



PKI CONSULTING

Av. Borges de Medeiros, 2500/1402

Porto Alegre-RS 90110-150

www.pkiconsulting.com

Fone: (51) 3398-5740

RELATÓRIO FINAL DE AUDITORIA Nº 22/2025

Auditoria de Conformidade Operacional

AR DIGIPAPER & BOX

Vinculada à(s) AC(s) SAFEWEB RFB e SAFEWEB CD

PKI Contabilidade e Auditoria Ltda

Letícia Tarda

I - Introdução

1 - Objetivo da Auditoria

Este relatório refere-se à auditoria operacional realizada como requisito para a manutenção do credenciamento como Autoridade de Registro na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. O objetivo da auditoria foi avaliar a conformidade dos processos e procedimentos adotados pela AR, em conformidade com as normas e regulamentos estabelecidos pela ICP-Brasil.

2 - Âmbito da Auditoria

Esta auditoria abrange as atividades de Autoridade de Registro - AR.

3 - Local da Auditoria

A auditoria foi realizada de forma remota com uso da ferramenta Teams, Portal PKI Consulting e contatos telefônicos.

II - Entidade Auditada

Nome:	AR DIGIPAPER & BOX
Razão Social:	DIGIPAPER & BOX LTDA
CNPJ:	28.654.776/0001-44
Endereço da AR:	R CORIOLANO MILHOMEM, 2390, SALA 12, CEP: 65.901-030, CENTRO, IMPERATRIZ/MA, BRASIL.
E-mail:	credenciamento@dpbox.com.br

III - Equipe de Auditoria

Auditor(a):	Letícia Tarda
Responsável Técnico(a):	Letícia Tarda
Revisor(a):	Henrique Queiroz da Silva
Coordenador(a):	Wenndel Laerth Lopes Aguiar

A Auditoria ocorreu dentro do período previsto no PLAAO.

IV - Período da Auditoria

A auditoria foi planejada conforme o documento "Anexo A - Cronograma e Planejamento da Auditoria" e conduzida pelas pessoas a seguir, nas data assinaladas:

Avaliação Documental - Data de Início	16/06/2025
Avaliação Documental - Data de Fim	20/06/2025
Auditoria Remota - Data de Início:	16/06/2025
Auditoria Remota - Data de Fim:	16/06/2025
Período de abrangência da Auditoria:	18/03/2024 a 16/06/2025

V - Riscos, Limitações e Responsabilidade

A equipe de auditoria teve como limitações o fato de que a análise de diversos itens foi realizada por amostragem, o que pode levar a que não tenham sido detectados erros ou falhas acaso existentes no conjunto total das informações.

VI - Escopo de Auditoria

A auditoria teve como escopo verificar a conformidade dos processos, procedimentos e ambientes da AR em relação aos regulamentos da ICP-Brasil, em especial:

- DOC-ICP-02 – V.4.0 – Política de Segurança da ICP-Brasil
- DOC-ICP-03 – V.7.2 – Critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil
- DOC-ICP-03.01 – V. 4.0 – Características Mínimas de Segurança para as ARs da ICP-Brasil
- DOC-ICP-05 – V.6.5 – Requisitos Mínimos Para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil
- DOC-ICP-05.02 – V.4.0 – Procedimentos para Identificação do Requerente e Comunicação de Irregularidades no Processo de Emissão de um Certificado Digital ICP-Brasil
- DOC-ICP-05.03 – V.3.1 – Procedimentos para Identificação Biométrica na ICP-Brasil
- DOC-ICP-05.05 – V.2.0 – Procedimentos para Identificação de Requerentes de Certificados Digitais por Videoconferência
- DOC-ICP-08 – V.5.0 – Critérios e procedimentos para realização de auditorias nas entidades da ICP-Brasil
- ADE-ICP-08.E – V.4.3 – Mapa de Processos Identificados na ICP-BRASIL
- WebTrust Principles and Criteria for Registration Authorities Version 1.1

VII - Antecedentes (Auditorias Anteriores)

Verificamos que esta é a primeira Auditoria Operacional da AR pelas cadeias da AC SAFEWEB.

VIII - Avaliação das Operações

Os tópicos cobertos pela auditoria de conformidade operacional incluíram:

- 1 – Manter Credenciamento de AR
- 2 – Atender Solicitação de Certificados
- 3 – Atender Solicitação de Revogação de Certificados
- 4 – Manter Segurança da Informação
- 5 – Manter Sistemas Aplicativos
- 6 – Manter Segurança Lógica e Rede
- 7 – Manter Infraestrutura
- 8 – Manter Recursos Humanos
- 9 – Descrição da Documentação Analisada

IX - Achados de Auditoria

1. Manter Credenciamento de AR

Verificamos se a AR mantém os requisitos de credenciamento, incluindo a avaliação da regularidade jurídica, fiscal e econômico-financeira, a análise da documentação para identificação de alterações contratuais e comunicação à AC, a revisão do relatório da última auditoria, com solicitação de evidências dos procedimentos adotados para regularização de pendências, quando aplicável, além da verificação de possíveis violações aos regulamentos da ICP-Brasil no período auditado, entre outros.

2. Atender Solicitação de Certificados

Avaliamos em relação à completude dos dossiês, procedimentos de validação e verificação (por agente de registro ou por meio de barramentos/aplicações oficiais), existência da trilha de auditoria, procedimentos de revogação (quando aplicável) e demais requisitos que tratam de Identificação e Autenticação no DOC-ICP-05. Nos certificados emitidos por videoconferência avaliamos os requisitos definidos no DOC-ICP-05.05.

Na gravação da videoconferência referente ao pedido 1006480485, identificamos que o AGR durante o processo de validação mencionou o nome de uma AR distinta, AR DIGITALTEC. Recomendamos que os AGRs sejam devidamente instruídos a informar o nome correto da AR que está realizando a validação.

3. Atender Solicitação de Revogação de Certificados

Avaliamos em relação à completude dos dossiês e procedimentos adotados na solicitação de revogação de certificados.

4. Manter Segurança da Informação

Analisamos a existência e adequação dos documentos de Segurança da Informação previstos nos itens 6.1.1 a 6.1.5 do DOC-ICP-03.01, tais como políticas, manuais, Plano de Continuidade de Negócios, Inventário de Ativos, entre outros. Também foi analisada a existência e publicação da Declaração de Práticas de Negócios.

Recomendamos que a AR inclua número de série de todos os seus equipamentos computacionais e biométricos no Inventário de Ativos.

5. Manter Sistemas Aplicativos

O sistema utilizado pela AR é fornecido pela Autoridade Certificadora vinculante, a qual se responsabiliza pela conformidade com os requisitos descritos no item 4.2 - Aplicativo da AR, do DOC-ICP-03.01.

6. Manter Segurança Lógica e Rede

A AR apresentou uma relação dos equipamentos habilitados no sistema. Com base nessa relação, foi calculada uma amostragem, para verificar se as configurações dos equipamentos estavam de acordo e analisar a eventual utilização de um único equipamento em mais de uma AR registrada em nosso banco de dados. Também foi solicitada a apresentação de comprovativos de posse ou propriedade dos equipamentos computacionais e dos equipamentos biométricos utilizados.

7. Manter Infraestrutura

Para comprovar o atendimento ao requisito previsto no item 3.2 do DOC-ICP-03.01, relativo à manutenção preventiva/corretiva das estações de trabalho da AR, foi solicitada a apresentação de documento assinado, demonstrando que as manutenções foram realizadas por profissional designado pela AC ou assistência técnica autorizada.

Foi avaliado também se a AR possui infraestrutura mínima para atendimento as atividades de Autoridade de Registro através de videoconferência ou visita in loco, quando aplicável.

8. Manter Recursos Humanos

A AR apresentou a relação dos AGRs ativos e daqueles que foram inativados durante o período abrangido pela auditoria. Com base nessa relação, foi calculada uma amostragem, para verificar se os dossiês estavam completos, se os AGRs possuíam vínculo empregatício com outras ARs e se as Entrevistas de Admissão/Desligamento e as Declarações de Completude dos dossiês foram assinadas por pessoa competente.

9. Descrição da Documentação Analisada

Analisamos os seguintes documentos:

Questionário Preliminar, 16/06/2025.

Videoconferência com AR para vistoria de ambiente físico, 16/06/2025.

Comunicação à AC de alterações contratuais da AR, 14/03/2025.

Link onde se encontra publicada a Declaração de Práticas de Negócio da AR, 16/06/2025

Se trata da primeira auditoria operacional da AR nas cadeias da AC SAFEWEB.

Publicação do Deferimento de Credenciamento no DOU, 18/03/2024.

Cartão CNPJ, 21/05/2025

Ato Constitutivo, 11/02/2025

Prova de inscrição no cadastro Municipal, 16/06/2025

Certidão Negativa de Débito de Tributos Federais e à Dívida Ativa da União, 06/02/2025

Certidão Negativa de Débito Estadual, 22/05/2025

Declaração de que não possui débitos imobiliários, 16/06/2025

Certidão de Tributos Mobiliários, 22/07/2025

Certidão do FGTS – CRF, 16/06/2025.

Balanços Patrimonial - 2023, 09/01/2024

Balanços Patrimonial e DRE - 2024, 14/02/2025

Certidão Negativa de Falência ou Concordata, 23/05/2025

Relação dos AGRs Ativos e Inativos, 16/06/2025.

Documentação dos Dossiês de Certificados Emitidos e Revogados solicitados para auditoria.

Inventário de ativos da AR - Dezembro, 02/06/2025

Inventário de ativos da AR - Janeiro, 02/06/2025

Inventário de ativos da AR - Fevereiro, 02/06/2025

Inventário de ativos da AR - Março, 02/06/2025

Inventário de ativos da AR - Abril, 02/06/2025

Inventário de ativos da AR - Maio, 02/06/2025

Pasta contendo diversos comprovantes de posse e propriedade dos Equipamentos computacionais, Leitores e Webcam.

Plano de Continuidade de Negócios e Teste anual de PCN, 06/06/2025

Documentos de Gestão de Riscos, 05/06/2025

Política para classificação da informação, 23/04/2024

Manuais Operacionais dos AGRs, 29/05/2025

Política para descarte de mídia, 23/04/2024

Topologia de rede, 05/05/2025

Documento descrevendo a marca e o modelo das mídias utilizadas, juntamente com o comprovante de homologação das mesmas, 16/06/2025.

Evidências dos equipamentos computacionais solicitados em auditoria.

Procedimentos de manutenção de equipamento, 16/06/2025.

Dossiês dos AGRs Inativos solicitados em auditoria.

Dossiês dos AGRs Ativos solicitados em auditoria.

X Não conformidade

Foram detectadas as seguintes não-conformidades:

4 – Manter Segurança da Informação						
Referência Normativa	Descrição do processo/subprocesso	Não Conformidades	Qtde. Ocorrências	Regularizada?	Risco	Recomendação

DOC.ICP.03.1, item 6.1.5.2.	A comprovação da posse ou propriedade dos equipamentos a que se refere o item anterior deverá ser feita sempre que assim requisitado pela AC Raiz, mediante a apresentação pela AR da respectiva nota fiscal, comodato, leasing, doação, contrato de locação de equipamentos ou documentação comprobatória equivalente.	A AR não possuía comprovação de posse/propriedade dos equipamentos computacionais e periféricos biométricos constantes no inventário de ativos, sendo eles: 8 Computacionais (DIGIPAPER-MA-02, DIGIPAPER-PA-01, DIGIPAPER-PA-03, DIGIPAPER-PI-01, DIGIPAPER-PI-02, DIGIPAPER-PI-04, DIGIPAPER-SP-01 e DIGIPAPER-MA-1-ZX2), 7 leitores biométricos e 8 webcams.	23	SIM	BAIXO	Que sejam habilitados apenas equipamentos de posse/propriedade da AR ou com origem comprovada e que a AR recupere as Notas Fiscais de Origem do equipamento computacional e de seus periféricos biométricos que possuem apenas documento de cessão de posse.
-----------------------------	---	--	----	-----	-------	--

6 – Manter Segurança Lógica e Rede

Referência Normativa	Descrição do processo/subprocesso	Não Conformidades	Qtde. Ocorrências	Regularizada?	Risco	Recomendação
20603004	Manter os equipamentos sincronizados com a FCT (Fonte Confiável do Tempo).	Sincronismo com fonte confiável de tempo não implementado no equipamento com hostname: DIGIPAPER-PA-03.	1	SIM	BAIXO	Que a AR mantenha os equipamentos computacionais sempre configurados de acordo com o manual de configuração da AC.

8 – Manter Recursos Humanos

Referência Normativa	Descrição do processo/subprocesso	Não Conformidades	Qtde. Ocorrências	Regularizada?	Risco	Recomendação
----------------------	-----------------------------------	-------------------	-------------------	---------------	-------	--------------

DOC.ICP.03 .1, item 2.2.3.	Os documentos 2.2.1.a até 2.2.1.h, que compõem o dossiê, devem ser examinados por uma das seguintes pessoas, que declarará, sob as penas da lei, a existência de tais documentos e que eles comprovam efetivamente que o Agente de Registro atende a todos os requisitos da ICP-Brasil pertinentes: a) Auditor interno da AR, cadastrado junto à ICP-Brasil conforme DOC-ICP-08 [5]; b) Auditor ou funcionário designado da Autoridade Certificadora à qual a AR se vincula; c) Representante Legal da própria AR, caso a AR não possua agente de registro como sócio.	Declaração de completude, sob as penas da lei, da AGR LAENY MELO GOMES DE CASTRO sem assinatura do declarante.	1	SIM	BAIXO	Recomendamos que a AR mantenha o dossiê dos AGRs devidamente atualizados.
----------------------------------	--	--	---	-----	-------	---

XI Recomendações e Sugestão de Melhorias

1 - Recomendações - Ações corretivas

A equipe de auditoria não evidenciou recomendações, além das informadas no item "X Não Conformidade".

2 - Sugestão de Melhorias

A equipe de auditoria não evidenciou pontos de melhoria durante o período de auditoria.

XII Parecer de Auditoria

Como forma de evidenciar as conclusões a que se chegou à presente auditoria, uma série de documentos foram requisitados à auditada, que por seu caráter confidencial encontram-se em cópia na nossa empresa e à disposição para futuras análises.

Também, nossa Matriz de Procedimentos Auditados encontra-se à disposição, para consultas.

Nossos trabalhos consistiram na aplicação de procedimentos de auditoria específicos, que tomaram por base a regulamentação da ICP-Brasil, a Declaração de Práticas de Certificação e a Política de Certificação das ACs às quais a AR está vinculada.

Ressaltamos que, devido às limitações inerentes a qualquer estrutura de controles internos, podem ocorrer erros que não sejam detectados na auditoria. Adicionalmente, projeções de qualquer avaliação dos controles internos para períodos futuros estão sujeitas ao risco de que tais controles venham a se tornar inadequados, em decorrência de mudanças nas condições do ambiente ou de diminuição do grau de aderência às políticas, normas e procedimentos existentes.

Assim, nossa conclusão refere-se apenas à auditoria de conformidade operacional da referida AR, efetuada no período acima indicado, não sendo consideradas eventuais modificações que possam ocorrer nos controles auditados após a data de conclusão da auditoria.

Para emissão do parecer de auditoria, calculamos a Média de Avaliação dos Riscos como sendo o somatório das não-conformidades, dividido pela quantidade total de controles avaliados. Havendo dúvida quanto ao enquadramento, pelo princípio do conservadorismo, adotamos o conceito de maior valor numérico (mais crítico).

A tabela a seguir mapeia os valores obtidos com os conceitos respectivos:

Tabela 1 – Conceitos de Auditoria

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

Na presente auditoria foi(ram) detectada(s) as não-conformidade(s) relatada(s) na Seção "X Não conformidade", com a seguinte avaliação de riscos:

Regularizadas:	3
Parcialmente Regularizadas:	0
Não regularizadas:	0

Com distribuição de riscos conforme segue:

Risco	(A) Qtde. de NCs	(B) Peso	(A*B)
Baixo	3	1	3
Médio	0	2	0
Alto	0	3	0
Crítico	0	4	0
Total NCs	3		3
MÉDIA GERAL DOS RISCOS			1
			Baixo

Nosso Parecer de Auditoria é que a AR apresenta Conceito:

ACEITÁVEL

Face ao descrito, considera-se que estão reunidas, embora com ressalvas, as condições necessárias para que a Entidade Auditada possa desenvolver a sua atividade num ambiente seguro e de confiança, desde que implementados as medidas recomendadas. Assim, a AR DIGIPAPER & BOX apresenta Conceito ACEITÁVEL.