Número da Norma	Revisão - Data	Emissão	Folha
06/IN06/CGSIC/IFS	00 - 20/12/2011	20/12/2011	1/6

GESTÃO DE SENHAS

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe (IFS) instituído pela Portaria número xxxx de xxx de xxx de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê Gestor de Segurança da Informação e Comunicação do IFS compete ao CGSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO.

Esta norma aplica-se a todo o IFS.

OBJETIVOS GERAIS.

Estabelecer critérios geração e manutenção de senhas de usuários

SUMÁRIO.

INFORMAÇÕES ADICIONAIS.

Esta norma observa a estrutura proposta pela Norma 01/IN01/CGSIC/IFS.

APROVAÇÃO

Presidente do CGSIC

GESTÃO DE SENHAS

1 OBJETIVO

Estabelecer critérios para geração de senhas fortes, de sua segurança e atualização

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na POSIC compete ao CGSIC do IFS determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFS.

3 GESTÃO DE SENHAS

3.1 O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais do IFS.

3.1.1 Senhas são confidenciais, intransferíveis e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade.

3.2 Para fins desta norma considera-se senha temporária a senha gerada inicialmente pelo Administrador de Sistemas e Rede para um usuário.

3.3 Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver univocamente assegurada.

3.4 Os usuários serão responsabilizados pelas ações de outros se, desrespeitando o item anterior, deliberadamente, compartilharem sua senha de acesso.

3.5 Senhas devem conter no mínimo oito caracteres incluindo números, letras minúsculas, letras maiúsculas e caracteres especiais e não devem possuir uma regra de formação perceptível.

3.6 Senhas devem ser trocadas periodicamente, num prazo não superior a seis (6) meses.

3.7 Os usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas.

3.8 Senhas temporárias podem ser entregues ao titular ou a outrem por procuração registrada em cartório.

3.9 Em caso de esquecimento da senha uma senha temporária pode ser fornecida, não sendo tecnicamente possível a recuperação da senha anterior.

3.10 A troca de senha temporária é obrigatória na primeira autenticação.

3.11 Cabe ao Administrador de Sistemas e Rede adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando os critérios gerais anteriores.

3.12 A robustez da senhas poderá ser auditada pela Diretoria de TI com fins de localização de senhas fracas.

3.13 O usuário que tiver sua senha encontrada pelos testes de robustez serão notificados para que as troquem por senha seguras em, no máximo, vinte e quatro horas. O descumprimento desta determinação terá como consequência o bloqueio de seus acessos aos serviços do IFS.

4 DISPOSIÇÕES GERAIS

4.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do CGSIC que, se considerar necessário fará convocação de reunião do Comitê.

5 VIGÊNCIA

5.1 Esta Norma entra em vigor a partir da data de sua publicação.

ANEXO

Considerações e sugestões para elaboração de senhas fortes

Uma boa senha possui de 8 a 12 dígitos. Mas, quanto mais longa, melhor.

Não utilize palavras e nomes conhecidos. Programas de quebra de senha possuem uma base bastante aprimorada com diversos dicionários, afim de testar cada uma destas palavras e tentar então quebrar essa senha.

Utilize caracteres alfanuméricos como números e sinais de pontuação, além de também alternar letras maiúsculas e minúsculas.

Evite anotar suas senhas em papéis ou divulgar para outras pessoas. Trabalhe num conjunto de caracteres que possam representar simbolicamente algo para você, e que possa ser facilmente lembrado.

Use senhas diferentes para suas contas. Obviamente é mais cômodo ter apenas uma boa senha, mas em caso de furto ou vazamento, todas as contas e sistemas nos quais você utiliza desta senha para acesso poderão ser facilmente acessados por quem se beneficiar.

Mude suas senhas com frequência. Isto com certeza pode te ajudar no caso de alguém estar bisbilhotando alguma conta sua (particular ou de trabalho) e não estiver deixando rastros.

A revista Businessweek publicou, no dia 27 de janeiro de 2011, um artigo mostrando a vulnerabilidade das senhas que usamos em nosso dia a dia. Segundo o artigo, as senhas mais usadas são: 123456, password, 12345678, qwerty, abc123.

A Tabela 1 representa o tempo necessário para quebrar uma senha, levando em conta seu tamanho e a regra de formação:

Tabela 1

Tamanho da senha	**Minúsculas**	**Maiúsculas**	**Nºs e Símbolos**
6 caracteres	10 minutos	10 horas	18 dias
7 caracteres	4 horas	23 dias	4 anos
8 caracteres	4 dias	3 anos	463 anos
9 caracteres	4 meses	178 anos	44.530 anos

O gasto médio das empresas para tratar de problemas relativos a troca de senha é de U$ 10,00. 30% dos chamados feitos a serviços de helpdesk são relativos a senhas. 50% dos

usuários escolhem senhas baseadas em palavras comuns, datas de aniversário, nomes de parentes, palavras de cunho religioso ou combinações simples de caracteres.

Sempre somos aconselhados a utilizar senhas seguras. Senhas seguras são aquelas que tem pelo menos 8 caracteres e são compostas por letras, números e caracteres especias.

Mas isso é um problema. Temos sempre muitas senhas para guardar e senhas com as características citadas acima não são nada mnemônicas. Como proceder então? Como criar senhas difíceis de serem quebradas e ao mesmo tempo fáceis de serem lembradas?

Uma solução muito boa é o uso de uma frase, por exemplo:

Eu nasci as 14:00 da tarde de 1980.

Se pegarmos as primeiras letras de cada palavra (respeitando maiúsculas e minúsculas) e os números temos a seguinte senha:

Ena14:00dtd1980.

Prestem atenção ao ponto ao final da senha!

Uma outra técnica interessante é utilizar o endereço do usuário. Por exemplo, vamos supor de uma empresa fictícia: Rapidinho Encomendas

O endereço da Rapidinho Encomendas é rua da Glória, número 325, sala 45!

Isso geraria a seguinte senha:

OedREerdG,n325,s45!

Mais uma vez atenção à exclamação ao final da senha!

Poderíamos deixar esta senha mais segura trocando a palavra número pelo símbolo #, e teríamos:

OedREerdG,#325,s45!

Tudo certo? Quase... Cuidado existem senhas com muitos caracteres estranhos e coisa do tipo, mas que são muito manjadas como:

Uma arroba é 15 Kilos:

U@é15Kg

ou

"Batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "!Bqnsepc" (o sinal de exclamação foi colocado no início para acrescentar um símbolo à senha). Esta senha encontra-se na Cartilha de Segurança disponibilizada no site do www.cert.br.

!BqnsepC"

Senhas desse tipo são muito usadas e fáceis de serem quebradas apesar da sua aparência de inquebrável.

A informação é um patrimônio inestimável da Instituição e cabe ao servidor zelar pela sua integridade, disponibilidade, autenticidade e veracidade.

Lei Nº 8.112, de 11 de dezembro de 1990, Art. 116: São deveres do servidor: … VII - **zelar pela economia do material e a conservação do patrimônio público;**

Referências:

http://www.dicas-l.com.br/arquivo/o_problema_das_senhas.php. Acessado em 07/04/2011.

http://www.dicas-l.com.br/arquivo/administracao_de_senhas_for_dummies.php. Acessado em 07/04/2011.

http://cartilha.cert.br/. Acessado em 07/04/2011.

http://www.planalto.gov.br/ccivil_03/Leis/L8112cons.htm. Acessado em 07/04/2011.