POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

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.

Propietario del Activo de Información:

- Cada Gerente o Jefe de Área es el responsable de determinar la clasificación inicial de los activos de información que genera o administra, basándose en el impacto del riesgo.
- El Propietario debe asegurar que la clasificación y el etiquetado se realicen en el momento de la creación del activo.

Revisión y Actualización: Esta política y su esquema de clasificación serán revisados y aprobados por la Alta Dirección al menos una vez al año o ante cualquier cambio significativo en la tecnología, normativa u operaciones.

2. Esquema de Clasificación y Etiquetado

Clasificación Obligatoria: Se establece y mantendrá un Esquema de Clasificación de la Información que permita identificar, etiquetar y proteger los activos de información según su criticidad.

Se adopta el siguiente esquema de clasificación formal, basado en la criticidad y el impacto que su divulgación o alteración causaría a la organización:

Nivel de Clasificación	Definición de Criticidad/Impacto
CONFIDENCIAL	**ALTO.** Divulgación o alteración causaría daño grave o irreparable, incluyendo incumplimiento legal severo.
INTERNA	**MEDIO/BAJO.** Información de uso exclusivo dentro de la organización. Su divulgación afectaría operaciones internas.
PÚBLICA	**INSIGNIFICANTE.** Información que puede ser compartida libremente sin perjuicio.

Clasificación por Defecto: En caso de duda o ausencia de etiqueta, el activo de información deberá ser tratado automáticamente como **CONFIDENCIAL**.

Lineamientos de Etiquetado:

- Todo activo clasificado como CONFIDENCIAL o INTERNO debe ser etiquetado de forma clara y visible (físico o digital) para asegurar su reconocimiento y manejo adecuado.
- Las etiquetas deben ser reconocibles y uniformes en toda la organización.

3. Manejo, Acceso y Controles de Protección

Controles Físicos y Lógicos: Se deben aplicar controles físicos, lógicos y administrativos adecuados a la clasificación del activo para proteger la información ante accesos no autorizados, pérdidas o alteraciones.

Gestión de Accesos

- Mínimo Privilegio: Los accesos se asignarán únicamente a la información estrictamente necesaria para el desempeño de las funciones del usuario (necesidad de conocer).
- MFA Obligatorio: El uso de Autenticación Multifactor (MFA) es de obligatoriedad para TODOS LOS USUARIOS con acceso al Correo Electrónico y el sistema ERP (incluyendo sus aplicaciones web).
- 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 laboral por parte del área de Recursos Humanos.

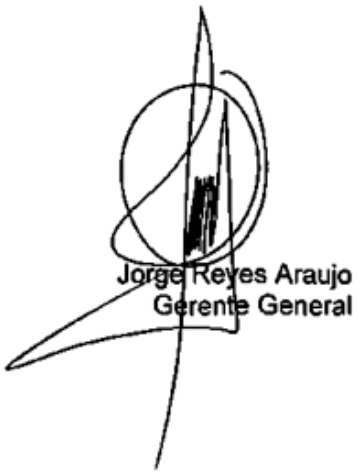
Criptografía y Respaldo

- Cifrado: La información clasificada como CONFIDENCIAL debe ser protegida mediante el uso de cifrado en almacenamiento (en reposo) y durante la transmisión (en tránsito).
- Respaldo Segregado: Los respaldos de la información crítica (CONFIDENCIAL) deben ser diarios. Además, debe garantizarse que al menos una copia de seguridad se almacene en un ambiente segregado (fuera de línea o almacenamiento aislado) para protegerse contra ataques de ransomware u otro malware.

4. Disposición de Medios y Cumplimiento

- Disposición Segura: La eliminación de activos de información (físicos o electrónicos) clasificados como CONFIDENCIAL o INTERNO debe realizarse mediante procedimientos de destrucción segura (borrado electrónico irreversible o trituración de papel) para evitar su recuperación.
- Formación Obligatoria: La capacitación en buenas prácticas de seguridad de la información y uso seguro de tecnologías (incluyendo phishing y manejo de información clasificada) debe ser obligatoria y realizarse al menos una vez al año para todos los trabajadores, contratistas y terceros.
- 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
01	17/11/2025	Creación del documento.