CRITÉRIOS PARA EMISSÃO DE PARECER DE AUDITORIA

1. O presente documento não esgota 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. Sempre caberá ao Auditor a responsabilidade pela escolha dos processos a serem auditados em cada PSC, individualmente, assim como a classificação dos riscos observados em cada processo/subprocesso a ser avaliado.

2. No Relatório de Auditoria será utilizada a tabela a seguir, para emissão de parecer de auditoria sobre o PSC 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.

2.1. 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 PSC, que constará do relatório de auditoria, refletirá a opinião do auditor sobre o nível de risco a que o PSC 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.

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 o Observatório Nacional (hora oficial brasileira).

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.

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 PSC.

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.*

XI) Ausência de licença de software proprietário de terceiros.

c) Risco médio:

I) Falha na apresentação de documentação fisco-tributária do PSC.

II) Falha no processo de treinamento de pessoal do PSC.

III) Falha no processo de avaliação do pessoal do PSC.

IV) Falha no sistema de gravação de imagens de CFTV.

V) Falha nos procedimentos de desligamento de empregados do PSC, mesmo que sem desligamento da empresa responsável pelo PSC.

d) Risco baixo:

I) Falha na manutenção, sistema elétrico e de combate a incêndio nas AR.

II) Falha na atualização de informações de instalações técnicas disponíveis nos repositórios.

III) 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:

Impacto			
	Médio	Alto	Crítico
	Baixo	Médio	Alto
	Baixo	Baixo	Médio
			Probabilidade

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 PSC 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.