Responsabilidades do Titular e-CNPJ

CERTIFICADO DIGITAL A3

Importante: é obrigatório possuir um hardware criptográfico (smart card ou token) para adquirir este produto.

Cartão

No e-CNPJ A3 em cartão inteligente (smart card), quem controla o certificado digital são as senhas PIN e PUK. O responsável pelo certificado digital deve configurar e manter o sigilo desses controles ou senhas.

PIN - funciona como bloqueio para restringir o uso do certificado digital armazenado no cartão inteligente.

- Todos os certificados digitais emitidos em cartões saem de fábrica com o mesmo PIN: 1234.
- O titular do certificado deve alterar esse PIN para uma senha de seu conhecimento exclusivo.
- A CARDS inova recomenda a alteração imediata do PIN original para garantir a segurança do seu certificado digital.
- Sugerimos ainda que o novo PIN seja guardado em local seguro.
- Para modificar o PIN, selecione no aplicativo Safesign as opções 'Token > Alterar PIN'.
- Se você digitar a senha PIN incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado.
- É possível o desbloqueio com o uso da senha PUK.
- Se você também digitar a senha PUK incorretamente por 3 vezes consecutivas o cartão será imediatamente bloqueado e inutilizado. É então necessário a emissão de um novo certificado e compra de um novo cartão.
  PUK - é utilizado para resgatar seu PIN em caso de bloqueio do cartão.
- Todos os certificados digitais emitidos em cartões saem de fábrica com o mesmo PUK: 1234.
- Assim, o PUK também deve ser alterado para uma senha que somente você conheça.

- A CARDS inova recomenda que você altere imediatamente o PUK original para segurança de seu certificado digital.
- Sugerimos ainda que o novo PUK seja guardado em local seguro, pois sua perda inviabilizará o desbloqueio do cartão.

ATENÇÃO: Se você digitar a senha PIN incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado. É possível o desbloqueio com o uso da senha PUK. Se você também digitar a senha PUK incorretamente por 3 vezes consecutivas, o cartão será imediatamente bloqueado e inutilizado, e um novo cartão com novo certificado precisará ser adquirido e emitido.

Token

No e-CNPJ A3 em token, quem controla o certificado digital é a senha PIN. O responsável pelo certificado digital deve configurar e manter em sigilo o PIN.

Essa senha funciona como um mecanismo de bloqueio para restringir o uso do certificado digital armazenado no token.

Todos os certificados digitais emitidos em token têm uma senha padrão original, a saber:

CERTIFICADO DIGITAL A1

No certificado e-CNPJ A1, o par de chaves pública/privada é gerado no computador do titular, utilizando as bibliotecas criptográficas existentes e apresentadas pelo navegador. Quando ocorre a geração das chaves, a chave privada é armazenada no disco rígido do computador.

É obrigatório o uso de senha para proteger a chave privada e garantir sua segurança. O titular do certificado e-CNPJ deve criar uma senha forte, com no mínimo 8 caracteres e utilizando caracteres especiais (&,*,$,#,@, etc.), evitando palavras ou caracteres que o associem à senha escolhida. Não devem ser utilizadas: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequencias numéricas simples ou curtas e palavras contidas em dicionários. Existem programas capazes de decifrar uma senha fraca em questão de horas.

Da mesma forma, é obrigatório requerer a imediata revogação do e-CNPJ caso o titular do certificado tome conhecimento de que a segurança do mesmo foi de alguma forma comprometida.

Após a geração das chaves, é aconselhável que a chave privada seja exportada e armazenada em cópia de segurança (back-up) externa (disquete,

token ou cartão inteligente - smart card) e seu titular deve protegê-la através de senha de acesso.

Todos os atos realizados perante à Receita Federal do Brasil utilizando o Certificado Digital é de responsabilidade única do titular.