POLÍTICA DE GESTÃO DE SENHAS E CREDENCIAIS DE ACESSO

1. Objetivo

Estabelecer diretrizes para criação, utilização, proteção, recuperação e gerenciamento de senhas e credenciais de acesso aos recursos tecnológicos da CREDLEVE, garantindo a segurança das informações e reduzindo os riscos de acessos não autorizados.

2. Abrangência

Aplica-se a colaboradores, diretores, prestadores de serviços, terceiros, consultores e fornecedores com acesso aos recursos tecnológicos da CREDLEVE.

3. Diretrizes Gerais

As credenciais são individuais, intransferíveis e confidenciais. É proibido compartilhar senhas, utilizar contas de terceiros, divulgar credenciais por e-mail ou aplicativos de mensagens e armazená-las em locais inseguros.

4. Solicitação e Recuperação de Senhas

As solicitações de criação de usuários, redefinição de senhas, desbloqueio de contas e alteração de permissões deverão ser realizadas pelo gestor imediato por e-mail para a equipe de Tecnologia da Informação. Sempre que possível, a senha deverá ser alterada no primeiro acesso.

5. Requisitos para Senhas

As senhas deverão possuir no mínimo 12 caracteres, contendo pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial. Não poderão conter nomes, datas de nascimento, CPF, telefone, sequências simples ou palavras do dicionário.

6. Renovação das Senhas

Sempre que tecnicamente possível, as senhas deverão ser alteradas a cada 90 dias, não poderão repetir as últimas 10 senhas e as contas serão bloqueadas após 5 tentativas inválidas de autenticação.

7. Senhas Privilegiadas

Contas administrativas deverão possuir senhas exclusivas, ser utilizadas apenas para atividades administrativas, ser autorizadas pela Diretoria ou responsável pela área e utilizar autenticação multifator (MFA), quando disponível.

8. Boas Práticas

Utilizar senhas diferentes para sistemas distintos, bloquear a estação ao se ausentar, alterar imediatamente a senha em caso de suspeita de comprometimento e comunicar qualquer uso indevido à equipe de TI.

9. Perda ou Comprometimento da Credencial

Em caso de perda da senha, suspeita de acesso indevido ou vazamento de credenciais, o usuário deverá comunicar imediatamente a TI, que bloqueará a credencial comprometida, redefinirá a senha e registrará a ocorrência.

10. Revogação de Credenciais

Em desligamentos, encerramento de contrato, mudança de função ou solicitação da Diretoria, a equipe de TI deverá revogar imediatamente os acessos do usuário.

11. Exceções

Qualquer exceção deverá ser aprovada formalmente pela Diretoria.

12. Revisão da Política

Esta política deverá ser revisada anualmente ou quando houver alterações relevantes na infraestrutura tecnológica.

13. Vigência

Esta política entra em vigor na data de sua aprovação.

Histórico de Revisões

Versão	Data		Revisões	Aprovador	Área
	Emissão	Aprovação			
01	09/02/2026	06/03/2026	Emissão da Política	Marcelo Carmanini	Diretoria