Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Senhas

Objetivo

Estabelecer os requisitos, procedimentos e protocolos para o controle de acesso aos dados, visando a proteção da confidencialidade de todas as informações da Instituição e de seus clientes.

Visão geral

O gerenciamento de credenciais de acesso aos sistemas da Instituição deve ser realizado de maneira a assegurar a confidencialidade das informações retidas pela Instituição. Para tal, devem ser realizados procedimentos de proteção e autenticação relacionados a todos os acessos aos sistemas e plataformas utilizados pela Instituição.

1. Gerenciamento de Contas de Usuário

Todo integrante da Instituição deve possuir uma conta de usuário única e que seja pessoal, intransferível e rastreável. Contas genéricas, compartilhadas, de serviço ou de grupo são de uso proibido nos sistemas e plataformas da Instituição, a não ser nas exceções definidas pelo Responsável pela Segurança da Informação.

EMBRASI

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Na criação de novas contas de usuários nos sistemas e plataformas da Instituição, o Responsável pela Segurança da Informação deve definir as credenciais de acesso adequadas, conforme as classificações da informação contidas na Política de Segurança da Informação.

As solicitações de inclusão, exclusão ou alteração de credenciais de acesso serão endereçadas ao Responsável pela Segurança da Informação.

Ao se conceder credenciais de acesso a uma determinada conta de usuário, deve-se criar um ID e senha únicos e separados da conta de usuário regular do integrante.

Nos casos em que um integrante da Instituição for demitido, o seu acesso aos sistemas e plataformas da Instituição será encerrado de forma imediata pelo Responsável pela Segurança da Informação.

As credenciais de acesso serão revisadas periodicamente de acordo com cronograma estabelecido pelo Responsável pela Segurança da Informação, e as contas inativas serão devidamente removidas dos bancos de dados e servidores da Instituição.

2. Gerenciamento de Senhas

As senhas dos integrantes da Instituição devem ser estabelecidas com o fim de garantir a confidencialidade das informações. Assim, devem ser realizados treinamentos periódicos para a conscientização dos integrantes da Instituição sobre

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

a necessidade de memorização das senhas, para evitar que elas sejam anotadas em meios físicos ou eletrônicos.

O Responsável pela Segurança da Informação deve determinar as situações em que as senhas serão complementadas com controles de acesso adicionais, tais como *smart cards*, *tokens* ou outros procedimentos de autenticação suplementar de dois ou três fatores.

Todas as senhas de usuário-padrão serão alteradas no primeiro *login* do usuário. Já as contas de usuário-padrão devem ser desativadas ou alteradas após a instalação de um novo *software* ou aplicativo.

Todos os usuários devem selecionar as senhas que atendam aos requisitos abaixo elencados, a fim de garantir complexidade e resiliência as suas senhas. Deste modo, as senhas dos usuários devem conter:

- Caracteres entre “a” e “z”, tanto em letras maiúsculas quanto em letras minúsculas;
- Números (0-9) e caracteres especiais (por exemplo, @, #, $, *);
- Um mínimo de pelo menos 08 caracteres.

Também devem ser utilizadas diferentes senhas para diferentes tipos de atividades, como por exemplo, acesso a e-mail ou acesso a arquivos, especialmente em sistemas que armazenam informações confidenciais da Instituição.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Deve-se evitar a utilização de senhas vulneráveis, consideradas aquelas que contenham os seguintes atributos:

- Palavras comuns encontradas no dicionário;
- Seja a mesma senha daquelas utilizada em alguma conta de uso pessoal, como por exemplo, e-mail pessoal, internet banking ou mídias sociais;
- Contenha informações pessoais, como nome de um cônjuge ou animal de estimação, cadastro de pessoas físicas, número da carteira de motorista, endereço de rua, número de telefone, etc.;
- Contenha sequências ou caracteres repetidos (1234, 3333, etc.).

Os treinamentos de segurança da informação devem incluir as seguintes disposições:

- Os riscos na utilização de senhas consideradas fracas;
- Os requisitos para a escolha de senhas;
- A proibição da seleção de recursos como o "lembre-se de mim" ou o "lembrar-se de senha" em aplicativos e navegadores da Web;
- Os cuidados na utilização de mídias sociais para que as senhas utilizadas não sejam comprometidas.
- As senhas utilizadas pelos usuários não poderão, sob quaisquer circunstâncias:
- Ser reveladas ou compartilhadas com qualquer outro indivíduo, dentro ou fora da Instituição;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Ser armazenadas por escrito ou transmitidas em texto claro e não criptografado;
- Ser inseridas em mensagens de e-mail não criptografadas ou outras formas de comunicação eletrônica.

Caso um membro da equipe suspeite de que sua senha foi comprometida ou disponibilizada a outras pessoas, ele deve imediatamente redefini-la ou altera-la e notificar o Responsável pela Segurança da Informação.

3. Procedimentos para Redefinição de Senha

As senhas devem ser alteradas regularmente de acordo com o seguinte cronograma:

- As senhas de usuário com credenciais devem ser alteradas pelo menos a cada 60 dias.
- As senhas do usuário regulares devem ser alteradas pelo menos a cada 90 dias.
- Ao realizar o procedimento, o usuário não poderá repetir nenhuma de suas cinco senhas anteriores.

4. Procedimentos de Senha nas Aplicações de Software

Os desenvolvedores de *softwares* e aplicativos devem garantir que os programas contenham as seguintes precauções de segurança:

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Os *softwares* e aplicativos devem exigir que cada usuário final tenha seu próprio ID de usuário exclusivo;
- Contas genéricas, compartilhadas, de serviço ou de grupo são terminantemente proibidas;
- Poderão ser utilizados grupos de segurança para listas de controle de acesso a certos recursos e funções de um aplicativo;
- Senhas de proteção que protegem informações sensíveis devem ser protegidas utilizando criptografia em repouso e em trânsito, sendo terminantemente proibida a sua transcrição em texto claro e explícito;
- Deve ser exigido que um usuário reinsira uma senha após um período de inatividade para recuperar o acesso ao seu aplicativo.