

Política de contraseñas

1. Objetivo

Garantizar la seguridad de la información mediante la implementación de contraseñas robustas y prácticas, reduciendo el riesgo de accesos no autorizados y protegiendo la confidencialidad e integridad de los datos de Lácteos San Antonio C.A.

2. Alcance

Esta política es aplicable a todos los colaboradores de Lácteos San Antonio C.A. en todas sus sedes, que utilicen sistemas y servicios que requieran autenticación mediante contraseñas en la red de la organización.

3. Definiciones

- **Contraseña:** Secuencia de caracteres utilizada para autenticar la identidad de un usuario.
- **Contraseña Robusta:** Combinación de letras, números y caracteres especiales, con longitud adecuada, que dificulta su descifrado.
- **Periodo de Cambio:** Frecuencia con la que los usuarios deben modificar sus contraseñas.
- **Mínimo de Caracteres:** Cantidad mínima de caracteres permitidos en una contraseña.
- **Bloqueo de Cuenta:** Medida de seguridad que se activa tras un número predefinido de intentos fallidos de inicio de sesión.
-

4. Documentos de Soporte

- No aplica.

5. Lineamientos Generales

- 5.1. Las contraseñas deben tener al menos 8 caracteres y contener una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.
- 5.2. Se debe cambiar la contraseña cada 90 días.
- 5.3. No se permiten contraseñas anteriores durante al menos 5 cambios.
- 5.4. No compartir contraseñas; cada usuario es responsable de su propia contraseña.
- 5.5. Las contraseñas no deben basarse en información fácilmente disponible o personal (datos personales, fechas de nacimiento, nombre de mascotas, etc.).
- 5.6. Cerrar sesión o bloquear cuando se abandone temporalmente la estación de trabajo.

6. Lineamientos Específicos

- 6.1. Los administradores de sistemas deben utilizar contraseñas más complejas y cambiarlas mínimo cada 90 días.
- 6.2. Realizar auditorías periódicas de contraseñas para identificar posibles vulnerabilidades.
- 6.3. Las contraseñas establecidas por cada uno de los empleados en los diferentes sistemas informáticos serán administradas y gestionadas bajo su responsabilidad.
- 6.4. No se debe escribir o almacenar contraseñas en lugares visibles o de fácil acceso.

- 6.5. El Departamento de TI configurará los sistemas informáticos para que el límite de intentos fallidos al ingresar una contraseña tenga un mínimo de 3 intentos; la solicitud de desbloqueo se realizara mediante creación de incidente GLPI.
- 6.6. Si un usuario sospecha que su contraseña ha sido comprometida, debe solicitar el cambio inmediatamente mediante creación de incidente GLPI.
- 6.7. Se prohíbe solicitar contraseñas vía telefónica o por escrito en medios como correo electrónico y redes sociales, en caso de necesitarlo el jefe inmediato del empleado al que corresponde el usuario deberá hacer la solicitud formal al departamento de sistemas.

7. Otras Disposiciones

- 7.1. En caso de haber compartido su contraseña deberá realizar la solicitud inmediata para el cambio mediante GLPI

Firmas



Sr. Luis David Moncayo S.

Gerente General