ATENÇÃO

A SENHA É **RESPONSABILIDADE DO USUÁRIO**

NÃO NOS RESPOSNABILIZAMOS PELA PERDA, ESQUECIMENTO DE SENHA OU BLOQUEIO DE TOKEN.

O Usuário tem 3 chances da senha PIN (Acesso) depois de 3 erros consecutivos terá 3 chances para desbloquear o TOKEN com a senha PUK. Caso erre também 3 vezes a senha PUK o Certificado Digital estará **BLOQUEADO, NÃO SE PODE MAIS DESBLOQUEAR.** O usuário terá que COMPRAR tudo de novo e AGENDAR NOVA VALIDAÇÃO.

Não existe nenhuma outra forma de se recuperar a senha. A OAB não fica com cópia das suas senhas, pois as senhas são PESSOAIS E INTRANSFERÍVEIS.

SUPORTE TÉCNICO: 11-3478-9444 ou 0300-789-2378 2ª À 6ª DAS 9:00 ÀS 20:HS

SENHA PIN: _____
(ACESSO)

SENHA PUK: _____
(DESBLOQUEIO)

Senhas: A cada utilização do seu Certificado Digital OAB será solicitada a senha PIN. Se a senha PIN for digitada três vezes incorretamente, o cartão ou token será **bloqueado**. Caso isto ocorra, o desbloqueio deve ser efetuado por meio da senha PUK. Se a senha PUK for digitada três vezes incorretamente, o dispositivo (Carteira Profissional do Advogado ou Token) pode ser **reinicializado e reutilizado**, mas o Certificado Digital OAB será perdido, sendo necessária a aquisição de um novo Certificado Digital OAB

IMPORTANTE

1. Faça a Instalação dos Programas **SEM o Token/Leitora Conectado** à maquina, para garantir que seu Certificado não seja deletado de dentro do Token.
2. ***NUNCA inicialize seu Token*** ***ou leitora***– isto formatará o dispositivo e excluirá sua certificação de dentro dele.
3. Caso ainda não tenha instalado, recomendamos fazer instalação do navegador **Mozilla Firefox,** pois, alguns sites só aceitam peticionamento por este navegador.

Ambientes

- Windows 7 – Windows Vista – Windows XP –Windows 8 – MAC OS

Pré-Requisitos

1. Os pré-requisitos para utilização do AIC AC OAB 3.13.0 são:
   - Conexão com a Internet E Privilégios de Administrador

   Como instalar o AIC AC OAB e o token GD Burti no seu computador:

Faça a Instalação do JAVA, com as observações abaixo:

VERSÕES DO JAVA: COMPATIBILIDADE COM E-SAJ E PJe

Prezados Advogados,

A respeito da atualização mais recente do aplicativo Java, seguem as seguintes considerações:

O sistema E-SAJ do Tribunal de Justiça do Estado de São Paulo está solicitando que os usuários realizem a atualização do Java para sua versão mais recente (Java 8.0). Contudo, a referida versão apresenta incompatibilidade com o sistema do PJE, utilizado na Justiça do Trabalho.

Diante disso, solicitamos aos advogados que **NÃO REALIZEM A ATUALIZAÇÃO DO JAVA, MANTENDO VERSÕES ANTERIORES INSTALADAS (Java 7.67 ou Java 7.71),** pois o sistema E-SAJ, ao menos em um primeiro momento, funcionará com as versões anteriores, assim como o PJE. Logo não terão problemas em utilizar nenhum dos dois sistemas.

Sugestão de site para download: http://www.oldapps.com/java.php

Acesse o endereço

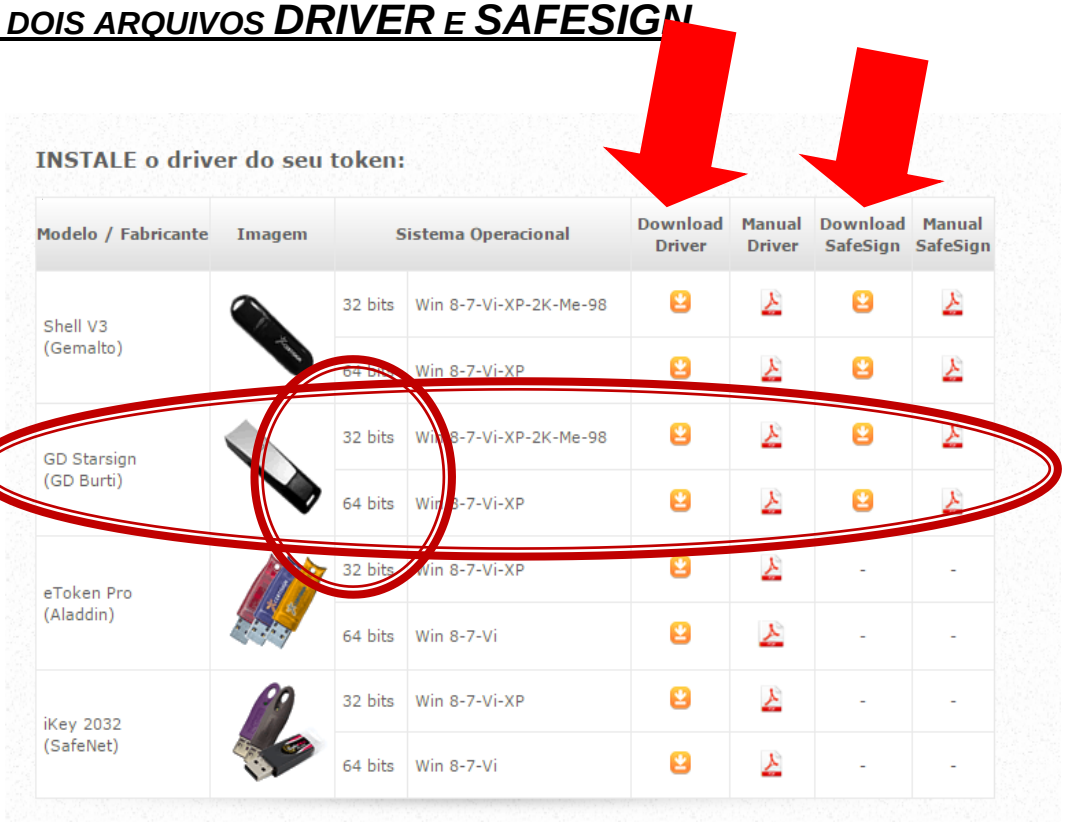
http://www.certisign.com.br/atendimento-suporte/downloads/tokens

Selecione o Sistema Operacional

TOKEN GD BURTI

WINDOWS

VERIFIQUE SE SEU SISTEMA OPERACIONAL É DE ***32 OU 64 BITS*** E PROCEDA COM A INSTALAÇÃO DO RESPECTIVO DRIVER, ***DEVE-SE FAZER A INSTALAÇÃO DOS DOIS ARQUIVOS DRIVER E SAFESIGN***



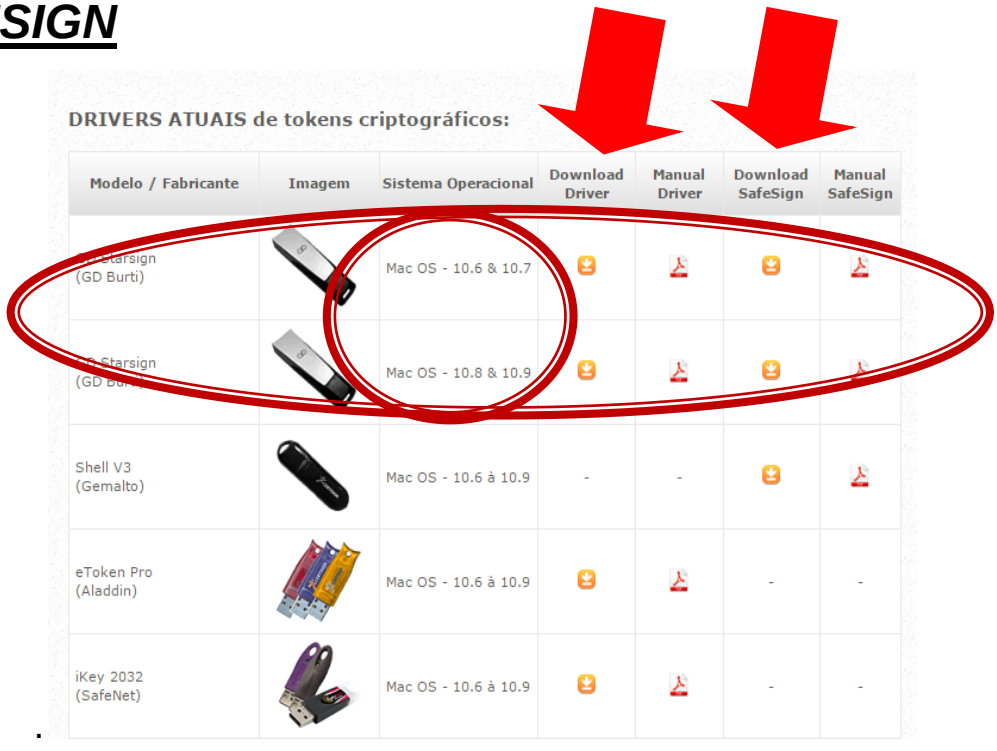
INSTALE o driver do seu token:

Modelo / Fabricante	Imagem	Sistema Operacional		Download Driver	Manual Driver	Download SafeSign	Manual SafeSign
Shell V3 (Gemalto)		32 bits	Win 8-7-Vi-XP-2K-Me-98				
		64 bits	Win 8-7-Vi-XP				
GD Starsign (GD Burti)		32 bits	Win 8-7-Vi-XP-2K-Me-98				
		64 bits	Win 8-7-Vi-XP				
eToken Pro (Aladdin)		32 bits	Win 8-7-Vi-XP			-	-
		64 bits	Win 8-7-Vi			-	-
iKey 2032 (SafeNet)		32 bits	Win 8-7-Vi-XP			-	-
		64 bits	Win 8-7-Vi			-	-

MAC

LOCALIZE GD Startsign (GD Burti*), verifique a versão de seu MAC* E PROCEDA COM A INSTALAÇÃO

DEVE-SE FAZER A INSTALAÇÃO DOS DOIS ARQUIVOS DRIVER E SAFESIGN



DRIVERS ATUAIS de tokens criptográficos:

Modelo / Fabricante	Imagem	Sistema Operacional	Download Driver	Manual Driver	Download SafeSign	Manual SafeSign
GD Starsign (GD Burti)		Mac OS - 10.6 & 10.7				
GD Starsign (GD Burti)		Mac OS - 10.8 & 10.9				
Shell V3 (Gemalto)		Mac OS - 10.6 à 10.9	-	-		
eToken Pro (Aladdin)		Mac OS - 10.6 à 10.9			-	-
iKey 2032 (SafeNet)		Mac OS - 10.6 à 10.9			-	-

TOKEN ALADIM

WINDOWS

VERIFIQUE SE SEU SISTEMA OPERACIONAL É DE ***32 OU 64 BITS*** E PROCEDA COM A INSTALAÇÃO DO RESPECTIVO DRIVER

INSTALE o driver do seu token:

Modelo / Fabricante	Imagem	Sistema Operacional		Download Driver	Manual Driver	Download SafeSign	Manual SafeSign
Shell V3 (Gemalto)		32 bits	Win 8-7-Vi-XP-2K-Me-98				
		64 bits	Win 8-7-Vi-XP				
GD Starsign (GD Burti)		32 bits	Win 8-7-Vi-XP-2K-Me-98				
		64 bits	Win 8-7-Vi-XP				
eToken Pro (Aladdin)		32 bits	Win 8-7-Vi-XP				
		64 bits	Win 8-7-Vi			-	-
iKey 2032 (SafeNet)		32 bits	Win 8-7-Vi-XP			-	-
		64 bits	Win 8-7-Vi			-	-

MAC

LOCALIZE eToken Pro (Aladin) E PROCEDA COM A INSTALAÇÃO DO RESPECTIVO DRIVER

DRIVERS ATUAIS de tokens criptográficos:

Modelo / Fabricante	Imagem	Sistema Operacional	Download Driver	Manual Driver	Download SafeSign	Manual SafeSign
GD Starsign (GD Burti)		Mac OS - 10.6 & 10.7				
GD Starsign (GD Burti)		Mac OS - 10.8 & 10.9				
Shell V3 (Gemalto)		Mac OS - 10.6 à 10.9	-	-		
eToken Pro (Aladdin)		Mac OS - 10.6 à 10.9				
iKey 2032 (SafeNet)		Mac OS - 10.6 à 10.9			-	

LEITORA

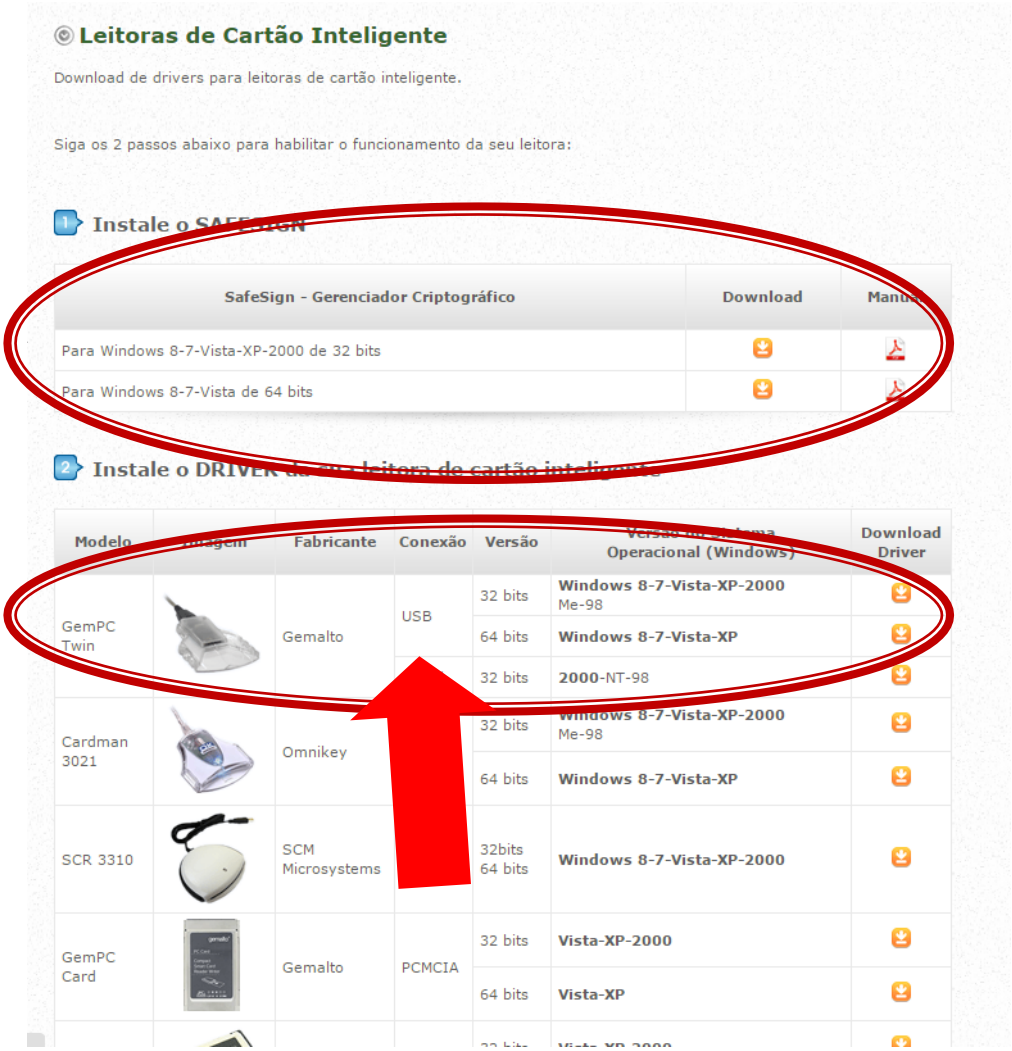
Acesse o endereço:
http://www.certisign.com.br/atendimento-suporte/downloads/leitoras

Selecione o Sistema Operacional

WINDOWS

VERIFIQUE QUAL A VERSÃO DE SEU SISTEMA E PROCEDA COM A INSTALAÇÃO DO SAFESIGN

APÓS INSTO LOCALIZE GemPC Twin – ***CONEXÃO USB***, VERIFIQUE SE SEU SISTEMA OPERACIONAL É DE ***32 OU 64 BITS*** E PROCEDA COM A INSTALAÇÃO DO RESPECTIVO DRIVER



Leitoras de Cartão Inteligente

Download de drivers para leitoras de cartão inteligente.

Siga os 2 passos abaixo para habilitar o funcionamento da seu leitora:

Instale o SAFESIGN

SafeSign - Gerenciador Criptográfico	Download	Manual
Para Windows 8-7-Vista-XP-2000 de 32 bits		
Para Windows 8-7-Vista de 64 bits		

Instale o DRIVER da sua leitora de cartão inteligente

Modelo	Imagem	Fabricante	Conexão	Versão	Versão do Sistema Operacional (Windows)	Download Driver
GemPC Twin		Gemalto	USB	32 bits	Windows 8-7-Vista-XP-2000 Me-98	
				64 bits	Windows 8-7-Vista-XP	
				32 bits	2000-NT-98	
Cardman 3021		Omnikey		32 bits	Windows 8-7-Vista-XP-2000 Me-98	
				64 bits	Windows 8-7-Vista-XP	
SCR 3310		SCM Microsystems		32bits 64 bits	Windows 8-7-Vista-XP-2000	
GemPC Card		Gemalto	PCMCIA	32 bits	Vista-XP-2000	
				64 bits	Vista-XP	

MAC

LOCALIZE O ARQUIVO E PROCEDA COM A INSTALAÇÃO DO RESPECTIVO DRIVER

Certisign » Atendimento e Suporte » Downloads » Leitoras de Cartão Inteligente » MAC

4

Leitoras de Cartão Inteligente - MAC

Download de drivers para leitoras de cartão inteligente.

ATENÇÃO: Todas as leitoras comercializadas pela Certisign são reconhecidas automáticamente pelos sistemas operacionais MacOS, sendo necessária somente a instalação do gerenciador criptográfico SafeSign.

SafeSign - Gerenciador Criptográfico	Download	Manual
Para MacOS 10.6 à 10.9		

TESTE SEU CERTIFICADO

Acesse o endereço http://www.certisign.com.br/atendimento-suporte/central-de-testes

Política de Garantia

Obrigada por escolher e adquirir os produtos e/ou serviços **CERTISIGN**.

Nossa Política de Garantia foi desenvolvida com o intuito de esclarecer os seus direitos em relação aos nossos produtos e serviços.

1. VALIDAÇÃO E EMISSÃO DO CERTIFICADO DIGITAL

1.1 A partir da data da confirmação do pagamento, o cliente terá o prazo de 180 (cento e oitenta) dias para realizar o procedimento de apresentação de documentos (validação presencial). A contar da data em que for realizada a validação presencial, o cliente terá o prazo de 30 (trinta) dias para realizar a emissão de seu certificado digital. Excedidos os prazos indicados, haverá a perda do direito de validação, emissão e devolução do valor pago.

2. CUIDE DAS SUAS SENHAS

2.1 A guarda do **PIN/PUK, PASSWORD** ou **SENHA**, nesta política de garantia denominada simplesmente como**"SENHA/SENHAS"**, é de responsabilidade do titular do Certificado Digital. Estas senhas são geradas e armazenadas diretamente no Cartão Inteligente/Token ou no computador do cliente, na hipótese do certificado A1.

2.2 Por determinação legal a **CERTISIGN** **não** tem acesso as **SENHAS** de seus clientes,

portanto, não poderá recuperá-la(s) em caso de perda ou esquecimento.

2.3 Ao digitar sua **SENHA**, atenção: **as tentativas são cumulativas**, ou seja, a desconexão do dispositivo na entrada USB ou a reinicialização do computador não zera o número de tentativas anteriores.

3. MÍDIAS CRIPTOGRÁFICAS ¿ CARTÃO INTELIGENTE/TOKEN

3.1 A **SENHA** será solicitada a cada utilização do certificado digital.

3.2 ATENÇÃO: Cada mídia criptográfica tem um padrão de utilização de senha, tais como: quantidade de caracteres e número de tentativas antes do bloqueio, os quais estão dispostos no **link** www.certisign.com.br/midias.

3.3 O não cumprimento dos padrões de utilização de **SENHA** acarretará o bloqueio da mídia criptográfica e a perda do direito de uso do certificado digital e/ou, ainda, do cartão inteligente.

4. NÃO EMPRESTE SEU CERTIFICADO DIGITAL

4.1 O Certificado Digital é de uso exclusivo do titular. Ao utilizá-lo é gerada uma assinatura digital com validade jurídica. Por isso, não confie a guarda e nem empreste o seu Certificado Digital ou sua **SENHA** a terceiros, pois a sua assinatura digital possui a mesma validade legal que a sua assinatura manuscrita.

4.2 Guarde o seu **Certificado Digital** e **SENHAS**, separadamente, em locais seguros.

5. GARANTIA

5.1 A **CERTISIGN** oferece a garantia contra vícios ou defeitos de emissão dos Certificados Digitais e de fabricação dos Dispositivos Criptográficos (tokens e cartões inteligentes) e Leitoras de Cartões Inteligentes, desde que mantidos em condições normais.

6. PRAZO DE GARANTIA

Garantia - 180 (cento e oitenta) dias

6.1 Conforme o artigo 26, II do Código de Defesa do Consumidor (CDC), é direito do consumidor apresentar reclamação por escrito acerca do vício, comprovadamente formulada no prazo de 90 (noventa) dias da data de emissão do Certificado Digital para que a **CERTISIGN** avalie a troca do produto adquirido por outro igual ou por produto equivalente superior. A reposição dos produtos em garantia está sujeita às condições de retorno, observando a garantia legal.

6.2 Além dos 90 (noventa) dias garantidos pelo CDC, a **CERTISIGN** oferece mais 90 (noventa) dias de garantia contra vícios ou defeitos dos Certificados Digitais e de fabricação dos Dispositivos Criptográficos (tokens e cartões inteligentes) e Leitoras de Cartões Inteligentes.

7. PROCEDIMENTOS

7.1 Durante o período de 180 (cento e oitenta) dias previsto acima, o consumidor que apresentar reclamação sobre o funcionamento dos Certificados Digitais, Dispositivos Criptográficos e/ou Leitoras de Cartões Inteligentes terá seu pedido analisado pela **CERTISIGN**. Testes técnicos serão realizados para identificar eventuais falhas de fabricação dos Dispositivos Criptográficos e/ou Leitoras de Cartão Inteligente.

7.2 Caso o SAC **CERTISIGN** constate defeito de fabricação nos Dispositivos Criptográficos e/ou Leitoras de Cartões Inteligentes que requeira sua substituição, a **CERTISIGN**:

- **7.2.1** Substituirá o Dispositivo Criptográfico e/ou Leitora de Cartão Inteligente, sem custo adicional para o cliente; e/ou;
- **7.2.2** Emitirá novo Certificado Digital, sem custo adicional para o cliente, caso o Certificado Digital apresente problema na emissão e/ou defeito de fabricação nos Dispositivos Criptográficos que resulte na perda do Certificado Digital.

8. ESTA GARANTIA NÃO COBRE:

8.1 Dispositivos Criptográficos e Certificados Digitais bloqueados ou inutilizados por **perda de SENHA ou utilização de SENHA incorreta**.

8.2 AS SENHAS (PIN, PUK OU PASSWORD) PARA ACESSO A ESSES DISPOSITIVOS SÃO PESSOAIS E INTRANSFERÍVEIS, SENDO DE CONHECIMENTO E RESPONSABILIDADE APENAS DO TITULAR OU RESPONSÁVEL DO CERTIFICADO DIGITAL. A CERTISIGN NÃO MANTÉM CÓPIAS NEM POSSUI MEIOS DE RECUPERÁ-LAS. CASO O DISPOSITIVO CRIPTOGRÁFICO SEJA BLOQUEADO OU INUTILIZADO DEVIDO À PERDA DAS SENHAS, O CERTIFICADO DIGITAL SERÁ PERDIDO. A REPOSIÇÃO DESTES DISPOSITIVOS E DE SEU CERTIFICADO DIGITAL NÃO É COBERTA PELA POLÍTICA DE GARANTIA CERTISIGN.

8.3 Certificados Digitais, Dispositivos Criptográficos e Leitoras de Cartão Inteligente **não adquiridos na CERTISIGN**. A comprovação de aquisição deverá ser realizada mediante apresentação da nota fiscal emitida.

8.4 Certificados Digitais bloqueados ou inutilizados por defeito detectado em mídia não adquirida na **CERTISIGN**.

8.5 Inobservância pelo cliente de suas obrigações legais e contratuais.

8.6 Dispositivo Criptográfico e/ou Leitora de Cartão Inteligente danificado por motivos de força maior, uso indevido, mau uso, negligência, acidente, desgaste, manipulação indevida, aplicação errada ou outras causas não relacionadas aos defeitos.

8.7 Dispositivo Criptográfico e/ou Leitora de Cartão Inteligente reparado, modificado ou alterado por pessoa que não seja um representante da **CERTISIGN** que cause ou contribua para o surgimento de defeito ou dano.

8.8 Falhas no funcionamento do Dispositivo Criptográfico e/ou Leitora de Cartão Inteligente decorrentes de insuficiência, interrupções, problemas ou falta de fornecimento de energia elétrica ou alta tensão; existência de objetos em seu interior estranhos ao seu funcionamento e finalidade de uso;

8.9 Perda ou inutilização de certificado digital A1 na hipótese do computador ser formatado, danificado ou substituído.

8.10 EM HIPÓTESE ALGUMA, A CERTISIGN SERÁ RESPONSABILIZADA EM VALOR SUPERIOR AO PREÇO DA COMPRA DO PRODUTO, POR QUALQUER PREJUÍZO COMERCIAL, PERDA DE LUCROS OU ECONOMIAS, POR OUTROS DANOS DIRETOS OU INDIRETOS, DECORRENTES DO USO OU IMPOSSIBILIDADE DE USO DO PRODUTO.

9. DIREITO DE ARREPENDIMENTO

9.1 O direito de arrependimento poderá ser exercido pelo cliente de acordo com o art. 49 do Código de Defesa do Consumidor. Somente será admitido o exercício do direito de arrependimento dentro do prazo de reflexão (07 dias), mediante a revogação do Certificado Digital pelo próprio cliente e a devolução do Dispositivo Criptográfico, embalagem e o guia de instalação que são entregues juntamente com o Certificado Digital e desde que estejam em estado novo e perfeitas condições de uso (não esteja bloqueado e/ou inutilizado).

9.2 Nos casos cobertos por essa Política de Garantia, os quais o SAC **CERTISIGN** verifique que o cliente faça jus a receber o reembolso, as seguintes condições deverão ser observadas:

- **9.2.1** Pagamentos efetuados com boleto bancário: o reembolso será depositado em conta corrente da Pessoa Física ou Pessoa Jurídica informada nos dados de faturamento da Nota Fiscal, em até 15 (quinze) dias úteis após a **CERTISIGN** ter recebido a solicitação do cliente e os dados bancários para a devolução. A **CERTISIGN** não se compromete a cumprir o prazo estipulado, caso ocorra inconsistência dos dados bancários informados, pois, nesta hipótese, caberá ao cliente entrar novamente em contato com a **CERTISIGN** para a correção dos seus dados.
- **9.2.2** Pagamentos efetuados com cartão de crédito: a solicitação do estorno será realizada pela **CERTISIGN** à operadora do cartão de crédito em até 15 (quinze) dias úteis. Atenção: O prazo para que o estorno seja efetuado na fatura do cliente será estabelecido pela operadora do cartão de crédito. Ultrapassado o prazo estabelecido pela operadora para a solicitação do estorno, o reembolso será realizado em conta corrente da Pessoa Física ou Pessoa Jurídica informada nos dados de faturamento da Nota Fiscal.

Todas as regras constantes nesta política de garantia estão de acordo com Código de Defesa do Consumidor e legislação vigente.

Esta política de garantia foi atualizada e registrada no 5° Oficial de Registro de Títulos e Documentos da Comarca de São Paulo - SP, sob o microfilme n°. 1.435.027, protocolado e prenotado sob o n°. 1.437.331 e passa a valer a partir de 06/08/2014.

Atualizada em agosto/2014.