ADE-ICP-08.I – MODELO E REQUISITOS PARA A ELABORAÇÃO DO RELATÓRIO FINAL DE AUDITORIA

Inserir o rótulo de classificação da informação

RELATÓRIO FINAL DE AUDITORIA Nº /ANO

(Nome da Entidade auditada)

Relatório de auditoria Pré-Operacional ou Operacional

Vinculada às (Entidades Vinculadas)

Local, dd de mm de aaaa

(EMPRESA DE AUDITORIA INDEPENDENTE OU INTERNO)

(Nome do Auditor Responsável Técnico pela auditoria)

1. INTRODUÇÃO

1.1. Objetivo da Auditoria

Nesta seção o auditor deve descrever o objetivo da auditoria.

1.2. Âmbito da Auditoria

Nesta seção o auditor deve assinalar quais os serviços que irão ser alvo de auditoria no âmbito da atividade da prestação de serviços de certificação ICP-Brasil, especificando:

1. Autoridade Certificadora- AC e respectivos PSSs
2. Autoridade de Registo - AR
3. Autoridade de Carimbo do Tempo – ACT e respectivos PSSs
4. Prestador de Serviço de Confiança – PSC e respectivos PSSs
5. Prestadores de Serviço Biométricos – PSBios e respectivos PSSs

Sempre que exista PSS na execução dos serviços acima listados, deve fazer referência ao prestador do serviço.

Não será emitido relatório de auditoria operacional para o Prestador de Serviço de Suporte – PSS.

1.3. Local da auditoria

Nesta seção o auditor deve descrever a localização ou localizações das instalações técnicas onde decorreu a auditoria

2. ENTIDADE AUDITADA

Dados relativos à entidade, entre outros:

- Nome do PSCert na ICP-Brasil (Ver nome no linK https://www.gov.br/iti/pt-br/assuntos/icp-brasil)
- Razão social e CNPJ do PSCert e
- Endereço
- E-mail

3. EQUIPE DE AUDITORIA

Nesta seção o auditor deve listar os nomes dos membros da equipe, com indicação do coordenador de equipe e responsável técnico.

4. PÉRIODO DA AUDITORIA

Nesta seção o auditor deve indicar o período de abrangência, o período de execução da auditoria e anexar o respectivo planejamento.

A auditoria abrange as operações realizadas no período de dd a dd+n de mm de aaaa.

A auditoria foi conduzida no período de dd a dd+n de mm de aaaa, de acordo com o cronograma previamente definido na fase de planejamento das atividades.

5. RISCOS, LIMITAÇÕES E RESPONSABILIDADE

Nesta seção o auditor deve descrever os riscos e limitações inerentes ao trabalho de auditoria realizado, bem como as responsabilidades de asseguração razoável, quando for o caso.

6. ESCOPO DE AUDITORIA

Nesta seção o auditor deve descrever os critérios adotados para a escolha dos Processos e Subprocessos descritos no ADE-ICP 08-E.

7. ANTECEDENTES (AUDITORIAS ANTERIORES)

Nesta seção o auditor deve descrever se existem auditorias anteriores. Caso existam, colocar a referência dos respectivos relatórios e informar os conceitos atribuídos.

8. AVALIAÇÃO DAS OPERAÇÕES

Nesta seção e seguintes o auditor deve fazer uma descrição sumária dos resultados identificados na execução da auditoria, conforme descrito no CAPÍTULO IV – DA REALIZAÇÃO DA AUDITORIA da Instrução Normativa ITI nº 32, de 23 de abril de 2025, preferencialmente fazendo menção aos Processos definidos no ADE-ICP 08.E.

Exemplos:

8.1. Credenciamento e manutenção de entidades operacionalmente vinculadas

8.2. Executar Fases do Ciclo de Vida dos Certificados e Manter Publicações

8.3. Manutenção de Credenciamento de AC

8.4. Manter segurança lógica e rede

8.5. Manter segurança da informação

8.6. Manter infraestrutura e sítio de contingência

8.7. Manter recursos humanos

8.8. Descrição da documentação analisada

Nesta seção o auditor deve listar os documentos que foram verificados nas várias fases da auditoria, com indicação da referência e data da última atualização.

Foram analisados os seguintes documentos: -Políticas de Segurança: Referência xyz, mm de aaaa; -Política de Certificados: Referência xyz, mm de aaaa; -Declaração de Práticas de Certificação: Referência xyz, mm de aaaa; -Planos de contingência/continuidade: Referência xyz, mm de aaaa; -Contrato de prestação de serviços: Referência xyz, mm de aaaa; -Manuais de Procedimentos internos: Referência xyz, mm de aaaa; -Deliberações do grupo de gestão da EC: Referência xyz, mm de aaaa; -Atas e reuniões: Referência xyz, mm de aaaa; -Relatórios de incidentes: Referência xyz, mm de aaaa; -Certificados digitais emitidos: Referência xyz, mm de aaaa; -Lista de Revogação de certificados: Referência xyz, mm de aaaa; -Documentos relativos ao contrato social ou estatuto legal: Referência xyz, mm de aaaa

No relatório a ser enviado ao ITI, além da descrição referida anteriormente, o auditor deve anexar a lista de verificação preenchida (ver Apêndice B), descrevendo os resultados observados, os métodos de avaliação utilizados (entrevista, questionários, verificação de documentação), o racional para a sua escolha e metodologia empregue.

9. NÃO CONFORMIDADE

Nesta seção o auditor deve descrever as NÃO CONFORMIDADES encontradas e enquadrá-las tendo em conta o requisito e o referencial.

Exemplos:

Foram detectadas as seguintes NÃO CONFORMIDADES:		
REFERÊNCIA NORMATIVA	**REQUISITO**	**DESCRIÇÃO**
DOC ICP 05	7.1.g)	A Declaração de Práticas de Certificação (DPC) não está atualizada. Não está definido nenhum processo para revisão da Declaração de Práticas de Certificação (DPC), bem como o respectivo fluxo de aprovação.
DOC ICP 05	7.2.7.d)	Não existem procedimentos para destruição das chaves da AC

DOC ICP 05	7.3.1.a) 7.3.1.b)	A AC não disponibiliza informação sobre os termos e condições da utilização dos certificados.
DOC ICP 02	7.4.1.a)	A AC não desenvolveu uma avaliação do risco de modo a determinar os riscos decorrentes da sua atividade. Foi efetuada apenas uma análise de risco no âmbito da segurança física às instalações da EC.
DOC ICP 02	7.4.1.c)	A entidade não tem definido qualquer política de segurança da informação
DOC ICP 02	7.4.2.a)	Não existe inventário onde conste todos os recursos (documentos, equipamento, software etc.) da EC.
DOC ICP 05	7.4.3.a)	A AC não dispõe de "*Job Descriptions*" que identifiquem claramente, de forma detalhada, as responsabilidades de cada indivíduo ou grupo.

10. RECOMENDAÇÕES E SUGESTÃO DE MELHORIAS

10.1. Recomendações - Ações corretivas

Nesta seção o auditor deve listar as ações corretivas (recomendações) tendo em conta as NÃO CONFORMIDADES e determinar o prazo para a regularização em comum acordo com a entidade auditada, não podendo exceder 90 dias.

A entidade auditada deverá proceder à produção de um calendário de implementação (Plano de Ação) das ações corretivas identificadas nesta seção, o qual deverá ser encaminhado para o auditor, para a AC e para o ITI.

As ações corretivas listadas nesta seção são de **implementação obrigatória.**

Exemplos de ações corretivas (recomendações)

A entidade auditada deverá proceder à produção de um calendário de implementação das correções identificadas nesta seção. As ações corretivas devem ser realizadas no mais curto espaço de tempo, não podendo em qualquer caso ultrapassar o prazo 90 dias para sua implementação.

10.1.1. Definir e estabelecer um processo para revisão periódica da DPC, bem como o respectivo fluxo de aprovação;

10.1.2. Revisão da configuração inicial de equipamentos para detectar vulnerabilidades inerentes da configuração padrão do fabricante

10.1.3. Conduzir uma avaliação de riscos;

10.1.4. Manter inventário atualizado;

10.1.5. Manter atualizado um inventário onde constem todos os recursos da entidade auditada, com diferentes graus de classificação, de modo a poderem ser alvo das medidas de proteção adequadas

10.1.6. Definir uma metodologia de classificação, onde conste (quem? e como?) e a forma de acesso ao respectivo recurso;

10.1.7. Criar procedimentos para resposta a incidentes;

10.1.8. Testar o plano de contingência de modo a assegurar continuidade das operações/atividades em caso de incidente grave/desastre;

10.2. SUGESTÃO DE MELHORIAS

Nesta seção o auditor deve listar as sugestões de melhoria que julgar adequadas tendo em conta a melhoria de determinados aspectos.

Não sendo consideradas "NÃO CONFORMIDADES", as sugestões de melhorias podem ser assumidas como indicadoras de "boas práticas", consubstanciadas na experiência.

As sugestões de melhorias listadas nesta seção não são de implementação obrigatória para a entidade auditada.

11. CONCLUSÕES

Nesta seção o auditor deve, com base nos resultados observados, efetuar um sumário descritivo das áreas avaliadas, com especial incidência para os serviços de certificação digital e terminar com comentário acerca observância das condições para desenvolvimento da atividade da entidade auditada.

Este sumário é estendido também às áreas críticas das operações, nomeadamente os processos definidos no ADE ICP 08.E.

Exemplo:

Da auditoria efetuada constata-se que as diversas operações e atividades desenvolvidas pela entidade auditada, enquanto autoridade certificadora que emite certificados do tipo A3, XXXX, são conduzidas em ambiente controlado e levadas a cabo por recursos humanos qualificados.

…

Considera-se que a condições de segurança nas tarefas e atividades de rotina, relacionadas com a gestão do ciclo de vida dos certificados e chaves são adequadas.

…

Verificaram-se ainda inconsistências nas matérias relativas à gestão e administração do Agentes de Registro, nomeadamente na implementação adequada de um sistema de gestão de contratação e avaliação de desempenho.

…

Considera-se existir carências na capacidade de desenvolver a sua atividade, recomendando a suspensão imediata das operações, sendo possível a retomada após a implementação do plano de ação para contenção desastre ou incidente grave.

…

No final da seção o Auditor deve pronunciar-se se estão reunidas as condições mínimas para o desenvolvimento da atividade da entidade auditada (com ou sem constrangimentos), tendo em conta as

eventuais “NÃO CONFORMIDADES” observadas, bem como deve informar o conceito geral atribuído, conforme tópico **Critérios para aplicação dos conceitos da** Instrução Normativa ITI nº 32, de 2025.

Exemplo:

Face ao descrito, considera-se que estão reunidas, embora com constrangimentos, as condições necessárias para que a Entidade Auditada possa desenvolver a sua atividade num ambiente seguro e de confiança, desde que implementados as medidas descritas em 10.1. Recomendações - Ações corretivas.

Por fim, de acordo com os critérios para emissão de parecer de auditoria na ICP-BRASIL estabelecidos na Instrução Normativa ITI nº 32, de 2025, aplica-se o conceito geral 0,89. Esse conceito geral atribuído conduz à atribuição do parecer ADEQUADO para a entidade XXXXXXX, CNPJ 999999.

APÊNCIDE A – PLANEJAMENTO DAS ATIVIDADES DO AUDITOR

Auditor Independente ou Auditor Interno

DATA	Atividade	Responsável
dd/mm/aaaa	Solicitação de documentação	Nome do Auditor
dd/mm/aaaa	Envio da documentação por parte da AC xxxx	Nome do Responsável da AC
dd/mm/aaaa a dd/mm/aaaa	Análise de documentação	Nome dos Auditores
dd/mm/aaaa a dd/mm/aaaa	Vista "*in loco*" PSCert – xxxxxxxxx	Nome dos Auditores
dd/mm/aaaa a dd/mm/aaaa	Revisão da documentação e evidencias coletadas e solicitada "*in loco*"	Nome dos Auditores
dd/mm/aaaa a dd/mm/aaaa	Geração do Relatório de Primeira Impressões	Nome dos Auditores
dd/mm/aaaa a dd/mm/aaaa	Envio e comunicação do Relatório de Primeira Impressões	Nome dos Auditores e Responsáveis da PSCert
dd/mm/aaaa a dd/mm/aaaa	Revisão e Assinatura do Relatório Final de Auditoria	Nome dos Auditores e Responsável Técnico

LISTA DE DISTRIBUIÇÃO:

Entidade auditada

Autoridade Credenciadora

…

APÊNDICE B – LISTA DE VERIFICAÇÃO DE CONFORMIDADE

Apêndice B (Lista de Verificação de Conformidade) ao RELATÓRIO FINAL DE AUDITORIA Nº___

ADE-ICP-08.E – Todos os itens objeto de análise conforme definido no escopo de auditoria					
REQUISITO	**CUMPRE**		**TÉCNICA DE AUDITORIA UTILIZADA**	**AMOSTRA UTILIZADA (% ou valor)**	**RESULTADO OBSERVADO**
	S	**N**			
10101001					
10101002					
10101005					
10101003					
6.2.b)					
6.2.c)					
6.2.d)					
6.2.e)					
6.2.f)					
6.2.g)					
6.2.h)					
6.2.i)					
6.3					

6.3.a)					
6.3.b)					
6.3.c)					
6.4					
7					
7.1					

APÊNDICE C - DECLARAÇÃO DE NÃO IMPEDIMENTO

DECLARAÇÃO DE NÃO IMPEDIMENTO

Neste documento a empresa de auditoria e os respectivos auditores participantes do trabalho firmam declaração de que não se enquadram nas causas de impedimento descritas no item 7.2 do Anexo da Resolução CG ICP-Brasil nº 185, de 18 de maio de 2021.

Auditores que compõem a equipe de auditoria

_____	_____	_____	_____
(Nome 1)	(Nome 2)	(Nome …	(Nome n