MANUAL – BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

USO DOS SISTEMAS

1. OBJETIVO

O objetivo deste manual é estabelecer boas práticas que devem ser observadas para utilização segura dos sistemas disponibilizados pela Fundação.

2. RECOMENDAÇÕES

2.1 CREDENCIAIS DE ACESSO – LOGIN E SENHA

A autenticação para acesso aos sistemas ocorre através do usuário (login) e senha (password). Tal processo visa garantir a confidencialidade no acesso à informação, ou seja, permitir acesso apenas por pessoas autorizadas.

Cada usuário é responsável pela escolha de suas senhas pessoais. Portanto, seguem algumas recomendações importantes:

a) Utilize senhas com pelo menos 6 caracteres;

b) Não defina senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;

c) Não defina senhas com caracteres repetidos ou sequenciais. Exemplo: 123456;

d) Nunca compartilhe, empreste ou divulgue suas credenciais de acesso com outras pessoas;

e) Altere as senhas periodicamente, com o objetivo de assegurar a confidencialidade das mesmas. É recomendável que as senhas sejam alteradas a cada 6 meses;

f) Nunca armazene suas credenciais (login e senha) em locais considerados inseguros, como anotações em papel;

g) Na hipótese do uso de senhas temporárias, sempre altere as senhas no primeiro acesso;

h) Cuidado ao digitar sua senha em ambientes públicos, além disso não digite senhas quando estiver sendo observado por alguém;

i) Na hipótese de suas credenciais terem sido comprometidas, ou seja, descobertas por outras pessoas, providencie imediatamente a alteração dos dados.

2.2 CERTIFICADO DIGITAL

Certificado digital é um documento eletrônico emitido por uma autoridade certificadora, utilizado para comprovação de identidade, permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não repúdio, assim como assinar digitalmente documentos.

Cada usuário que recebe o certificado é responsável pela sua guarda e utilização. Algumas recomendações importantes:

a) Nunca forneça o certificado digital a terceiros. O certificado digital é um documento pessoal e intransferível;

b) Ao solicitar o e-CPF o signatário recebe uma senha pessoal, denominada PIN, além de assinar um termo de responsabilidade no qual se compromete a não compartilhar sua senha e não emprestar o smartcard a terceiros, garantindo assim que de fato é o portador que assina os documentos;

c) É obrigatório o uso de senha (PIN) para proteger a chave privada e garantir sua segurança. O titular do certificado e-CPF deve criar uma senha forte, com no mínimo 8 caracteres, evitando palavras ou caracteres que o associem à senha escolhida;

d) Não defina senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;

e) Não defina senhas com caracteres repetidos ou sequenciais. Exemplo: 123456;

f) Nunca compartilhe, empreste ou divulgue suas credenciais de acesso com outras pessoas;

g) Nunca armazene suas credenciais (login e senha) em locais considerados inseguros, como anotações em papel;

h) Caso o titular do certificado tome conhecimento de que a segurança do mesmo foi de alguma forma comprometida, é de sua responsabilidade requerer a imediata revogação do e-CPF, visto que perante a Receita Federal do Brasil, todos os atos executados através do uso do certificado são de responsabilidade única e exclusiva do titular.