1. Objetivo

Esta política define los requisitos aplicables a la creación, gestión y protección de contraseñas, con el propósito de garantizar la seguridad de los activos informáticos críticos y los sistemas de la empresa. Debido al acceso privilegiado que posee a la infraestructura tecnológica, el personal corporativo está obligado a cumplir con protocolos de seguridad más estrictos.

2. Responsabilidades

- **Área de T.I.:** Son responsables de cumplir con esta política en su totalidad, gestionar sus contraseñas de forma segura y reportar inmediatamente cualquier sospecha de compromiso.
- **Área de T.I.:** Es responsable de hacer cumplir la política, realizar auditorías periódicas y asegurar que el equipo reciba la capacitación necesaria.
- **Administradores de Sistemas:** Es responsable de configurar los sistemas para que apliquen técnicamente esta política (longitud, complejidad, caducidad) y de monitorear intentos de acceso no autorizados.

3. Requisitos para las Contraseñas

3.1. Creación de Contraseñas Fuertes:

Todas las contraseñas deben cumplir con los siguientes criterios mínimos:

- **Longitud Mínima:** 14 caracteres.
- **Complejidad:** Debe incluir una combinación de al menos tres de los siguientes cuatro tipos de caracteres:
    - Letras mayúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiales (¡por ejemplo, !, @, #, $, &, *)
- **Prohibiciones:**
    - No utilizar información personal (nombres, fechas de nacimiento, matrículas).
    - No utilizar palabras del diccionario en cualquier idioma.
    - No utilizar patrones simples (123456, qwerty, abcd).

- No reutilizar las últimas 5 contraseñas.

3.2. Contraseñas de Sistemas Críticos y Cuentas Privilegiadas:
Para cuentas de administrador, servidores, routers, firewalls, bases de datos y cualquier sistema considerado crítico, se aplican reglas adicionales:

- **Longitud Mínima:** 16 caracteres.
- **La contraseña debe ser compleja por defecto** (usar los cuatro tipos de caracteres).
- **Donde sea posible, se debe implementar la autenticación multifactor (MFA/2FA) como requisito obligatorio.**

4. Gestión y Almacenamiento de Contraseñas

4.1. Almacenamiento Seguro:

- **Prohibido:** Anotar contraseñas en post-its, libretas sin custodiar, archivos de texto sin cifrar en el equipo o enviarlas por correo electrónico en claro.
- **Permitido:** Se deberá utilizar la aplicación **OneNote** incluida en nuestra suscripción de **Office 365** para el resguardo de todas las contraseñas relacionadas con actividades laborales. Las libretas deberán estar asociadas a la cuenta de correo institucional y las secciones con credenciales deberán protegerse con contraseña. Queda prohibido almacenar contraseñas en archivos sin protección, correos electrónicos o medios no autorizados. El cumplimiento será supervisado por el área de TI.

4.2. Caducidad y Renovación:

- **Contraseñas de usuario estándar de T.I.:** Deben cambiarse cada **90 días** (En caso de ser olvidada la contraseña se deberá solicitar al área de TI únicamente por correo electrónico).
- **Contraseñas privilegiadas (Admin):** Deben cambiarse cada **60 días** o inmediatamente después de cualquier cambio de personal o sospecha de compromiso.

4.3. Confidencialidad:

- Queda estrictamente prohibido compartir las contraseñas personales con cualquier persona, incluidos compañeros de trabajo o supervisores. Cada contraseña es de uso único e intransferible, y el usuario es el único responsable de las acciones realizadas bajo sus credenciales.

Para los casos en que sea necesario un acceso compartido a un sistema, se deberán utilizar cuentas funcionales genéricas, las cuales serán gestionadas exclusivamente por el Departamento de Tecnologías de la Información (TI). Las credenciales de dichas cuentas se almacenarán en el gestor de contraseñas corporativo, y todo acceso quedará debidamente registrado en los logs del sistema.

5. Protocolo de Acceso y Autenticación

- **Bloqueo de Sesión:** Las estaciones de trabajo y sistemas deben configurarse para bloquearse automáticamente después de **10 minutos** de inactividad, requiriendo contraseña para desbloquear.
- **Autenticación Multifactor (MFA):** Es obligatorio habilitar y utilizar MFA para todos los accesos remotos (VPN, escritorio remoto) y servicios en la nube (Azure, AWS, paneles de administración).
- **Acceso Remoto:** El acceso a los sistemas de la red interna desde el exterior solo se permitirá a través de la VPN corporativa.

6. Incidentes y Violaciones de Seguridad

Cualquier incidente relacionado con contraseñas debe ser reportado de inmediato al equipo de Seguridad Informática y/o a la jefatura de T.I. Esto incluye:

- Sospecha de que una contraseña ha sido robada o adivinada.
- Pérdida o robo de un dispositivo donde se tuvieran contraseñas almacenadas (aunque sea en un gestor).
- Recepción de un correo de phishing que solicite credenciales.

7. Sanciones

El incumplimiento de la presente política por parte de cualquier integrante del corporativo constituirá una **falta grave** y podrá dar lugar a la **imposición de medidas disciplinarias** conforme al Reglamento Interno de la Empresa y demás disposiciones aplicables, que podrán ir desde una **amonestación por escrito** hasta la **terminación de la relación laboral**, según la **gravedad de la infracción**, la **reincidencia** y el **daño real o potencial** ocasionado. Lo anterior se aplicará con **apego al debido proceso** y **sin perjuicio** de las acciones civiles o penales que pudieran corresponder.

8. Revisión y Actualización

La presente política será revisada, **al menos una vez al año**, por el Área de Tecnologías de la Información, con el fin de **verificar su eficacia** y **asegurar su adecuada adaptación** a amenazas emergentes, avances tecnológicos y requerimientos regulatorios. **Sin perjuicio de lo anterior**, podrán efectuarse **revisiones extraordinarias** cuando así lo exijan cambios relevantes en el entorno de riesgo.