SUMMARY OPINION – OPERATIONAL COMPLIANCE AUDIT
AC RAIZ DA ICP – BRASIL – ROOT CA

To the
Administrators,
AC Raiz da ICP-Brasil – Root CA
Brasília – DF

We present the summary report of the Operational Compliance Audit of the ICP-Brasil Certification Authority – Root CA verifying compliance with the requirements and criteria present in DOC-IP-01 – Declaration of Certification Practices of the ICP-Brasil Root Certification Authority v.6.1 and DOC-ICP-02 – ICP-Brasil Security Policy v.4.0 and issuance of an opinion based on DOC-ICP-08.01 – Criteria for Issuing an Audit Opinion at ICP-Brasil v.1.0 during the period from September 9, 2023 to September 8, 2024, for operations at Brasília- Brazil and Rio de Janeiro – Brazil.

We use technical methods and processes applied by sampling, with the relevant aspects exposed in this report, which is strictly confidential, for the exclusive use of AC Raiz, the National Institute of Information Technology – ITI and the ICP-Brasil Management Committee within the scope of the Brazilian Public Key Infrastructure – ICP-Brasil, and is intended to guide interested parties on the sufficiency of the controls implemented to mitigate existing risks, and should not be presented or distributed to third parties, in view of the specific purpose of this work.

Audit Scope

The audit aimed to assess whether the processes, procedures, activities and controls of the Root Certification Authority are in compliance with the Certification Practices Statements, Security Policy and other standards and procedures established by the ICP-Brasil Management Committee for the Root Certification Authority.

We performed the work between October to December 2024, referend to the period at 09/09/2023 and 09/08/2024.

Processes Assessed

The topics covered by the audit are listed below by area and the overall audit opinion is included at the end of the report:

Maintaining the Accreditation of the CA and Related Entities

We have obtained sufficient evidence and observed adequate control procedures of the PSC Certification Service Providers by AC Raiz.

AC Raiz maintains controls to provide reasonable assurance that the logical and physical security requirements, the management of cryptographic keys and the life cycle of certificates operated efficiently and in compliance with the ICP-Brasil guidelines.

Digital Certificate Life Cycle, Maintaining Publications and Repository

The processes for requesting, issuing and revoking digital certificates by the Root CA were evaluated, as well as the criteria for the cryptographic algorithm used and controls over the Root CA's private key. The procedures for updating the Root CA's Certification Practices Statement – CPS, generating CRLs and maintaining the repository were also evaluated.

Information Security

We evaluate the controls and documents related to AC Raiz's information security, involving aspects of risk management, backup copies, Business Continuity Plan, asset management and inventory, and information classification policy.

Logical and Network Security

The logical security controls of the equipment involved in the certificate life cycle, log management, operating system updates, software against malicious codes, firewall, intrusion detection, media controls, security breach controls and respective records, synchronization with a reliable time source and logical access controls were evaluated.

Application Systems

We assess controls, documents related to the life cycle of systems and cryptographic key management, verifying security aspects, updates, access control mechanisms and backup procedures. Verification of security controls applied to AC Raiz servers related to the life cycle of certificates, segregation of development and production environments, among other aspects.

Personnel Control

We review personnel management procedures, as well as AC Raiz's compliance with the requirements for admission, training, performance evaluation and dismissal set forth in ICP-Brasil regulations.

Physical Infrastructure

The physical security controls applied to the equipment involved in the certificate life cycle were assessed. Physical access controls and records in secure areas, validation of access levels, image monitoring, cabling structure, alternative power supply in cases of power outages, motion alarms, fire detection and suppression, and security aspects of the vault. The main and contingency sites were considered.

Conclusion and Audit Opinion

We believe that the evidence obtained is appropriate and sufficient to support our conclusion. We issued the opinion in accordance with the criteria established in DOC-ICP 08.01 applied to entities that are members of ICP-Brasil, as per the table below:

Grade	Opinion	Condition*
1	Adequate	Absence of non-conformities
2	Acceptable	Average risk assessment considered low
3	Deficient	Average risk assessment considered medium
4	Inadequate	Average risk assessment considered high
5	Unacceptable	Average risk assessment considered critical

The assignment of the general concept reflects the audit opinion regarding the level of risk for AC Raiz's internal controls. For each control, its risk was calculated, qualitatively, based on values assigned to the probability of occurrence and the impact of the identified vulnerability.

Considering the result of the risk analysis, we assigned **AC RAIZ** the General Concept **2 (ACCEPTABLE)**, with an average risk assessment considered **Low.**

The concept represents those one or more non-conformities were identified in relation to the normative requirements of DOC-ICP 01 and DOC-ICP 02. Based on the assessments carried out and detailed in the AC Raiz Operational Audit Report, in the historical records and in the mitigation, factors implemented by AC Raiz, we found that there was no materialization of the risks associated with the controls in the period between September 9, 2023 and September 8, 2024.

Brasília-DF, December 27, 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 15:26-03:00

MOREIRA ASSOCIADOS AUDITORES INDEPENDENTES S/S
CRC RS 004632/0 S DF
DIEGO ROTERMUND MOREIRA
Contador CRC RS 68603 S DF
CNAI N° 1128
Partner – Technical Manager