# POLÍTICA DE CIBERSEGURIDAD

PAPELERA REYES S.A.C., establece la presente política con el objetivo de proteger su infraestructura tecnológica, sistemas informáticos y activos digitales, garantizando la confidencialidad, integridad y disponibilidad de la información frente a riesgos y amenazas cibernéticas.

Esta política es de aplicación obligatoria para todos los trabajadores, contratistas, proveedores y terceros que accedan a los recursos tecnológicos de la organización.

En virtud de este compromiso, PAPELERA REYES S.A.C. adopta los siguientes lineamientos:

## a) Gobierno y Responsabilidad

- Asignación de Responsabilidad: 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 de la Política: Esta política será revisada y aprobada por la Gerencia General y el Representante BASC al menos una vez al año o inmediatamente después de un incidente grave de seguridad que afecte a la organización.

## b) Gestión de Accesos y Credenciales

- Gestionar los accesos digitales asignando credenciales individuales, exigiendo Autenticación Multifactor (MFA) obligatoriedad para TODOS LOS USUARIOS con acceso al Correo Electrónico y el sistema ERP (incluyendo sus aplicaciones web), y asignando niveles de permisos de acuerdo con las funciones.
- Rigor en Contraseñas: Las credenciales deben cumplir estrictamente con la Política de Contraseñas Reforzada definida en el P-TI-002.
- Eliminar accesos al finalizar la relación laboral o contractual y restringir el uso de dispositivos o software no autorizados.
- 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.

## c) Monitoreo y Auditoría de Acceso

- La organización establece el mandato de que todos los sistemas que manejan información crítica (incluyendo el ERP, el Sistema de Toma de Pedidos, el Correo Electrónico y los Servidores) deben estar configurados para registrar de forma inmutable y con sello de tiempo (timestamp):

  **Todos los Intentos de Inicio de Sesión Fallidos**: Para detectar ataques de fuerza bruta.
  **Todos los Inicios de Sesión Exitosos (Conformes):** Para asegurar la trazabilidad (quién, cuándo y desde dónde accedió).

- El Jefe de TI es responsable de asegurar que estos logs sean retenidos por un mínimo de 90 días y que el personal de TI los revise periódicamente conforme al umbral y el flujo definidos en el P-TI-002.

### d) Protección de Infraestructura y Sistemas

- Proteger la infraestructura tecnológica mediante controles preventivos, uso de software licenciado y actualizado, y mecanismos de seguridad aplicables a redes, servidores y dispositivos.
- Gestión de Vulnerabilidades: Todos los sistemas operativos, firmware y aplicaciones deben ser sometidos a procesos de actualización y parcheo periódico para mitigar vulnerabilidades conocidas.

### e) Respaldo, Recuperación y Continuidad

- Realizar respaldos periódicos de la información crítica y garantizar mecanismos de recuperación para la continuidad de las operaciones.
- Frecuencia y Segregación: Los respaldos de la información crítica deben ser diarios. 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.

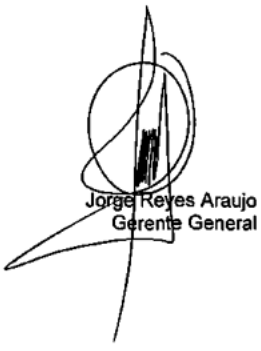
### f) Gestión de Incidentes y Evaluación de Riesgos

- Gestionar los incidentes de ciberseguridad, mediante procedimientos establecidos para su detección, análisis, tratamiento y mejora.
- Tiempos de Respuesta (SLA): 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.
- Evaluar los riesgos tecnológicos, implementando acciones correctivas cuando se identifiquen vulnerabilidades en la infraestructura informática.
- Periodicidad del Riesgo: La evaluación formal de riesgos tecnológicos y vulnerabilidades se realizará como mínimo una vez al año.
- Ejecutar ejercicios prácticos y/o simulacros de ciberseguridad, que permitan verificar la eficacia de los controles y reforzar la preparación ante incidentes.

### g) Formación y Mejora Continua

- Promover la mejora continua del sistema de ciberseguridad, mediante auditorías, revisión de políticas y fortalecimiento de capacidades.
- 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.

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 políticas de seguridad, (MFA) obligatorio para sistemas críticos (Correo Electrónico y ERP)<br>Refuerzo de Trazabilidad y Seguridad (BASC/ISO): Se incluye el mandato obligatorio de Registro de Auditoría (Logging) de todos los intentos de inicio de sesión fallidos y conformes en sistemas críticos, estableciendo el requisito de retención mínima de 90 días (3 meses) y revisión periódica de dichos logs. |