



TecnoTech
Sistemas

POLÍTICA DE CRIAÇÃO E USO DE SENHAS

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO



Felipe Santos de Andrade / Wanderson Camara dos Santos

Política de Criação e uso de senhas

Versão 1.0

Tecnotech Sistemas

Diretoria de Implementação e Projetos

Política criada sob a supervisão de
Romney Dutra / Lucas Diniz - Prolinx

Março de 2023

Conteúdo

Lista de Tabelas	4
1 INTRODUÇÃO	5
2 PROPÓSITO	6
3 ABRANGÊNCIA	7
4 DIRETRIZES DO USO DE SENHAS NA TECNOTECH	8
5 BOAS PRÁTICAS ADOTADAS PELA TECNOTECH PARA CRIAÇÃO DE SENHAS SEGURAS E CONFIÁVEIS	10
6 PERDA DA CREDENCIAL	12
7 SENHAS DE ACESSO AOS AMBIENTES E EQUIPAMENTOS EXTERNOS DA TECNOTECH	13
8 DESLIGAMENTO	14
9 INTERVALO DE TEMPO PARA A ALTERAÇÃO DE SENHAS	15
10 GERENCIAR E ARMAZENAR MÚLTIPLAS SENHAS DE FORMA SEGURA	16
11 DESVIO DA POLÍTICA DE CRIAÇÃO E USO DE SENHAS	17
12 MUDANÇAS NA POLÍTICA	18
13 CONTROLE DE VERSÕES	19
14 CONCORDÂNCIA	20

Lista de Tabelas

13.1 Tabela de versões	19
----------------------------------	----

Capítulo 1

INTRODUÇÃO

A segurança da informação é essencial para a tecnotech sistemas e a autenticação é um elemento crucial para garantir essa segurança. As credenciais de acesso, como nome de usuário, senhas e tokens, desempenham um papel fundamental nesse processo. É crucial utilizar senhas fortes, com alta complexidade, para minimizar os riscos e evitar ações mal-intencionadas. Senhas fracas podem comprometer todo o ambiente tecnológico.

Cada usuário é exclusivamente responsável por suas próprias senhas de acesso, que são pessoais, intransferíveis e de uso exclusivo. É fundamental mantê-las em sigilo e segurança. As senhas de acesso permitem identificar o usuário como o responsável pelas atividades praticadas na infraestrutura e nas operações da empresa, portanto, é vital que elas sejam fortes. É necessário conscientizar os colaboradores sobre a importância de manter senhas seguras e evitar compartilhá-las com terceiros, a fim de garantir a segurança da informação e a integridade de suas credenciais e dados que tenham acesso.

Capítulo 2

PROPÓSITO

O objetivo deste documento é estabelecer um conjunto de regras para a criação, gerenciamento e uso de senhas seguras, a fim de evitar que pessoas mal-intencionadas descubram suas senhas e acessem sua conta, obtendo acesso não autorizado a informações confidenciais da tecnotech em seu nome.

Para garantir a segurança de suas informações, é essencial que você siga algumas práticas recomendadas pelas melhores práticas de segurança da informação, como criar senhas com no mínimo 8 caracteres, combinando letras maiúsculas e minúsculas, números e símbolos especiais. É importante criar senhas exclusivas para cada conta que você possui, evitando reutilizar senhas em diferentes plataformas.

Capítulo 3

ABRANGÊNCIA

É essencial que todos que atuam em nome da tecnotech, incluindo diretores, Funcionários, Estagiários, Parceiros Comerciais (consultores, agentes comerciais e conveniados) e fornecedores (outros contratados e subcontratados pela empresa) sigam as regras e orientações estabelecidas neste documento.

A adesão a essas normas garantirá a segurança de informações confidenciais da empresa e minimizará os riscos de violações de segurança e acesso não autorizado. Portanto, é fundamental que todos estejam cientes e cumpram essas práticas de segurança de informações.

Capítulo 4

DIRETRIZES DO USO DE SENHAS NA TECNOTECH

Usuário é o único responsável pelo uso de suas credenciais de acesso na tecnotech sistemas. Como a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em sigilo. Qualquer transação realizada durante o uso da senha é de responsabilidade do usuário. Portanto, é crucial que o usuário nunca revele sua senha a ninguém, nem mesmo ao seu gestor, e nunca permita que outras pessoas utilizem os sistemas da tecnotech autenticados com seu login e senha.

Para garantir a segurança das senhas na tecnotech, elas não devem ser compartilhadas em mensagens de e-mail, em chamados ou em aplicativos de mensagens instantâneas. Além disso, não é permitido anotar ou armazenar senhas em dispositivos móveis, exceto em aplicativos específicos que possuam criptografia forte.

Os sistemas, serviços e dispositivos da tecnotech são configurados para exigir senhas fortes com os seguintes padrões mínimos:

- Deve conter pelo menos 3 dos seguintes itens.
- Pelo menos uma letra maiúscula.
- Pelo menos uma letra minúscula.
- Pelo menos um número (0 a 9).
- Pelo menos um símbolo.
- Comprimento mínimo de 8 caracteres.
- Proibir o uso das 5 senhas anteriores.
- Alteração de senha obrigatória a cada 90 dias.

A tecnotech sistemas vai fornecer as senhas iniciais diretamente aos usuários e configurá-las de modo que, no primeiro acesso, seja solicitada automaticamente a troca de senha.

Capítulo 5

BOAS PRÁTICAS ADOTADAS PELA TECNOTECH PARA CRIAÇÃO DE SENHAS SEGURAS E CONFIÁVEIS

A tecnotech adota as seguintes práticas para criação de senhas seguras, incluindo a recomendação de evitar o uso de:

- 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.
- Sequência do teclado (ex.: asdfg123).
- Palavras do dicionário, nomes de times de música, de produtos, de personagens de filme.

Para criar senhas seguras, é recomendado utilizar:

- Números aleatórios.
- Tamanho de no mínimo 8 caracteres.
- Diferentes tipos de caracteres, como letras maiúsculas e minúsculas, números e símbolos.
- Caracteres especiais.
- Substituir uma letra por um número que tenha semelhança visual, como substituir "o" por "0".

Uma estratégia é criar uma frase e usar as primeiras letras de cada palavra para formar uma senha.

Capítulo 6

PERDA DA CREDENCIAL

No caso de perda, esquecimento da credencial, é importante que o usuário avise imediatamente ao seu gestor, para que as medidas necessárias possam ser tomadas. Os responsáveis pela gestão de acessos serão informados e, em seguida, tomarão as seguintes ações:

- Desabilitar a conta e as senhas associadas.
- Verificar se houve alguma atividade suspeita ou não autorizada.
- Identificação do usuário antes de fornecer uma nova senha.
- Verificar se a perda da credencial resultou em qualquer tipo de acesso não autorizado ou violação de segurança.
- Envio de nova credencial.

Capítulo 7

SENHAS DE ACESSO AOS AMBIENTES E EQUIPAMENTOS EXTERNOS DA TECNOTECH

Para garantir a segurança das contas e minimizar riscos de invasões, as senhas serão fornecidas diretamente ao usuário escolhido pelo gestor através de um procedimento. Dessa forma, o usuário terá uma senha única e segura. Lembre-se de que a segurança da informação é responsabilidade de todos e o uso correto da senha é essencial para proteger as informações contra possíveis violações de segurança.

Capítulo 8

DESLIGAMENTO

No caso de término do vínculo do usuário com a tecnotech sistemas, o cancelamento de todos os direitos de acesso vigentes do usuário deve ocorrer de forma imediata, geral em todos os ativos de tecnologia da informação, quando a pessoa encerrar o vínculo, é importante lembrar que o usuário deve devolver todos os dispositivos e equipamentos de propriedade da empresa que possam conter informações confidenciais. A gestão de usuário e passe para acesso a ativos de tecnologia da informação devem estar em conformidade com a Política de criação e uso de senhas, quanto o controle de acesso lógico, independentemente do sistema de autenticação utilizado.

A gestão de usuário deve considerar que:

- O usuário não pode ser excluído, ele deve ser inativado ou desabilitado..
- A inativação de usuário deve existir quando houver regras de bem definidas e implementações viáveis em programa de computador.
- A inativação pode fundamentar-se, também, em análise crítica que apresenta o risco do usuário ativo à segurança da informação, ou desconformidade com algum normativo vigente.

Capítulo 9

INTERVALO DE TEMPO PARA A ALTERAÇÃO DE SENHAS

Como já vimos anteriormente para uma boa prática de segurança cibernética, o período de alteração da senha é de 90 a 180 dias o que permite equilibrar a segurança das contas com a conveniência do usuário, evitando que senhas sejam esquecidas ou anotadas em locais inseguros. No entanto, é importante destacar que senhas fracas ou comprometidas devem ser trocadas imediatamente, independentemente do período estabelecido para a troca regular de senhas.

- O intervalo de 90 dias é o ideal para a troca de senhas como uma boa prática de segurança.

Capítulo 10

GERENCIAR E ARMAZENAR MÚLTIPLAS SENHAS DE FORMA SEGURA

Os gerenciadores de senhas são ferramentas que ajudam a criar e armazenar senhas seguras para cada conta. Eles geralmente funcionam com uma chave mestra criptografada que você usa para desbloquear todas as suas outras senhas.

Alguns exemplos populares de gerenciadores de senhas com criptografia incluem LastPass, 1Password e Bitwarden.

O backup das senhas é muito importante, se você usar um gerenciador de senhas é de extrema importância fazer backup de suas senhas para caso de perda ou esquecimento. Muitos gerenciadores de senhas possuem esse recurso de backup embutido, mas você também pode criar um backup manualmente.

Capítulo 11

DESVIO DA POLÍTICA DE CRIAÇÃO E USO DE SENHAS

Qualquer desvio ou exceção em relação às políticas de criação e uso de senhas deve ser comunicado à área de Segurança da Informação da TecnoTech, que fará uma avaliação adequada e tomará as medidas cabíveis.

Capítulo 12

MUDANÇAS NA POLÍTICA

A presente versão 1.0 desta Política de criação e uso de senhas foi atualizada pela última vez em: 07/03/2023. O editor se reserva o direito de modificar, a qualquer momento as presentes normas, especialmente para adaptá-las às evoluções, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Esta Política de criação e uso de senhas poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.

Capítulo 13

CONTROLE DE VERSÕES

Tabela 13.1: Tabela de versões

Versão	Descrição	Responsável	Publicação
1.0	Versão para divulgação	Wanderson câmara - Felipe Andrade	07/03/2023

Capítulo 14

CONCORDÂNCIA

Eu li e entendi a Política de criação e uso de senhas da TECNOTECH SISTEMAS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da TECNOTECH SISTEMAS.

Assinatura do funcionário Data