POLÍTICA DE GESTÃO DE SENHAS E CREDENCIAIS DE ACESSOS

1. OBJETIVO

A presente Política visa a Gestão de Senhas, no ambiente CREDFRANCO, estabelecendo um padrão de criação e utilização de senhas fortes, visando evitar violações a estas.

2. ABRANGÊNCIA

A Política de Gestão de Senhas e Credenciais de Acessos tem abrangência corporativa em toda estrutura da CREDFRANCO.

3. DIRETRIZES DO USO DE SENHAS

3.1. Solicitações e/ou Recuperações de Acesso

As solicitações de acesso devem ser realizadas através do GLPI e autorizadas pelo gestor imediato.

As solicitações de recuperação de senhas de e-mail e máquina, por esquecimento ou outro motivo, devem ser realizadas através do GSI. As senhas de acesso e bancos devem ser realizadas para o setor suporte via plataforma web JARVIS e seguirão procedimento de validação de informações do usuário para disponibilização das senhas iniciais.

As senhas devem ser fornecidas de modo seguro e confidencial aos usuários, sendo configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra de modo automático.

3.2. Senhas de Uso Normal

O usuário é o único responsável pelo uso de suas credenciais de acesso. Considerando que a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em segredo, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso.

A senha de qualquer usuário nunca deverá ser revelada a terceiros, sejam gestores e/ou superiores imediatos, bem como não poderá ser utilizada por estes para acessos, logins e/ou autenticações nos sistemas CREDFRANCO e/ou gerenciados por esta.

As senhas não devem ser trafegadas em mensagens de e-mail, chamados, aplicativos de mensagens instantâneas e afins. Ademais, não deverão ser anotadas e/ou armazenadas em dispositivos móveis, salvo em aplicativo específico para tal funcionalidade que contenha criptografia forte.

Os sistemas, serviços e dispositivos da CREDFRANCO devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação, conforme as recomendações abaixo:

i. Conter pelo menos 3 das 4 diretrizes abaixo:
   - i.i. Conter pelo menos uma letra maiúscula;
   - i.ii. Conter pelo menos uma letra minúscula;
   - i.iii. Conter números (0 a 9);
   - i.iv. Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ;

ii. Tamanho de, no mínimo, 8 caracteres;

iii. Não é permitido utilizar as 10 (dez) últimas senhas cadastradas;

iv. Mandatório alterar a senha a cada 30 dias;

v. A conta do usuário é bloqueada após 3 (três) tentativas de acesso com senha errada.;

vi. Histórico mínimo de 10 (dez) senhas utilizadas;

vii. Novas senhas não podem ter sido usadas nos últimos 365 dias e devem ser validadas em lista à parte a fim de evitar palavras previsíveis.

3.3. Senhas de Uso Privilegiado

Todas as contas privilegiadas (Ex.: administrador, root, etc.) devem ter as senhas trocadas, renomeadas e desabilitadas.

Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que terão perfis de administradores e autorização restrita de acesso para essas funcionalidades.

Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas “contas de serviço”, não sendo utilizadas para qualquer tipo de acesso.

As senhas não devem ser introduzidas em linhas de comando (códigos fontes) e/ou em scripts abertas, mas caso seja necessário, devem ser criptografadas e consideradas “contas de serviço”.

Todas as senhas em trânsito, ou seja, que sejam trafegadas pela rede, obrigatoriamente deverão estar encriptadas.

4. BOAS PRÁTICAS PARA CRIAÇÃO DE SENHAS

4.1. Evitar a utilização de:

i. Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas;

ii. Sequência do teclado (ex.: asdfg123);

iii. Palavras do dicionário, nomes de times de futebol, de música, de produtos, de personagens de filmes etc.

4.2. Poderão ser utilizados:

i. Números aleatórios;

ii. Vários e diferentes tipos de caracteres;

iii. Caracteres especiais;

iv. Substituir uma letra por número com semelhança visual;

v. A primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha "?OCbcaRddus" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).

5. DAS PERDAS DE CREDENCIAIS

No caso de perda da credencial, o usuário deverá avisar imediatamente ao Service Desk(GLPI), via Chamado, o qual entrará em contato com os responsáveis pela gestão de acessos e estes irão:

(i) Invalidar a credencial antiga.
(ii) em até um dia útil enviar uma nova credencial.

6. DO DESLIGAMENTO/ REMOÇÃO DE ACESSO

No caso de interrupção de vínculo do colaborador com a CREDFRANCO, o gestor deste deverá solicitar ao GLPI a remoção de todos os acessos.

A área de Recursos Humanos (RH) poderá solicitar, de forma proativa, a revogação dos acessos.

A conta deve ser inativada de forma imediata pela área técnica e consequentemente bloqueados os acessos em todos os recursos tecnológicos e áreas físicas da CREDFRANCO.

7. DESVIO E EXCEÇÃO

Todo e qualquer desvio e/ou exceção deve ser comunicado à área de Segurança da Informação que fará a devida avaliação.

Qualquer uso indevido da credencial, seja intencional ou não, será comunicado ao responsável pelo usuário e/ou ao Departamento de Recursos Humanos para que sejam tomadas as medidas administrativas e/ou legais cabíveis.

8. REVISÕES E ATUALIZAÇÕES

Visando promover uma melhor experiência aos Colaboradores, Clientes e Parceiros CREDFRANCO, os termos desta Política poderão ser atualizados ou adaptados, anualmente, conforme o início de cada ano, para que reflitam as

nossas práticas, bem como estejam sempre em conformidade com a legislação aplicável.

9. CONSIDERAÇÕES FINAIS

Esta Política deverá ser adotada a partir desta data e todas as alterações estruturais que se fizerem necessárias deverão ser previamente aprovadas pela área de Governança e Compliance.

Histórico de Revisões

Versão	Data		Revisões	Aprovador	Área
	Atualização	Aprovação			
01	-	19/07/2021	Emissão da Política	Everton Alves	Tecnologia da Informação
02	16/05/2022	16/05/2022	Atualização do Layout e Revisão do Conteúdo	Bárbara Fideles/ Gustavo Ferreira	Governança e Compliance/ Tecnologia da Informação
03	19/09/2022	19/09/2022	Inclusão de texto – Item 3.1; Inclusão do item VII – Item 3.2.	Bárbara Fideles	Governança e Compliance
04	14/06/2023	14/06/2023	Atualização do item 3.2 IV e VI	Gustavo Ferreira / Emily Assumpção	Tecnologia da Informação/ Governança e Compliance
05	01/03/2024	01/03/2024	Revisão de conteúdo	Gustavo Ferreira / Emily Assumpção	Tecnologia da Informação/ Governança e Compliance
06	07/02/2025	07/02/2025	Atualização do item 3.1 (nome do sistema de crédito consignado) / Revisão de conteúdo	Gustavo Ferreira / Hemerson Rodrigues / Thays Cristina	Tecnologia da Informação / Compliance
07	29/01/2026	29/01/2026	Revisão de conteúdo e atualização do item 5	Gustavo Ferreira Lais Santos Gabriel Bortoloto Hemerson Rodrigues	Tecnologia da Informação