

INSTRUÇÃO NORMATIVA ITI N° 22, DE 23 DE MARÇO DE 2022

Aprova a versão revisada e consolidada do documento Padrões e Algoritmos Criptográficos da ICP-Brasil – DOC-ICP-01.01.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, pelo art. 1º da [Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004](#), e pelo art. 2º da [Resolução nº 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020](#),

CONSIDERANDO a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

RESOLVE:

Art. 1º Esta Instrução Normativa aprova a versão revisada e consolidada do documento Padrões e Algoritmos Criptográficos da ICP-Brasil – DOC-ICP-01.01.

Art. 2º Fica aprovada a versão 5.0 do documento DOC-ICP-01.01 – Padrões e Algoritmos Criptográficos da ICP-Brasil.

Art. 3º Ficam revogadas:

- I - a [Instrução Normativa nº 03, de 22 de outubro de 2008](#);
- II - a [Instrução Normativa nº 01, de 04 de junho de 2014](#);
- III - a [Instrução Normativa nº 03, de 10 de julho de 2014](#);
- IV - a [Instrução Normativa nº 03, de 25 de agosto de 2015](#);
- V - a [Instrução Normativa nº 01, de 31 de março de 2016](#);
- VI - a [Instrução Normativa nº 14, de 09 de novembro de 2018](#);
- VII - a [Instrução Normativa nº 15, de 26 de novembro de 2018](#); e
- VIII - a [Instrução Normativa nº 08, de 31 de outubro de 2019](#).

Art. 4º Esta Instrução Normativa entra em vigor em 1º de abril de 2022.

CARLOS ROBERTO FORTNER



Infraestrutura de Chaves Públicas Brasileira

ANEXO

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL

DOC ICP-01.01

Versão 5.0

23 de março de 2022



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

| | |
|------------------------------------------------------------------|----|
| CONTROLE DE ALTERAÇÕES | 3 |
| LISTA DE SIGLAS E ACRÔNIMOS..... | 5 |
| 1 INTRODUÇÃO | 7 |
| 2 APLICABILIDADE DOS ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS..... | 7 |
| 3 PADRÕES DE HARDWARE | 13 |
| 4 DOCUMENTOS REFERENCIADOS | 15 |



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

| Ato que aprovou a alteração | Item alterado | Descrição da alteração |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IN ITI nº 22, de 23.03.2022 Versão 5.0 | | Revisão e consolidação conforme o Decreto nº 10.139, de 28 de novembro de 2019. |
| IN nº 08, de 31.10.2019. Versão 4.2 | Item 2 (tabelas) | Retira dos Algoritmos e Suítes de Assinatura a função hash SHA-1 e os algoritmos criptográficos RSA 1024 bits para certificados de usuário final e RSA 2048 bits para certificados de AC. |
| IN nº 15, de 26.11.2018. Versão 4.1 | Item 2 (tabelas) | Atualização dos Algoritmos e das Suítes de Assinatura e define parâmetros para a curva E521. |
| IN nº 14, de 09.11. 2018. Versão 4.0 | Item 2 (tabelas) | Regulamenta novas curvas elípticas e algoritmos de resumo (hash). |
| Resolução nº 123, de 06.07.2017 Versão 3.2 | Item 3 (tabela) | Atualiza tabela com padrões mínimos a serem empregados nos hardwares criptográficos. |
| IN nº 01, de 31.03.2016. Versão 3.1 | Tabela - Geração de Chaves Simétricas de AC. | Gerenciamento de IDN - PSBio. |
| Resolução nº 115, de 11.11.2015. Versão 3.0 | Tabela - Geração de Chaves Assimétricas de Usuário Final | Criação de Política de Certificado A CF - e - SAT. |
| IN nº 03, de 25.08.2015 Versão 2.6 | Item 2, tabela Padrões de Assinatura ICP-Brasil. Item 2, tabela Geração de Chaves Assimétricas | Regulamentação PAdES. Ajuste no texto de algoritmos obrigatórios. |



Infraestrutura de Chaves Públicas Brasileira

| Ato que aprovou a alteração | Item alterado | Descrição da alteração |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IN nº 03, de 10.07.2014 Versão 2.5 | Acrescenta NOTA (1) às tabelas referentes a geração de chaves assimétricas, do item 2, do DOC-ICP-01.01, versão 2.4. | Esclarece a manutenção de SHA1 e tamanho de chaves RSA para preservar compatibilidade de certificados anteriores a 2012. |
| IN nº 01, de 04.06.2014 Versão 2.4 | Tabelas de Geração de Chaves Assimétricas de AC e de usuário final (pág. 4). | Substituição das Curvas Elípticas NIST pelo ECC <i>Brainpool</i> . |
| Resolução nº 89, de 05.07.2012 Versão 2.3 | Substitui s NOTA (4) e acrescenta-se a NOTA (5) ao item 3, do DOC-ICP-01.01, versão 2.2 | Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de certificação digital. |
| Resolução nº 85, de 09.11.2011 Versão 2.2 | Acrescenta as NOTAS (3) e (4) ao item 3, do DOC-ICP-01.01, versão 2.1 | Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de certificação digital. |
| IN nº 08, de 01.10.2010 Versão 2.1 | | Aprova e autoriza a disponibilização no sítio do ITI, os documentos DOC-ICP-01.01 em sua Versão 2.1; DOC-ICP-10.02 em sua Versão 3.0; DOC-ICP-10.07 em sua Versão 1.0. |
| Resolução nº 65, de 09.06.2009 Versão 2.0 | | Aprova a versão 2.0 do documento Padrões e Algoritmos Criptografados da ICP-BRASIL, e o plano de migração relacionado. |
| IN nº 3, de 22.10.2008 Versão 1.1 | | Altera o documento Padrões e Algoritmos Criptografados da ICP-BRASIL |
| IN nº 4, de 18.05.2006 Versão 1.0 | | Aprova a versão 1.0 do documento Padrões e Algoritmos Criptografados da ICP-BRASIL |



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

| SIGLA | DESCRIÇÃO |
|------------|----------------------------------------------------------|
| AC | Autoridade Certificadora |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| AR | Autoridade de Registro |
| CAAdES | <i>CMS Advanced Electronic Signature</i> |
| CBC | <i>Cipher Block Chaining</i> |
| CF-e | Cupom Fiscal Eletrônico |
| DOC-ICP | Documentos Principais da ICP-Brasil |
| ECC | <i>Elliptic Curve Cryptography</i> |
| ECDH | <i>Elliptic Curve Diffie-Hellman</i> |
| ECMQV | <i>Elliptic Curve Menezes-Qu-Vanstone</i> |
| GCM | <i>Galois/Counter Mode</i> |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IDN | Identificador de Registro Biométrico |
| INMETRO | Instituto Nacional de Metrologia, Qualidade e Tecnologia |
| LEA | Laboratórios de Ensaios e Auditoria |
| NIST | <i>National Institute of Standards and Technology</i> |
| NSH | Níveis de Segurança e Homologação |
| OCSP | <i>On-line Certificate Status Protocol</i> |
| PAdES | <i>PDF Advanced Electronic Signature</i> |
| PKCS | <i>Public Key Cryptography Standards</i> |
| PSS | Prestador de Serviço de Suporte |
| RFC | <i>Request For Comments</i> |



Infraestrutura de Chaves Públicas Brasileira

| | |
|-------|---------------------------------------------|
| RSA | <i>Rivest, Shamir and Adleman Algorithm</i> |
| SAT | Sistema de Autenticação e Transmissão |
| SHA | <i>Secure Hash Algorithm</i> |
| SHAKE | <i>Secure Hash Algorithm and Keccak</i> |
| XAdES | <i>XML Advanced Electronic Signature</i> |



Infraestrutura de Chaves Públicas Brasileira

1 INTRODUÇÃO

1.1 Este documento regulamenta os padrões de hardware, os algoritmos e parâmetros criptográficos a serem empregados em todos os processos realizados no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, que incluem, entre outros:

- a) geração de chaves criptográficas;
- b) solicitação, emissão e revogação de certificados digitais;
- c) geração e verificação de assinaturas digitais;
- d) cifração de mensagens;
- e) autenticação com certificados digitais.

1.2 As diretrizes aqui constantes devem ser obrigatoriamente observadas pelas Autoridades Certificadoras - ACs, Autoridades de Registro - ARs, Prestadores de Serviço de Suporte - PSSs, Empresas de Auditoria Independente, Laboratórios de Ensaio e Auditoria - LEAs e outras entidades credenciadas ou cadastradas na ICP-Brasil, bem como pelos titulares finais e desenvolvedores de aplicativos que utilizam certificados digitais da ICP-Brasil.

2 APLICABILIDADE DOS ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS

2.1 Este item relaciona os principais procedimentos que envolvem criptografia, no âmbito da ICP-Brasil, com os algoritmos e parâmetros que devem ser utilizados, obrigatoriamente, para sua execução e também com os documentos normativos que tratam desses procedimentos.

| Solicitação de Certificados à AC | |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-01 - item 4.2.1.2 DOC-ICP-01 - item 6.1.3.1 DOC-ICP-04 - item 6.1.3 DOC-ICP-05 - item 4.1.1.3 |
| Formato | Padrão PKCS#10 |

| Entrega de Certificados Emitidos pela AC | |
|-------------------------------------------------|-----------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-01 - item 4.3.1.7 DOC-ICP-01 - item 6.1.4.1 DOC-ICP-04 - item 6.1.4 |



Infraestrutura de Chaves Públicas Brasileira

| | |
|---------|-------------------------|
| | DOC-ICP-05 - item 6.1.4 |
| Formato | Padrão PKCS#7 |

Geração de Chaves Assimétricas de AC

| | |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-01 - item 6.1.1.3 DOC-ICP-04 - item 6.1.1.3 DOC-ICP-01 - item 6.1.5 DOC-ICP-05 - item 6.1.5 |
| Algoritmo | RSA ou ECC-Brainpool (conforme RFC 5639) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032). |
| Tamanho de chave | RSA 4096 ou brainpoolP512r1 ou Ed448 (448 bits) ou E-521 (521 bits). |

Geração de Chaves Assimétricas de Usuário Final

| | |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-04 - item 6.1.5.2 |
| Algoritmo | RSA ou ECC-Brainpool (conforme RFC 5639) ou Curve25519 (Conforme RFC 7748) ou Ed25519 (PureEdDSA e HashEdDSA, conforme RFC 8032) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032). |
| Tamanho de chave A1, A2, A3, A CF-e-SAT, S1, S2, S3, T3, OM-BR | RSA 2048 ou brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits) |
| Tamanho da chave A4, S4, T4 | RSA 2048 ou RSA 4096 ou brainpoolP512r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits) |



Infraestrutura de Chaves Públicas Brasileira

Assinatura de Certificados de AC

| | |
|----------------------|----------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-01 - item 7.1.3 DOC-ICP-05 - item 7.1.3 |
| Suíte de Assinatura | sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph |

Assinatura de Certificados de Usuário Final

| | |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-04 - item 7.1.3 |
| Suíte de Assinatura | sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph |

Assinatura de Listas de Certificados Revogados e Respostas OCSP

| | |
|-------------------------|-------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-01 - item 7.3 DOC-ICP-04 - item 7.3 DOC-ICP-05 - item 7.3 |
| Algoritmo de Assinatura | |



Infraestrutura de Chaves Públicas Brasileira

| | |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Guarda da Chave Privada da Entidade Titular e de seu Backup

| | |
|------------------------------|-------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-04 - item 6.1.1.4 DOC-ICP-04 - item 6.2.4.3 DOC-ICP-05 - item 6.2.4.4 |
| Algoritmo e Tamanho de chave | 3DES – 112 bits AES – 128 ou 256 bits |
| Modo de operação | CBC ou GCM |

Assinaturas Digitais ICP-Brasil

| | |
|----------------------|------------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-15, item 6.1 |
| Função resumo | SHA - 1 SHA - 256 SHA – 512 SHAKE - 256 |
| Suíte de Assinatura | sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption |



Infraestrutura de Chaves Públicas Brasileira

| | |
|--|------------------------------------------------------------------------|
| | id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph |
|--|------------------------------------------------------------------------|

Assinatura de Pedidos e Respostas de Carimbos do Tempo

| | |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normativo ICP-Brasil | DOC-ICP-12, item 7.2 |
| Função resumo | SHA - 1 SHA - 256 SHA - 512 SHAKE - 256 |
| Suíte de Assinatura | sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph |

Esquemas de Acordos de Chaves

| |
|---------------------|
| ECDH256 ou ECMQV256 |
| ECDH512 ou ECMQV512 |
| ECDHE X25519 |
| ECDHE X448 |
| RSA 2048 |



Infraestrutura de Chaves Públicas Brasileira

Esquemas de Acordos de Chaves

RSA 4096

Esquema de Envelopes Criptográficos

3desWithRSA2048Encryption

aes128WithRSA2048Encryption

aes256WithRSA4096Encryption

aes128WithECIES256Encryption

aes256WithECIES512Encryption

Geração de Chaves Simétricas para IDN

| | |
|------------------------------|--------------------------|
| Normativo ICP-Brasil | DOC-ICP-05-04 - item 1.1 |
| Algoritmo e Tamanho de chave | AES – 256 bits |
| Modo de operação | CBC |

Parâmetros para a curva E521

| Parâmetros | Valor |
|----------------------|-------------------------------------------------------------|
| p | p da E-521 (i.e., $2^{521} - 1$) |
| b | 528 |
| Codificação do GF(p) | 527-bit codificação little-endian de $\{0, 1, \dots, p-1\}$ |
| H(x) | SHAKE256(dom5(phflag,context) x, 132) |
| phflag | 0 |



Infraestrutura de Chaves Públicas Brasileira

| | |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| c | logaritmo base 2 do cofator da E-521 (i.e., 2) |
| n | 520 |
| d | d da E-521(i.e., -376014) |
| a | 1 |
| B | (X(P),Y(P)) da E-521 (i.e., (1571054894184995387535939749894317568645297350402905821437625181152304994381188529632591196067604100772673927915114267193389905003276673749012051148356041324, 12)) |
| L | ordem da E-521 (i.e., 1716199415032652428745475199770348304317358825035826352348615864796385795849413675475876651663657849636693659065234142604319282948702542317993421293670108523) |
| PH(x) | x (i.e., a função identidade) |

2.2 Ed521ph é o mesmo, mas com PH sendo SHA-3 (512 bits) ou SHAKE256(x, 64) e phflag sendo 1, i.e., é feito um *hash* antes da assinatura com Ed521, com a constante *hash* modificada.

2.3 dom5(x, y): na geração de chave, uma *string* vazia. Na assinatura e verificação, a *string* do octeto "SigEd521" || octet(x) || octet(OLEN(y)) || y, onde x está no range 0-255 e y é uma *string* de octeto com no máximo 255 octetos. "SigEd521" está em ASCII (8 octets).

3 PADRÕES DE HARDWARE

3.1 A tabela a seguir relaciona os padrões mínimos a serem empregados nos *hardwares* criptográficos com sua utilização na ICP-Brasil e com os documentos normativos que tratam dessa utilização.

| Utilização | Padrões Obrigatórios | Normativo |
|------------------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------|
| Módulo criptográfico de geração de chaves assimétricas de usuário final | Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-04 item 6.2.1 DOC-ICP-05 item 6.2.1.2 |
| Módulo criptográfico para armazenamento da chave privada de titular do certificado | Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-04 item 6.2.1.2 |



Infraestrutura de Chaves Públicas Brasileira

| Utilização | Padrões Obrigatórios | Normativo |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------|
| Parâmetros de geração de chaves assimétricas de usuário final | Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-04 item 6.1.6 |
| Módulo criptográfico de geração de chaves assimétricas de AC | Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-05 item 6.2.1.1 |
| Módulo criptográfico para armazenamento da chave privada de AC | Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-05 item 6.1.1.6 |
| Parâmetros de geração de chaves assimétricas de AC | Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-05 item 6.1.6.1 |
| Módulo criptográfico de geração de chaves Assimétricas da AC Raiz | Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-01 item 6.2.1 |
| Módulo criptográfico para armazenamento da chave privada da AC Raiz | Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-01 item 6.2.7 |
| Parâmetros de geração de chaves assimétricas da AC Raiz | Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-01 item 6.1.6.1 |
| Processo para verificação de parâmetros de geração de chaves assimétricas da AC Raiz | Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO | DOC-ICP-01 item 6.1.6.2 DOC-ICP-04 item 6.1.6 DOC-ICP-05 item 6.1.6.2 |



Infraestrutura de Chaves Públicas Brasileira

4 DOCUMENTOS REFERENCIADOS

4.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterado, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as resoluções que os aprovaram.

| REF. | NOME DO DOCUMENTO | CÓDIGO |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| [1] | DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 01, de 25 de setembro de 2001 | DOC-ICP-01 |
| [2] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001 | DOC-ICP-04 |
| [3] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL Aprovado pela Resolução nº 08, de 12 de dezembro de 2001 | DOC-ICP-05 |
| [4] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008 | DOC-ICP-12 |
| [5] | VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL Aprovado pela Resolução nº 62, de 09 de janeiro de 2009 | DOC-ICP-15 |

4.1 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as instruções normativas que os aprovaram.

| REF. | NOME DO DOCUMENTO | CÓDIGO |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| [6] | PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE SIMÉTRICA PARA GERAÇÃO DO IDN Aprovado pela Instrução Normativa nº 08, de 10 de dezembro de 2015 | DOC-ICP-05.04 |