Política de Certificação

Assinatura Digital

Autoridade Certificadora e Autoridade de Registro SESI/BA

PC A2 DA AC SESI/BA
Versão 1.0 - 12 de Outubro de 2015

Política de Certificação para Assinatura Digital Tipo A2 – PRÓPRIO - da Autoridade Certificadora e Autoridade de Registro SESI/BA

Com o objetivo de implantar um processo e estrutura informatizada para digitalização, assinatura digital, armazenamento e recuperação de informações acadêmicas o SESI/BA implanta a solução Secretaria Acadêmica Digital – SeAD, uma metodologia criada para transposição de documentos, procedimentos e processos que se encontram em meio físico nas secretarias acadêmicas e de cursos para o meio digital.

Para a execução desta metodologia são necessárias alterações na gestão dos documentos, processos e procedimentos acadêmicos: o papel será substituído pelo documento eletrônico; a assinatura física será substituída por uma assinatura digital; e o arquivo físico de documentos será substituído por mídias digitais.

Para o processo de assinatura digital serão utilizados os certificados digitais disponibilizados pela Autoridade Certificadora e Autoridade de Registro do SESI/BA - AC SESI/BA, criadas para assegurar o cumprimento das regras estabelecidas neste documento.

Esta política de certificação digital estabelece os requisitos a serem obrigatoriamente observados pela AC SESI/BA na emissão dos certificados digitais. Estes requisitos obedecem às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo PRÓPRIO/INTERNO.

Este documento tem como objetivo estabelecer as regras e parâmetros para o uso da certificação digital dentro dos projetos desenvolvidos pelo SESI/DR/BA que necessitam de garantias de autenticidade, integridade e validade jurídica em meio digital.

1. Introdução

Esta "Política de Certificação" (PC) descreve as regras para emissão e uso de certificados de Assinatura Digital Tipo – PRÓPRIO - da Autoridade Certificadora Interna e Autoridade de Registro Própria SESI/BA, conforme previsto no § 2º, art. 10 da MP 2.200-2, de 24 de agosto de 2001.

A estrutura desenvolvida e implantada permite ao SESI/BA emitir certificados digitais aos seus funcionários, ficando os mesmos capacitados a utilizar a certificação digital para realizar operações seguras em meio eletrônico.

Os certificados digitais emitidos na estrutura criada pelo SESI/BA estão vinculados aos seus processos internos, sendo válidos exclusivamente para uso nos seus procedimentos, processos, documentos e serviços indicados por este.

2. Identificação

Esta PC refere-se exclusivamente à Autoridade Certificadora SESI/BA - AC SESI/BA e à Autoridade de Registro SESI/BA - AR SESI/BA no âmbito da Infraestrutura de Pares de Chaves da Instituição SESI/BA.

Esta PC descreve o uso relacionado ao Certificado de Assinatura Digital correspondente ao tipo PRÓPRIO – CERTIFICADOS NÃO ICP-BRASIL - em conformidade a MP 2.200-2, de 24 de agosto de 2001, em seu art. 10, § 2º.

Será utilizada a Autoridade Certificadora Raiz CONSAE que é responsável pela validação dos certificados da AC SESI/BAHIA que está a ela diretamente subordinada. A Autoridade Certificadora Raiz CONSAE – AC CONSAE foi desenvolvida e é mantida para uso das instituições que utilizam da metodologia desenvolvida para a Secretaria Acadêmica Digital – SeAD. O objetivo da AC CONSAE é tornar viável o uso dos Certificados Digitais nos procedimentos, processos e documentos acadêmicos.

Os certificados digitais a que se refere esta PC serão emitidos aos profissionais que desenvolvam atividades de digitalização de documentos.

3. Autoridade Certificadora e Autoridade de Registro SESI/BA

AR SESI/BA é responsável por conferir a documentação dos profissionais que solicitem certificados e fazer a liberação do processo de emissão destes certificados. A Autoridade Certificadora SESI/BA será responsável por emitir, renovar ou revogar certificados digitais liberados pelo AR SESI/BA.

As pessoas identificadas pelo SESI/DR/BA no item anterior ficarão também responsáveis por recolher o Termo de Titularidade (Anexo II) do solicitante, fazendo a liberação do respectivo certificado digital.

4. Práticas e Procedimentos de Emissão dos Certificados Digitais

As práticas e os procedimentos de certificação da AC SESI/BA e da AR SESI/BA estão descritos neste documento.

A emissão dos certificados digitais se dará através do portal da CONSAE - www.dcda.com.br no qual o solicitante deverá ser cadastrado.

Após cadastramento, o solicitante, deverá requisitar o certificado digital, emitir o Termo de Titularidade, entregar este documento devidamente assinado à equipe da Autoridade Certificadora SESI/BA descrita no item 3 dessa PC. Os fluxos utilizados no processo estão detalhados no Anexo I.

5. Titulares de Certificado

Pessoas físicas que desenvolvam atividades de digitalização de documentos poderão ser titulares de certificados digitais emitidos dentro da cadeia de acreditação criada exclusivamente para o projeto do SESI/BA.

6. Aplicabilidade

O certificado digital emitido pela AC SESI/BA poderá ser utilizado para documentos nos quais seja necessária a aplicação de assinatura em meio digital, atribuindo aos mesmos a garantia de autenticidade, integridade e validade jurídica, conforme § 2º do art. 10 da MP 2.200-2, de 24 de agosto de 2001.

A AC SESI/BA leva em conta o nível de segurança previsto para o certificado definido por esta PC no uso das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos com observância de aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular do certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

Os certificados emitidos pela AC SESI/BA podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações e assinatura de documentos digitalizados pela instituição, em conformidade com a Portaria SENESu nº 255, de 12 de dezembro de 1990, Portaria nº 1.224, de 18 de dezembro de 2013 e Despacho nº 97, de 16 de maio de 2014.

O "Termo de Titularidade" (Anexo II), disponibilizado pela AC SESI/BA que recebe e valida o pedido de emissão de certificado poderá limitar as aplicações para as quais são adequados os certificados de assinatura – tipo A2 emitidos pela AC SESI/BA, determinando restrições ou proibições de uso destes certificados.

7. Geração do Certificado Digital

O Certificado Digital, com os pares de chaves criptográficas é gerado sempre pelo próprio titular, solicitante, seguindo os passos descritos no Anexo I.

A geração do Certificado Digital, com os pares de chaves criptográficas, ocorre em ambiente seguro, monitorado, sendo a chave privada armazenada apenas pelo próprio titular.

A chave privada é de exclusivo controle, uso e conhecimento do próprio titular, conforme Parágrafo Único do art. 6º da MP 2.200-2, de 24 de agosto de 2001.

O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está de acordo com os Padrões e Algoritmos Criptográficos Internacionais – SRA, associado à função de criptografia hash.

O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC SESI/BA é de, no mínimo, 2048 bits.

Os parâmetros de geração de chaves assimétricas dos titulares de certificados seguirão padrões internacionais, visando sempre a maior segurança no processo.

8. Armazenamento do Certificado Digital

O meio de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) a chave privada utilizada na geração de uma assinatura deverá conter segurança razoável, não podendo ser deduzida, sendo armazenada de maneira a protege-la de terceiros de má-fé; e

c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros, tendo em vista que temos um duplo fator de segurança: posse da chave privada e senha de utilização da chave.

O meio de armazenamento não poderá modificar os dados a serem assinados, nem impedir que estes dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado emitido pela AC SESI/BA e descrito nesta PC é o PRÓPRIO/INTERNO.

A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada armazenada na mídia externa ou no computador é do titular do certificado, conforme especificado no Termo de Titularidade emitido no ato da requisição.

Não é permitida a recuperação de chaves privadas de assinatura.

Em nenhuma hipótese será permitida a cópia de segurança de chave privada, mesmo que realizada com o consentimento do respectivo titular de certificado.

É vedada à AC SESI/BA a possibilidade de manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

A AC SESI/BA não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados, mesmo que solicitado pelo próprio titular.

A ativação da chave privada do titular do certificado se dará por senha criada pelo próprio titular.

As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC SESI/BA são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para a verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

O período máximo de validade admitido para certificados de Assinatura Digital Tipo A2 da AC SESI/BA é de 1 (um) ano.

A senha de ativação da chave privada do titular do certificado protegerá contra uso não autorizado.

O titular do certificado é responsável pela segurança da mídia externa ou do computador escolhidos para armazenamento da chave privada e deve zelar por sua integridade.

A mídia externa onde poderão ser armazenados os pares de chaves criptográficas do titular do Certificado deve permanecer sobre sua guarda.

9. Quebra de Sigilo e Revogação do Certificado Digital

Caso o titular do certificado digital acredite que a sua chave privada ou senha de ativação da mesma não esteja mais seguro ou restrito ao seu uso, deverá comunicar imediatamente à Autoridade Certificadora SESI/BA para que o respectivo certificado digital seja revogado.

Tendo o certificado digital revogado, o profissional deverá requisitar novo certificado, efetuando novamente todos os passos para criação do mesmo.

10. Após o Vencimento do Certificado Digital

Após o vencimento do certificado digital, aqui previsto como válido por 1 (um) ano, o profissional deverá fazer a geração de um novo certificado digital.

11. Alterações na PC

Sempre que houver necessidade de realização de revisões desta PC, as contribuições serão encaminhadas para as Gerencias de Educação e Qualidade de Vida do SESI/BA, com posterior aprovação da Assessoria de TI do SESI/BA.

12. Políticas de Publicação e Notificação

A AC SESI/BA mantém em sua página a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web "http://sesi.fieb.org.br/sesi/Institucional/Transparencia/".

ANEXO I – EMITINDO O CERTIFICADO DIGITAL EM OITO PASSOS

PRIMEIRO PASSO

SEGUNDO PASSO

TERCEIRO PASSO

QUARTO PASSO

QUINTO PASSO

SEXTO PASSO

SÉTIMO PASSO

OITAVO PASSO

ANEXO II – TERMO DE TITULARIDADE

TERMO DE TITULARIDADE E RESPONSABILIDADE

Autoridade de Registro SESI/BA
Certificado Digital de Assinatura

Nome:[pessoa.nome]
RG: _____**CPF:** [pessoa.cpf]
E-mail: [pessoa.email]

Declaro ter solicitado uma **Certificação Digital de Assinatura junto à AR SESI/BA**, e que li, aceito e concordo com todas as condições e obrigações estipuladas neste documento e ainda, que assumo a responsabilidade exclusiva:

- pela guarda e sigilo da senha de acesso ao certificado digital;
- por todos os atos praticados utilizando o meu certificado digital e a sua chave privada correspondente;
- pela obrigatoriedade de utilizar senha forte (letras e números) para garantir a confiabilidade da minha chave privada do certificado digital;
- por armazenar a chave, preferencialmente, em um dispositivo de segurança próprio, restrito ao token ou smartcard;
- e por solicitar a revogação, em até 24 (vinte e quatro) horas, no caso de perda, extravio, comprometimento da chave privada ou suspeita de quebra de sigilo da senha.

Eu, assinante deste termo, estou ciente quanto à utilização deste certificado digital e declaro também conhecer e concordar com as cláusulas e condições contidas na **Política de Certificados (PC) e uso da certificação digital no âmbito interno das Unidades que compõem a AR SESI/BA,** documento este enviado por correio eletrônico e publicados no diretório público da rede da Instituição, denominado “intranet”, aceitando como válidas as declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de certificação disponibilizado pela Autoridade Certificadora - AC RAIZ CONSAE.
Declaro ainda que as informações na forma eletrônica, editadas com o uso desse certificado digital, presumem-se verdadeiras em relação ao signatário, tudo em conformidade com a legislação vigente.

Assumo total e exclusiva responsabilidade pela veracidade dos dados informados.
Assino o presente termo na presença de dois membros da Autoridade Certificadora de Registro da SESI/BA.

Nome:_____Assinatura:_____
MEMBRO DA COMISSAO DE CERTIFICAÇAO DA AR SESI/BA/Posto de Registro Vinculado

Nome:_____Assinatura:_____
GERENTE DE UNIDADE DE NEGÓCIO SESI/BA

Titular: _____
(nome por extenso)

ANEXO III - Definições e Acrônimos

PC	Documento pelo qual se institui as práticas no campo da certificação digital dentro de uma organização.
AC	Autoridade Certificadora: refere-se à estrutura capaz de emitir e gerenciar certificados digitais vinculando os mesmos aos seus respectivos titulares.
AR	Autoridade de Registro: estrutura capaz de agenciar a emissão dos certificados digitais, fazendo a validação da identidade física dos titulares de certificados. s
Certificado Digital	Arquivo digital que identifica usuário/autor de um documento ou transação eletrônica, garantindo a autenticidade, a integridade e a validade jurídica do documento ou transação eletrônica.
Certificado Digital TIPO A2 - PRÓPRIO	Certificado digital de uso interno a projetos do SESI/BA emitidos conforme §2º do art. 10 da MP 2.200-2 de 24 de agosto de 2001.
Pares de Chaves Criptográficas	O certificado digital se dá pela associação de pares de chaves criptográficas a um respectivo titular. Os pares de chaves são criados em um sistema pelo próprio titular que levará consigo a sua chave privada de assinatura.
Chave Privada de Assinatura	Ferramenta capaz de associar a um documento uma chave pública de assinatura.
Chave Pública de Assinatura	Ferramenta capaz de identificar a pessoa, o titular daquele certificado digital.
Criptografia	Forma de cifrar um texto ou arquivo com código conhecido apenas pelo destinatário do texto ou arquivo.
Função de Criptografia HASH	Ferramenta utilizada para garantir a autenticidade e integridade do documento. Todo documento possui um único código hash, que seria como o nosso “DNA”. A certificação digital faz uso desse “DNA” para garantir que nenhuma parte do documento foi alterada após a aplicação da assinatura.
SRA	Algoritmo de criptografia de dados criado por professores do MIT – Instituto de Tecnologia de Massashusetts, utilizado internacionalmente.