1. Política de Troca Regular de Senhas

Objetivo:

A presente política tem como objetivo definir diretrizes para a criação, uso e troca regular de senhas, visando aumentar a segurança dos sistemas e dados da empresa, proteger as informações confidenciais e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

Abrangência:

Esta política se aplica a todos os colaboradores, prestadores de serviços, terceiros e qualquer outro indivíduo que tenha acesso aos sistemas, redes e informações da empresa.

---

1. Diretrizes para a Criação de Senhas

As senhas devem ser criadas de acordo com os seguintes requisitos mínimos:

- **Comprimento Mínimo**: As senhas devem conter, no mínimo, 12 caracteres.
- **Complexidade**: As senhas devem incluir uma combinação de:
  - Letras maiúsculas e minúsculas;
  - Números;
  - Caracteres especiais (ex.: @, , $, %, &).
- **Proibição de Senhas Comuns**: Não devem ser utilizadas senhas previsíveis, como “123456”, “senha123”, ou qualquer variação que inclua informações pessoais facilmente identificáveis (nome, data de nascimento, CPF, etc.).

2. Frequência de Troca de Senhas

- **Periodicidade**: As senhas de acesso aos sistemas da empresa devem ser alteradas a cada **90 dias**.
- **Notificação de Troca**: Os usuários serão notificados com 7 dias de antecedência sobre a necessidade de troca de senha. Caso a senha não seja alterada até o prazo final, o acesso será bloqueado até a redefinição.

3. Proibições Relacionadas ao Uso de Senhas

- **Reutilização de Senhas**: Não é permitido reutilizar as últimas **5 senhas**.
- **Compartilhamento de Senhas**: As senhas são pessoais e intransferíveis. O compartilhamento de senhas entre usuários é estritamente proibido.

- **Armazenamento de Senhas**: Não é permitido armazenar senhas em arquivos de texto, planilhas, blocos de notas, ou qualquer local não seguro e de fácil acesso. Recomenda-se o uso de **gerenciadores de senhas** confiáveis para o armazenamento seguro.

4. Acesso Imediato em Caso de Comprometimento

Se houver qualquer suspeita de que a senha foi comprometida, como em casos de phishing, vazamento de dados ou uso não autorizado, o usuário deverá:

- Alterar imediatamente a senha comprometida;
- Informar o departamento de TI sobre o incidente para que possam ser tomadas medidas adicionais de segurança.

5. Responsabilidades dos Usuários

- **Atualização Proativa**: É responsabilidade de cada colaborador realizar a troca de senhas no prazo estabelecido e garantir que suas senhas estejam seguras.
- **Proteção das Senhas**: Os usuários devem evitar escrever suas senhas em locais visíveis ou acessíveis a terceiros. Todos os dispositivos devem ser protegidos por senhas e bloqueados quando não estiverem em uso.

6. Responsabilidades da Empresa

A empresa compromete-se a:

- **Monitorar** o cumprimento da troca regular de senhas e notificar os usuários sobre prazos de expiração;
- **Prover** treinamento sobre a importância de senhas seguras e as boas práticas de segurança digital;
- **Investigar** e mitigar quaisquer incidentes relacionados ao comprometimento de senhas.

7. Sanções

O não cumprimento desta política pode resultar em medidas disciplinares, que variam de advertências até a rescisão do contrato de trabalho, dependendo da gravidade do incidente.

Revisão e Atualização

Esta política será revisada anualmente ou conforme necessário para garantir que continue eficaz e em conformidade com as leis e regulamentações aplicáveis.