerencia de Tecnologías de la información o área interna encargada correspondiente para el caso de Filiales.
- 5.17. La Política de Escritorios Limpios será revisada periódicamente para asegurar su relevancia y eficacia, y se actualizará según sea necesario para adaptarse a nuevas amenazas y desafíos de seguridad.

POLÍTICA DE ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 5 de 6

6. Roles y Responsabilidades

- **Vicepresidencia de Tecnologías de la Información y Comunicaciones:** Supervisar y garantizar que los sistemas y aplicaciones utilizados cumplan con los requisitos de seguridad establecidos, así como proporcionar el soporte técnico necesario para mantener la seguridad de los escritorios limpios.
- **Information Security & Cybersecurity Manager:** es responsable de la creación y comunicación de la política en el negocio, como también garantizar su implementación, permitiendo de este modo que la información se mantenga segura y protegida en todo momento, minimizando los riesgos de fuga de información o acceso no autorizado. Debe comunicar al negocio mediante campañas sobre la importancia de mantener escritorios limpios y seguros.
- **Colaboradores:** cada colaborador es responsable de mantener su espacio de trabajo limpio y ordenado, asegurándose que no haya información sensible visible cuando no estén presentes, guardar documentos o dispositivos con información confidencial de manera segura, seguir las políticas de limpieza establecidas.

Para Filiales:

- **Gerencia de Tecnologías de la Información o área interna encargada:** supervisar y garantizar que los sistemas y aplicaciones utilizados cumplan con los requisitos de seguridad establecidos, así como proporcionar el soporte técnico necesario para mantener la seguridad de los escritorios limpios. Colabora estrechamente con la Information Security & Cybersecurity Manager para el cumplimiento de las directrices y la implementación de las políticas de Seguridad de la Información en Filiales, asegurando que la información se mantenga protegida en todo momento, minimizando los riesgos de fuga de información o acceso no autorizado.

7. Cumplimiento de Política

7.1. Excepción

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

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 de General de Seguridad de la Información
- POL-004 Política de Gestión de Activos de la Información Tecnológica
- POL-013 Política de Destrucción de Información

POLÍTICA DE ESCRITORIO LIMPIO		Versión	1.1
Ref.	POL-002	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 6 de 6

9. Control de Versiones

Versión	Modificación		Descripción de Modificación
	Fecha	Nombre	
1.0	Dic-2023	Creación	Creación documento
1.0	Mar-2025	Revisión	Revisión anual sin modificaciones
1.1	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	