INSTRUÇÃO NORMATIVA ITI Nº 06, DE 20 DE MAIO DE 2021

Aprova a versão 1.0 do documento Critérios para Emissão de Parecer de Auditoria na ICP-Brasil – DOC-ICP-08.01.

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

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, e

CONSIDERANDO a indicação contida no Anexo da Resolução CG ICP-Brasil n° 185, de 18 de maio de 2021, de que os critérios para emissão de parecer de auditoria na ICP-Brasil devem ser definidos por instrução normativa da AC Raiz,

RESOLVE:

Art. 1° Aprovar a versão 1.0 do documento DOC-ICP-08.01 – Critérios para Emissão de Parecer de Auditoria na ICP-Brasil, anexa a esta Instrução Normativa.

Art. 2° Esta Instrução Normativa entra em vigor em 1° de junho de 2021.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2021.05.20 16:41:06 -03'00'

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

ANEXO

CRITÉRIOS PARA EMISSÃO DE PARECER DE AUDITORIA NA ICP-BRASIL

DOC-ICP-08.01

Versão 1.0

20 de maio de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
IN ITI nº 06, de 20.05.2021 Versão 1.0		Criação do DOC-ICP-08.01, que estabelece os critérios para emissão de parecer de auditoria na ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridade de Registro
CFTV	Circuito Fechado de Televisão
FCT	Fonte Confiável do Tempo
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
LCR	Lista de Certificados Revogados
PSCert	Prestador de Serviço de Certificação

1 DISPOSIÇÕES GERAIS

1.1 O presente documento suplementa a regulamentação, no âmbito da ICP-Brasil, das atividades de auditoria a serem realizadas em sua cadeia de certificação digital. Não esgota, no entanto, os processos e subprocessos existentes na cadeia da ICP-Brasil, devendo ser entendido apenas como um balizador ou ponto de partida para cada trabalho de auditoria.

1.2 Cabe ao auditor a responsabilidade pela escolha dos processos a serem auditados em cada Prestador de Serviço de Certificação - PSCert, individualmente, assim como a classificação dos riscos observados em cada processo/subprocesso a ser avaliado.

2 RELATÓRIO DE AUDITORIA

2.1 No Relatório de Auditoria será utilizada a tabela a seguir, para emissão de parecer de auditoria sobre o PSCert auditado.

Conceito	Parecer	Situação*
1	Adequado	Ausência de não conformidades
2	Aceitável	Média da avaliação dos riscos considerada baixa
3	Deficiente	Média da avaliação dos riscos considerada média
4	Inadequado	Média da avaliação dos riscos considerada alta
5	Inaceitável	Média da avaliação dos riscos considerada crítica

(*) A média aritmética é o somatório dos riscos encontrados nos controles que apresentaram inconformidade, dividido pela respectiva quantidade de controles que apresentaram não conformidade.

2.2 Havendo dúvida quanto ao enquadramento, pelo princípio do conservadorismo, será adotado o conceito de maior valor numérico (mais crítico).

3 CRITÉRIOS PARA APLICAÇÃO DOS CONCEITOS

3.1 A atribuição do conceito geral do PSCert, que constará do relatório de auditoria, refletirá a opinião do auditor sobre o nível de risco a que o PSCert estiver exposto. Para auxiliar nesta atribuição de conceito, o auditor poderá se valer do valor médio das inconformidades encontradas, que não poderá prevalecer sobre a opinião do auditor.

3.2 A atribuição da criticidade de cada não conformidade é de responsabilidade do auditor, que deve se basear na metodologia adotada, confrontada com as condições identificadas, dentro do contexto auditado. Apenas a título de exemplo meramente ilustrativo, a criticidade das não conformidades podem ser classificadas como:

a) Risco crítico:

i. certificado emitido com tamanho de chave inferior ao mínimo estabelecido;

ii. LCR – Lista de certificados revogados:

a) inexistência de LCR;

b) intervalo de tempo sem LCR;

c) LCR sem conteúdo; e

d) LCR com campo errado ou incorreto.

iii. ausência de cobertura de seguro de responsabilidade civil;

iv. ausência de realização de auditoria operacional anual;

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

vi. vulnerabilidade em ambiente lógico de segurança de rede;

vii. ausência de sincronismo de tempo entre os servidores e a Fonte Confiável do Tempo - FCT;

viii. uso de algoritmo de criptografia diferente do estabelecido nas normas;

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

x. falhas nos sistemas de controle de acesso físico e lógico aos recursos de AC;

xi. ausência de sincronismo dos aplicativos de AC entre os sítios principal e de contingência da AC; e

xii. falha de integridade das aplicações e bases de dados da AC.

b) Risco alto:

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

ii. erros ou falhas em campos de certificados emitidos;

iii. erros ou falhas em campos de LCR emitidas;

iv. falha na apresentação de certidões de pessoal vinculado ao PSCert;

v. 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;

vi. falha na identificação de equipamentos que se conectam à solução de certificação digital da AC;

vii. ausência de testes de funcionamento do sítio de contingência;

viii. ausência de testes de recuperação de cópia de segurança de LCR, *logs* de aplicativos e bases de dados;

ix. ausência ou deficiências nos procedimentos de testes de vulnerabilidade de rede;

x. ausência ou falhas na monitoração de ocorrências registradas em *logs*; e

xi. ausência de licença de *software* proprietário de terceiros.

c) Risco médio:

i. falha na apresentação de documentação fisco-tributária do PSCert;

ii. falha no processo de treinamento de pessoal do PSCert;

iii. falha no processo de avaliação do pessoal do PSCert;

iv. falha no sistema de gravação de imagens de CFTV; e

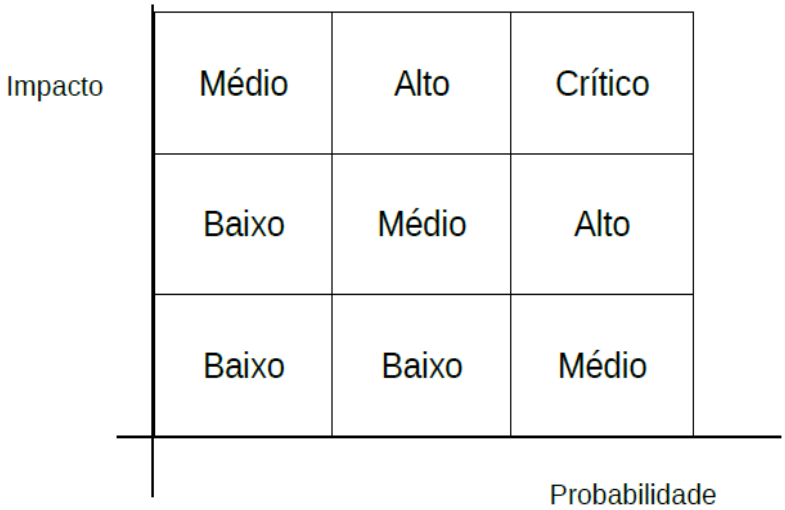
v. falha nos procedimentos de desligamento de empregados do PSCert, mesmo que sem desligamento da empresa responsável pelo PSCert.

d) Risco baixo:

i. falha em inventário de ativos.

3.3 Toda vez que os conceitos forem modificados em decorrência da convicção do auditor, o relatório de auditoria destacará a situação de forma fundamentada, cujas evidências deverão ser anexadas à cópia destinada ao ITI.

3.4 Para estabelecimento do nível do risco de uma não conformidade, será utilizada ferramenta de avaliação do risco, pelo menos com a utilização da matriz impacto versus probabilidade, onde:



3.5 Os valores a serem atribuídos aos eixos X e Y serão sempre em múltiplos de 3 (0 a 3; 0 a 6; 0 a 9; etc.); sempre em ordem crescente de exposição. Por exemplo, se adotada a escala de 0 a 9 teríamos a gradação de zero = sem qualquer impacto, até nove = impacto máximo possível.

3.6 Poderá ser utilizada outra metodologia para atribuição do nível do risco, desde que faça parte da documentação aprovada no credenciamento, ou seja evidenciada sua aplicação de forma sistematizada pela entidade de auditoria.

3.7 No relatório de auditoria constará, em parágrafo destacado, o conceito geral do PSCert atribuído pelo auditor ao auditado e os motivos que levaram à referida conceituação. A opinião do auditor será registrada no Parecer de Auditoria, que poderá ser: Adequado; Aceitável; Deficiente; Inadequado ou Inaceitável.