

Orientações de Segurança ao Usuário - Certificado Digital INVIA

Versão 1.0 - 09/08/2017



AUTORIDADE DE REGISTRO CERTIFICAÇÃO DIGITAL

Obrigado por confiar à **AR-INVIA** a emissão de seu certificado digital!

Agora, para sua segurança, é importante que você tenha conhecimento de certas precauções quanto ao uso do seu certificado digital:

Certificado Digital modelo A1

1. Armazenamento e *Backup* do Certificado Digital:

É altamente recomendado que o arquivo do certificado digital esteja armazenado em um local seguro. Não é recomendado deixar o arquivo em um computador de fácil acesso a pessoas não autorizadas pelo cliente.

O *backup* do arquivo do certificado digital é também de extrema importância. Este backup envolve o armazenamento de uma cópia do arquivo em um local seguro, que não seja a própria máquina onde o certificado digital está instalado. Locais de armazenamento seguro incluem:

- Pen-drive de utilização pessoal do responsável do certificado digital
- Armazenamento em nuvem (*cloud*)
- E-mail de utilização pessoal do responsável do certificado digital
- Servidor seguro

Obs: O armazenamento e a manutenção do *backup* do arquivo do certificado digital são de responsabilidade do responsável pelo certificado digital. Em caso de dúvidas ou de necessidade de auxílio técnico, é recomendável entrar em contato com nosso setor técnico.

2. Compartilhamento do Certificado Digital e Senha com Terceiros:

Outro cuidado especial que deve ser tomado é quanto ao compartilhamento do arquivo com outras pessoas, lembrando sempre do risco de mau uso do certificado digital por terceiros. O mesmo vale para a senha do arquivo do seu certificado digital. O certificado digital e a senha devem, preferencialmente, ser guardados apenas pelo responsável, e de forma segura.

3. Controle da Senha:

A INVIA não armazena senhas de certificados digitais e também não possui controle sobre elas, portanto é muito importante o responsável do certificado digital manter um controle da senha do arquivo.

4. Utilização Correta do Certificado Digital:

Seu certificado digital é a sua assinatura digital na rede, portanto é recomendado sempre tomar cuidado com qualquer ação feita utilizando um certificado digital, para evitar eventuais transtornos. Em caso de dúvida, sempre se informe com seu Contador, Órgão Competente ou com outra Pessoa Responsável.

Certificado Digital modelo A3

1. Distribuição do Certificado Digital e Senhas a Terceiros:

É altamente recomendado tomar um cuidado especial quanto à disponibilização do token ou cartão à outras pessoas, lembrando sempre do risco de mau uso do certificado digital por terceiros. O mesmo vale para as senhas PIN e PUK do seu Token ou Cartão. O certificado digital e as senhas devem, preferencialmente, ser guardados apenas pelo responsável, e de forma segura.

2. Formatação ou Exclusão do Conteúdo do Token ou Cartão:

É de extrema importância para o usuário o cuidado para não formatar ou excluir o conteúdo do Token ou Cartão. Isto pode ocorrer acidentalmente caso o usuário utilize as ferramentas de administração do Token ou Cartão. Portanto, é recomendado entrar em contato com nosso setor técnico antes de utilizar qualquer ferramenta de administração.

3. Dano ou Extravio do Token ou Cartão:

Para evitar que o Token ou Cartão seja danificado, é recomendado:

- Conectar o dispositivo somente quando for necessário utilizar o certificado digital, para evitar possíveis danos ao dispositivo causados por quedas de luz.
- Certificar-se em não conectar o dispositivo em uma porta USB danificada ou com defeito.
- Não causar pressão física demasiada no dispositivo, para evitar comprometimento das peças internas.
- Não molhar o dispositivo com nenhum tipo de líquido
- Não expor o dispositivo à altas temperaturas.
- Não deixar o dispositivo próximo de aparelhos que emitam ondas magnéticas

Em caso de extravio do Token ou Cartão, entre em contato com nosso setor comercial imediatamente, será realizada a revogação imediata do seu certificado digital.

4. Controle das Senhas PIN e PUK:

A INVIA não armazena senhas de certificados digitais e também não possui controle sobre elas, portanto é muito importante o responsável do certificado digital manter um controle das senhas PIN e PUK. Erros repetidos da sua senha PIN irão resultar em bloqueio da mesma, sendo permitido o desbloqueio somente através da senha PUK. Erros repetidos da sua senha PUK irão resultar no bloqueio definitivo do certificado digital, sendo necessária a emissão de um novo. Portanto, em caso de digitação incorreta de senha, é altamente recomendado entrar em contato com nosso suporte técnico antes de fazer novas tentativas.

5. Utilização Correta do Certificado Digital:

Seu certificado digital é a sua assinatura digital na rede, portanto é recomendado sempre tomar cuidado com qualquer ação feita utilizando um certificado digital, para

evitar eventuais transtornos. Em caso de dúvida, sempre se informe com seu Contador, Órgão Competente ou com outra Pessoa Responsável.

Suporte Técnico INVIA

- **Chat Online:**
<http://invia.com.br/> - Suporte Técnico
- **Skype:**
suporte_invia
- **Telefone:**
(51) 3022-4996 - Ramal 2

Suporte Comercial

- **Telefone:**
(51) 3022-4996 - Ramal 1
- **E-mail:**
invia@invia.com.br

Setor de Suporte Técnico de Certificação Digital - AR-INVIA
(51) 3022-4996 - Ramal 2

Este manual é de propriedade intelectual da **Autoridade de Registro INVIA**, e não poderá ser alterado por terceiros sem a devida permissão. Fica livre a cópia e distribuição deste documento, na sua forma integral.