POLÍTICA DE USO ACEPTABLE DE RECURSOS TECNOLÓGICOS

Establecer las normas, límites y responsabilidades para el uso correcto, ético y legal de todos los recursos tecnológicos y activos de información de **PAPELERA REYES S.A.C.,** con el fin de proteger la infraestructura, garantizar la seguridad y apoyar la continuidad del negocio, asegurando la confidencialidad, integridad y disponibilidad de la información frente a riesgos y amenazas cibernéticas**.**

La presente política es de **aplicación obligatoria** para todos los trabajadores, contratistas, proveedores y terceros que accedan, utilicen o interactúen con los recursos tecnológicos de la organización.

1. Gobierno y Responsabilidad

- **Patrocinio Gerencial:** La Gerencia General es el responsable final de la Seguridad de la Información y de asegurar los recursos necesarios para el cumplimiento de esta política.
- **Responsable de Gestión:** El Jefe de Tecnología de la Información (TI) es el responsable de la supervisión, implementación y cumplimiento de esta política y de los procedimientos de ciberseguridad relacionados.
- **Revisión y Actualización:** Esta política será revisada y aprobada por la Alta Dirección al menos una vez al año o ante cualquier cambio significativo en la tecnología, normativa u operaciones.

2. Gestión de Accesos y Credenciales

El uso de los recursos tecnológicos es para fines laborales. Todo usuario es el responsable directo de su cuenta y sus acciones en el sistema.

- **Asignación Individual:** Se gestionarán los accesos digitales asignando credenciales individuales.
- **Rigor en Contraseñas:** Las credenciales deben cumplir estrictamente con la Política de Contraseñas Reforzada definida en el P-TI-002.
- **Autenticación Multifactor (MFA):** El uso de MFA es obligatorio para TODOS LOS USUARIOS con acceso al Correo Electrónico y el sistema ERP (incluyendo sus aplicaciones web).
- **Prohibición de Compartir:** Está estrictamente prohibido compartir, divulgar o usar las credenciales de otro usuario.
- **Desactivación Inmediata:** La eliminación o desactivación de cuentas de acceso (red, correo, ERP, etc.) debe realizarse de forma inmediata (plazo máximo de 1 hora) tras la notificación oficial de cese por parte del área de Recursos Humanos.

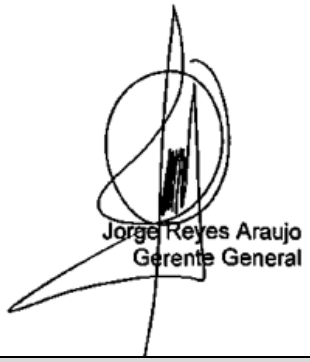
3. Uso Aceptable de Sistemas e Infraestructura

- **Clasificación de la Información:** Todo usuario debe manejar la información según el Esquema de Clasificación de la Información (Confidencial, Interna, Pública).
- **Software Autorizado:** Proteger la infraestructura tecnológica mediante el uso de software licenciado y actualizado, y queda restringido el uso de dispositivos o software no autorizados en los equipos corporativos.
- **Gestión de Vulnerabilidades:** Todos los sistemas operativos, firmware y aplicaciones deben ser sometidos a procesos de actualización y parcheo periódico para mitigar vulnerabilidades conocidas.
- **Uso de Internet y Correo:** El uso de Internet y el correo electrónico corporativo debe priorizar actividades relacionadas con el trabajo.
- **Respaldo y Continuidad:** Se debe garantizar la realización de respaldos periódicos de la información crítica y contar con mecanismos de recuperación para la continuidad de las operaciones. Los respaldos de información crítica deben ser diarios y al menos una copia debe almacenarse en un ambiente segregado (fuera de línea o aislado).

4. Gestión de Incidentes y Comunicación

- **Reporte Obligatorio:** Cualquier incidente o sospecha de incidente de seguridad debe ser reportado de forma inmediata al área de TI.
- **Métrica de Respuesta:** Los procedimientos de respuesta a incidentes deben establecer un objetivo de contención para incidentes de alta prioridad no superior a 4 horas desde su detección.
- **Formación Obligatoria:** Todos los trabajadores, contratistas y terceros que accedan a recursos tecnológicos deben completar formación obligatoria en concienciación de ciberseguridad (incluyendo phishing y manejo de información) al menos una vez al año.
- **Cumplimiento:** El incumplimiento de esta política puede resultar en la suspensión del acceso a los recursos tecnológicos y/o en acciones disciplinarias, de acuerdo con la normativa interna.

Callao, 17 de noviembre del 2025



CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
00	17/11/2025	Creación del documento.