

POLÍTICA DE DESTRUCCIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 1 de 6

Política de Destrucción de Información

Hanseatic Global Terminals Latin America S.A.

12 2023

Information & Communication Technologies

POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	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 RESPALDO, CUSTODIA Y RECUPERACIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 3 de 6

1. Resumen

La política de destrucción de información destaca por ser un pilar fundamental para garantizar la confidencialidad de la información. Enfocada en prácticas seguras de borrado y destrucción de dispositivos, esta medida proactiva busca mitigar riesgos asociados con la divulgación no autorizada, consolidando así un entorno más seguro y confiable para la gestión de la información.

2. Objetivos

Preservar la integridad y confidencialidad de la información, minimizando riesgos y consolidando estándares de seguridad robustos, asegurando con ello la ejecución eficiente de procesos de destrucción segura, concentrándose en el borrado seguro y la eliminación irreversible de dispositivos no reasignado.

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, y abarca la totalidad de dispositivos y datos administrados por la Compañía y filiales, asegurando la implementación de prácticas seguras desde la identificación hasta la ejecución del proceso de destrucción. Este alcance también incluye a terceros, garantizando un cumplimiento consistente y transparente en todas las instancias de manejo de datos.

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 RESPALDO, CUSTODIA Y RECUPERACIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 4 de 6

5. Principios

- 5.1. Se establecen tres métodos para la eliminación de la información, los cuales varían según los niveles de clasificación de la Información:
 - Borrado Seguro: Realizado mediante un aplicativo que utiliza sobreescritura, este proceso debe llevarse a cabo al menos una vez.
 - Eliminación: Se refiere a la información descartada sin ninguna medida de protección, ya que su divulgación no afecta al negocio, no perjudica a los activos corporativos, no genera pérdidas financieras y no causa daño a ningún colaborador de Hanseatic Global Terminals Latin America y filiales.
 - Destrucción: Es la última medida de sanitización, ya que después de su ejecución, el dispositivo no puede volver a ser utilizado. Esta destrucción implica diversos métodos, como desintegración, incineración o pasar documentación o discos por una picadora de papel.
- 5.2. Toda información en formato físico que sea de carácter confidencial debe ser destruida de manera que no pueda ser reconstruida, ya sea mediante una picadora de papel o incineración.
- 5.3. Si la Información se encuentra almacenada en bodegas de un proveedor, este debe garantizar un proceso de eliminación seguro conforme a los periodos de retención establecidos en Hanseatic Global Terminals Latin America.
- 5.4. Si un equipo va a ser dado de baja, su unidad de almacenamiento debe ser destruida.
- 5.5. Al dar de baja un equipo, se mantiene un registro detallado, poniendo énfasis en el motivo de la baja, las medidas específicas tomadas para garantizar la eliminación segura de los datos, fecha y responsable de la acción, cumpliendo con las buenas prácticas de seguridad de la información de la industria.
- 5.6. En el caso de reutilización de equipos, se establece la obligatoriedad de aplicar un proceso de borrado seguro. Este proceso debe garantizar la eliminación completa de la información anterior mediante técnicas seguras de sobreescritura, cumpliendo con los estándares de seguridad establecidos.
- 5.7. En caso de fallo en el procedimiento de borrado seguro, la unidad de almacenamiento debe de ser destruida, garantizando que la información no pueda ser recuperada mediante técnicas forenses.
- 5.8. Realizar pruebas periódicas de los procesos de destrucción, evaluando la eficacia de los métodos implementados y asegurando de que cumplan con los estándares de seguridad establecidos.
- 5.9. Establecer protocolos específicos de eliminación rápida para situaciones de emergencia que requieran la destrucción inmediata de información sensible.
- 5.10. La información generada por terceros se somete a procesos detallados de eliminación, siguiendo las directrices de la política aplicados a la información interna.
- 5.11. Garantizar la integridad de la cadena de custodia, durante todo el proceso, desde la identificación hasta la destrucción.
- 5.12. Todos los equipos que se encuentren a la espera de su proceso de borrado seguro deben ser resguardados bajo llave, garantizando la protección de la información contenida en ellos.
- 5.13. Dado que las impresoras pueden tener capacidad de almacenamiento con información sensible, el proceso de baja de estos dispositivos debe llevarse a cabo mediante esta política.
- 5.14. Se deben revisar y actualizar periódicamente los métodos y herramientas utilizados para la eliminación de información, garantizando que estén alineados con las últimas mejores prácticas de seguridad.

POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	Fecha de Vigencia	Octubre 2025
Clasificación	Uso Interno	Página	Página 5 de 6

- 5.15. Se deben establecer políticas claras para la retención de datos, definiendo los plazos específicos durante los cuales la información debe ser custodiada antes de su posible eliminación.

6. Roles y Responsabilidades

- **Information Security & Cybersecurity Manager:**
 - Supervisar y coordinar la implementación de la política de destrucción de la información, para Hanseatic Global Terminals Latin America y Filiales.
 - Garantizar el cumplimiento de los estándares de seguridad establecidos.
 - Evaluar y actualizar regularmente los procedimientos de destrucción segura.
- **IT Operations Manager:**
 - Implementar medidas técnicas para la destrucción segura de datos, incluido el borrado seguro en los dispositivos y la gestión de eliminación de carpetas y archivos.
 - Coordinar con Information Security & Cybersecurity Manager para asegurar la integridad de los procedimientos técnicos.
- **Equipo Respuesta ante incidentes:**
 - Activar los protocolos de destrucción segura en caso de incidentes de seguridad.
 - Colaborar con las partes interesadas para mitigar riesgos y minimizar el impacto de cualquier brecha de seguridad.

Para Filiales:

- **Gerencia de Tecnologías de la Información o área interna encargada:**
 - Implementar medidas técnicas para la destrucción segura de datos en las filiales.
 - Colaborar con Information Security & Cybersecurity Manager de Hanseatic Global Terminals Latin America en asuntos de seguridad de la información en filiales.
 - Supervisar la ejecución de procedimientos técnicos relacionados con la destrucción segura de la información en las filiales

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-012 Política de Respaldo, Custodia y Recuperación de Información
- POL-016 Política de Incidentes de Seguridad de la Información

POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE INFORMACIÓN		Versión	1.1
Ref.	POL-013	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 cambios
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	