INSTRUÇÃO NORMATIVA ITI Nº 15, DE 10 DE JUNHO DE 2021

Aprova a versão 1.0 do documento Critérios para Aplicação de Penalidades na ICP-Brasil – DOC-ICP-09.01.

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

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

CONSIDERANDO a indicação contida no Anexo da Resolução CG ICP-Brasil n° 186, de 18 de maio de 2021, de que os critérios para Aplicação de Penalidades na ICP-Brasil devem ser definidos por instrução normativa da AC Raiz,

RESOLVE:

Art. 1º Aprovar a versão 1.0 do documento DOC-ICP-09.01 – Critérios para Aplicação de Penalidades na ICP-Brasil, anexa a esta Instrução Normativa.

Art. 2º Esta Instrução Normativa entra em vigor em 1º de julho de 2021.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2021.06.11 18:44:18 -03'00'

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

ANEXO

CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES NA ICP-BRASIL

DOC-ICP-09.01

Versão 1.0

10 de junho de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
IN ITI nº 15, de 10.06.2021 Versão 1.0		Criação do DOC-ICP-09.01, que estabelece os critérios para aplicação de penalidades na ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
CFTV	Circuito Fechado de Televisão
CG ICP-BRASIL	Comitê Gestor da ICP-Brasil
DAFN	Diretoria de Auditoria, Fiscalização e Normalização
FCT	Fonte Confiável do Tempo
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
LCR	Lista de Certificados Revogados
PAF	Processo Administrativo de Fiscalização
PC	Política de Certificado
PSCert	Prestador de Serviço de Certificação
RF	Relatório de Fiscalização

1 DISPOSIÇÕES GERAIS

1.1 Este documento dispõe sobre as infrações e penalidades aplicáveis às entidades auditadas, supervisionadas ou fiscalizadas pelo Instituto Nacional de Tecnologia da Informação – ITI.

1.2 Na aplicação das penalidades estabelecidas serão considerados, na medida em que possam ser determinados:

a) a gravidade e a duração da infração;

b) a relevância do serviço para o ciclo de vida do certificado da ICP-Brasil;

c) o grau de lesão ou o perigo de lesão à ICP-Brasil, à instituição ou a terceiros;

d) a reincidência das condutas nos últimos 5 (cinco) anos; e

e) a colaboração do infrator com o ITI para a apuração da infração.

1.3 O disposto neste documento se aplica às entidades:

a) integrantes ou candidatas a integrar a ICP-Brasil que atuem como operadoras ou prestadores de serviço; e

b) que prestem serviço de auditoria independente e certificação de produtos.

2 DAS PENALIDADES

2.1 O ITI, no exercício das atividades de fiscalização e auditoria, poderá aplicar, pelo descumprimento das obrigações legais e/ou regulamentares, as seguintes penalidades, conforme a gravidade da infração, o grau de culpabilidade e a reincidência.

a) advertência;

b) restrição da realização de determinadas atividades ou modalidades de operação relacionadas ao objeto da fiscalização até que sejam sanadas as irregularidades apontadas no RF;

c) proibição de credenciamento de novas PCs ou de novas vinculações até que sejam sanadas as irregularidades apontadas no RF;

d) suspensão temporária da emissão de novos certificados por prazo determinado ou até que sejam sanadas as irregularidades apontadas no RF; e

e) descredenciamento.

2.1.1 As penalidades previstas podem ser aplicadas isoladas ou cumulativamente.

2.2 A penalidade de **advertência** consistirá na publicação de texto especificado na decisão condenatória, contendo, no mínimo, o nome do apenado, a conduta ilícita praticada e a sanção imposta.

2.2.1 A notícia sobre a imposição da pena de advertência e o texto especificado na decisão condenatória serão publicados na página eletrônica do ITI, sem prejuízo de outras formas de publicação previstas em regulamentação.

2.2.2 A penalidade de **advertência** não impede o normal prosseguimento das atividades e operações do PSCert e será aplicada quando:

a) se tratar de fato já consumado e que não possa ser ou já esteja regularizado, independentemente da criticidade da inconformidade, como, por exemplo, intervalo de tempo sem publicação de LCR; e

b) houver uma ou mais ocorrências classificadas como de baixa criticidade e que não estejam regularizadas, como por exemplo:

i. falha na atualização de informações disponíveis nos repositórios;

ii. falha em inventário de ativos;

iii. falha na emissão do relatório de auditoria, que não comprometa a atribuição de conceito do PSCert auditado, mas esteja em desacordo com a documentação apresentada quando do credenciamento.

2.3 A penalidade de **restrição** de realizar determinadas atividades ou modalidades de operação implicará o impedimento de exercer as atividades as quais foi autorizado, pelo período máximo de 180 (cento e oitenta) dias.

2.3.1 A penalidade de **restrição** será aplicada quando o PSCert incorrer em não conformidades de risco médio ou maior, não regularizada ou com prazo de regularização vencido, como por exemplo:

a) falha na apresentação ou ausência de documentação fisco-tributária do PSCert;

b) falha no processo de treinamento de pessoal do PSCert;

c) falha no processo de avaliação do pessoal do PSCert;

d) falha no sistema de gravação de imagens de CFTV;

e) falha no dossiê de certificado emitido, quanto a documentação, poderes e assinatura;

f) erros ou falhas em campos de certificados emitidos;

g) erros ou falhas em campos de LCR emitidas;

h) falha na apresentação de certidões de pessoal vinculado ao PSCert;

i) falha na manutenção de sistemas de ar-condicionado, sistema elétrico e de combate a incêndio que comprometa as atividades do sítio principal e de contingência da AC;

j) falha na identificação de equipamentos que se conectam à solução de certificação digital da AC;

k) ausência de testes de funcionamento do sítio de contingência;

l) ausência de testes de recuperação de cópia de segurança de LCR, *logs* de aplicativo e base de dados;

m) ausência ou deficiências nos procedimentos de testes de vulnerabilidade de rede;

n) ausência ou falhas na monitoração de ocorrências registradas em *logs*;

o) ausência de licença de *software* proprietário de terceiros;

p) falha nos procedimentos de desligamento de empregados do PSCert, mesmo que sem desligamento da empresa responsável pelo PSCert;

q) atribuição de conceito INACEITÁVEL em Relatório de Auditoria; e

r) for identificada inconsistência no Relatório de Auditoria que fira quaisquer dos princípios da auditoria, mas não comprometa a cadeia de confiança da ICP-Brasil.

2.4 A penalidade de **proibição** de credenciamento de novas PCs ou de novas vinculações impedirá que a entidade credenciada, ou entidades a ela vinculadas, solicite novo credenciamento pelo período máximo de 90 (noventa) dias, ou enquanto durar o descumprimento das obrigações legais especificado nos termos da decisão que a aplicou.

2.4.1 A penalidade de **proibição** de credenciamento de novas PCs ou de novas vinculações será aplicada quando o PSCert incorrer em não conformidades que impliquem prejuízo considerável ao desenvolvimento das atividades autorizadas e/ou configurem sistemática inadimplência do PSCert, como por exemplo:

a) certificado emitido com tamanho de chave inferior ao mínimo estabelecido;

b) LCR – Lista de Certificados Revogados:

i. inexistência de LCR;

ii. intervalo de tempo sem LCR;

iii. LCR sem conteúdo;

iv. LCR com campo errado ou incorreto.

c) ausência de cobertura de seguro de responsabilidade civil;

d) ausência de realização de auditoria operacional anual;

e) qualquer ato intencional de omissão ou manipulação de dados, alteração de documentos ou registros eletrônicos, ou qualquer ato que possa ser enquadrado como fraude;

f) vulnerabilidade em ambiente lógico de segurança de rede;

g) ausência de sincronismo de tempo entre os servidores e Fonte Confiável do Tempo – FCT;

h) uso de algoritmo de criptografia diferente do estabelecido nas normas;

i) ausência de testes de restauração de cópia de segurança de base de dados, de *logs*, de LCR e de certificados digitais;

j) falhas nos sistemas de controle de acesso físico e lógico aos recursos de AC;

k) ausência de sincronismo dos aplicativos de AC entre os sítios principal e de contingência da AC;

l) falha de integridade das aplicações e bases de dados da AC;

m) falha no dossiê de certificado emitido, quanto a documentação, poderes e assinatura;

n) falha na manutenção de sistemas de ar-condicionado, sistema elétrico e de combate a incêndio que comprometa as atividades do sítio principal e de contingência da AC;

o) falha na identificação de equipamentos que se conectam à solução de certificação digital da AC;

p) ausência de testes de funcionamento do sítio de contingência;

q) ausência de testes de recuperação de cópia de segurança de LCR, *logs* de aplicativos e bases de dados;

r) ausência ou deficiências nos procedimentos de testes de vulnerabilidade de rede;

s) ausência ou falhas na monitoração de ocorrências registradas em *logs*;

t) ausência de licença de *software* proprietário de terceiros; e

u) atribuição de conceito INADEQUADO em Relatório de Auditoria.

2.5 A penalidade de **suspenção temporária** de emissão de novos certificados implicará o impedimento de emissão total de novos certificados digitais, ou emissão de novo carimbo de tempo, ou armazenamento de chaves privadas dos usuários finais, pelo período máximo de 90 (noventa) dias, ou enquanto durar as condições de não conformidade apontadas em relatório de fiscalização ou auditoria.

2.6 A penalidade de **suspenção temporária** de emissão de novos certificados será aplicada quando o PSCert incorrer em não conformidades de risco alto ou crítico, não regularizada ou com prazo de regularização vencido, como por exemplo:

a) atribuição de conceito INACEITÁVEL em Relatório de Auditoria;

b) falha em diversos dossiês de certificado emitido, quanto a documentação, poderes, verificação biométrica e assinatura;

c) erros ou falhas em campos de certificados emitidos que comprometem o seu uso;

d) não publicação de LCR por tempo superior ao estabelecido em norma;

e) ausência de realização de auditoria operacional anual por mais de uma vez no período de 5 (cinco) anos;

f) qualquer ato intencional de omissão ou manipulação de dados, alteração de documentos ou registros eletrônicos, ou qualquer ato que possa ser enquadrado como fraude; e

g) emissão de certificado sem coleta ou verificação biométrica na forma estabelecida em norma.

2.7 A penalidade de **descredenciamento** implicará o impedimento do ente credenciado em exercer as atividades para as quais foi autorizado, em acordo com as normas específicas do CG ICP-Brasil.

2.8 A penalidade de **descredenciamento** será aplicada quando o PSCert incorrer em não conformidades de risco crítico, não regularizada ou com prazo de regularização vencido, como por exemplo:

a) adulteração de documentos praticada por agente de registro, empregado ou administradores da entidade fiscalizada ou auditada;

b) inserção ou manutenção de registros ou informações falsos em demonstrações operacionais ou em relatórios de auditoria de pessoas jurídicas, supervisionadas ou fiscalizadas pelo ITI;

c) atribuição de conceito INACEITÁVEL em Relatório de Auditoria por mais de uma vez no período de até 5 (cinco) anos;

d) participação direta (dolo) de agente de registro, empregado ou administradores da entidade fiscalizada ou auditada na obtenção de certificado digital por meio de fraude;

e) embaraço à fiscalização do ITI;

f) emissão de certificado sem identificação presencial ou sem garantir o nível de segurança equivalente, exigido nas normas técnicas da ICP-Brasil;

g) houver comprometimento da cadeia de confiança da ICP-Brasil, por ação ou omissão do PSCert, evidenciada em relatório de auditoria operacional;

h) for identificada inconsistência no relatório de auditoria que fira quaisquer dos princípios de auditoria e que comprometa a cadeia de confiança da ICP-Brasil; e

i) nos casos de entidades de auditoria, em que houver descumprimento de normas da ICP-Brasil ou do código de ética do auditor estabelecido por órgãos reguladores ou de classe.