1. OBJETIVO

Establecer los lineamientos para el uso, gestión, protección y control de los recursos tecnológicos y del sistema ERP de Grupo RIMOVA, asegurando la confidencialidad, integridad y disponibilidad de la información, así como la continuidad operativa.

2. ALCANCE

Esta política aplica a:
•Todo el personal interno y externo que utilice recursos del área de sistemas.
•Infraestructura tecnológica (hardware, software, redes).
•Sistemas de información, incluyendo el ERP.
•Información digital y física gestionada por el área de sistemas.

3. RESPONSABILIDADES

Alta Dirección
•Aprobar y vigilar el cumplimiento de la presente política.
•Proveer los recursos necesarios para el mantenimiento y soporte de los sistemas informáticos.

Area de Sistemas
•Implementar, mantener y mejorar los controles para el buen funcionamiento de los sistemas informáticos de la organización.
•Gestionar de manera oportuna los incidentes internos y los respaldos en tiempos programados para asegurar la continuidad de las operaciones administrativas.
•Administrar los recursos disponibles del ERP, así como capacitar y difundir los cambios y funcionamiento del ERP.

Usuarios
•Cumplir con lo establecido en la presente política y cualquier otro documento que ayude al mantenimiento y seguridad de los recursos informáticos.
•Proteger sus accesos y credenciales otorgadas por el área de sistemas.
•Reportar cualquier incidente presentado en los programas, equipos o herramientas gestionadas por el área de sistemas.

4. DEFINICIONES

Antivirus: Software de ciberseguridad diseñado para detectar, bloquear y eliminar código malicioso (malware) como virus, ransomware, spyware y troyanos de ordenadores y dispositivos. Actúa como un escudo protector en tiempo real, analizando archivos, descargas y navegación para evitar daños, robo de información o secuestro del sistema.

Disco duro externo: Dispositivo portátil de almacenamiento de datos que se conecta a una computadora u otro equipo mediante cable (generalmente USB o Thunderbolt) para aumentar la capacidad de memoria, realizar copias de seguridad (backup) o transportar archivos pesados. Funcionan como una unidad adicional, sin necesidad de instalarlos internamente.

ERP: sistema de software que integra y automatiza los procesos clave de una empresa en una única base de datos. Permite centralizar la gestión, mejorar la productividad y obtener información en tiempo real para tomar decisiones estratégicas.

Google Drive: servicio de alojamiento y almacenamiento en la nube de Google que permite guardar, sincronizar y compartir archivos de forma segura desde cualquier dispositivo, permitiendo editar documentos en tiempo real.

Hardware: Conjunto de componentes físicos, tangibles y electrónicos que conforman un sistema informático, como computadoras, teléfonos o servidores. Incluye todo lo que se puede tocar, desde piezas internas (procesador, memoria RAM, disco duro) hasta periféricos externos (teclado, monitor, mouse).

NAS Synology: Servidor de almacenamiento en red (Network Attached Storage) que funciona como tu propia nube privada y segura. Permite centralizar archivos, realizar copias de seguridad automáticas, gestionar multimedia y compartir datos desde cualquier lugar.

PIN: Código numérico o alfanumérico secreto de seguridad utilizado para verificar la identidad de un usuario y proteger el acceso a sistemas, dispositivos o servicios.

Software: Conjunto de componentes lógicos, instrucciones, programas y reglas informáticas necesarios para hacer funcionar un dispositivo (computadora, teléfono, etc.), permitiéndole realizar tareas específicas. Es la parte intangible, en contraposición al hardware (físico), actuando como el "cerebro" que le dice al equipo qué hacer.

5. PRINCIPIOS GENERALES

•La información manejada y contenida en los dispositivos es un activo crítico de la organización.
•El acceso a sistemas debe estar basado en el principio de mínimo privilegio, es decir, que cualquier usuario, aplicación o sistema debe tener solo los permisos mínimos necesarios para realizar su función.
•Todos los usuarios son responsables del uso adecuado de los recursos tecnológicos.
•Se garantizará la continuidad del negocio mediante controles preventivos y correctivos.

6. SEGURIDAD DE LA INFORMACIÓN

Se deben mantener los mecanismos para asegurar la confidencialidad (acceso solo a personal autorizado), integridad (datos exactos y sin alteraciones no autorizadas) y disponibilidad (acceso cuando se requiera).

6.1. Clasificación de la Información

•Pública: Incluye documentos, registros y datos en cualquier formato que estén en posesión de sujetos obligados (entes públicos), elaborados o adquiridos en el ejercicio de sus funciones, según la Ley General de Transparencia y Acceso a la Información Pública.
•Interna: Es todo dato generado y consumido dentro de la propia organización, vital para la toma de decisiones, la operación diaria y la estrategia competitiva. Incluye registros financieros, nóminas, manuales, comunicaciones, estrategias de marketing y propiedad intelectual.
•Confidencial: Abarca datos sensibles cuya divulgación puede dañar su competitividad, reputación o seguridad, incluyendo secretos comerciales, financieros, listas de clientes, estrategias de negocio y datos personales de empleados o clientes. Esta información está protegida legalmente para evitar el acceso no autorizado
•Restringida: Incluye datos sensibles cuya divulgación puede causar daños financieros, legales o de reputación, como secretos comerciales, financieros, personales de empleados/clientes (PII), contraseñas y estrategias de mercado. Esta información requiere alta protección y acceso limitado, siendo fundamental para la seguridad y el cumplimiento legal.

6.2. Control de Accesos

•Todo acceso a sistemas tecnológicos y ERP deberá estar autorizado y será basado en roles.
•Se implementarán usuarios únicos e intransferibles.
•Todo equipo asignado deberá contar obligatoriamente con contraseñas seguras o PIN de bloqueo y su renovación será periódica.
•Se eliminarán accesos inmediatamente tras la baja del colaborador, sin embargo, el área podrá reasignar los accesos al colaborador que autorice su jefe inmediato.

6.3. Protección de la Información

•Se utilizarán herramientas de ciberseguridad (antivirus, firewalls) para proteger la información contra accesos no autorizados y software malicioso.

7. USO DE RECURSOS DEL ÁREA DE SISTEMAS

•Los recursos tecnológicos son para uso laboral exclusivamente, por lo que:
- oEl usuario es responsable del resguardo físico del equipo, tanto dentro de las instalaciones como al retirarlo (si aplica) de las instalaciones.
- oEl usuario debe manejar adecuadamente las carpetas locales (Descargas, Documentos, Escritorio e Imágenes) para facilitar futuros respaldos y evitar desorganización.

•Queda prohibido:
- oInstalar software no autorizado.
- oAcceder a contenido inapropiado.
- oCompartir credenciales.
- oUsar nubes o correos personales para almacenar o transmitir información corporativa.
- oRealizar modificaciones masivas o eliminaciones sin notificar previamente a los integrantes del área.

•El uso de internet y correo electrónico será monitoreado.
•Los usuarios deben reportar cualquier anomalía del funcionamiento del equipo asignado, así como de los programas o software instalado.

8. GESTIÓN DEL ERP

•El ERP es el sistema central de operación, por lo que:
- oSe debe garantizar la integridad de los datos.
- oTodo cambio en configuraciones debe ser autorizado.
- oSe deben mantener registros (logs) de operaciones.

•Se realizarán validaciones periódicas de la información.
•Se restringirá el acceso por roles y responsabilidades.

9. RESPALDOS Y RECUPERACIÓN DE INFORMACIÓN

9.1. Respaldos

Cada jefatura o dueño de proceso es responsable de la información respaldada y los medios (físicos o digitales) en los cuales se realizará el respaldo, así mismo, debe informar al área de sistemas:
•El periodo en los cuales se realizarán los respaldos.
•Las ubicaciones donde se almacenarán (local y/o nube) mismas que deben ser seguras.
•La verificación periódica para asegurar la integridad de sus respaldos.

Las opciones autorizadas son:
a) Google Drive (Seguridad Alta): Repositorio principal para documentos operativos y del día a día.
b) NAS Synology (Seguridad Alta): Para archivos pesados y carpetas compartidas.
c) ERP Odoo (Seguridad Muy Alta): Fuente oficial de la operación. Los respaldos se ejecutan diariamente (verificados mediante Log), se almacenan en 3 ubicaciones (2 Europa, 1 Canadá) y se mantiene un historial de al menos 30 días.
d) Disco Duro Externo (Seguridad Media): Respaldo físico de emergencia. Debe almacenarse en un lugar seguro, con protección ambiental y distinto a la sala de servidores.
e) Equipo Físico (Seguridad Baja): Solo para trabajo temporal. Guardar archivos únicamente aquí no se considera un respaldo válido.

9.2. Recuperación

El área de sistemas y los propietarios de la información realizarán pruebas periódicas de restauración para asegurar que los archivos generados sean íntegros y funcionales.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

•Todo incidente deberá ser reportado inmediatamente al área de sistemas.
•Se clasificará según su impacto y urgencia.
•En caso de robo o extravío de equipo, sospecha de virus, falla en la sincronización o accesos no autorizados, el usuario debe reportarlo inmediatamente al área de sistemas.
•El área de sistemas procederá a bloquear cuentas, contener el incidente y restaurar la información desde los respaldos. Cualquier falla en el proceso de respaldo del ERP será reportada de inmediato al proveedor para su corrección.

11.GESTIÓN DE ACTIVOS DEL ÁREA DE SISTEMAS

•Todos los activos deben estar inventariados y etiquetados.
•El Área de Sistemas es responsable de mantener el control, asignación e inventario del hardware, software y licenciamiento de la empresa
•Se asignarán responsables por cada activo.
•El área de sistemas realizará auditorías y monitoreo de forma anual para asegurar el cumplimiento de esta política, detectar vulnerabilidades y garantizar la continuidad operativa.

12. DIVULGACIÓN Y CAPACITACIÓN

Esta política será difundida a todo el personal mediante:
•Inducción al nuevo ingreso (cuando aplique).
•Capacitaciones programadas con las áreas.
•Publicación en los medios de difusión establecidos.

13. CUMPLIMIENTO

El incumplimiento de esta política puede derivar en medidas disciplinarias de acuerdo con su gravedad y conforme a la matriz de sanciones de Grupo RIMOVA.

14. CONTROL DE CAMBIOS

VERSIÓN	FECHA	MOTIVO	RESPONSABLE
00	Abril 2026	Documento Nuevo	Roberto Pérez Diaz