


Norma de Procedimentos	
Assunto: POLÍTICA DE SENHAS	Página 1 de 3

1. INTRODUÇÃO

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. 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 FGV que permitem identificar o destinatário como o responsável pelas atividades que praticar usando a infraestrutura da Fundação Getulio Vargas – FGV 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 FGV, como se fosse o proprietário.

3. ABRANGENCIA

As regras e diretrizes aqui estabelecidas deverão ser seguidas pelos membros do Conselho Curador, Presidente, Vice-Presidentes, Funcionários (incluindo Professores), Estagiários, Professores visitantes, Alunos, Parceiros Comerciais (consultores, agentes comerciais e conveniados), pesquisadores que atuam em nome da FGV e fornecedores (outros contratados e subcontratados pela FGV).

4. DIRETRIZES DO USO DE SENHAS

1. 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 FGV 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 moveis (salvo em

aplicativo específico para tal funcionalidade que conte com criptografia forte);

c) Os sistemas, serviços e dispositivos da FGV 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:
 - I. Conter pelo menos uma **letra maiúscula**;
 - II. Conter pelo menos uma **letra minúscula**;
 - III. Conter números (0 a 9);
 - IV. 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 10 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 do Service Desk e autorizadas pelo gestor imediato;

e) As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através do Service Desk 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.

2. Senhas de Uso Privilegiado

a) Todas as contas privilegiadas (ex: administrator, asgv, root, etc.) devem ter as senhas trocadas, renomeadas e desabilitadas;

b) 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;

c) 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;

d) 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”.

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

3. 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 "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).

4. Perda da Credencial

a) No caso de perda da credencial o usuário deverá avisar imediatamente ao Service Desk 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.

5. Desligamento / Remoção do acesso

- a) No caso de interrupção de vínculo do usuário com a FGV, deverá ser solicitado ao Service Desk 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 FGV.

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

Política de Segurança da Informação da FGV;
ABNT NBR ISO/IEC 27002:2013 Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação;
Cert.br - Cartilha de Segurança para Internet.