COMPLEMENTO DA PSI - GERENCIAMENTO DE SENHAS

NOVEMBRO - 2021

Sumário

Responsável:	Emilson Queiroz (Gerente TI e Cloud)
Aprovado por:	Suleiman Bragança (CEO)
Políticas Relacionadas:	Política da Segurança da Informação, Código de Conduta e Normas e Procedimentos da Vector Informática
Localização de Armazenamento:	Escritórios de Barueri (SP) / Cuiabá (MT) e Florianopólis (SC)
Data de Aprovação:	09/2021
Data de Revisão:	04/2024
Versão atual:	3.0

1 – INTRODUÇÃO

Para complementar as normas sobre o gerenciamento de Senhas, foi realizado pela TI da Vector essa Política Complementar de Gerenciamento de Senhas. Aonde consta as informações de forma direta do item 15 (Política de Senhas), da Política de Segurança da Informação.

As credenciais de acesso (conta de usuário e senha) são mecanismos fundamentais de autenticação. A senha certifica que o usuário é quem diz ser e que tem o direito de acesso ao recurso disponibilizado. Uma senha forte minimiza os riscos e inibe uma ação mal-intencionada; uma senha fraca, por sua vez, pode comprometer todo o ambiente tecnológico da Vector. Por conta disto, todos os usuários que necessitam de acesso restrito devem seguir os padrões estabelecidos nesta política.

Uma senha forte é aquela que é difícil ser descoberta e fácil de ser lembrada. Desta maneira, uma senha deve ser formada por vários mecanismos que a tornem complexa suficiente para um atacante e, por estratégias ou artifícios, que seja fácil de ser lembrada pelo usuário, sem que seja necessário escrevê-la.

2 - OBJETIVOS

Estabelecer um padrão de criação e utilização de senhas fortes, no intuito de evitar que que pessoas mal-intencionadas as descubram e se passem por outras pessoas, acessando, por exemplo: contas de correio eletrônico, de rede, de computador e de sistemas; sites indevidos ou informações privilegiadas da Vector, como se proprietário fosse.

3 - ABRAGÊNCIA

Esta política se aplica a todos os colaboradores da Vector, quais sejam: colaboradores, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da Vector. Todos os esses colaboradores serão tratados nesta política como usuários.

4 - REFERÊNCIAS

- Código de Conduta e Ética da Vector Informática;
- Política de Gestão de Riscos;
- Política da Segurança da Informação;
- Política Complementar da Segurança da Informação / Cibernética.

5 – DIRETRIZES DO USO DE SENHAS

1. **Senhas de Uso Normal:**

- A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
- A senha inicial só será fornecida ao próprio colaborador, pessoalmente, sendo exigida a troca ao primeiro uso. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;

- As senhas não devem ser trafegadas em mensagens de e-mail ou em outros formulários de uso de comunicação eletrônica;
- É proibido o compartilhamento de login para funções de administração de sistemas;
- As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
- Os sistemas, serviços e dispositivos do ambiente tecnológico da Vector devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação, conforme as recomendações abaixo:

  I -Tenham no mínimo 8 (oito) caracteres;

  II - Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;

  III - Não deve haver repetição de letras ou números na definição da senha, ou seja 3 (três) ou mais caracteres iguais sequenciados (ex: 111aaabBBBA);

  IV - Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc);

  IV - As senhas deverão ser substituídas, no máximo, a cada 180 (cento e oitenta) dias de utilização. Na substituição, os sistemas não devem aceitar o reuso da última senha utilizada;

  V - As digitações das senhas devem ser mascaradas na tela, armazenadas e trafegadas de forma criptografada, pelo sistema ou aplicação;

  VI - Após 5 (cinco) tentativas erradas de digitação de uma senha, a conta do usuário deverá ser bloqueada. As solicitações de desbloqueio devem ser solicitadas para a TI, que seguirão um procedimento de validação de informações do usuário para efetuar os desbloqueios.
- As solicitações de acesso devem ser realizadas através de Solicitação para a e autorizadas pelo gestor imediato;
- As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através de solicitação para a TI e seguirão um procedimento de validação de informações do usuário para disponibilizar as senhas iniciais;

- O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
  I - Desligamento do colaborador;
  II - Mudança de função do colaborador;
  III - Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
- Para os cancelamentos acima mencionados, o RH ficará responsável por informar prontamente o TI acerca dos desligamentos e mudança de função dos colaboradores.

2. Senhas de Uso Privilegiado:

- Todas as contas privilegiadas (ex: administrator, sa, 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 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) abertas, mas, caso seja necessário, devem ser criptografadas e consideradas “contas de serviço”.

3. Autenticação:

- A Vector utiliza Autenticação multi fatores interna através do aplicativo Jumpcloud – domínio em nuvem (Cloud Domain);
- E a Autenticação Externa utiliza o Google;
- Com a autenticação multifator tem um maior controle sobre a segurança e as políticas da conta, além de alinhamento com outros aplicativos em uso, tornando a experiência do usuário mais consistente.

6 – BOAS PRÁTICAS

1. **Evitar a utilização de:**

- Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família (ex.: Maria, Souza, msilva);
- Números de documentos ou de telefone (ex.: 121521487-63, 988356215);
- Placa de carros (ex.: REC1805);
- Datas de aniversários, festivas, etc. ex.: 16/05/2016, 25/12/2016);
- Sequência do teclado (ex.: asdfg123); Palavras do dicionário (ex.: Paralelepípedo);
- Nomes de times de futebol, de música, de produtos, de personagens de filmes (ex.: Garota de Ipanema, GGTISee, Mickey, Mcdonalds).

2. **Utilizar:**

- Números aleatórios;
- Vários e diferentes tipos de caracteres;
- Caracteres especiais;
- Substituir uma letra por número com semelhança visual;
- Frase longa com letras e números;
- A primeira, segunda ou última letra de uma frase incluindo números (ex.: “Água mole em pedra dura, tanto bate até que fura” pode gerar a senha “Am3Pd,Tba9F”).

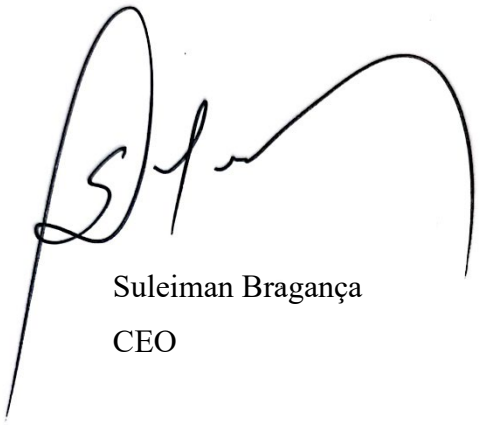
7 – ADEQUAÇÃO Á POLÍTICA

- Os novos projetos de desenvolvimento ou novas aquisições de sistemas devem seguir os padrões estabelecidos nesta política;
- As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo de 1(um) ano, a partir de sua publicação;
- Caso não seja possível a adequação das ferramentas, o Comitê da Segurança da Informação deve documentar essa informação, bem como seus motivos, para fins de auditoria interna.

8 – VIGÊNCIA E INTRUMENTALIZAÇÃO

A presente Política Complementar de Gerenciamento de Senhas da Vector tem vigência a partir de sua data de publicação e validade indeterminada, e ser decidido pela Diretoria, TI e RH, e posteriormente divulgado a todos os interessados.

Barueri, novembro de 2021



Suleiman Bragança
CEO