PORTARIA Nº 01, DE 17 DE MARÇO DE 2016.

Dispõe sobre a padronização nacional da Carteira de Identificação Estudantil - CIE

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, autarquia federal vinculada à Casa Civil da Presidência da República, em cumprimento à Lei Federal nº 12.933, de 26 de dezembro de 2013, e ao Decreto nº 8.537, de 05 de outubro de 2015, que tratam, entre outros, do benefício da meia-entrada em espetáculos artístico-culturais e esportivos;

CONSIDERANDO que a lei estabelece o direito à meia-entrada mediante a apresentação da Carteira de Identificação Estudantil (CIE), emitida conforme modelo único padronizado e publicamente disponibilizado;

CONSIDERANDO a liminar proferida nos autos da Ação Direta de Inconstitucionalidade (ADI) nº 5108-DF, no sentido de excluir a Associação Nacional de Pós-Graduandos (ANPG), a União Nacional dos Estudantes (UNE) bem como a União Brasileira dos Estudantes Secundaristas (Ubes) da participação na padronização do referido modelo;

CONSIDERANDO, portanto, que restou unicamente ao ITI a fixação e disponibilização do padrão nacional da CIE,

RESOLVE:

Art. 1º Fica instituído o modelo único nacionalmente padronizado da Carteira de Identificação Estudantil (CIE).

Parágrafo único. As especificações estão dispostas no documento em anexo “Padronização da Carteira de Identificação Estudantil (CIE) – Versão 1.0”, que se encontra disponibilizado no seguinte endereço eletrônico: www.iti.gov.br.

Art. 2º O ITI não possui competência legal para emitir ou fiscalizar a emissão da CIE.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI
Diretor-Presidente
Instituto Nacional de Tecnologia da Informação

Infraestrutura de Chaves Públicas Brasileira

Anexo I

Padronização da
Carteira de Identificação Estudantil (CIE)
(Art. 1.º, § 2º da Lei nº 12.933, de 26/12/2013)

Versão 1.0

17 de março de 2016

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
Portaria Nº 01, de 17.03.2016.		Criação do documento.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridade de Registro
A3/A4	Certificado Digital de Assinatura (tipo 3 ou tipo 4)
CIE	Carteira de Identificação Estudantil
DOC-ICP-16	Documento de Padronização do Certificado de Atributo da ICP-Brasil
CA	Certificado de Atributo
EEA	Entidade Emissora de Atributos
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
LCAR	Lista de Certificados de Atributos Revogados

1. INTRODUÇÃO

Em cumprimento à Lei Federal nº 12.933, de 26 de dezembro de 2013, e ao Decreto nº 8.537, de 05 de outubro de 2015, que tratam, entre outros, do benefício da meia-entrada em espetáculos artístico-culturais e esportivos, o referido direito deve ser exercido mediante a apresentação da Carteira de Identificação Estudantil (CIE) emitida conforme modelo único padronizado e publicamente disponibilizado por esta Autarquia, nos termos da liminar proferida nos autos da Ação Direta de Inconstitucionalidade – ADI nº 5108/DF.

1.1. Objetivo

Este documento visa apresentar as especificações, características técnicas e gráficas da Carteira de Identificação Estudantil (CIE) conforme estabelecido em lei.

1.2. Tecnologia

A CIE é uma carteira de identificação em suporte físico, no formato de um cartão, e com o respectivo equivalente digital no formato de Certificado de Atributo com base na certificação digital padrão ICP-Brasil.

A tecnologia utilizada para suportar o uso da certificação digital conforme estabelecido na legislação é o Certificado de Atributo, que viabiliza de forma segura a implementação da CIE no formato digital.

O Certificado de Atributo é uma das tecnologias disponíveis a partir do sistema de Certificação Digital padrão ICP-Brasil, padronizado no DOC-ICP-16 e DOCI-ICP-16.01.

2. Especificações da Carteira de Identificação Estudantil

2.1. Modelo da CIE

O cartão para a CIE deve seguir o modelo conforme apresentado na figura 1.

Figura 1 – Modelo da Carteira de Identificação Estudantil (CIE) – frente e verso

2.1.1. Conteúdo do cartão da CIE

No anverso (ou seja, na frente) do cartão devem constar os seguintes dados:

a) Nome;
b) Nome social (opcional);
c) Instituição de Ensino (nome da instituição; grau de escolaridade; nome do curso – nos casos de técnico, graduação e pós-graduação);
d) Data de Nascimento;
e) Matrícula na Instituição de Ensino.
f) Documento de Identidade (opcional);
g) CPF (opcional);
h) Código de Uso (opcional) - sequência alfanumérica personalizada para cada estudante conforme regras da entidade emissora da CIE;
i) QR-Code;
j) Marca da entidade emissora da CIE (opcional);
k) Ano corrente;

No verso do cartão devem constar as seguintes informações:

a) Número do serviço de atendimento ao estudante da entidade emissora;
b) Características locais/regionais (opcional);
c) Marca do Certificado de Atributo conforme manual da marca disponível;
d) Tarja Magnética (opcional);
e) Texto contendo: "*Documento padronizado nacionalmente conforme a Lei nº 12.933/2013. Válido em todo território nacional até 31 de março do ano seguinte*".

2.1.2. Layout do cartão da CIE

A descrição dos elementos gráficos que compõem a CIE é apresentada na figura 2.

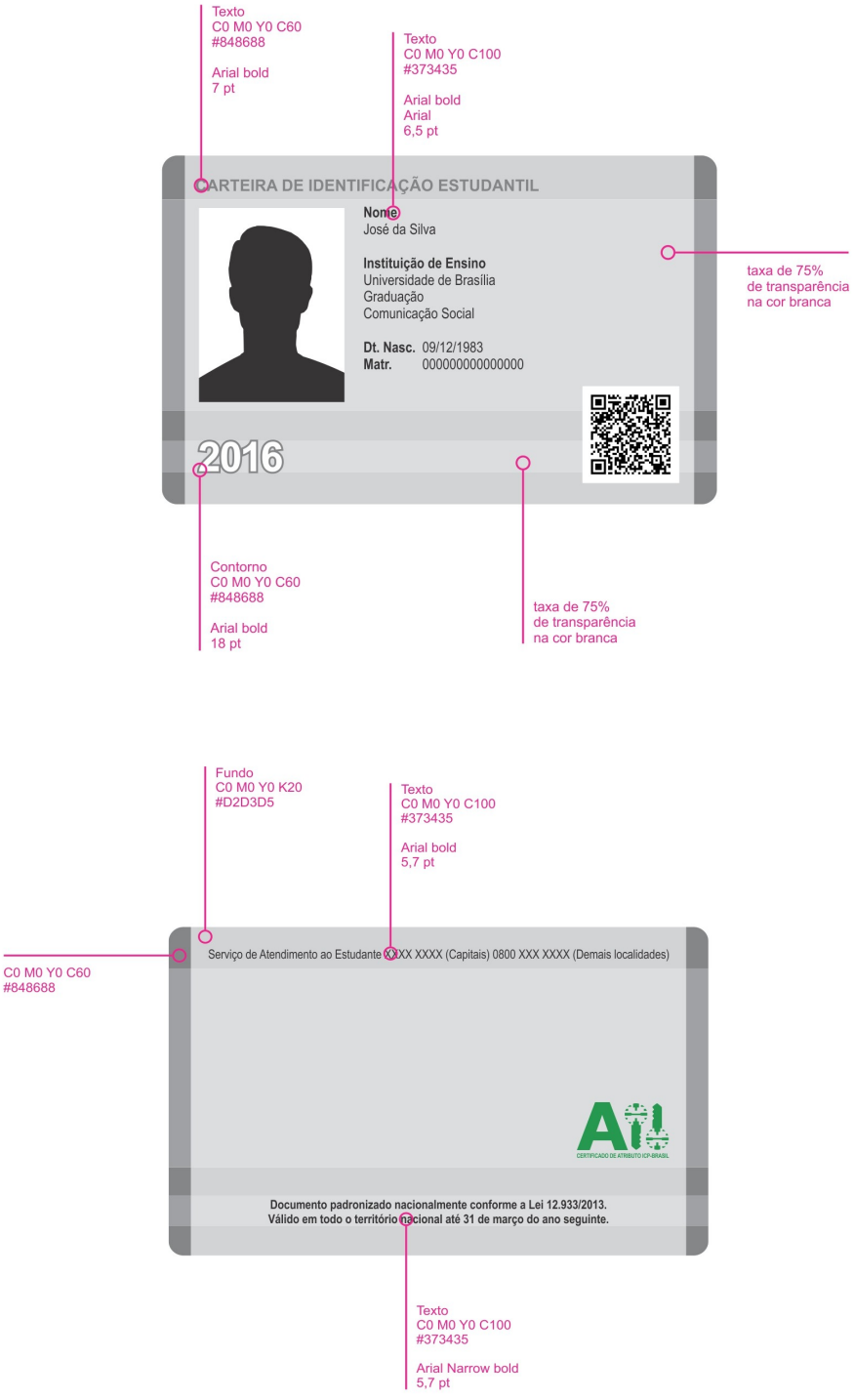

Figura 2 – Descrição gráfica da CIE

2.2. Requisitos físicos do cartão

2.2.1 Formato

a) Largura: 85,6 ± 0,12 mm;
b) Altura: 53,98 ± 0,05 mm;
c) Espessura: 0,76 ± 0,08 mm;
d) Bordas arrendondadas raio: 3,18 ± 0,30 mm.

2.2.2 Material de confecção

a) PVC (em todas as camadas)
b) PET (em todas as camadas; opcional)
c) Laminação brilhante (opcional)

As características de resistência mecânica, química, entre outros, devem estar de acordo com a norma ISO/IEC 7816.

A CIE, para atender as normas estaduais ou municipais, pode conter tarja magnética de alta coercitividade de forma opcional.

2.2.3 Elementos gráficos de segurança

O único elemento obrigatório de segurança gráfica do cartão é a fotografia da face do portador titular dos dados integrada/impressa na CIE, conforme ilustrado na figura 3.

Opcionalmente, poderão ser empregados outros elementos de segurança gráfica a critério da entidade emissora da CIE, observadas as áreas destinadas às informações opcionais, conforme ilustrado também na figura 3. Os elementos de segurança contidos deverão respeitar as normas estaduais e municipais em relação ao uso da CIE.

Figura 3 – Elementos de segurança gráfica da CIE

2.3. Requisitos digitais da CIE

A CIE deverá ter um certificado de atributo padrão ICP-Brasil, emitido e assinado digitalmente pela entidade emissora, e necessariamente armazenado em banco de dados, disponibilizado para consulta “on-line” a partir de “QR-Code” personalizado.

Opcionalmente, o certificado de atributo poderá ser também armazenado no cartão com chip ou em aplicativo de dispositivo móvel (APP).

2.3.1 Especificação do Certificado de Atributo da CIE

O formato digital da CIE será implementado por meio do uso de certificado de atributo (DOC-ICP-16), do tipo autônomo, conforme estabelecido pela ICP-Brasil.

Conforme estabelecido nos documentos DOC-ICP-16 e DOC-ICP-16.01, o perfil do certificado de atributo deverá implementar os campos apresentados na Tabela I.

Seq.	Campo	
1	Versão	version v2(1)
2	Titular do Certificado de Atributo	holder
3	Emissor	issuer
4	Algoritmo de Assinatura	signature
5	Número de Série	serialNumber
6	Período de Validade	attCertValidityPeriod
7	Atributos	attributes
8	Extensões	extensions
9	Assinatura Digital	SignatureValue

Tabela I – Conteúdo do certificado de atributo

2.3.1.1. Versão

Deve ser adotada a versão v2, representada pelo valor inteiro (1).

2.3.1.2. Titular do Certificado de Atributo

O nome do titular do certificado de atributo, pessoa física, constante no campo *Holder*, deverá adotar o *Distinguished Name* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = nome fantasia ou sigla da Entidade Emissora de Atributo (EEA)

CN = nome do titular do atributo

Na composição dos nomes, aplicam-se as restrições de nome conforme definido no item 2.3.1.2.1 deste documento.

2.3.1.2.1. Restrição de nomes

Na composição de nomes, aplicam-se as seguintes restrições:

a) Não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) Além dos caracteres alfanuméricos, poderão ser utilizados somente os caracteres especiais apresentados na Tabela II.

Caractere	*Código NBR9611 (hexadecimal)*
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29

Caractere	*Código NBR9611 (hexadecimal)*
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

Tabela II - Caracteres especiais admitidos na descrição de nomes

2.3.1.3. Emissor do Certificado de Atributo

O nome da entidade emissora do certificado de atributo, pessoa jurídica, constante no campo *Issuer*, deverá adotar o *Distinguished Name* (DN) do padrão ITU X.500/ISO 9594, no mesmo formato de codificação e conteúdo do campo *Subject* do certificado da signatária do certificado de atributo (EEA).

2.3.1.4. Algoritmo de Assinatura

Contém o identificador do algoritmo utilizado para validar a assinatura do certificado de atributo. Este algoritmo deve ser um dos algoritmos de assinatura de certificados de usuário final definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC-ICP-01.01).

2.3.1.5. Número de Série

Este campo deve possuir o par *issuer/serialNumber* ÚNICO. O campo *serialNumber* deve ser um número inteiro e positivo sequencial com um limite máximo de até 20 octetos.

2.3.1.6. Período de Vigência

O campo período de vigência deve possuir o formato *GeneralizedTime*, padrão ASN.1 e expresso em UTC (*Universal Time Coordinated*) AAAAMMDDHHMMSSZ.

2.3.1.7. Atributos

Este campo deve conter a informação de estudante concedida ao titular do certificado de atributo com uso do tipo:

```
Attribute ::= SEQUENCE {
        type      AttributeType,
        values    SET OF AttributeValue
          -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

São definidos como obrigatórios os seguintes componentes para o atributo estudante previsto na Lei n° 12.933-2013, nesta ordem:

a) **OID = 2.16.76.1.10.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 15 (quinze) posições subsequentes, o número da matrícula do estudante; nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular do atributo; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

b) **OID = 2.16.76.1.10.2 e conteúdo** = nas primeiras 40 (quarenta) posições, o nome da instituição de ensino; nas 15 (quinze) posições subsequentes, o grau de escolaridade; nas 30 (trinta) posições subsequentes, o nome do curso, nas 20 (vinte) posições subsequentes, o município da instituição e nas 2 (duas) posições subsequentes, a UF do município.

Os componentes para os atributos devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo atributo deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

b) Quando os números de CPF e RG não estiverem disponíveis, os campos

correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF;

d) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado o tamanho máximo disponível para o campo;

e) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF da instituição de ensino;

f) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 2.3.1.2.1 deste documento, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.

g) Quando o tamanho do campo de cada elemento do conteúdo não for suficiente para o preenchimento completo da informação correspondente, deve-se promover a truncagem ou abreviatura dessa informação.

2.3.1.8. Extensões

Este campo deve conter as informações adicionais de associação entre os titulares dos Certificados de Atributo e seus atributos. As extensões definidas pela RFC 5755 são:

- Audit Identity
- AC Targeting
- Authority Key Identifier
- Authority Information Access
- CRL Distribution Points
- No Revocation Available

São obrigatórias as seguintes extensões:

a) ***"Authority Key Identifier"*, não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública do certificado digital da EEA;
b) ***"Authority Information Access"*, não crítica:** A primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação;
c) ***"CRL Distribution Points"*, não crítica**: o campo deve conter o endereço na *Web* onde se obtém a LCAR correspondente ao certificado de atributo.

2.3.1.8.1. Perfil de LCAR para certificados de atributo

2.3.1.8.1.1. Número(s) de versão

As LCARs geradas pela EEA responsável deverão implementar a versão 2 do padrão ITU X.509, de acordo com o perfil de LCR estabelecido na RFC 5280.

2.3.1.8.1.2. Extensões de LCAR para certificados de atributo e de suas entradas

São obrigatórias as seguintes extensões de LCAR:

a) "***Authority Key Identifier***": deve conter o *hash* SHA-1 da chave pública da EEA que assina a LCAR; e
b) "***CRL Number***", **não crítica**: deve conter um número sequencial para cada LCAR emitida pela EEA.

A frequência máxima admitida para a emissão de LCAR para os certificados de atributo é de 6 (seis) meses.

2.3.2 Especificação do Banco de Dados

Os certificados de atributos gerados deverão estar disponíveis em banco de dados para validação de autenticidade. Cada entidade emissora de CIE será a responsável pelo conteúdo e manutenção do seu respectivo banco de dados, e o apontamento para o acesso ao certificado de atributo deverá ser representado por QR-Code já especificado para o uso no cartão.

O QR-Code é um código de barra bidimensional que possibilita conversão para texto, números, endereços web, dados de contatos entre outros.

O padrão de QR-Code estabelecido para uso na CIE é o padrão QR-Code 2005 cuja especificação simbológica é dada pela ISO/IEC 18004:2006.

A especificação simbológica do QR-Code deverá remeter ao endereço de internet (endereço *web*) que proverá acesso ao banco de dados para possibilitar a obtenção do certificado de atributo associado a CIE emitida.
O QR-CODE deve representar a URL da Entidade Emissora de Atributo (EEA) acrescido de uma chave de acesso única e personalizada para cada estudante de modo a não permitir de forma direta a identificação dos dados deste mesmo estudante.

2.4. Requisitos eletrônicos do cartão (opcional)

2.4.1 Chip do cartão (opcional)

2.4.1.1 Com contato

Todas as especificações/arquiteturas do chip com contato devem possuir características eletromagnéticas, químicas, físicas, mecânicas, de ordenamento lógico, entre outros de acordo com as recomendações ISO/IEC 7816, 10373 e 19784.

2.4.1.2 Sem contato

Todas as especificações/arquiteturas do chip sem contato devem possuir características eletromagnéticas, químicas, físicas, mecânicas, de ordenamento lógico, entre outros de acordo com as recomendações ISO/IEC 14443.

2.4.2 Cartão MIFARE (opcional)

A Carteira de Identificação Estudantil pode ser um cartão do tipo MIFARE. Os dados contidos devem respeitar as normas estaduais e municipais em relação ao uso e serviço que a CIE se prestará.

3. Requisitos para o processo de emissão da CIE

O processo de cadastro, emissão, cobrança, conferência e guarda dos dados e entrega da CIE ao estudante é de total responsabilidade da entidade emissora, respeitando-se os padrões estabelecidos e o previsto na Lei nº 12.933/13 e no Decreto nº 8537/15.

4. Requisitos gerais

4.1. Banco de dados

As entidades emissoras da CIE deverão manter e disponibilizar ao Poder Público, estabelecimentos, produtoras e promotoras de eventos banco de dados com acesso “on-line” contendo todos os certificados de atributos dos estudantes, acessível via código personalizado para cada estudante.

Nesse banco de dados deverão ser armazenadas e disponibilizadas para consulta todas as informações especificadas neste regulamento no formato de certificado de atributo. O acesso ao banco de dados via internet deve ser via protocolo “https” com certificado SSL emitido no âmbito da ICP-Brasil para a entidade emissora da CIE.

Os dados armazenados no banco são privados e serão usados exclusivamente para atestar a autenticidade da CIE via código de acesso único e individualizado para cada estudante.

4.2. Certificação digital

Toda CIE emitida possuirá um Certificado de Atributo devidamente assinado e armazenado em banco de dados administrado pela entidade emissora.

O certificado de atributo da CIE deverá ser assinado com o certificado digital de pessoa jurídica padrão ICP-Brasil da entidade emissora da CIE.

O certificado digital da entidade emissora, denominado de Entidade Emissora de Atributo (EEA) da CIE deve ser do tipo A3 ou A4 conforme padrões da ICP-Brasil. Este certificado deverá ser usado para a emissão de certificados de atributos e também assinatura da Lista de Certificados de Atributos Revogados (LCAR).

O certificado de atributo da CIE deve ser do tipo autônomo e estar disponível para consulta individualizada a partir de uma chave de acesso única e personalizada que está inserida no próprio QR-Code juntamente com a URL da entidade emissora da CIE.

A autenticidade da CIE deverá ser verificada a partir de QR-Code, que apontará para o respectivo certificado de atributo válido armazenado no banco de dados. A validação do certificado de atributo deve ser feita por aplicação local genérica capaz de ler um certificado de atributo e identificar as informações existentes em conformidade com os mesmos dados apresentados no cartão da CIE.

4.3. Validação e verificação da CIE

A verificação da CIE é feita por meio digital, atestando-se a autenticidade do documento apresentado pelo estudante com o certificado de atributo emitido.