RESOLUÇÃO CG ICP-BRASIL Nº 185, DE 18 DE MAIO DE 2021

Aprova a versão revisada e consolidada do documento Critérios e Procedimentos para Realização de Auditorias nas Entidades da ICP-Brasil – DOC-ICP-08.

A COORDENADORA DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6°, §1°, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4° da Medida Provisória n° 2.200-2, de 24 de agosto de 2001, em reunião ordinária, realizada em sessão por videoconferência em 18 de maio de 2021,

CONSIDERANDO a determinação estabelecida pelo Decreto n° 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,

RESOLVEU:

Art. 1° Esta Resolução aprova a versão revisada e consolidada do documento Critérios e Procedimentos para Realização de Auditorias nas Entidades da ICP-Brasil.

Art. 2° Fica aprovada a versão 5.0 do documento DOC-ICP-08 – Critérios e Procedimentos para Realização de Auditorias nas Entidades da ICP-Brasil.

Art. 3° Ficam revogadas:

I - a Resolução n° 44, de 18 de abril de 2006;

II - a Resolução n° 72, de 18 de novembro de 2009;

III - a Resolução n° 114, de 30 de setembro de 2015;

IV – a Resolução n° 119, de 06 de julho de 2017;

V - a Resolução n° 130, de 19 de setembro de 2017;

VI - a Resolução n° 145, de 07 de novembro de 2018; e

VII - a Resolução n° 155, de 03 de dezembro de 2019.

Art. 4° Esta Resolução entra em vigor em 1° de junho de 2021.

JULIANA RIBEIRO SILVEIRA

Assinado de forma digital por JULIANA RIBEIRO SILVEIRA
Dados: 2021.05.18 18:03:31 -03'00'

JULIANA RIBEIRO SILVEIRA

Infraestrutura de Chaves Públicas Brasileira

ANEXO

CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES DA ICP-BRASIL

DOC-ICP-08

Versão 5.0

18 de maio de 2021

SUMÁRIO

Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução CG ICP-Brasil nº 185, de 18.05.2021 Versão 5.0		Revisão e consolidação conforme o Decreto nº 10.139, de 28 de novembro de 2019.
Resolução nº 155, de 03.12.2019 Versão 4.7	3.1	Alteração nas previsões de entidades para execução de auditorias.
Resolução nº 151, de 30.05.2019 Versão 4.6	1.4, 2.1, 3.1, 4, 5, 6.1.1, 6.1.12, 7.1, 7.7, 8.2, 9.6 e 9.10	Simplificação dos processos da ICP-Brasil.
Resolução nº 145, de 07.11.2018 Versão 4.5	7.5	Altera item que trata de requisitos para auditoria independente.
Resolução nº 132, de 10.11.2017 Versão 4.4	1.1, 2, 3.1, 4.1, 4.2, 5.5,	Institui o Prestador de Serviço de Confiança.
Resolução nº 130, de 06.07.2017 Versão 4.3	5.2.”c” e 5.3	Ajuste nos critérios do Plano Anual de Auditoria Operacional para AR e suas instalações técnicas.
Resolução nº 119, de 06.07.2017 Versão 4.2	4.2 e 6.1.1	Aprova a obrigatoriedade de realização de auditorias WebTrust e de implementação de respostas OCSP para certificados do tipo SSL/TLS.
Resolução n° 114, de 30.09.2015 Versão 4.1	2.a, 3.1(tabela), 4.1.a, 4.5.a, 5.4 (novo)	Estabelece o funcionamento do sistema biométrico da ICP-Brasil.
Resolução nº 72, de 18.11.2009 Versão 4.0	Diversos	Revogada pela Resolução 56.
Resolução nº 56, de 19.11.2008 Versão 3.0	1.5, 2.2, 2.4, 3.1, 3.7, 5.2, 5.3, 5.4, 7.3, 8.1,	Inclusão de referências a Autoridades de Carimbo de Tempo

	8.2, 8.3, 8.4, 8.5, 8.6, 9.5	
Resolução nº 44, de 18.04.2006 Versão 2.0	Diversos	Criação do DOC-ICP-08, consolidando documentos anteriores.
Resolução nº 24, de 28.08.2003 Versão 1.0		Criação do DOC-ICP-08, consolidando documentos anteriores, revogada pela Resolução 44.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
ABR	Auditoria Baseada em Risco
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo de Tempo
AR	Autoridade de Registro
AUDIBRA	Instituto dos Auditores Internos do Brasil
CFC	Conselho Federal de Contabilidade
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CGAFI	Coordenação Geral de Auditoria e Fiscalização
CGU	Controladoria Geral da União
CISA	*Certified Information System Auditor*
CISM	*Certified Information Security Manager*
CISSP	*Certified Information Systems Security Professional*
CNAI	Cadastro Nacional de Auditores Independentes
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations*
CRE	Comitê Administrador do Programa de Revisão Externa de Qualidade
CVM	Comissão de Valores Mobiliários
DAFN	Diretoria de Auditoria, Fiscalização e Normalização
DOU	Diário Oficial da União
FGTS	Fundo de Garantia do Tempo de Serviço

IBRACON	Instituto dos Auditores Independentes do Brasil
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IIA	*The Institute of Internal Auditors*
ISACA	*Information Systems Audit and Control Association*
PAF	Processo Administrativo de Fiscalização
PC	Política de Certificado
PDF	*Portable Document Format*
PLAAO	Plano Anual de Auditoria Operacional
PSBio	Prestador de Serviço Biométrico
PSC	Prestadores de Serviço de Confiança
PSCert	Prestadores de Serviço de Certificação
PSS	Prestadores de Serviço de Suporte
RF	Relatório de Fiscalização
SHA	*Secure Hash Algorithm*
SICAF	Sistema de Cadastramento Unificado de Fornecedores
TCU	Tribunal de Contas da União

1 DISPOSIÇÕES GERAIS

1.1 Este documento regula, no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, as atividades de auditoria a serem realizadas em sua cadeia de certificação digital.

1.2 O código de ética e os princípios éticos para o exercício das atividades de auditoria interna e independente estabelecidos pelos diversos órgãos reguladores ou de classe (TCU, CGU, CFC, CVM, IBRACON, ISACA, AUDIBRA e IIA) integram, para todos os fins, este normativo. As demais normas emitidas pelos citados órgãos serão observadas naquilo em que não conflitarem com este documento.

1.3 No presente documento o conceito de METODOLOGIA de auditoria se refere a todo o instrumental necessário à realização de trabalhos de auditoria como: manuais, roteiros, papéis de trabalho, mapa de riscos, procedimentos, técnicas, formulários, relatórios e modelos.

1.4 Toda correspondência tratada neste documento deve ser formalizada, preferencialmente, por meio de correio eletrônico, em formato PDF, com assinatura digital ICP-Brasil da autoridade competente. Os arquivos devem ter calculados os respectivos *hashes*, com algoritmo SHA-1, cujos valores serão relacionados em arquivo no formato texto puro (extensão TXT), contendo o nome do arquivo e o respectivo *hash*, separados por ponto e vírgula (;).

1.5 Todas as comunicações e requerimentos à AC Raiz deverão ser encaminhados por intermédio da cadeia de AC, ou candidatos à AC, operacionalmente vinculados. Inicia-se a tramitação pela AC de nível imediatamente superior ao do interessado. A tramitação prossegue, a partir daí, respeitando a hierarquia de AC, até chegar à AC Raiz.

1.6 As notificações e intimações de que trata este documento serão realizadas, preferencialmente, por correio eletrônico assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente.

2 TIPOS DE AUDITORIA

2.1 As auditorias são classificadas em PRÉ-OPERACIONAIS e OPERACIONAIS, a saber:

a) Pré-operacionais: são as auditorias realizadas antes do início das atividades do candidato a Prestador de Serviço de Certificação (PSCert), quer seja Autoridade Certificadora (AC), Autoridade de Carimbo do Tempo (ACT), Autoridade de Registro (AR), Prestador de Serviço de Suporte (PSS), Prestador de Serviço Biométrico (PSBio) ou PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas; e

b) Operacionais: são as auditorias realizadas anualmente, considerado o ano civil, em todos os PSCerts para manutenção do credenciamento junto à ICP-Brasil. Tais auditorias ocorrerão a partir do primeiro ano civil seguinte à data da publicação no DOU do credenciamento do PSCert.

3 ENTIDADES QUE PODEM REALIZAR AUDITORIAS

3.1 As auditorias na cadeia da ICP-Brasil são realizadas exclusivamente pelo Comitê Gestor da ICP-Brasil, pelo Instituto Nacional de Tecnologia da Informação (ITI) ou por entidades credenciadas para o fim, observada a seguinte tabela:

ENTIDADE	EXECUTOR DA AUDITORIA	
	Pré-operacional	**Operacional**
AC Raiz	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados
AC de 1º Nível, e seus PSS	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
AC subsequente e seus PSS	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
ACT	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
AR	AC ou PSS credenciados junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI AC ou PSS credenciados junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
AR no Exterior	ITI/DAFN/CGAFI ou, a seu critério, AC ou PSS credenciados junto ao ITI	AC credenciada junto ao ITI Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI

PSBio	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas	ITI/DAFN/CGAFI	Empresa de Auditoria Independente, credenciada junto ao ITI

3.1.1 A AC de 1º nível é aquela cujo certificado é emitido pela AC Raiz e AC subsequente é aquela cujo certificado não é emitido pela AC Raiz.

3.2 O ITI poderá, a seu exclusivo critério ou por determinação do Comitê Gestor, executar auditorias pré-operacionais e operacionais em quaisquer das entidades integrantes ou candidatas a integrar a ICP-Brasil, utilizando servidores do quadro próprio do ITI/DAFN/CGAFI, devidamente qualificados.

3.3 As auditorias operacionais realizadas pelo ITI com base na prerrogativa do item anterior, não suprem a exigência de realização de auditoria operacional a ser realizada em conformidade com o item 2.1.“b” acima.

4 CREDENCIAMENTO DE EMPRESAS DE AUDITORIA INDEPENDENTE E ÓRGÃOS DE AUDITORIA INTERNA

4.1 São dois (2) os tipos de entidades credenciadas para realizar auditoria na cadeia da ICP-Brasil:

a) Tipo 1: entidades autorizadas a realizar auditoria em AC, ACT, AR, PSBio, PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas, com respectivos PSSs. Este tipo é destinado às empresas de auditoria independente cadastradas junto ao CNAI.

b) Tipo 2: entidades autorizadas a realizar auditoria somente em AR. Este tipo é destinado às empresas enquadradas na alínea anterior e às unidades de Auditoria Interna formalmente instituídas.

4.2 As entidades de auditoria independente candidatas a realizar trabalhos de auditoria na cadeia da ICP-Brasil indicarão o tipo a que pleiteiam e apresentarão o formulário ADE-ICP-08.A[1], anexando:

a) documentação demonstrando que a estrutura organizacional e a metodologia de auditoria são claras e, formalmente definidas, para permitir a realização de trabalhos de auditoria;

b) documentação indicando que o sistema de controle de qualidade formalmente estabelecido atende às normas profissionais vigentes e são adotados procedimentos que garantam o seu cumprimento na realização dos trabalhos de auditoria;

c) comprovação de constituição legalmente registrada, onde conste a atividade de auditoria de sistemas ou de tecnologia da informação no objeto social da candidata;

d) comprovação de inscrição no Cadastro Nacional da Pessoa Jurídica;

e) comprovação de inscrição estadual e municipal, relativo ao domicílio sede da candidata;

f) certidões negativas de débito junto as fazendas Federal, Estadual e Municipal; inclusive Seguridade Social e ao Fundo de Garantia do Tempo de Serviço - FGTS;

g) certidão negativa de falência e de recuperação judicial;

h) certidão negativa de execução patrimonial;

i) declaração de que não está cumprindo nenhuma penalidade da Administração Pública Federal, Estadual e Municipal;

j) declaração de que não foi declarada inidônea nas esferas de Governo Federal, Estadual e Municipal;

k) currículo dos sócios, dos diretores e dos responsáveis técnicos que integram o quadro de auditores com poderes para emitir e assinar relatório de auditoria em nome da candidata;

l) atestado de capacidade técnica, emitido por pessoa jurídica, que comprove a execução de serviços em auditoria de software ou de sistemas de informação, bem como comprove a quantidade de horas de serviços de auditoria prestada;

m) rol dos trabalhos realizados nos últimos 2 (dois) anos, contendo tabela indicando:

   i. a classificação dos serviços realizados;

   ii. a quantidade de auditores alocados em cada serviço; e

   iii. a quantidade de horas de auditoria em cada trabalho.

n) cópia de dois trabalhos de auditoria realizados em ambiente de TI, que tenham sido realizados nos dois últimos anos, contendo relatórios e respectivos papéis de trabalho;

   i. caso a empresa esteja impedida de apresentar a documentação por força de sigilo profissional, poderá dar vistas ao ITI aos dois últimos trabalhos; ou,

   ii. apresentar relatório de avaliação executado por outra empresa de auditoria, no programa de avaliação pelos pares, denominado Comitê Administrador do Programa de Revisão Externa de Qualidade (CRE).

o) comprovação de inscrição no CNAI – Cadastro Nacional de Auditores Independentes; e

p) comprovação de licenciamento WebTrust, para entidades interessadas em realizar auditorias do Tipo 1.

4.3 As entidades de auditoria interna candidatas a realizar trabalhos de auditoria na cadeia da ICP-Brasil só poderão pleitear o credenciamento para o tipo 2 e apresentarão o formulário ADE-ICP-08.B[2], anexando:

a) a documentação estabelecida nas alíneas “a”, “b”, “k”, “m” e “n” do item 4.2 anterior;

b) comprovação de estar formalmente constituída, com vinculação direta ao principal órgão administrador ou controlador da empresa onde estiver inserida ou instituída por força de dispositivo legal.

4.4 As unidades de auditoria interna credenciadas só poderão realizar trabalhos de auditoria no âmbito da própria empresa onde inseridas, isto é, que possuam o mesmo CNPJ ou radical de CNPJ.

4.5 As empresas de auditoria independente autorizadas a realizar auditorias no âmbito da ICP-Brasil atenderão aos seguintes requisitos mínimos, que serão avaliados e considerados quando do exame do pedido de credenciamento:

a) para o tipo 1: experiência comprovada de pelo menos 2 (dois) anos em:

   i. áreas de segurança da informação (ambiente físico e lógico), criptografia, infraestrutura de chaves públicas, segurança patrimonial e sistemas de processamento eletrônico de informações;

   ii. utilização de pelo menos um dos padrões de auditoria reconhecidos internacionalmente, como por exemplo: COBIT, "Webtrust", ABR ou COSO;

   iii. caso de PSBio, áreas de sistema biométrico (ambientes físicos e lógicos), criptografia, segurança patrimonial, protocolos de comunicação em rede e sistemas de processamento eletrônico de informações.

b) para o tipo 2: deverão possuir corpo técnico de auditores com experiência comprovada de pelo menos 2 (dois) anos em:

   i. segurança da informação, segurança patrimonial e nível básico de sistemas de processamento eletrônico de informações;

   ii. utilização de pelo menos um dos padrões reconhecidos internacionalmente de avaliação gerencial ou de gestão, como por exemplo: COBIT, COSO ou ABR.

4.6 Para as empresas de auditoria candidatas ao credenciamento para o tipo 1, é desejável que o corpo técnico de auditores possua alguma certificação internacional (CISA-*Certified Information System Auditor*; CISM-*Certified Information Security Manager*, CISSP-*Certified Information Systems Security Professional*, etc).

4.7 O pedido de credenciamento deve ser encaminhado ao Protocolo Geral da AC Raiz, assinado pela entidade candidata, anexando os arquivos eletrônicos, conforme item 1.4.

4.8 O ITI poderá solicitar a complementação da documentação, só voltando a ser contado o prazo a partir do recebimento do que for solicitado.

4.9 Se a solicitação não for atendida em até 15 (quinze) dias, o processo será arquivado, mediante despacho fundamentado da DAFN.

4.10 A documentação apresentada pela candidata para credenciamento constituirá processo específico, por prazo não inferior a 5 (cinco) anos, exceto quanto à eventual documentação de auditorias realizadas, que será considerada confidencial, ficando à disposição apenas dos próprios solicitantes do credenciamento.

4.11 Sobre o pedido de credenciamento ou de renovação, o Diretor da DAFN, por meio de despacho fundamentado, poderá:

a) deferir o pedido;

b) notificar a candidata para, no prazo máximo de 15 (quinze) dias corridos, complementar a documentação apresentada;

c) indeferir o pedido se, vencido o prazo da alínea “b”, não forem cumpridas as exigências constantes da notificação retromencionada; e

d) indeferir o pedido que não atenda aos requisitos técnicos estabelecidos.

4.12 O credenciamento será publicado no Diário Oficial da União - DOU e será renovado a cada cinco (5) anos, a contar da data da publicação do respectivo credenciamento ou renovação.

4.13 Nas renovações, mediante solicitação à DAFN, a entidade de auditoria anexará a mesma documentação apresentada para o credenciamento inicial, podendo, para os documentos que não sofreram alteração desde o último deferimento, serem substituídos por declaração expressa do Representante Legal, sob as penas da lei. Nestes casos, serão renovadas as certidões negativas fisco tributárias exigíveis.

4.14 As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores - SICAF, registro oficial do Poder Executivo Federal, poderão, para fins de comprovação da situação tributária federal, apresentar seu extrato em substituição às respectivas certidões negativas exigíveis, que será complementado pelas certidões estaduais e municipais exigíveis, se for o caso.

4.15 Qualquer alteração ocorrida, quer seja em atos constitutivos, estatuto, contrato social, organograma ou vinculação da entidade, quer seja dos dirigentes ou da equipe técnica de auditores, será submetida imediatamente ao conhecimento da DAFN, mediante formalização protocolada no Protocolo Geral da AC Raiz e que fará parte do processo de credenciamento da respectiva entidade de auditoria. Nestes casos será reavaliada a manutenção das condições exigidas para o credenciamento, observadas as regras para as renovações, podendo ser dispensada a apresentação de certidões ainda não exigíveis.

4.16 A apresentação de documentos para fins de credenciamento ou descredenciamento será sempre por meio eletrônico, com assinatura digital da cadeia da ICP-Brasil.

4.17 É responsabilidade das entidades de auditoria credenciadas a solicitação à AC Raiz da atualização de seus dados e certidões no Cadastro de Entidades de Auditoria Credenciadas, observando o item 1.4.

4.18 A entidade de auditoria credenciada poderá solicitar o descredenciamento à AC Raiz, a qualquer tempo.

4.19 Indeferido o pedido de credenciamento ou de renovação de credenciamento, a DAFN notificará diretamente ao interessado, por meio de ofício, procedendo aos ajustes cabíveis nos registros de empresas de auditoria credenciadas.

4.20 A AC Raiz deverá, no prazo de 15 (quinze) dias corridos, a contar do deferimento do credenciamento, da renovação ou do recebimento do pedido de descredenciamento, atualizar o Cadastro de Auditorias Independentes, disponível no endereço http://www.iti.gov.br.

5 PLANO ANUAL DE AUDITORIA OPERACIONAL (PLAAO)

5.1 Cada AC e ACT protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, contemplando todos os PSCerts diretamente subordinados (AC subsequente e AR), por meio do formulário ADE-ICP-08-C[3].

5.2 As auditorias operacionais serão realizadas anualmente nos seguintes PSCerts:

a) AC credenciada e respectivos PSSs;

b) ACT credenciada e respectivos PSSs;

c) AR credenciada.

5.3 Cada PSBio protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, contemplando os PSSs subordinados, por meio do formulário ADE-ICP-08-C[3].

5.4 Cada PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, por meio do formulário ADE-ICP-08.C [3].

6 REALIZAÇÃO DAS AUDITORIAS

6.1 Aspectos gerais da realização das auditorias

6.1.1 As auditorias têm por objetivo avaliar se os processos, procedimentos, atividades e controles estão em conformidade com as respectivas Políticas, Declaração de Práticas, Política de Segurança e demais normas e procedimentos estabelecidos pelo Comitê Gestor da ICP-Brasil. O documento ADE-ICP-08-E[4] detalha os processos que compõem a cadeia de certificação e deverá nortear as auditorias realizadas na cadeia da ICP-Brasil. Adicionalmente, as auditorias do tipo 1 também devem avaliar os princípios e critérios definidos pelo *WebTrust*.

6.1.2 Cada PSCert manterá dossiê de auditoria, preferencialmente em meio digital, organizado e constituído de pastas, contendo cada uma:

a) os relatórios de auditoria pré e operacionais,

b) as evidências de regularização das não conformidades identificadas e apontadas em relatórios de auditoria,

c) as correspondências trocadas sobre a regularização de inconformidades.

6.1.3 Os relatórios de auditoria deverão concluir sobre os processos e procedimentos de responsabilidade do PSCert sob avaliação, manifestando sobre a suficiência dos controles executados para mitigação dos riscos existentes, devendo observar os Critérios para Emissão de Parecer de Auditoria na ICP-Brasil definidos por Instrução Normativa da AC Raiz.

6.1.4 A entidade de auditoria, no exercício de suas atividades no âmbito da ICP-Brasil, deve cumprir e fazer cumprir, por seus prepostos e empregados, as normas da ICP-Brasil, observadas ainda as normas para o exercício da profissão de auditor independente ou interno, conforme o caso.

6.1.5 As auditorias serão executadas em conformidade e aderência com a metodologia que deu base ao credenciamento da entidade responsável pela execução da auditoria.

6.1.6 Os serviços de auditoria serão executados diretamente pela entidade de auditoria credenciada junto à ICP-Brasil, vedada a subcontratação total ou parcial dos serviços.

6.1.7 O auditor, no exercício de suas funções, terá livre acesso a todas as dependências da entidade auditada, assim como aos documentos e registros indispensáveis ao cumprimento de suas atribuições, não lhe podendo ser sonegado, sob qualquer pretexto, documentos, acessos ou informações.

6.1.8 A entidade auditada deve fornecer ao auditor todos os elementos e condições necessárias ao perfeito desempenho de suas funções.

6.1.9 Os Papeis de Trabalho, registros e demais elementos materiais que deram subsídio à elaboração dos relatórios ficarão sob a guarda da entidade executante da auditoria, pelo prazo mínimo de 5 (cinco) anos. A AC Raiz, a qualquer tempo e a seu critério, poderá solicitar cópia do material, fixando prazo para entrega, preferencialmente por meio eletrônico, observado o item 1.4.

6.1.10 O relatório final de auditoria será emitido com a seguinte destinação:

a) original, entidade auditada;

b) cópia, AC subordinante, se for o caso, ou a ACT responsável;

c) cópia à AC de primeiro nível, se for o caso; e

d) cópia, ITI.

6.1.11 A cópia do relatório de auditoria destinada ao ITI será entregue à Diretoria de Auditoria, Fiscalização e Normalização do ITI, observado item 1.4, diretamente pela entidade de auditoria. pré-relatórios ou relatórios parciais não devem ser encaminhados ao ITI.

6.1.12 No caso de uma AC optar por auditar com seus profissionais suas ARs, deverá observar o disposto nos itens acima, excetuados os itens 6.1.5 e 6.1.6.

6.2 Aspectos específicos das auditorias pré-operacionais

6.2.1 Também nos relatórios de auditoria pré-operacional, serão emitidos conceitos de auditoria para os candidatos a PSCert em conformidade com os Critérios para Emissão de Parecer de Auditoria na ICP-Brasil definidos por Instrução Normativa da AC Raiz.

6.2.2 Nos casos em que for identificada qualquer não conformidade, o relatório de auditoria só será encaminhado ao ITI após a certificação, pela entidade de auditoria, da regularização das inconformidades encontradas. A entidade de auditoria deverá anexar as evidências das regularizações ao relatório de auditoria pré-operacional.

6.3 Aspectos específicos das auditorias operacionais

6.3.1 O relatório de auditoria conterá avaliação do PSCert e respectivos PSSs, podendo estender-se às ARs vinculadas – quando se tratar de auditoria em AC –, e conceituará o PSCert auditado, em conformidade com os Critérios para Emissão de Parecer de Auditoria na ICP-Brasil definidos por Instrução Normativa da AC Raiz.

6.3.2 Considerando o nível de exposição aos riscos, a entidade de auditoria poderá excluir processos ou subprocessos das avaliações de auditoria, de forma justificada. Tais exclusões e justificativas constarão do corpo do relatório de auditoria ou de anexo específico, a critério da entidade de auditoria e em conformidade com a metodologia apresentada quando do credenciamento da entidade de auditoria.

6.3.3 Nas auditorias operacionais nas ACs, o relatório de auditoria deverá informar se são atendidos os critérios de realização de auditorias operacionais nas ARs subordinadas e se são adotados controles para acompanhamento daquelas auditorias.

7 RELAÇÃO ENTRE OS AUDITORES INDEPENDENTES E AS ENTIDADES AUDITADAS

7.1 Aplica-se ao auditor independente, no que couber, as regras de suspeição e impedimento estabelecidas nos artigos 134 e 135 do Código de Processo Civil; além das demais normas para o exercício da profissão de auditor independente ou interno.

7.2 A empresa de Auditoria Independente ou qualquer de seus auditores serão declarados impedidos de realizar auditoria, quando:

a) houver motivo íntimo declarado;

b) for amigo íntimo ou inimigo capital de membros da entidade auditada;

c) for credor ou devedor da entidade auditada ou de um de seus membros;

d) tiver recebido, nos últimos 5 (cinco) anos, da entidade auditada, pagamentos referentes à prestação de serviços, excetuando-se os recebimentos de valores referentes à prestação de auditoria;

e) tiver interesse no resultado da auditoria a ser realizada; e

f) houver relacionamento, de fato ou de direito, como cônjuge, parente, consanguíneo ou afim, com algum dos membros da entidade auditada, em linha direta ou na colateral até o terceiro grau.

7.2.1 Entende-se como membros da entidade auditada todas as pessoas que de alguma forma participem do capital social ou tenham influência na gestão do PSCert auditado.

7.3 A empresa de auditoria independente e respectivos auditores que participarem dos trabalhos de auditoria no âmbito da ICP-Brasil, firmarão declaração, sob as penas da lei, de que não se enquadram em qualquer das causas de impedimento tratadas neste documento.

7.4 As declarações previstas neste documento constarão como anexos obrigatórios ao relatório de auditoria a ser entregue ao ITI.

7.5 Exceto quanto às entidades de Auditoria Interna, será obrigatória a rotação integral da equipe de auditoria (responsável técnico, diretor, gerente e qualquer outro integrante) e recomendada a rotação das empresas de Auditoria Independente a intervalos menores ou iguais a cinco (5) anos consecutivos, observado o intervalo mínimo de três (3) anos para o retorno.

7.6 As entidades de auditoria independente contratadas por entes da administração pública direta ou indireta (Federal, Estadual ou Municipal) que estejam impedidas do rodízio previsto no item anterior, por força de dispositivo legal, para atenderem a rotatividade estabelecida, quando completarem os cinco anos e durante os próximos três anos dos prazos estabelecidos no item anterior, deverão submeter seus trabalhos à revisão por outra entidade de auditoria, que emitirá relatório circunstanciado sobre a correta aplicação das normas profissionais e técnicas utilizadas nestes trabalhos, encaminhando-o ao ITI.

7.7 Ocorrendo o impedimento da entidade de auditoria, esta deverá concluir os trabalhos cujas atividades de campo já tenham iniciado, estando impedida de iniciar novos trabalhos de campo.

7.7.1 Eventuais relatórios de auditoria recebidos em desacordo com o item 7.7 serão sumariamente arquivados e não terão nenhuma validade perante o ITI, no que se refere ao cumprimento da obrigatoriedade de realização de auditorias.

8 ANÁLISE DO RELATÓRIO DE AUDITORIA PELO ITI

8.1 O relatório de auditoria será analisado pela Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz, que poderá solicitar esclarecimentos ou documentos complementares aos executantes da auditoria ou aos respectivos PSCerts auditados.

8.2 A documentação de auditoria será avaliada em comparação com a metodologia de auditoria aprovada no credenciamento da entidade de auditoria, exceto quando realizado por AC ou PSS diretamente em suas ARs.

8.3 Se, a qualquer tempo, a Diretoria de Auditoria, Fiscalização e Normalização constatar que o relatório de auditoria entregue apresenta incorreções, omissões ou descumprimento de norma profissional de auditoria, comunicará o fato à entidade que executou a auditoria. Neste caso, a entidade de auditoria deverá justificar as incorreções no prazo de 15 (quinze) dias da data do recebimento da notificação.

8.4 Caso a entidade de auditoria não apresente as justificativas ou estas sejam consideradas insatisfatórias, bem como em caso de reincidência no mesmo ou em outro PSCert, o Diretor da DAFN poderá aplicar penalidades, observado o disposto no item 9.13.

9 NÃO CONFORMIDADES EM RELATÓRIOS DE AUDITORIA

9.1 Cabe à entidade auditada cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir as não conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas. Tais regularizações serão comunicadas formalmente à entidade a que se vincula o PSCert auditado, na data de vencimento do prazo concedido no relatório de auditoria.

9.2 Cabe à entidade subordinante do PSCert controlar o cumprimento das recomendações de auditoria das entidades vinculadas, comunicando ao ITI o não cumprimento de recomendações de auditoria, mantendo registros formais do acompanhamento.

9.3 Caso qualquer recomendação não seja cumprida no prazo estabelecido no relatório de auditoria, o PSCert subordinante comunicará o fato ao ITI, anexando cópia de correspondências trocadas, evidências da inconformidade e das ações adotadas até o momento para mitigação do risco envolvido. Essa comunicação será preferencialmente por correio eletrônico assinado por representante legal do PSCert com certificado da ICP-Brasil, observando item 1.4.

9.4 O cumprimento e efetivação das recomendações de auditoria e de sugestões de melhoria acaso existentes no relatório de auditoria, devem ser objeto de análise e manifestação na auditoria subsequente.

9.5 As entidades encarregadas da execução das auditorias manifestarão sobre o atendimento das recomendações da auditoria imediatamente anterior, em documento anexo ao relatório de auditoria a ser emitido.

9.6 No ITI, os casos de não conformidade que ensejaram recomendações à entidade auditada serão acompanhados pela área de auditoria e incluídos nos planos de trabalho de auditorias posteriores na mesma entidade.

9.7 Cabe à AC Raiz tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-Brasil, podendo descredenciar a entidade auditada, mediante decisão motivada.

9.8 Se a entidade auditada for considerada INACEITÁVEL o ITI suspenderá imediatamente suas operações até que as não conformidades sejam solucionadas.

9.9 A entidade cujo conceito atribuído seja cinco (5) – INACEITÁVEL – em duas auditorias operacionais consecutivas, poderá ser descredenciada da ICP-Brasil.

9.10 Na ocorrência do descredenciamento mencionado no item 9.10, a entidade não poderá ter um novo pedido de credenciamento aceito pelo ITI pelo período mínimo de dois (2) anos.

9.11 O descredenciamento será publicado no Diário Oficial da União, em consonância com os demais procedimentos de descredenciamento descritos nas normas da ICP-Brasil.

9.12 Toda vez que um PSCert receber um conceito 3 ou 4 no relatório de auditoria operacional, poderá sofrer penalidades.

9.13 A aplicação de penalidades deve ser precedida de processo administrativo, assegurada a ampla defesa e o contraditório, observados os critérios e o procedimento estabelecidos no DOC-ICP-09 [5].

10 DISPOSIÇÕES FINAIS

10.1 O Diretor da DAFN, em casos de iminente dano irreparável ou de difícil reparação a terceiros, suspenderá cautelarmente, no todo ou em parte, a emissão de certificado e/ou carimbo do tempo pelo respectivo PSCert, podendo a suspensão ser também estendida ao PSCert de nível imediatamente subsequente ou superior àquele.

10.2 É de inteira responsabilidade da entidade de auditoria credenciada a veracidade das informações e documentos apresentados ao ITI.

10.3 A não declaração de fato superveniente que possa desconstituir o teor de documentação já apresentada ou a falsa declaração, pela entidade credenciada ou por qualquer dos auditores que realizaram a auditoria, sujeita-os às penalidades cabíveis.

10.4 A empresa estrangeira que não tenha filial ou representante legal no país atenderá às exigências estabelecidas mediante a apresentação de documentos equivalentes autenticados pelo respectivo consulado e traduzido por tradutor juramentado.

11 DOCUMENTOS REFERENCIADOS

11.1 O documento abaixo é aprovado por Resolução 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 desse documento e a resolução que o aprovou.

REF.	NOME DO DOCUMENTO	CÓDIGO
[5]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003.	DOC-ICP-09

11.2 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE EMPRESA DE AUDITORIA ESPECIALIZADA E INDEPENDENTE	ADE-ICP.08.A
[2]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ÓRGÃO DE AUDITORIA INTERNA	ADE-ICP.08.B
[3]	Modelo de PLAAO – PLANO ANUAL DE AUDITORIA OPERACIONAL	ADE-ICP.08.C
[4]	Descrição dos PROCESSOS DAS ENTIDADES DA ICP-BRASIL	ADE-ICP.08.E