QUESTOR

Política de Senhas

ÁREAS RESPONSÁVEIS	APROVADO POR	DATA DA ÚLTIMA ATUALIZAÇÃO
Tecnologia da Informação	Comitê de Segurança da Informação	21/07/2023
VERSÃO	**CLASSIFICAÇÃO**	**CÓDIGO**
02	Uso Interno	Questor_PolíticadeSenhas

Sumário

1- Introdução

As credenciais de acesso (conta de usuário e senha) são mecanismos fundamentais de autenticação. A senha confirma a identidade do usuário e permite o acesso ao recurso disponibilizado. O uso de senha forte minimiza os riscos e inibe uma ação mal-intencionada; uma senha fraca, por sua vez, pode comprometer todo o ambiente tecnológico. Assim, cada Destinatário é exclusivamente responsável por todas as suas senhas de acesso, que são pessoais, intransferíveis e de uso exclusivo do destinatário, que assume integral responsabilidade pelo uso indevido por terceiros e compromete-se a mantê-las em sigilo e guardá-las em segurança. Por esse motivo, as senhas de acesso aos ativos da Questor que permitem identificar o destinatário como o responsável pelas atividades que praticar usando a infraestrutura da Questor Sistemas – devem ser fortes.

2- Finalidade

Estabelecer um padrão de criação e utilização de senhas fortes, no intuito de evitar 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 Questor, como se fosse o proprietário.

3- Abrangência

As regras e diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da Questor S.A., quais sejam: funcionários, servidores, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da empresa.

4- Diretrizes do Uso de Senhas

Senhas de Uso Normal

a) 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. Então, nunca revele sua senha a ninguém, nem mesmo o seu gestor e jamais deixe que alguém utilize os sistemas da Questor autenticado com o seu login e senha.

b) As senhas não devem ser trafegadas em mensagens de e-mail, em chamados, em aplicativos de mensagens instantâneas, não devem ser anotadas e ou armazenadas em dispositivos móveis (salvo em aplicativo específico para tal funcionalidade que conte com criptografia forte);

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

Conter pelo menos 3 das 4 diretrizes abaixo:

- Conter pelo menos uma letra maiúscula;
- Conter pelo menos uma letra minúscula;
- Conter números (0 a 9);
- Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ;
- Tamanho de no mínimo 8 caracteres;
- Não é permitido utilizar as 5 últimas senhas cadastradas;
- Mandatório alterar a senha a cada 180 dias;
- A conta do usuário é bloqueada após 5 tentativas de acesso com senha errada;
- A conta permanecerá bloqueada por 30 minutos. Após os 30 minutos, a conta é automaticamente desbloqueada para até 10 tentativas de acesso;

d) As solicitações de acesso devem ser realizadas através da TI e autorizadas pelo gestor imediato;

e) As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através da TI e seguirão um procedimento de validação de informações do usuário para disponibilizar as senhas iniciais;

f) As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente.

Boas práticas para Criação de Senhas

a) Evitar a utilização 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 futebol, de música, de produtos, de personagens de filmes, etc.

b) Utilizar:

- Números aleatórios;
- Vários e diferentes tipos de caracteres;
- Caracteres especiais;
- Substituir uma letra por número com semelhança visual;
- A primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase “Com grandes poderes vêm grandes responsabilidades” você pode gerar a senha "?CGpvGr" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).

Perda da Credencial

a) No caso de perda da credencial, o usuário deverá avisar imediatamente ao TI que entrará em contato com os responsáveis pela gestão de acessos e esses irão:

1. Invalidar a credencial antiga; e
2. Em até um dia útil enviar uma nova credencial.

Desligamento / Remoção do acesso

a) No caso de interrupção de vínculo do usuário com a Questor, deverá ser solicitado ao TI a remoção de todos os acessos com, pelo menos, dois dias úteis de antecedência;

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

c) 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 Questor.

5- Desvio e Exceção

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

b) 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.

6- Referências

ABNT NBR ISO/IEC 27002:2013:

ABNT NBR ISO/IEC 27001:2005:

ABNT NBR ISO/IEC 27701:2019;

Normas de Boas Práticas da TI;

Tecnologia da Informação;

Técnicas de Segurança;

Código de Prática para controles de segurança da informação;

Marco Civil da Internet – Lei 12965:2014.

7- Revisões e Responsabilidades

Data	Versão	Descrição	Autor
21.07.2022	1.0	Criação da Política	Setor de TI
21.07.2023	2.0	Atualização da Formatação da Política	Setor de Proteção de Dados