POLÍTICA DE SEGURIDAD DE LA INFORMACION

PAPELERA REYES S.A.C., establece la presente política con el fin de proteger sus activos de información, sistemas tecnológicos, datos sensibles y procesos críticos ante posibles riesgos, accesos no autorizados, pérdidas o alteraciones, garantizando su confidencialidad, integridad y disponibilidad.

La presente política es de cumplimiento obligatorio y se aplica a todos los trabajadores, contratistas, proveedores y terceros que accedan a información de la organización.

En el marco del Sistema de Gestión en Control y Seguridad (SGCS BASC), la organización asume y establece los siguientes compromisos y lineamientos específicos:

1. Gobierno y Responsabilidad

- Patrocinio Gerencial: La Gerencia General es el responsable final de la Seguridad de la Información, asegurando los recursos necesarios para el cumplimiento de esta política.
- Revisión y Actualización: Esta política y las medidas de seguridad asociadas serán revisadas y aprobadas por la Alta Dirección al menos una vez al año o ante cualquier cambio significativo en la tecnología, normativa u operaciones.

2. Clasificación y Protección de la Información

- Clasificación Obligatoria: Se establecerá y mantendrá un Esquema de Clasificación de la Información que permita identificar, etiquetar y proteger los activos de información (Confidencial, Interna, Pública) según su criticidad.
- Controles Físicos y Lógicos: Proteger la información ante accesos no autorizados, pérdidas o alteraciones, aplicando controles físicos, lógicos y administrativos adecuados a la clasificación del activo.
- Confidencialidad: Preservar la confidencialidad de la información de origen interno y externo, cumpliendo con las disposiciones legales y contractuales aplicables.

3. Gestión de Sistemas y Controles de Acceso

- Ciberseguridad: La protección de sistemas, redes y plataformas digitales, así como el control de accesos y monitoreo de su uso, debe realizarse en estricto cumplimiento de la Política de Ciberseguridad (PO-TI-002) y sus procedimientos asociados; incluyendo el P-TI-002 para contraseñas, el cual establece la obligatoriedad de la renovación de credenciales cada 90 días, y el P-TI-001 para la gestión de bajas de usuarios.

4. Gestión de Riesgos y Auditoría

- Evaluación Periódica: Se realizarán evaluaciones formales de riesgos de seguridad de la información y auditorías internas al menos una vez al año, que permitan detectar vulnerabilidades y reforzar controles.
- Mitigación de Riesgos: Implementar acciones correctivas y preventivas oportunas ante la identificación de riesgos o vulnerabilidades.

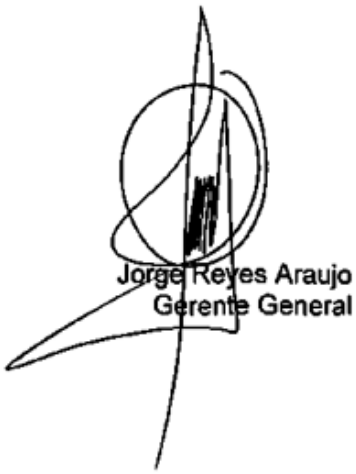
5. Gestión de Incidentes

- Atención Oportuna: Gestionar los incidentes de seguridad conforme a protocolos establecidos.
- Métrica de Respuesta: Los protocolos de respuesta a incidentes deben garantizar la atención oportuna, estableciendo un objetivo de contención para incidentes críticos no superior a 4 horas desde su detección.

6. Formación y Factor Humano

- Formación Obligatoria: La capacitación en buenas prácticas de seguridad de la información y uso seguro de tecnologías debe ser obligatoria y realizarse al menos una vez al año para todos los trabajadores, contratistas y terceros.

Callao, 15 de noviembre del 2025



CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
00	01/07/2025	Creación del documento.
01	15/11/2025	Actualización y Refuerzo de Compromisos: Inclusión de mandatos específicos sobre la revisión anual de la política, clasificación de la información, obligatoriedad de formación anual, y establecimiento de frecuencia de riesgos y métrica de tiempo para incidentes (SLA).