Serviço Público Federal

MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA-**INMETRO**

PORTARIA Nº 130, DE 19 DE MARÇO DE 2021

Aprova os Requisitos de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil – Consolidado.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO, no exercício da competência que lhe foi outorgada pelos artigos 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, e 3º, incisos I e IV, da Lei nº 9.933, de 20 de dezembro de 1999, combinado com o disposto nos artigos 18, inciso V, do Anexo I ao Decreto nº 6.275, de 28 de novembro de 2007, e 105, inciso V, do Anexo à Portaria nº 2, de 4 de janeiro de 2017, do então Ministério da Indústria, Comércio Exterior e Serviços, considerando o que determina o Decreto nº 10.139, de 28 de novembro de 2019, e o que consta no Processo SEI nº 0052600.011827/2020-35, resolve:

Objeto e âmbito de aplicação

Art. 1º Ficam aprovados os Requisitos de Avaliação da Conformidade e as Especificações para o Selo de Identificação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil, fixados, respectivamente, nos Anexos I e II, disponíveis em http://www.inmetro.gov.br/legislacao/.

§ 1º A avaliação da conformidade, por meio do mecanismo de certificação, deve ser realizada por Organismo de Certificação de Produto – OCP, estabelecido no Brasil e acreditado pelo Inmetro, consoante os Requisitos ora aprovados.

§ 2º Aplicam-se os presentes Requisitos aos equipamentos de certificação digital para uso no âmbito da ICP-Brasil, incluindo:

I – cartões criptográficos (**smart cards**);

II – leitoras de cartões inteligentes;

III – **tokens** criptográficos; e

IV – módulo de segurança criptográfica.

§ 3º Encontram-se excluídos do escopo de abrangência desses Requisitos os equipamentos de certificação digital para uso em âmbitos diferentes da ICP-Brasil.

§ 4º Ao Instituto Nacional de Tecnologia da Informação (ITI) cabe a definição, por meio de ato normativo próprio, quanto à compulsoriedade da certificação de equipamentos de certificação digital para uso no âmbito da ICP-Brasil.

Art. 2º Não compete ao Inmetro a regulamentação técnica de equipamentos de certificação digital para uso no âmbito da ICP-Brasil, o exercício de poder de polícia administrativa quanto ao objeto, bem como a definição de prazos de adequação para o setor, cabendo, exclusivamente a supervisão quanto ao uso da marca, tendo por foco o cumprimento das regras de Avaliação da Conformidade.

Prazos e disposições transitórias

Art.3º A publicação desta Portaria não implica na necessidade de que seja iniciado novo processo de certificação com base nos requisitos ora consolidados.

Parágrafo único. Os certificados já emitidos deverão ser apenas revisados na próxima etapa de avaliação, para referência à Portaria ora publicada.

Cláusula de revogação

Art. 4º Ficam revogadas, na data de vigência desta Portaria:

I – Portaria Inmetro nº 8, de 8 de janeiro de 2013, publicada no Diário Oficial da União de 10 de janeiro de 2013, seção 01, página 59;

II – Portaria Inmetro nº 394, de 10 de agosto de 2015, publicada no Diário Oficial da União de 12 de agosto de 2015, seção 01, páginas 59 e 60;

III – Portaria Inmetro nº 596, de 17 de dezembro de 2015, publicada no Diário Oficial da União de 18 de dezembro de 2015, seção 01, página 114; e

IV – Portaria Inmetro nº 543, de 24 de novembro de 2016, publicada no Diário Oficial da União de 29 de novembro de 2016, seção 01, página 41.

Vigência

Art. 5º Esta Portaria entra em vigor em vigor em 01 de abril de 2021, conforme art. 4º do Decreto nº 10.139, de 2019.

MARCOS HELENO GUERSON DE OLIVEIRA JÚNIOR

Presidente

INMETRO	**ANEXO I - REQUISITOS DE AVALIAÇÃO DA CONFORMIDADE PARA EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL PADRÃO ICP-BRASIL**

1. OBJETIVO

Estabelecer critérios e procedimentos de avaliação da conformidade para equipamentos de certificação digital padrão ICP-Brasil, com foco na segurança da informação, por meio do mecanismo de certificação, atendendo os requisitos dos Manuais de Conduta Técnica (MCT) 1, 2, 3 e 7, Volumes I e II, e DOC-ICP-01.01, aprovados pelo Comitê Gestor da ICP-Brasil, em versão mais recente, visando à interoperabilidade e à operação segura dos Equipamentos de Certificação Digital Padrão ICP-Brasil.

1.1 Agrupamento para efeitos de certificação

1.1.1 Para certificação do objeto deste RAC, aplica-se o conceito de marca/modelo.

1.1.2 A certificação de Cartões Criptográficos Padrão ICP-Brasil deve ser realizada para cada modelo de equipamento, de uma mesma marca, que é representado por exemplares constituídos pelos mesmos componentes eletrônicos, pela mesma configuração física e por igual especificação e versão de **hardware, middleware, software** e **firmware** embarcados.

1.1.3 A certificação de Leitoras de Cartões Inteligentes Padrão ICP-Brasil deve ser realizada para cada modelo de equipamento, de uma mesma marca, que é representado por exemplares constituídos pelos mesmos componentes eletrônicos e mecânicos, pela mesma interface de comunicação, pelos mesmos *drivers* e por igual especificação e versão de **hardware, software** e **firmware embarcados.**

1.1.4 A certificação de **Tokens** Criptográficos Padrão ICP-Brasil deve ser realizada para cada modelo de equipamento, de uma mesma marca, que é representado por exemplares constituídos pelos mesmos componentes eletrônicos, pelas mesmas interfaces de comunicação, pelos mesmos **drivers** e por igual especificação e versão de **hardware, middleware, firmware** e **software** embarcados.

1.1.5 A certificação de Modulo de Segurança Criptográfica Padrão ICP-Brasil deve ser realizada para cada modelo de equipamento, de uma mesma marca, que é representado por exemplares constituídos pelas mesmas interfaces de comunicação, pelos mesmos **drivers**, pelos mesmos mecanismos de segurança física e de controle de acesso físico e lógico e por igual especificação e versão de **hardware, middleware, firmware** e **software** embarcados.

2. SIGLAS

CNPJ	Cadastro Nacional de Pessoas Jurídicas
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CPF	Cadastro de Pessoas Físicas
DOC-ICP	Documento normativo emitido pela Infraestrutura de Chaves Públicas Brasileira ICP-Brasil Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
MCT	Manual de Conduta Técnica
MSC	Módulo de Segurança Criptográfica
NSC	Nível de Segurança de Certificação
URL	Localizador Universal de Recursos (endereço de um site)

3. DOCUMENTOS COMPLEMENTARES

Portaria Inmetro vigente	Requisitos Gerais de Certificação de Produtos (RGCP)
Normativo ICP-Brasil - DOC-ICP-01.01	Padrões e Algoritmos Criptográficos da ICP-Brasil.
Manual de Conduta Técnica 1 – Volume I	Requisitos, Materiais e Documentos Técnicos para Certificação de Cartões Criptográficos (**Smart Cards**) no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 1 – Volume II	Procedimentos de Ensaios para Avaliação da Conformidade aos Requisitos Técnicos de Cartões Criptográficos (**Smart Cards**) no Âmbito da ICP- Brasil.
Manual de Conduta Técnica 2– Volume I	Requisitos, Materiais e Documentos Técnicos para Certificação de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 2 – Volume II	Procedimentos de Ensaios para Avaliação da Conformidade aos Requisitos Técnicos de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 3 – Volume I	Requisitos, Materiais e Documentos Técnicos para Certificação de **Tokens** Criptográficos no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 3 – Volume II	Procedimentos de Ensaios para Avaliação da Conformidade aos Requisitos Técnicos de *Tokens* no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 7 – Volume I	Requisitos, Materiais e Documentos Técnicos para Certificação de MSC Criptográficos no Âmbito da ICP-Brasil.
Manual de Conduta Técnica 7 – Volume II	Procedimentos de Ensaios para Avaliação da Conformidade aos Requisitos Técnicos de MSC no Âmbito da ICP-Brasil.

4. DEFINIÇÕES

Para fins deste RAC, são adotadas as definições a seguir, complementadas pelas definições contidas nos documentos citados no item 3.

4.1 Autoridade certificadora

Entidade que emite, renova ou revoga certificados digitais de outras autoridades ou de titulares finais.

4.2 Certificação de equipamentos de certificação digital padrão ICP-Brasil

Processo sistematizado de avaliação da conformidade por terceira parte, no âmbito do SBAC, incluindo avaliações de manutenção periódicas, de forma a propiciar adequado grau de confiança de que os Equipamentos de Certificação Digital Padrão ICP-Brasil atendem aos requisitos estabelecidos nos Regulamentos da ICP-Brasil.

4.3 Certificação Digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

4.4 Equipamentos de certificação digital padrão ICP-Brasil

Todo e qualquer aparelho, dispositivo ou elemento físico que compõe meio necessário ou suficiente à realização da certificação digital Padrão ICP-Brasil.

4.5 Fornecedor de equipamentos de certificação digital padrão ICP-Brasil

Pessoa jurídica titular dos direitos de propriedade intelectual dos Equipamentos de Certificação Digital Padrão ICP-Brasil objetos da certificação. No caso de pessoa jurídica não sediada no Brasil, esta deve se fazer representar por pessoa física, constituída como seu procurador, devidamente qualificado e domiciliado no Brasil, com poderes para representá-la administrativa e judicialmente, inclusive para receber citações judiciais ou intimações administrativas em seu nome, desde a data da solicitação de certificação e durante a validade da certificação.

4.6 Nível de Segurança de Certificação (NSC)

Diferentes graus de confiabilidade presumida nos resultados de ensaio obtidos, em função dos diferentes esforços realizados pelo laboratório acreditado, conforme o rigor necessário para a avaliação da conformidade do Equipamento de Certificação Digital Padrão ICP-Brasil.

4.7 Nível de Segurança de Certificação 1 (NSC 1)

Aplicável quando se necessita de confiança na operação correta do Equipamento de Certificação Digital Padrão ICP-Brasil, porém sua utilização está prevista para ocorrer em ambiente em que as ameaças à segurança estejam bem controladas e a ocorrência de eventuais problemas de interoperabilidade não é visto como fator importante. No NSC 1, a avaliação é feita com profundidade básica, a partir do depósito de amostras do objeto e baseada no fornecimento, pelo fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil, de documentação básica sobre o objeto de certificação. Consiste de testes de funcionalidades, de acordo com as especificações do fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil e da avaliação da documentação fornecida. Para esse nível de avaliação, não é necessário o depósito de códigos-fonte.

4.8 Nível de Segurança de Certificação 2 (NSC 2)

Aplicável quando se necessita de confiança na operação correta do Equipamento de Certificação Digital Padrão ICP-Brasil, tendo sua utilização prevista para ocorrer em ambiente em que as ameaças à segurança e a ocorrência de eventuais problemas de interoperabilidade são vistos como relevantes. No NSC 2, a avaliação é feita com profundidade moderada, a partir do depósito de amostras do objeto de certificação e baseada no fornecimento, pelo fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil, de informações de projeto, resultados de testes já realizados e depósitos de parte de códigos-fonte.

4.9 Nível de Segurança de Certificação 3 (NSC 3)

Aplicável quando se necessita de confiança na operação correta do sistema ou Equipamento de Certificação Digital Padrão ICP-Brasil e sua utilização está prevista para ocorrer em ambiente em que as ameaças à segurança ou problemas de interoperabilidade são vistos como críticos. No NSC 3, a avaliação é feita com profundidade alta, a partir do depósito de amostras do objeto de certificação e baseada no fornecimento, pelo fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil, de informações mais detalhadas do projeto, resultados de testes já realizados, depósito de todo o código fonte e comprovação da utilização no produto de práticas para garantir sua segurança.

5. MECANISMO DE AVALIAÇÃO DA CONFORMIDADE

O mecanismo de avaliação da conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil é o da certificação.

6. ETAPAS DO PROCESSO DE AVALIAÇÃO DA CONFORMIDADE

Este RAC estabelece 2 (dois) modelos de certificação distintos, cabendo ao fornecedor optar por um deles:

a) Modelo de Certificação 4 – Avaliação inicial consistindo de ensaios em amostras retiradas no fabricante seguido de avaliação de manutenção periódica através de coleta de amostras do produto na fábrica.

b) Modelo de Certificação 5 – Avaliação inicial consistindo de ensaios em amostras retiradas no fabricante, incluindo auditoria do Sistema de Gestão da Qualidade, seguida de avaliação de manutenção periódica através de coleta de amostra do produto na fábrica e auditoria do SGQ.

6.1 Modelo de Certificação 4

6.1.1 Avaliação Inicial

6.1.1.1 Solicitação de Certificação

6.1.1.1.1 O fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil deve encaminhar uma solicitação formal ao OCP, indicando o NSC do objeto a ser certificado e fornecendo a documentação descrita no RGCP, além dos seguintes itens:

a) Se pessoa jurídica sediada no Brasil:

- Dados do fabricante (razão social, endereço, CNPJ, URL, telefone e fax).
- Dados do responsável administrativo e do responsável técnico (nome, telefone, fax e e-mail).
- Listagem dos Equipamentos de Certificação Digital, com a identificação do item e sua respectiva descrição, modelo, versão/série e NSC requerido.
- Informações comerciais sobre o(s) sistema(s) ou equipamento(s) de certificação digital que deseja certificar, tais como, vendas realizadas, clientes atendidos, entre outras.
- Para as sociedades empresariais, estatuto ou contrato social em vigor, devidamente registrado e, quando sociedades por ações, acompanhado de documentos de eleição de seus administradores.
- Para as sociedades civis, Registro de Ato Constitutivo no Registro Civil das Pessoas Jurídicas, acompanhado de documento que comprove a composição da administração em exercício.
- Documento oficial de identidade com foto dos administradores, que permita sua identificação física.
- CPF dos administradores.
- Prova de Inscrição no CNPJ.
- Termo de Propriedade Intelectual, Tipo I – Pessoa Jurídica Sediada no Brasil (Anexo A), devidamente preenchido e assinado pelos representantes legais do fornecedor, em duas vias, com firma reconhecida.
- Termo de Sigilo, Tipo I – Pessoa Jurídica Sediada no Brasil (Anexo C), devidamente preenchido e assinado pelos representantes legais do fornecedor, em duas vias, com firma reconhecida.

b) Se pessoa jurídica não sediada no Brasil:

- Dados do procurador (nome, endereço, CPF, telefone, fax e e-mail).
- Dados do fabricante (razão social, endereço, CNPJ, URL, telefone e fax).
- Listagem dos Equipamentos de Certificação Digital, com a identificação do item e sua respectiva descrição, modelo, versão/série e NSC requerido.
- Informações comerciais sobre o(s) sistema(s) ou equipamento(s) de certificação digital que deseja certificar, tais como, vendas realizadas, clientes atendidos, entre outras.
- Instrumento público de mandato que comprove constituição e manutenção de procurador, nos termos do disposto no item 4.5. Se o instrumento público de mandato for estrangeiro, o mesmo deve possuir a devida autenticação consular do país de origem e no Brasil, seguida de tradução pública juramentada e registro no cartório de títulos e documentos.
- Documento oficial de identidade com foto do procurador constituído, que permita sua identificação física.
- CPF do procurador constituído.
- Termo de Propriedade Intelectual, Tipo II – Pessoa Jurídica Não Sediada no Brasil (Anexo B), devidamente preenchido e assinado pelos representantes legais do fornecedor, em duas vias, com firma reconhecida.
- Termo de Sigilo, Tipo II – Pessoa Jurídica Não Sediada no Brasil (Anexo D), devidamente preenchido e assinado pelos representantes legais do fornecedor, em duas vias, com firma reconhecida.

6.1.1.1.2 Com exceção dos formulários e termos, todos os demais documentos exigidos nos itens 6.1.1.1.1 devem ser apresentados em suas versões originais e cópias. As cópias devem ficar retidas com o OCP.

6.1.1.1.3 O fornecedor deve indicar se o modelo a ser certificado é similar a outro que já obteve certificação e que possui Certificado de Conformidade válido.

6.1.1.2 Análise da Solicitação e da Conformidade da Documentação

A análise da solicitação e da conformidade da documentação deve seguir conforme estabelecido no RGCP.

6.1.1.3 Plano de Ensaios Iniciais

O plano de ensaios iniciais deve seguir conforme estabelecido no RGCP. Os ensaios iniciais devem ser realizados em amostra coletada pelo OCP, de forma aleatória, no processo produtivo do produto objeto da solicitação, desde que o produto já tenha sido inspecionado e liberado pelo controle de qualidade da fábrica, ou na área de expedição, em embalagens prontas para comercialização.

6.1.1.3.1 Definição dos Ensaios a Serem Realizados

6.1.1.3.1.1 Os ensaios a serem realizados estão estabelecidos e detalhados no Volume II do MCT 1, 2, 3 e 7, de acordo com o NSC do objeto a ser certificado.

6.1.1.3.1.2 Em caso de modelo similar a outro já certificado e com Certificado de Conformidade válido, do mesmo fornecedor, cabe ao OCP definir os ensaios dos MCTs a serem ensaiados.

6.1.1.3.2 Definição da Amostragem

A definição da amostragem deve seguir as condições gerais expostas no RGCP, além da seguinte:

6.1.1.3.2.1 O OCP é responsável por realizar presencialmente a coleta da amostra do objeto a ser certificado.

6.1.1.3.2.2 De acordo com o procedimento específico definido pelo OCP, a amostra deve ser identificada, lacrada e encaminhada para avaliação da conformidade.

6.1.1.3.2.3 O OCP, ao realizar a coleta da amostra, deve elaborar um relatório de amostragem, detalhando as condições em que esta foi obtida, a data, o local e a identificação do lote.

6.1.1.3.2.4 A quantidade e a especificação dos componentes físicos, componentes em **software** executável e documentação técnica que devem ser coletados para os ensaios estão definidos no Volume I dos MCTs 1, 2, 3 e 7.

6.1.1.3.2.5 Produtos que sejam protótipos não podem constituir amostra para avaliação da conformidade.

6.1.1.3.3 Definição do Laboratório

A definição do laboratório deve seguir as condições gerais expostas no RGCP, além da seguinte:

6.1.1.3.3.1 Os laboratórios de ensaio devem ser entidades com capacitação técnica necessária à realização dos ensaios para avaliação da conformidade de Equipamentos de Certificação Digital Padrão ICP-Brasil, devendo atender os seguintes critérios:

a) Ser localizado em território nacional.

b) Comprovar a capacitação técnica por meio da existência de pessoal qualificado, voltado ao objeto da avaliação da conformidade de Equipamentos de Certificação Digital Padrão ICP-Brasil, seja nos quadros do organismo, ou fora dele, devendo, neste último caso, ser comprovada a vinculação contratual com o pessoal qualificado. O pessoal deve comprovar a capacitação técnica quanto à formação profissional, experiência profissional e capacidade técnica, constantes em currículo na plataforma Lattes do CNPq.

c) Ter instalações operacionais e recursos de segurança física e lógica compatíveis com as atividades de ensaios.

d) Atender os requisitos de segurança de pessoal, segurança física, segurança lógica, segurança de rede, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios e análise de registros de eventos, especificados no Anexo E.

e) Demonstrar capacidade de tratamento sigiloso de informações, devendo o laboratório providenciar que seus empregados, prepostos e representantes adotem medidas e procedimentos para a proteção de informações e materiais sigilosos, respondendo sobre qualquer acesso ou divulgação não autorizados.

6.1.1.4 Tratamento de não Conformidades na Etapa de Avaliação Inicial

O tratamento de não conformidades na etapa de avaliação inicial deve seguir as condições descritas no RGCP.

6.1.1.5 Emissão do Certificado de Conformidade

6.1.1.5.1 O OCP deve conceder a certificação, emitindo o Certificado de Conformidade para o(s) modelo(s) de produto(s) que atenda(m) aos requisitos desse RAC.

6.1.1.5.2 O Certificado de Conformidade deve conter as informações listadas a seguir, além daquelas descritas no RGCP para a Emissão do Certificado de Conformidade na etapa de avaliação inicial:

a) Identificação do fornecedor do Equipamento de Certificação Digital Padrão ICP-Brasil.

b) Identificação do fabricante do Equipamento de Certificação Digital Padrão ICP-Brasil, quando o fornecedor não for o fabricante.

c) Identificação da marca, modelo e versão de cada **hardware, software** e **firmware** do Equipamento para Certificação Digital.

d) Identificação do NSC.

e) Número do(s) relatório(s) de ensaio da etapa de avaliação inicial.

f) Identificação do OCP e assinatura do responsável técnico e do responsável pelo OCP.

g) Data de emissão do certificado e validade.

6.1.1.5.3 O fornecedor deve informar ao OCP todas as alterações e atualizações de **software** ou **firmware** no Equipamento de Certificação Digital Padrão ICP-Brasil já certificado e o OCP deve avaliar a necessidade de novos ensaios ou novo processo de certificação.

6.1.1.5.4 O Certificado de Conformidade deve ter validade de 06 (seis) anos.

6.1.2 Avaliação de Manutenção

Os critérios para a Avaliação da Manutenção devem seguir conforme definido no RGCP. Depois da concessão do Certificado de Conformidade, o acompanhamento da Certificação é realizado pelo OCP, que deve programar a realização de ensaios, conforme a periodicidade definida neste RAC, para constatar se as condições técnico-organizacionais que deram origem à concessão inicial da certificação continuam sendo cumpridas.

6.1.2.1 Plano de Ensaios de Manutenção

Os ensaios de manutenção devem ser realizados a cada 12 (doze) meses, a contar da data da emissão do Certificado de Conformidade, ou sempre que existirem fatos que recomendem a sua realização antes deste período, em amostras coletadas no comércio ou, caso o fornecedor comprove, através de nota fiscal, que o produto não é de prateleira, na expedição do processo produtivo.

6.1.2.1.1 Definição dos Ensaios a serem realizados

A definição dos ensaios a serem realizados deve seguir o definido no item 6.1.1.3.1 deste RAC.

6.1.2.1.2 Definição da Amostragem de Manutenção

A definição da amostragem de manutenção deve seguir o definido no item 6.1.1.3.2 deste RAC.

6.1.2.1.3 Definição do Laboratório

A definição do laboratório deve seguir as condições descritas no item 6.1.1.3.3.

6.1.2.2 Tratamento de Não Conformidades na Etapa de Avaliação de Manutenção

O tratamento de não conformidades na etapa de avaliação de manutenção deve seguir as condições descritas no RGCP.

6.1.2.3 Confirmação da Manutenção

A confirmação da manutenção deve seguir as condições descritas no RGCP.

6.1.3 Avaliação de Recertificação

A Avaliação de Recertificação ocorre a cada 6 (seis) anos, devendo ser finalizada até a data de validade do Certificado de Conformidade, devendo seguir as condições descritas no RGCP.

6.2 Modelo de Certificação 5

6.2.1 Avaliação Inicial

6.2.1.1 Solicitação de Certificação

6.2.1.1.1 O fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil deve encaminhar uma solicitação formal ao OCP, observado o disposto no subitem 6.1.1.1 deste RAC.

6.2.1.2 Análise da Solicitação e da Conformidade da Documentação

A análise da solicitação e da conformidade da documentação deve seguir o definido no item 6.1.1.2 deste RAC.

6.2.1.3 Auditoria Inicial do Sistema de Gestão da Qualidade

A auditoria inicial do Sistema de Gestão da Qualidade deve seguir conforme estabelecido no RGCP.

6.2.1.4 Plano de Ensaios Iniciais

O plano de ensaios iniciais deve seguir conforme descrito no RGCP. Os ensaios iniciais devem ser realizados em amostra coletada pelo OCP, de forma aleatória, no processo produtivo do produto objeto da solicitação, desde que o produto já tenha sido inspecionado e liberado pelo controle de qualidade da fábrica, ou na área de expedição, em embalagens prontas para comercialização.

6.2.1.4.1 Definição dos Ensaios a Serem Realizados

Os ensaios iniciais devem seguir o definido no item 6.1.1.3.1 deste RAC.

6.2.1.4.2 Definição da Amostragem

A definição da amostragem deve seguir o definido no item 6.1.1.3.2 deste RAC.

6.2.1.4.3 Definição do Laboratório

A definição do laboratório deve seguir o definido no item 6.1.1.3.3 deste RAC.

6.2.1.5 Tratamento de Não Conformidades na Etapa de Avaliação Inicial

O tratamento de não conformidades na etapa de avaliação inicial deve seguir as condições descritas no RGCP.

6.2.1.6 Emissão do Certificado

6.2.1.6.1 O OCP deve conceder a certificação, emitindo um instrumento formal nos termos do definido pelo subitem 6.1.1.5 deste RAC.

6.2.1.6.2 O Certificado de Conformidade deve ter validade de 08 (oito) anos.

6.2.2 Avaliação de Manutenção

Os critérios para a Avaliação de Manutenção devem seguir o estabelecido no RGCP. Depois da concessão do Certificado de Conformidade, o controle da Certificação é realizado pelo OCP, conforme a periodicidade definida neste RAC, para constatar se as condições técnico-organizacionais que deram origem à concessão inicial da certificação continuam sendo cumpridas.

6.2.2.1 Auditoria de Manutenção do Sistema de Gestão da Qualidade

A auditoria de manutenção do Sistema de Gestão da Qualidade deve ocorrer a cada 24 (vinte e quatro) meses.

6.2.2.2 Plano de Ensaios de Manutenção

Os ensaios de manutenção devem ser realizados a cada 24 (vinte e quatro) meses, a contar da data da emissão do Certificado de Conformidade, ou sempre que existirem fatos que recomendem a sua realização antes deste período, em amostras coletadas no comércio.

6.2.2.2.1 Definição dos Ensaios a Serem Realizados

A definição dos ensaios a serem realizados deve seguir o definido no item 6.1.1.3.1 deste RAC.

6.2.2.2.2 Definição da Amostragem de Manutenção

A definição da amostragem de manutenção deve seguir o definido no item 6.1.1.3.2 deste RAC.

6.2.2.2.3 Definição do Laboratório

A definição do laboratório deve seguir o definido no item 6.1.1.3.3 deste RAC.

6.2.2.3 Tratamento de Não Conformidades na Etapa de Avaliação De Manutenção

O tratamento de não conformidades na etapa de avaliação de manutenção deve seguir as condições descritas no RGCP.

6.2.2.4 Confirmação da Manutenção

A Confirmação da Manutenção deve seguir as condições descritas no RGCP.

6.2.3 Avaliação de Recertificação

A Avaliação de Recertificação ocorre a cada 8 (oito) anos, devendo ser finalizada até a data de validade do Certificado de Conformidade, devendo seguir as condições descritas no RGCP.

7. TRATAMENTO DE RECLAMAÇÕES

O Tratamento de Reclamações deve seguir as condições descritas no RGCP.

8. ATIVIDADES EXECUTADAS POR MEMBRO DO MLA OU IAF

As atividades de avaliação da conformidade, executadas por um organismo acreditado por membro do MLA do IAF, podem ser aceitas, desde que observadas as condições descritas no RGCP.

9. TRANSFERÊNCIA DA CERTIFICAÇÃO

A Transferência da Certificação deve seguir as condições descritas no RGCP.

10. ENCERRAMENTO DA CERTIFICAÇÃO

O Encerramento da Certificação deve seguir as condições descritas no RGCP.

11. SELO DE IDENTIFICAÇÃO DA CONFORMIDADE

Os critérios gerais para o Selo de Identificação da Conformidade estão contemplados no RGCP e no Anexo II da Portaria Inmetro.

12. AUTORIZAÇÃO PARA O USO DO SELO DE IDENTIFICAÇÃO DA CONFORMIDADE

A Autorização para o Uso do Selo de Identificação da Conformidade deve seguir as condições descritas no RGCP.

13. RESPONSABILIDADES E OBRIGAÇÕES

Os critérios para responsabilidades e obrigações devem seguir as condições descritas no RGCP, adicionadas das seguintes:

13.1. O fornecedor de Equipamentos de Certificação Digital Padrão ICP-Brasil, o OCP e laboratórios de ensaio devem emitir relatórios consolidados e demais documentos, quando exigidos pelo ITI, devendo os fluxos de informação observar a política de sigilo (Anexos C e D) e de segurança da informação (Anexo E).

13.2. O OCP deve demonstrar capacidade de tratamento sigiloso de informações, devendo providenciar que seus empregados, prepostos e representantes adotem medidas e procedimentos para proteção de informações e materiais sigilosos, respondendo sobre qualquer acesso ou divulgação não autorizados.

13.3. O OCP deve informar ao ITI sempre que um Certificado de Conformidade for cancelado ou suspenso.

13.4. O fornecedor deve considerar os prazos dados pelo OCP, pelo laboratório de ensaios e pelo Inmetro para entrar tempestivamente com a avaliação da manutenção e a recertificação.

14. ACOMPANHAMENTO NO MERCADO

O acompanhamento no mercado deve seguir as condições descritas no RGCP.

15. PENALIDADES

A aplicação de penalidades deve seguir as condições descritas no RGCP.

16. DENÚNCIAS, RECLAMAÇÕES E SUGESTÕES

Os critérios para denúncias, reclamações e sugestões devem seguir os requisitos estabelecidos no RGCP.

ANEXO A: TERMO DE PROPRIEDADE INTELECTUAL – TIPO I

TERMO DE PROPRIEDADE INTELECTUAL

A [Pessoa Jurídica] com sede social na [endereço completo], inscrita no CNPJ sob o nº [XX.XXX.XXX/XXX-XX], neste ato representada pelo(s) seu(s) representante(s) legal(ais), o(s) Sr(s). [Nome(s) Completo(s)], de acordo com o Estatuto/Contrato Social em anexo, vem por meio deste declarar, para todos os efeitos do que dispõe a Portaria Inmetro que estabelece os Requisitos de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil e a legislação atinente ou que faça menção aos direitos e deveres relacionados à propriedade intelectual, que é titular dos direitos de propriedade intelectual sobre os sistemas e/ou equipamentos listados em relação anexa, respondendo, com exclusividade, por todos os atos que gerem qualquer obrigação ou direito a estes atribuídos.

Declaro(amos), sob as penas da lei, serem verdadeiras as informações prestadas no presente.

_____, ___ de _____ de _____.

_____

[Pessoa Jurídica]

OBSERVAÇÕES:

a) Todo conteúdo expresso na forma [...] deverá ser substituído pelos dados reais correspondentes do interessado.

b) Todos os representantes legais relacionados deverão assinar o presente Termo.

ANEXO B: TERMO DE PROPRIEDADE INTELECTUAL – TIPO II

TERMO DE PROPRIEDADE INTELECTUAL

A [Pessoa Jurídica] com sede social na [endereço completo da Pessoa Jurídica], neste ato representada pelo(a) seu(ua) PROCURADOR(A), o(a) Sr(a). [XXXXXXX], portador(a) da cédula de identidade sob o registro geral R.G. nº [XXXXXXXX] e do Cadastro de Pessoa Física CPF nº [XXXXXXXXXXX], residente à [endereço completo do Procurador(a)], de acordo com o Instrumento Público de Mandato em anexo, com a devida autenticação consular, vem por meio deste declarar, para todos os efeitos do que dispõe a Portaria Inmetro que estabelece os Requisitos de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil e a legislação atinente ou que faça menção aos direitos e deveres relacionados à propriedade intelectual, que é titular dos direitos de propriedade intelectual sobre os sistemas e/ou equipamentos listados em relação anexa, respondendo, com exclusividade, por todos os atos que gerem qualquer obrigação ou direito a estes atribuídos.

Declaro(amos), sob as penas da lei, serem verdadeiras as informações prestadas no presente.

_____, ___ de _____ de _____.

_____

[Nome do Procurador(a)]

OBSERVAÇÃO:
Todo conteúdo expresso na forma [...] deverá ser substituído pelos dados reais correspondentes do interessado.

ANEXO C: TERMO DE SIGILO – TIPO I

TERMO DE SIGILO

São partes neste instrumento:

O(a) [Organismo de Certificação de Produtos]**,** organismo de certificação acreditado pelo Inmetro, neste ato representado pelo seu Presidente em exercício, doravante denominado simplesmente, [Organismo de Certificação de Produtos]; e

A [Pessoa Jurídica] com sede social à [endereço completo], inscrita no CNPJ sob o nº [XX.XXX.XXX/XXX-XX], neste ato representada pelo(s) seu(s) representante(s) legal(ais), o(s) Sr(s). [Nome(s) Completo(s)], de acordo com o Estatuto/Contrato Social em anexo, doravante denominada simplesmente, [Pessoa Jurídica].

CONSIDERANDO:

- que a [Pessoa Jurídica] submeterá ao [Organismo de Certificação de Produtos] Equipamentos de Certificação Digital Padrão ICP-Brasil com o fito de certificá-los junto ao Inmetro, em consonância ao disposto na Portaria Inmetro que estabelece os Requisitos de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil;

- que para tanto o [Organismo de Certificação de Produtos] receberá da [Pessoa Jurídica] informações do seu processo de negócios, bem como, informações técnicas a respeito de seus sistemas e/ou equipamentos e, eventualmente, de seus clientes;

- que no decurso do processo de certificação, serão divulgados ou entregues pela [Pessoa Jurídica] segredos e informações confidenciais, com a finalidade de permitir que o [Organismo de Certificação de Produtos] proceda a necessária avaliação de conformidade aos padrões e especificações técnicas mínimos estabelecidos;

A [Pessoa Jurídica] e o [Organismo de Certificação de Produtos] firmam o presente instrumento sob as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DEFINIÇÕES

Para os fins deste instrumento, entende-se por:

1.1. Informações: os dados, os documentos e os materiais que lhe sejam pertinentes;

1.2. Informações Confidenciais: todas e quaisquer informações fornecidas, comunicadas ou reveladas pela [Pessoa Jurídica] ao [Organismo de Certificação de Produtos], cujo conhecimento irrestrito ou divulgação possa acarretar danos à mesma, independentemente do meio ou forma de transmissão;

1.3. Tratamento: significa a consulta, produção, transmissão, conservação, alteração, utilização, acesso e eliminação de informações;

1.4. Sigilo: proteção contra o tratamento não autorizado de informações confidenciais.

CLÁUSULA SEGUNDA - DIVULGAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1. O [Organismo de Certificação de Produtos], a contar da data do efetivo recebimento e/ou conhecimento de informação confidencial, se compromete e se obriga a:
a) manter sob absoluto sigilo, pelo prazo de 15 (quinze) anos, todas as informações confidenciais que lhe forem transmitidas pela [Pessoa Jurídica] visando à certificação de seus Equipamentos de Certificação Digital Padrão ICP-Brasil;
b) utilizar as informações confidenciais, exclusivamente, para a finalidade para a qual as mesmas lhe foram transmitidas;
c) não conferir tratamento às referidas informações confidenciais em benefício próprio ou de terceiro, para qualquer finalidade;
d) proteger as informações confidenciais contra a divulgação a terceiros;
e) limitar a divulgação das informações confidenciais recebidas nos termos deste instrumento a pessoas dentro de sua organização ou a seus prestadores de serviço, que no desenvolvimento de suas atividades tenham necessidade de conhecê-las; e
f) instruir devidamente as pessoas responsáveis pelo tratamento das informações confidenciais a proteger e manter a confidencialidade das mesmas.

2.2. O [Organismo de Certificação de Produtos], para fins de sigilo, obriga-se por seus administradores, servidores e prestadores de serviços.

CLÁUSULA TERCEIRA - LIMITAÇÃO DAS OBRIGAÇÕES

3.1. Não são consideradas informações confidenciais para fins do presente Termo de Sigilo aquelas que:
a) ao tempo de sua transmissão ao [Organismo de Certificação de Produtos], ou posteriormente, sejam ou venham a ser de conhecimento público, conforme evidenciado por publicações idôneas, desde que sua divulgação não tenha sido causada pelo próprio [Organismo de Certificação de Produtos];
b) já estivessem na posse legal do [Organismo de Certificação de Produtos] por ocasião da divulgação, desde que tenham sido recebidas legitimamente de terceiro, sem violação de obrigação legal e/ou obrigação de sigilo assumida com a [Pessoa Jurídica];
c) forem independentemente tratadas pelo [Organismo de Certificação de Produtos], sem utilização direta ou indireta de informações confidenciais da [Pessoa Jurídica]; ou ficando ressalvado que esta deverá, nesse caso, avisar o [Organismo de Certificação de Produtos] imediatamente, por escrito.
d) forem necessariamente divulgadas pela [Pessoa Jurídica] no cumprimento de ordem judicial, ficando ressalvado que esta deverá, nesse caso, avisar o [Organismo de Certificação de Produtos] imediatamente, por escrito.

CLÁUSULA QUARTA - PROPRIEDADE DAS INFORMAÇÕES CONFIDENCIAIS

4.1. O [Organismo de Certificação de Produtos] concorda que a [Pessoa Jurídica] é, e continuará sendo, a exclusiva proprietária de suas informações confidenciais e de todas as patentes, direitos autorais, segredos, marcas registradas e outros direitos de propriedade intelectual. Nenhuma licença ou transferência de qualquer desses direitos ao [Organismo de Certificação de Produtos] é concedida ou fica implícita nos termos deste instrumento.

CLÁUSULA QUINTA - PRAZO DE VIGÊNCIA

5.1. Este acordo permanecerá em vigor pelo período de 12 (doze) meses a contar da data de sua assinatura, podendo ser prorrogado por igual período por manifestação expressa das partes. As obrigações constantes na Cláusula Segunda - Divulgação das Informações Confidencias, na Cláusula Terceira - Limitação das Obrigações e na Cláusula Quarta - Propriedade das informações Confidenciais sobreviverão ao prazo de vigência deste instrumento.

CLÁUSULA SEXTA - DISPOSIÇÕES FINAIS

6.1. O [Organismo de Certificação de Produtos] assumirá inteira responsabilidade por qualquer forma de tratamento não autorizado pela [Pessoa Jurídica] de suas informações confidenciais, quando feito por seus administradores, servidores e prestadores de serviço, em violação ao presente Termo de Sigilo.

6.2. Este Termo de Sigilo substitui todos os ajustes anteriores, verbais ou escritos, acordados entre as partes, relativamente à matéria objeto deste instrumento e não poderá ser modificado, alterado ou rescindido, no todo ou em parte, exceto por documento escrito assinado pelo [Organismo de Certificação de Produtos] e pela [Pessoa Jurídica].

CLÁUSULA SÉTIMA – FORO

7.1. Fica eleita a Seção Judiciária do Distrito Federal, como competente para dirimir e julgar quaisquer disputas relacionadas com o presente instrumento, com renúncia a qualquer outro, por mais privilegiado que seja.

E assim, estando justas e contratadas, as partes assinam o presente instrumento, em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo.

_____, ___de_____de_____.

_____

[Pessoa Jurídica]

_____

[Organismo de Certificação de Produtos]

Testemunhas:

_____ _____

Nome:
RG:

Nome:
RG:

OBSERVAÇÕES:

a) todo conteúdo expresso na forma [...] deverá ser substituído pelos dados reais correspondentes do interessado;

b) todos os representantes legais relacionados deverão assinar o presente Termo.

ANEXO D: TERMO DE SIGILO – TIPO II

TERMO DE SIGILO

São partes neste instrumento:

O(a) [Organismo de Certificação de Produtos]**,** organismo de certificação acreditado pelo Inmetro, neste ato representado pelo seu Presidente em exercício, doravante denominado simplesmente, [Organismo de Certificação de Produtos]; e

A [Pessoa Jurídica] com sede social à [endereço completo da Pessoa Jurídica], neste ato representada pelo(a) seu(ua) PROCURADOR(A), o(a) Sr(a). [XXXXXXX], portador(a) da cédula de identidade sob o registro geral R.G. nº [XXXXXXXX] e do Cadastro de Pessoa Física CPF nº [XXXXXXXXXXX], residente à [endereço completo do Procurador(a)], de acordo com o Instrumento Público de Mandato em anexo, com a devida autenticação consular, doravante denominada simplesmente, [Pessoa Jurídica].

CONSIDERANDO:

- que a [Pessoa Jurídica] submeterá ao [Organismo de Certificação de Produtos] Equipamentos de Certificação Digital Padrão ICP-Brasil com o fito de certificá-los junto ao Inmetro, em consonância ao disposto na Portaria Inmetro que estabelece os Requisitos de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil;

- que para tanto o [Organismo de Certificação de Produtos] receberá da [Pessoa Jurídica] informações do seu processo de negócios, bem como, informações técnicas a respeito de seus sistemas e/ou equipamentos e, eventualmente, de seus clientes;

- que no decurso do processo de certificação, serão divulgados ou entregues pela [Pessoa Jurídica] segredos e informações confidenciais, com a finalidade de permitir ao [Organismo de Certificação de Produtos] proceder a necessária avaliação de conformidade aos padrões e especificações técnicas mínimos estabelecidos;

A [Pessoa Jurídica] e o [Organismo de Certificação de Produtos] firmam o presente instrumento sob as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DEFINIÇÕES

Para os fins deste instrumento, entende-se por:

1.1. Informações: os dados, os documentos e os materiais que lhe sejam pertinentes;

1.2. Informações Confidenciais: todas e quaisquer informações fornecidas, comunicadas ou reveladas pela [Pessoa Jurídica] ao [Organismo de Certificação de Produtos], cujo conhecimento irrestrito ou divulgação possa acarretar danos à mesma, independentemente do meio ou forma de transmissão;

1.3. Tratamento: significa a consulta, produção, transmissão, conservação, alteração, utilização, acesso e eliminação de informações;

1.4. Sigilo: proteção contra o tratamento não autorizado de informações confidenciais.

CLÁUSULA SEGUNDA - DIVULGAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1. O [Organismo de Certificação de Produtos], a contar da data do efetivo recebimento e/ou conhecimento de informação confidencial, se compromete e se obriga a:
a) manter sob absoluto sigilo, pelo prazo de 15 (quinze) anos, todas as informações confidenciais que lhe forem transmitidas pela [Pessoa Jurídica] visando à certificação de seus Equipamentos de Certificação Digital Padrão ICP-Brasil;
b) utilizar as informações confidenciais, exclusivamente, para a finalidade para a qual as mesmas lhe foram transmitidas;
c) não conferir tratamento às referidas informações confidenciais em benefício próprio ou de terceiro, para qualquer finalidade;
d) proteger as informações confidenciais contra a divulgação a terceiros;
e) limitar a divulgação das informações confidenciais recebidas nos termos deste instrumento a pessoas dentro de sua organização ou a seus prestadores de serviço, que no desenvolvimento de suas atividades tenham necessidade de conhecê-las; e
f) instruir devidamente as pessoas responsáveis pelo tratamento das informações confidenciais a proteger e manter a confidencialidade das mesmas.

2.2. O [Organismo de Certificação de Produtos], para fins de sigilo, obriga-se por seus administradores, servidores e prestadores de serviços.

CLÁUSULA TERCEIRA - LIMITAÇÃO DAS OBRIGAÇÕES

3.1. Não são consideradas informações confidenciais para fins do presente Termo de Sigilo aquelas que:
a) ao tempo de sua transmissão ao [Organismo de Certificação de Produtos], ou posteriormente, sejam ou venham a ser de conhecimento público, conforme evidenciado por publicações idôneas, desde que sua divulgação não tenha sido causada pelo próprio [Organismo de Certificação de Produtos];
b) já estivessem na posse legal do [Organismo de Certificação de Produtos] por ocasião da divulgação, desde que tenham sido recebidas legitimamente de terceiro, sem violação de obrigação legal e/ou obrigação de sigilo assumida com a [Pessoa Jurídica];
c) forem independentemente tratadas pelo [Organismo de Certificação de Produtos], sem utilização direta ou indireta de informações confidenciais da [Pessoa Jurídica]; ou ficando ressalvado que esta deverá, nesse caso, avisar o [Organismo de Certificação de Produtos] imediatamente, por escrito.
d) forem necessariamente divulgadas pela [Pessoa Jurídica] no cumprimento de ordem judicial, ficando ressalvado que esta deverá, nesse caso, avisar o [Organismo de Certificação de Produtos] imediatamente, por escrito.

CLÁUSULA QUARTA - PROPRIEDADE DAS INFORMAÇÕES CONFIDENCIAIS

4.1. O [Organismo de Certificação de Produtos] concorda que a [Pessoa Jurídica] é, e continuará sendo, a exclusiva proprietária de suas informações confidenciais e de todas as patentes, direitos autorais, segredos, marcas registradas e outros direitos de propriedade intelectual. Nenhuma licença ou transferência de qualquer desses direitos ao [Organismo de Certificação de Produtos] é concedida ou fica implícita nos termos deste instrumento.

CLÁUSULA QUINTA - PRAZO DE VIGÊNCIA

5.1. Este acordo permanecerá em vigor pelo período de 12 (doze) meses a contar da data de sua assinatura, podendo ser prorrogado por igual período por manifestação expressa das partes. As obrigações constantes na Cláusula Segunda - Divulgação das Informações Confidencias, na Cláusula Terceira - Limitação das Obrigações e na Cláusula Quarta - Propriedade das Informações Confidenciais sobreviverão ao prazo de vigência deste instrumento.

CLÁUSULA SEXTA - DISPOSIÇÕES FINAIS

6.1. O [Organismo de Certificação de Produtos] assumirá inteira responsabilidade por qualquer forma de tratamento não autorizado pela [Pessoa Jurídica] de suas informações confidenciais, quando feito por seus administradores, servidores e prestadores de serviço, em violação ao presente Termo de Sigilo.
6.2. Este Termo de Sigilo substitui todos os ajustes anteriores, verbais ou escritos, acordados entre as partes, relativamente à matéria objeto deste instrumento e não poderá ser modificado, alterado ou rescindido, no todo ou em parte, exceto por documento escrito assinado pelo [Organismo de Certificação de Produtos] e pela [Pessoa Jurídica].

CLÁUSULA SÉTIMA – FORO

7.1. Fica eleita a Seção Judiciária do Distrito Federal, como competente para dirimir e julgar quaisquer disputas relacionadas com o presente instrumento, com renúncia a qualquer outro, por mais privilegiado que seja.

E assim, estando justas e contratadas, as partes assinam o presente instrumento, em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo.

_____, ___de_____de_____.

_____

[Pessoa do Procurador(a)]

_____

[Organismo de Certificação de Produtos]

Testemunhas:

Nome:	Nome:
RG:	RG:

OBSERVAÇÕES:
a) todo conteúdo expresso na forma [...] deverá ser substituído pelos dados reais correspondentes do interessado;
b) todos os representantes legais relacionados deverão assinar o presente Termo.

ANEXO E: REQUISITOS MÍNIMOS DE SEGURANÇA PARA LABORATÓRIOS DE ENSAIOS

1. DISPOSIÇÕES GERAIS

1.1 Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos a serem adotados pelos laboratórios de ensaios acreditados para o Programa de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil.

1.2 Os requisitos abaixo informados devem ser critérios para a acreditação pela Cgcre e mantidos atualizados durante seu funcionamento enquanto o laboratório estiver acreditado.

1.3 O laboratório deve ter uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que devem ser seguidos em suas dependências e atividades.

1.4 Deve existir um exemplar da Política de Segurança da Informação no formato impresso disponível para consulta no Nível 1 de segurança do laboratório.

1.5 A Política de Segurança da Informação deve ser seguida por todo pessoal envolvido nos projetos coordenados pelo laboratório, do seu próprio quadro ou contratado.

1.6 Este documento define normas de segurança que devem ser aplicadas nas áreas internas ao laboratório assim como no trânsito de informações e materiais com entidades externas.

1.7 Os requisitos devem ser observados quanto à segurança de pessoal, segurança física, segurança lógica, segurança de rede, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios e análise de registros de eventos.

2 SEGURANÇA DE PESSOAL

2.1 O laboratório deve ter uma Política de Gestão de Pessoas que disponha sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.

2.2 A comprovação da capacidade técnica do pessoal envolvido nos projetos coordenados pelo laboratório deve estar à disposição para eventuais auditorias e fiscalizações.

2.3 Todo pessoal envolvido nos projetos coordenados pelo laboratório, do próprio quadro ou contratado, deve assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.

2.4 O termo de sigilo da informação deve conter cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos desse RAC.

2.5 Aplica-se o termo de sigilo de informações a quaisquer outras entidades que porventura tenham acesso às informações internas e de terceiros, originárias dos projetos coordenados pelo laboratório.

2.6 O laboratório deve ter procedimentos formais de apuração e responsabilização em caso de

descumprimento das regras estabelecidas pelas suas políticas ou por esse RAC.

2.7 O pessoal do laboratório e contratados devem possuir um dossiê contendo os seguintes documentos:

a) contrato de trabalho ou cópia das páginas da carteira de trabalho onde consta o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;
b) Currículo Lattes devidamente cadastrado no CNPq.
c) Comprovante da verificação de antecedentes criminais.
d) Comprovante da verificação de situação de crédito.
e) Comprovante da verificação de histórico de empregos anteriores.
f) Comprovação de residência.
g) Comprovação de capacidade técnica.
h) Resultado da entrevista inicial, com a assinatura do entrevistador.
i) Declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir os requisitos desse RAC.
j) Termo de sigilo.

2.8 Não são admitidos estagiários no exercício das atividades do laboratório.

2.9 Quando da demissão, o referido dossiê deve possuir os seguintes documentos:

a) Evidências de exclusão dos acessos físico e lógico nos ambiente do laboratório;
b) Declaração assinada pelo empregado ou servidor de que não possui pendências.

3 SEGURANÇA FÍSICA

3.1 O ambiente físico do laboratório deve ser dividido em áreas claramente delimitadas, cada qual com diferentes requisitos de segurança, e organizada em níveis de segurança crescente.

3.2 O laboratório deve ter cinco níveis de segurança, resumidos na tabela a seguir:

Nível	Descrição
1	Atendimento
2	Operação
3	Sensível (Ambiente de Tecnologia da Informação e Ensaios)
4	Depósito
5	Depósito individual

3.3 NÍVEL 1 - ATENDIMENTO

3.3.1 O primeiro nível, ou nível 1, deve situar-se após a primeira barreira de acesso às instalações do laboratório.

3.3.2 Os visitantes, para entrar em uma área de nível 1, devem ter seu acesso autorizado por empregado do laboratório com essa atribuição.

3.3.3 Nenhum tipo de processo operacional ou administrativo do laboratório, excetuando-se recebimento ou devolução de material de ensaio, deve ser executado neste nível.

3.3.4 Excetuados os casos previstos em lei, o porte de armas não será admitido no nível 1 do laboratório.

3.4 NÍVEL 2 – OPERAÇÃO

3.4.1 O segundo nível, ou nível 2, será interno ao primeiro. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo técnico operacional do laboratório.

3.4.2 Deve existir um registro automático dos acessos das pessoas ao nível 2 informando o horário de entrada e o horário de saída.

3.4.3 O acesso de pessoas ao segundo nível deve ser restrito por uma porta com tranca.

3.4.4 Os visitantes podem ter permissão de acesso concedida por empregado do laboratório com essa atribuição

3.4.5 Neste nível, equipamentos de gravação, fotografia, vídeo ou som terão sua entrada controlada e somente podem ser utilizados mediante autorização e supervisão.

3.5 NÍVEL 3 – SENSÍVEL

3.5.1 No terceiro nível, ou nível 3, interior ao segundo, é onde devem ocorrer as atividades especialmente sensíveis da operação do laboratório.

3.5.2 O acesso de pessoas ao nível 3 se dará por uma porta com autenticação automática com a combinação de dois fatores de segurança entre os seguintes: leitora de cartão, biometria e senha individual, devendo todos esses acessos ser obrigatoriamente registrados e mantidos em ambientes redundantes separados.

3.5.3 O acesso e permanência de visitantes neste nível serão permitidos somente quando autorizados e acompanhados por um empregado do laboratório com essa atribuição.

3.5.4 Todos os materiais inseridos e removidos do ambiente nível 3 também devem ser registrados de forma automática (sistema de leitora de código de barras ou similares).

3.5.5 Telefones celulares, *tokens*, mídias de armazenamento, **notebook**, PDA, bem como outros equipamentos portáteis de comunicação e componentes sem-fio (**wireless**), exceto aqueles exigidos para a operação do laboratório, não serão admitidos no nível 3.

3.5.6 Podem existir vários ambientes de nível 3, com as seguintes áreas:

a) Ambiente de Tecnologia da Informação.
b) Laboratório de ensaios.

3.5.7 O Ambiente de Tecnologia da Informação deve acomodar equipamentos como:

a) Equipamentos de rede (**firewall**, roteadores, **switches** e servidores).
b) Servidores do laboratório (arquivos, correio eletrônico, etc.).
c) Servidores de sistemas de segurança.

3.5.8 O acesso ao Ambiente de Tecnologia da Informação deve ser controlado, e somente

pessoas que necessitem realizar atividades de instalação, suporte ou manutenção de servidores, equipamentos e sistemas devem ter permissão de acesso físico.

3.5.9 Nenhum ativo de ensaio deve ser retirado do nível 3 exceto no momento de sua devolução ao solicitante de Laudo de Conformidade ou para os níveis 4 e 5 do próprio laboratório.

3.6 NÍVEL 4 – SALA DEPÓSITO

3.6.1 O quarto nível, ou nível 4, interior ao nível 3, refere-se a uma sala, um cofre ou um gabinete reforçado trancado.

3.6.2 Ativos físicos de ensaio e ativos eletrônicos de ensaio armazenados em mídia removível devem ser guardados em ambiente de nível 4 ou superior.

3.6.3 Para garantir a segurança do material armazenado, a sala, o cofre ou o gabinete deve possuir tranca com chave.

3.6.4 O nível 4 deve possuir os mesmos controles de acesso do nível 3 a cada acesso ao ambiente, conforme o item 3.5.2.

3.6.5 Deve existir um livro de acesso, ou aplicativo destinado a esse fim, no qual deve ser registrado o motivo do acesso ao nível.

3.7 NÍVEL 5 – DEPÓSITO INDIVIDUAL

3.7.1 O quinto nível, ou nível 5, interior ao ambiente de nível 4, pode ser composto de dois tipos de depósitos, de acordo com o tipo de ativo armazenado:

a) Depósito físico: deve consistir de pequenos depósitos localizados no interior do nível 4. Cada um desses depósitos deve dispor de fechadura individual. Deve existir um livro-ata de custódia de material, individual para cada depósito, no qual devem constar os itens retirados ou devolvidos e o motivo da transferência;

b) Depósito eletrônico: deve consistir de uma hierarquia de diretórios ou arquivos individuais protegidos com criptografia (envelope digital). O sistema responsável pela criptografia dos arquivos deve possuir registros de todas as ações críticas, como os responsáveis por cifrar e decifrar os documentos, quando aconteceu e quem realizou tais operações. O servidor que hospeda tais depósitos deve estar localizado em um ambiente nível 3. O acesso a material associado a cada depósito eletrônico deve ser controlado por meio de um sistema de registros eletrônicos e outro manual de contingência (como um livro de controle de acesso), manual este em que devem constar os itens acessados e o motivo do acesso.

3.8 DISPOSIÇÕES GERAIS DE SEGURANÇA FÍSICA

3.8.1 O ambiente físico do laboratório deve conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos.

3.8.2 O laboratório deve conter imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente.

3.8.3 É mandatório o sincronismo de data e hora entre os mecanismos de segurança física garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem.

3.8.4 Todos que transitam no ambiente físico do laboratório devem portar crachás de identificação, inclusive os visitantes.

3.8.5 Só é permitido o trânsito de material de terceiros pelos ambientes físicos do laboratório mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação.

3.8.6 O laboratório deve conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico.

3.8.7 Todo material crítico inservível, descartável ou não mais utilizável deve ter tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção deve ter seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do laboratório.

3.8.8 Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, devem estar inventariados com informações que permitam a identificação inequívoca.

3.8.9 Em caso de inoperância dos sistemas automáticos, o controle de acesso físico deve ser realizado provisoriamente por meio de um livro de registro onde constará quem acessou, a data, hora e o motivo do acesso.

3.8.10 Devem ser providenciados mecanismos para garantir a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote.

4 SEGURANÇA LÓGICA

4.1 O acesso lógico ao ambiente computacional do laboratório se dará no mínimo mediante usuário individual e senha, que deve ser trocada periodicamente.

4.2 Todos os equipamentos do parque computacional devem ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas.

4.3 Os equipamentos devem ter mecanismos de bloqueio de sessão inativa.

4.4 O laboratório deve ter explícita a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários devem estar cadastrados em perfis de acesso que permitam privilégio mínimo para realização de suas atividades.

4.5 Os usuários especiais (a exemplo do **root** e do **administrator**) de sistemas operacionais, de banco de dados e de aplicações em geral devem ter suas senhas segregadas de forma que o acesso lógico a esses ambientes se dê por pelo menos duas pessoas autorizadas. Toda e qualquer alteração feita no sistema, banco de dados e aplicações deve ser registrada.

4.6 Todo equipamento do laboratório deve ter **log** ativo e seu horário sincronizado com uma fonte

confiável de tempo.

4.7 As informações como **log**, trilhas de auditoria, registros de acesso (físico e lógico) e imagens devem ter cópia de segurança cujo armazenamento será de 5 anos.

4.8 Os softwares dos sistemas operacionais, os antivírus e aplicativos de segurança devem ser mantidos atualizados.

5 SEGURANÇA DE REDE

5.1 O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

5.2 Não podem ser admitidos acessos do mundo externo a rede interna do laboratório. As tentativas de acessos externos devem ser inibidas e monitoradas por meio de aplicativos que criem barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão.

5.3 Devem ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada 3 meses. Os testes na rede devem ser documentados e as vulnerabilidades detectadas corrigidas.

6 CLASSIFICAÇÃO DA INFORMAÇÃO

6.1 Toda informação gerada e custodiada pelo laboratório deve ser classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação.

6.2 A classificação da informação no laboratório deve ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada.

6.3 A informação pode ser classificada em:

a) Público: qualquer ativo de informação, de propriedade do laboratório ou não, que pode vir ao público sem maiores consequências danosas ao funcionamento normal do laboratório. Pode ser acessado por qualquer pessoa, seja interna ou externa ao laboratório. Integridade da informação não é vital.

b) Pessoal: qualquer ativo de informação relacionado à informação pessoal. Por exemplo: mensagem pessoal de correio eletrônico, arquivo pessoal, dados pessoais, etc.

c) Interna: qualquer ativo de informação, de propriedade do laboratório ou não, que não seja considerada pública. Ativo de informação relacionado às atividades do laboratório que é direcionada estritamente para uso interno. A divulgação não autorizada do ativo de informação poderia causar impacto à imagem do laboratório. Por exemplo: código fonte de programa, cronograma de atividades, atas de reuniões, etc.

d) Confidencial: qualquer ativo de informação que seja crítico para as atividades do laboratório em relação ao sigilo e integridade. Qualquer material e informação recebida para ensaio, assim como qualquer resultado do ensaio (como relatório) deve ser considerado confidencial.

6.4 Caso o Laboratório seja entidade da Administração Pública Federal - APF, devem ser aplicadas as disposições do Decreto nº 4.553/2002 e demais normas aplicáveis à APF, no que couber.

7 SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

7.1 O laboratório deve, em sua Política de Segurança da Informação, definir como será realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado **backup**.

7.2 A salvaguarda de ativos da informação, backup, deve seguir as mesmas restrições de segurança do ativo da informação que está sofrendo backup, descritas no item 3.7.1.

7.3 A salvaguarda de ativos da informação deve ter descritas as formas de execução dos seguintes processos:

a) Procedimentos de **backup**;
b) Indicações de uso dos métodos de **backup**;
c) Tabela de temporalidade;
d) Local e restrições de armazenamento e salvaguarda em função da fase de uso;
e) Tipos de mídia;
f) Controles ambientais do armazenamento;
g) Controles de segurança.
h) Teste de restauração de **backup**.

7.4 O laboratório deve ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

8 GERENCIAMENTO DE RISCOS

O laboratório deve ter um processo de gerenciamento de riscos, atualizado, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando à elaboração de planos de ação apropriados para proteção aos componentes ameaçados atualizado, no mínimo, anualmente.

9 PLANO DE CONTINUIDADE DE NEGÓCIOS

Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado no laboratório, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.

10 ANÁLISES DE REGISTROS DE EVENTOS

Todos os registros de eventos (**logs**, trilhas de auditorias e imagens) devem ser analisados, no mínimo, mensalmente e um relatório deve ser gerado com assinatura do responsável pelo laboratório.

INMETRO	**ANEXO II - ESPECIFICAÇÃO DE SELO DE IDENTIFICAÇÃO DA CONFORMIDADE**

II.1. O Selo de Identificação da Conformidade deve ser marcado no próprio Equipamento de Certificação Digital Padrão ICP-Brasil, impresso ou aposto à embalagem ou, simplesmente, impresso no Certificado de Conformidade.

II.2. Quando o Selo de Identificação da Conformidade não for marcado no próprio Equipamento de Certificação Digital Padrão ICP-Brasil ou impresso ou aposto à embalagem ou impresso, a comprovação de cumprimento dos requisitos de avaliação de conformidade deve ser feita por meio do Certificado de Conformidade.

II.3. O Selo de Identificação da Conformidade deve ser escrito em português, podendo ser utilizado outros idiomas em caso de exportação.

II.4. O Selo de Identificação da Conformidade não deve ser aposto em acessórios ou partes removíveis do produto. Na embalagem do produto a aposição do Selo de Identificação da Conformidade pode ser feita por impressão, clichê ou colagem.

II.5. O Selo de Identificação da Conformidade deve possuir as seguintes características dimensionais e construtivas:

Fundo claro:

Fundo escuro:

Redução máxima