

## 1. OBJETIVO

Establecer lineamientos claros y efectivos para resguardar los respaldos de información, software y sistemas asegurando la integridad, confidencialidad y disponibilidad de la información en conformidad al área de Tecnologías de la Información (T.I.).

## 2. RESPONSABILIDADES

### *Usuario*

- Debe realizar el correcto manejo de la información que se encuentre en su equipo de cómputo.
- Manejar las carpetas (Descargas, Documentos, Escritorio e Imágenes) para futuros respaldos y evitar desorganización de la info.
- Evitar modificaciones sin notificar a los integrantes en las carpetas compartidas.

### *Personal Externo*

- Cumplir con los lineamientos descritos dentro de esta política

## 3. POLÍTICA

Grupo Rimova S. A. DE C.V. es una empresa con experiencia en el mercado, trabajando para gobiernos y dependencias privadas, fabricando mobiliario y recursos didácticos.

### **Dentro del área de Sistemas TI cuentan con los siguientes lineamientos:**

Se debe contar con un plan de respaldo, en relación con las capacidades de la organización, cada jefatura, dueño de proceso y/o propietario de activos de información quien será responsable de informar al área TI aquella información, software y/o sistemas que por su naturaleza requiera ser incluida en el plan de respaldo.

- Toda la información digital, de software y sistemas que se resguarda en site y oficina de T.I debe ser almacenada en un lugar físico distinto de las salas de servidores, a una distancia suficiente para evitar cualquier daño ante desastres.
- Los respaldos (Backus) deben realizarse de forma periódica y almacenarse en ubicaciones seguras.
- Las cintas de respaldo tendrán un lugar de protección física y ambiental adecuada para mantener la confidencialidad, la integridad y la disponibilidad de la información digital, de software y sistemas informáticos.
- El acceso al lugar de almacenamiento de las cintas de respaldo será restringido y sólo podrán acceder a aquellas personas autorizadas por el área de TI.
- En el plan de respaldo, se debe considerar las pruebas de restauración de respaldos realizados en los periodos anteriores.
- La información debe clasificarse en niveles de confidencialidad (pública, interna, confidencial y restringida) según su sensibilidad y criticidad.
- El acceso a la información debe ser autorizado por los responsables del área de T.I. y limitado según los roles y responsabilidades de los colaboradores.
- Se utilizarán herramientas de ciberseguridad (antivirus, firewalls) para proteger la información contra accesos no autorizados, malware (programa maligno) y otros riesgos.
- El área de T.I. realizará auditorías y monitoreo de forma anual, para asegurar el cumplimiento de esta política y detectar vulnerabilidades.

El cumplimiento de la política de respaldo, sus normas, procedimientos y estándares, sus correspondientes actualizaciones y/o modificaciones, serán publicadas para los proveedores, clientes y cualquier usuario que se encuentre interesado en la empresa se encontrara visible en la página web de GRUPO RIMOVA, en la dirección <https://gruporimova.com/nosotros/nuestras-politicas/>

La presente política de resguardo de la información de TI tiene vigencia a partir del 02 de enero del 2025, y tendrá vigencia hasta nueva directriz.