Política de Contraseñas – [Nombre de la Empresa]

1. Objetivo
El propósito de esta política es proteger la información y los sistemas de [Nombre de la Empresa] mediante el uso responsable y seguro de contraseñas por parte de todos los empleados, contratistas y colaboradores.

2. Alcance
Esta política se aplica a todas las cuentas, servicios, dispositivos y plataformas que requieran autenticación para acceder a información o recursos corporativos.

3. Requisitos de las contraseñas

- Las contraseñas deben tener **al menos 12 caracteres**.
- Deben incluir letras mayúsculas, minúsculas, números y símbolos.
- No deben contener información personal, como nombres, fechas o datos de la empresa.
- Cada cuenta debe tener una contraseña única.
- No está permitido compartir contraseñas por correo electrónico, chat u otros medios no seguros.

4. Almacenamiento y gestión

- Las contraseñas deben almacenarse exclusivamente en un **gestor de contraseñas autorizado** por la empresa (por ejemplo, **NordPass Business** o **1Password Business**).
- Está prohibido anotar contraseñas en papel o documentos digitales sin cifrar.

5. Cambios de contraseña

- Las contraseñas solo deberán cambiarse si existe sospecha de compromiso o indicios de filtración.
- Ante cualquier sospecha de acceso no autorizado, el empleado debe informar inmediatamente al departamento de TI o al responsable de seguridad.

6. Autenticación multifactor (MFA)

- Siempre que sea posible, se deberá activar la **autenticación multifactor** en todas las cuentas corporativas.

7. Responsabilidad del empleado
Cada usuario es responsable de proteger sus credenciales y de cumplir esta política. El incumplimiento podrá derivar en medidas disciplinarias internas.

Aprobada por: [Nombre / Cargo]
Fecha de entrada en vigor: [DD/MM/AAAA]