POLÍTICA DE SENHAS

POLI-0008-01

MANTENHA APENAS UM: CONFIDENCIAL | RESTRITO | **USO INTERNO** | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2021	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0008-01	Política	Uso Interno

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Segurança da Informação (T.I.)
Política de Segurança Física
Política de Mesa e Tela Limpa

Aprovação da Diretoria

Diretor	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Introdução

Como forma segura, a área de Tecnologia da Informação é responsável por definir a política de senha para usuários. Deixamos algumas recomendações para tornar a **Epeople** mais segura contra ataques de senha.

Política de Segurança

A política de segurança diz respeito às regras que devem ser elaboradas e seguidas pelos usuários dos recursos de informação de uma **Epeople**.

A formação de um conjunto de boas práticas, com o objetivo de desenvolvimento de uma política/cultura de segurança é essencial para a **Epeople**, já que a informação é um dos ativos mais valiosos.

As decisões relacionadas à segurança que o responsável da **Epeople** toma, determinam quão segura a rede desta é, quantas funções ela irá disponibilizar e como será a sua utilização. Por isso, é preciso determinar metas de segurança.

Para a elaboração de uma política de segurança, devemos levar em consideração alguns fatores, como os riscos e benefícios associados à falta de segurança e os custos de implementação dos mecanismos.

Importância da Segurança

Computadores são fontes de inúmeras tarefas, como armazenamento de dados, comunicação (e-mails, chats etc.), transações financeiras (pagamento de contas, compras etc.), que podem ter cunho pessoal ou comercial (uso da **Epeople**).

Alguns fatos podem acontecer por falta de uma segurança adequada, como o furto de senhas e números de cartões de crédito, dados pessoais ou comerciais podem ser alterados, a conta de acesso à internet ou sistema operacional utilizados por pessoas não autorizadas e, por último, o computador pode até deixar de funcionar, por comprometimento e corrompimento de arquivos essenciais.

Existem diversas razões para que um terceiro queira invadir um sistema ou máquina, como:

- Utilização para fim de práticas ilegais;
- Utilização do computador de outros para promover ataques;
- Destruição de informações;
- Disseminação de spams;
- Furto de números de cartões de crédito e senhas de banco; e
- Furto de informações salvas nas máquinas.

Política de Senha

A senha é a forma mais convencional de identificação e acesso do usuário. Se um terceiro tem acesso a sua senha, ele poderá utilizá-la ilegalmente ou para se passar por você.

A política de senhas tem as seguintes regras:

- Letras Maiúsculas e Minúsculas;
- Caracteres Especiais;
- Números;
- Exigido no mínimo 8 dígitos;
- Não repetir as últimas 5 senhas; e
- Ser alterada a cada 90 dias.

O que Proibir na Criação de Senha

Nomes, sobrenomes, números de documentos, telefones, placas de carro e datas não devem ser utilizados em senhas, pois são dados que podem ser obtidos com uma certa facilidade e que possivelmente vão ser alvos de tentativa para descobrir a senha do usuário.

Conscientização

Como de costume, frisamos a importância da conscientização dos colaboradores para o sucesso de qualquer medida de segurança de dados. Logo, usuários mal-informados frequentemente são a principal porta de entrada para ameaças. Ou seja, eles devem entender a importância da confidencialidade da senha e das demais medidas de segurança.

Entre as principais orientações, destacam-se:

- Certificar-se de que não está sendo observado enquanto utiliza suas senhas;
- Não fornecer a senha a terceiros;
- Não utilizar a senha em computadores de terceiros (Ex.: *lan houses*, cybercafés etc.);
- Certificar que o provedor utilizado tem serviços criptografados;
- Não usar a mesma senha para acessar todos os sistemas; e
- Separar as senhas corporativas das senhas pessoais.

Gerenciamento Corporativo

Além das boas práticas já citadas, o gerenciamento de contas corporativas envolve outras ações. Alguns exemplos de ações de gerenciamento são:

- Bloqueio do usuário após um determinado número de tentativas com a senha errada;
- Criar políticas de recuperação de senhas que passem pelo administrador do sistema;

- Se necessário, uso de autenticação de dois fatores em sistemas críticos;
- Bloqueio imediato do acesso de colaboradores desligados; e
- Não permitir o envio de senhas em forma de textos descoberto através de e-mails e mensagens.

Além disso, existem softwares desenvolvidos especificamente para este propósito, como os chamados cofres de senha. Eles permitem uma visão do nível de segurança de cada senha, monitoramento de usuários com acessos privilegiados, entre outras funções.

Importante lembrar sempre que a senha é a chave para toda a sua infraestrutura. Se ela não é segura o suficiente, significa que toda a rede da **Epeople** pode ser comprometida. Investir em soluções sofisticadas é, muitas vezes, necessário, mas as práticas básicas não podem ser esquecidas.