PARECER RESUMO – AUDITORIA DE CONFORMIDADE OPERACIONAL AC RAIZ DA ICP – BRASIL

À
Diretoria da
AC Raiz da ICP-Brasil
Brasília – DF

Prezados Senhores:

Apresentamos o parecer resumo da Auditoria de Conformidade Operacional da Autoridade Certificadora AC Raiz da ICP-Brasil verificando o atendimento aos requisitos e critérios presentes nos DOC-IP-01 – Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil v.6.1 e DOC-ICP-02 – Política de Segurança da ICP-Brasil v.4.0 e emissão de parecer com base no DOC-ICP-08.01 – Critérios para Emissão de Parecer de Auditoria na ICP-Brasil v.1.0 durante o período de 09 de setembro de 2023 a 08 de setembro de 2024, para as operações realizadas em Brasília e no Rio de Janeiro.

Utilizamos métodos e processos técnicos aplicados por amostragem, estando os aspectos relevantes expostos neste relatório, que é estritamente confidencial, de uso exclusivo da AC Raiz, do Instituto Nacional de Tecnologia da Informação – ITI e do Comitê Gestor da ICP-Brasil no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, e tem como finalidade nortear os interessados sobre a suficiência dos controles executados para mitigação dos riscos existentes, não devendo ser apresentado ou distribuído a terceiros, tendo em vista a finalidade específica deste trabalho.

Escopo da Auditoria

A auditoria teve por objetivo avaliar se os processos, procedimentos, atividades e controles da Autoridade Certificadora Raiz estão em conformidade com a Declarações de Práticas de Certificação, Política de Segurança e demais normas e procedimentos estabelecidos pelo Comitê Gestor da ICP-Brasil à AC Raiz.

Executamos os trabalhos entre outubro e dezembro de 2024, referente ao período de 09/09/2023 a 08/09/2024.

Processos Avaliados

Os tópicos cobertos pela auditoria estão listados abaixo por área e no final do relatório consta o parecer geral da auditoria:

Manter Credenciamento da AC e Entidades Vinculadas

Obtivemos evidências suficientes e observamos procedimentos adequados de controle dos Prestadores de Serviço de Certificação PSCs pela AC Raiz.

A AC Raiz mantém controles para fornecer garantia razoável de que os requisitos de segurança lógica, física, a gestão das chaves criptográficas e ciclo de vida dos certificados operaram de forma eficiente e em cumprimento às diretrizes da ICP-Brasil.

Ciclo de Vida dos Certificados Digitais, Manter Publicações e Repositório

Foram avaliados os processos de solicitação, emissão e revogação de certificados digitais pela AC Raiz, assim como critérios do algoritmo criptográfico utilizado e controles da chave privada da AC Raiz. Também foram avaliados os procedimentos de atualização da Declaração de Práticas de Certificação – DPC da AC Raiz, geração de LCR e manutenção do repositório.

Segurança da Informação

Avaliamos os controles e documentos relativos à segurança da informação da AC Raiz envolvendo aspectos de Gestão de Riscos, Cópias de Segurança, Plano de Continuidade de Negócios, Gestão e Inventário de Ativos e Política de Classificação da Informação.

Segurança Lógica e Rede

Foram avaliados os controles de segurança lógica dos equipamentos envolvidos no ciclo de vida de certificados, gestão de logs, atualizações do sistema operacional, software contra códigos maliciosos, firewall, detecção de intrusão, controles de mídias, controles de violações de segurança e respectivos registros, sincronização com fonte confiável de tempo e controles de acessos lógicos.

Sistemas Aplicativos

Avaliamos os controles, documentos relacionados ao ciclo de vida dos sistemas e gestão de chaves criptográficas, verificando aspectos de segurança, atualizações, mecanismos de controle de acesso e procedimentos de cópias de segurança. Verificação dos controles de segurança aplicados aos servidores da AC Raiz relacionados com o ciclo de vida dos certificados, segregação de ambientes de desenvolvimento e produção, dentre outros aspectos.

Controle de Pessoal

Avaliamos os procedimentos de gestão de pessoas, assim como o atendimento pela AC Raiz dos requisitos para admissão, capacitação, avaliação de desempenho e desligamento previstos nos normativos ICP-Brasil.

Infraestrutura Física

Foram avaliados os controles de segurança física aplicados aos equipamentos envolvidos nos processos do ciclo de vida de certificados. Controles e registros de acessos físicos em áreas seguras, validação dos níveis de acesso, monitoramento por imagem, estrutura de cabeamento, suprimento alternativo para os casos de falta de energia elétrica, alarmes de movimento, detecção e supressão de incêndio e aspectos de segurança da sala-cofre. Foram considerados os sites principal e de contingência.

Conclusão e Parecer da Auditoria

Acreditamos que as evidências obtidas são apropriadas e suficientes para embasar a nossa conclusão. Emitimos o parecer observando os critérios estabelecidos no DOC-ICP 08.01 aplicado para entidades integrantes da ICP-Brasil, conforme tabela abaixo:

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 media
4	Inadequado	Média da avaliação dos riscos considerada alta
5	Inaceitável	Média da avaliação dos riscos considerada crítica

A atribuição do conceito geral reflete a opinião da auditoria acerca do nível de risco para os controles internos da AC Raiz. Para cada controle foi calculado o seu risco, de forma qualitativa, a partir de valores atribuídos para a probabilidade de ocorrência e o impacto da vulnerabilidade identificada.

Considerando o resultado da análise de riscos, atribuímos à AC RAIZ o Conceito Geral **2 (ACEITÁVEL),** com média de avaliação dos riscos considerada **Baixa.**

O conceito representa que foram identificadas uma ou mais não conformidades em relação aos requisitos normativos dos DOC-ICP 01 e DOC-ICP 02. Com base nas avaliações realizadas e detalhadas no Relatório de Auditoria Operacional da AC Raiz, nos registros históricos e nos fatores de mitigação implementados pela AC Raiz, verificamos que não houve a concretização dos riscos associados aos controles no período compreendido entre 09 de setembro de 2023 e 08 de setembro de 2024.

Brasília-DF, 27 de dezembro de 2024.

DIEGO ROTERMUND MOREIRA:90693922087

Digitally signed by DIEGO ROTERMUND MOREIRA:90693922087
DN: cn=DIEGO ROTERMUND MOREIRA:90693922087 c=BR o=ICP-Brasil ou=certificado digital
Reason: I am the author of this document
Location:
Date: 2024-12-27 15:27-03:00

MOREIRA ASSOCIADOS AUDITORES INDEPENDENTES S/S
CRC RS 004632/0 S DF
DIEGO ROTERMUND MOREIRA
Contador CRC RS 68603 S DF
CNAI N° 1128
Sócio - Responsável Técnico