Política de Certificado e Declaração de Práticas de Certificação

Versão 1.0 - Criado em Junho de 2026

Rede Nacional de Ensino e Pesquisa

1. INTRODUÇÃO

1.1 Visão Geral

Este documento combinado de Política de Certificado ("PC") e Declaração de Práticas de Certificação ("DPC") ("PC/DPC") descreve as práticas de serviços de certificação da ICPEdu Certificado de Assinatura Única (CertAU) da Rede Nacional de Ensino e Pesquisa (RNP).

Os serviços da ICPEdu CertAU incluem, mas não estão limitados a, emissão, gerenciamento, validação e revogação de Certificados publicamente confiáveis de forma consistente com esta PC/DPC.

Esses serviços são fornecidos ao público em geral, com exceções conforme determinado pela gestão da RNP ou de acordo com a legislação relevante.

Outros documentos relacionados ao comportamento e controle da ICPEdu CertAU podem ser encontrados em https://repositorio.icpedu.rnp.br/.

De acordo com o IETF PKIX RFC 3647, esta PC/DPC é dividida em nove componentes que abrangem controles de segurança, práticas e procedimentos para os serviços de certificação fornecidos pela ICPEdu CertAU.

As Autoridades Certificadoras cobertas por este documento podem ser encontradas no Lista de Serviços Confiáveis (LSC) da RNP em https://repositorio.icpedu.rnp.br/public/lsc.

Este trabalho é baseado no documento CPS/CP do Let's Encrypt https://github.com/letsencrypt/cp-cps e está licenciado sob a Licença Creative Commons Attribution 4.0 International. Para visualizar uma cópia dessa licença, visite https://creativecommons.org/licenses/by/4.0/ ou envie uma carta para Creative Commons, PO Box 1866, Mountain View, CA 94042, EUA.

1.2 Nome do Documento e Identificação

Este é a PC/DPC da ICPEdu CertAU da RNP. Este documento foi aprovado pela RNP para publicação e está disponível em https://repositorio.icpedu.rnp.br/public/home/certau/dpc.

As seguintes revisões foram feitas:

Data	Alterações	Versão
16/06/2026	Primeira versão publicada	1.0

1.3 Participantes da ICP

1.3.1 Autoridades Certificadoras

Esta PC/DPC se aplica às ACs da ICPEdu CertAU.

1.3.2 Autoridades de Registro

Não há Autoridades de Registro atreladas à ICPEdu CertAU. As funções de registro e identificação das pessoas é feita pela Instituição de Ensino e Pesquisa que adere ao serviço. Para a emissão de certificados, a verificação da identidade do solicitante do certificado é descrita na Seção 3.2.3.

1.3.3 Assinantes

Veja a definição de "Assinante" na Seção 1.6.1 Definições.

1.3.4 Partes Confiáveis

Veja a definição de "Parte Confiável" na Seção 1.6.1 Definições.

1.3.5 Outros Participantes

Outros participantes incluem ACs que assinam ou emitem subordinados à ICPEdu CertAU.

Fornecedores e prestadores de serviços da ICPEdu CertAU com acesso a informações confidenciais ou sistemas privilegiados são obrigados a operar em conformidade com esta PC/DPC.

1.4 Uso de Certificado

1.4.1 Usos Apropriados de Certificado

Os certificados emitidos no âmbito desta PC/DPC destinam-se exclusivamente à realização e verificação de assinaturas digitais, com a finalidade de comprovar a autoria, a integridade e, quando aplicável, o comprometimento do titular com o conteúdo assinado.

1.4.2 Usos Proibidos de Certificado

Os certificados não podem ser usados:

- Para qualquer aplicação que exija desempenho à prova de falhas, como: a) operação de instalações de energia nuclear; b) sistemas de controle de tráfego aéreo; c) sistemas de navegação de aeronaves; d) sistemas de controle de armas; ou e) qualquer outro sistema em que a falha possa levar a lesões, morte ou danos ambientais.
- Para arquiteturas de software ou hardware que fornecem instalações para interferência em comunicações criptografadas, incluindo, mas não se limitando a: a) escuta ativa (por exemplo, ataques de "man-in-the-middle"); ou b) gerenciamento de tráfego de nomes de domínio ou endereços de protocolo de internet que a organização não possui ou controla. Observe que essas restrições se aplicam independentemente de uma parte confiante que se comunique através da arquitetura de software ou hardware ter conhecimento de sua capacidade de interferir nas comunicações criptografadas.

Observe que os Certificados não garantem nada em relação à reputação, honestidade ou ao estado atual da segurança do ponto final. Um Certificado apenas representa que as informações nele contidas foram verificadas como razoavelmente corretas quando o Certificado foi emitido.

1.5 Administração da Política

1.5.1 Organização que Administra o Documento

A RNP mantém este documento.

1.5.2 Pessoa de Contato

A RNP pode ser contatada em:

Rede Nacional de Ensino e Pesquisa
SAUS Quadra 5, Lote 6, Bloco H - Asa Sul
Brasília
Brasil

Relatórios de Problemas de Certificado podem ser enviados por email para:

atendimento@rnp.br

1.5.3 Pessoa que Determina a Adequação da PC/DPC para a Política

RNP é responsável por determinar a adequação desta PC/DPC. A política da RNP é informada por resultados e recomendações recebidas de auditores e pesquisadores.

1.5.4 Procedimentos de Aprovação da PC/DPC

RNP aprova qualquer revisão a esta PC/DPC após uma revisão formal.

1.6 Definições e Acrônimos

1.6.1 Definições

Repositório de Certificados: Um repositório de informações sobre certificados da RNP. Está localizado em: https://repositorio.icpedu.rnp.br/

Repositório de Políticas e Legislação: Um repositório de documentos de política e legais relacionados à ICPEdu CertAU. Está localizado em: https://repositorio.icpedu.rnp.br/

Instalações Seguras de ICP: Instalações projetadas para proteger a infraestrutura sensível de ICP, incluindo chaves privadas da AC.

Contribuidor Confiável: Um contribuidor que desempenha um Papel Confiável. Contribuidores Confiáveis podem ser funcionários, contratados ou membros da comunidade. Contribuidores Confiáveis devem ser devidamente treinados e qualificados e ter as obrigações legais adequadas antes de desempenhar um Papel Confiável.

Papel Confiável: Um papel que qualifica uma pessoa a acessar ou modificar sistemas, infraestrutura e informações confidenciais da ICPEdu CertAU.

Consulte os Requisitos Básicos para definições adicionais.

1.6.2 Acrônimos

Acrônimo	Significado
MSC	Módulo de Segurança de Hardware
IP	Protocolo de Internet
RNP	Rede Nacional de Ensino e Pesquisa
PMA	Autoridade de Gestão de Políticas
SAN	Nome Alternativo do Sujeito
TLD	Domínio de Nível Superior

Consulte os Requisitos Básicos para acrônimos adicionais.

1.6.3 Referências

Requisitos Básicos do CA/Browser Forum para a Emissão e Gestão de Certificados Publicamente Confiáveis

Requisitos de Segurança de Sistema e Certificado de Rede do CA/Browser Forum

1.6.4 Convenções

Os termos não definidos de outra forma nesta PC/DPC devem ser interpretados conforme definidos nos acordos aplicáveis, manuais de usuário, Políticas de Certificado e Declarações de Práticas de Certificação da AC.

As palavras-chave "DEVE", "NÃO DEVE", "OBRIGATÓRIO", "DEVERÁ", "NÃO DEVERÁ", "DEVERIA", "NÃO DEVERIA", "RECOMENDADO", "PODE" e "OPCIONAL" nesta PC/DPC devem ser interpretadas de acordo com o RFC 2119.

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

O PC/DPC combinado da RNP, Política de Privacidade, Termo de Uso e outros documentos estão disponíveis publicamente no Repositório de Políticas e Legislação, que pode ser encontrado em:

https://repositorio.icpedu.rnp.br/

2.2 Publicação de Informações

Registros de todos os certificados de AC Raiz e Subordinados da RNP, incluindo aqueles que foram revogados, estão disponíveis no LSC:

https://repositorio.icpedu.rnp.br/public/lsc

2.3 Tempo ou Frequência de Publicação

Novos ou atualizados PC/DPC combinados da RNP, Política de Privacidade, Termo de Uso e documentos de auditoria são disponibilizados publicamente o mais rápido possível. A RNP revisará, aprovará e publicará documentos atualizados da PC/DPC pelo menos quinquenalmente.

Novos ou atualizados certificados de AC Raiz e Subordinados da RNP são disponibilizados publicamente o mais rápido possível em https://repositorio.icpedu.rnp.br/public/lsc.

2.4 Controles de Acesso aos Repositórios

O acesso apenas para leitura ao Repositório de Políticas e Legislação e informações de certificados é irrestrito. O acesso para gravação é protegido por controles lógicos e/ou físicos.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Nomeação

3.1.1 Tipos de nomes

Os nomes distintos dos certificados e os nomes alternativos do sujeito estão em conformidade com os Requisitos Básicos.

3.1.2 Necessidade de nomes significativos

Os certificados RNP incluem um campo "Sujeito" que identifica a entidade do sujeito (ou seja, organização ou FQDN). A entidade do sujeito é identificada usando um nome distinto.

Os certificados RNP incluem um campo "Emissor" que identifica a entidade emissora. A entidade emissora é identificada usando um nome distinto.

3.1.3 Anonimato ou pseudonimato de assinantes

Nenhuma estipulação.

3.1.4 Regras para interpretar várias formas de nomes

Os nomes distintos nos certificados devem ser interpretados usando os padrões X.500 e a sintaxe ASN.1.

3.1.5 Exclusividade dos nomes

Nenhuma estipulação.

3.1.6 Reconhecimento, autenticação e papel das marcas registradas

A RNP reserva-se o direito de tomar todas as decisões relativas aos nomes dos assinantes nos certificados. As entidades que solicitam certificados serão obrigadas a demonstrar seu direito de usar os nomes (por exemplo, através de um provedor de identidade).

3.2 Validação inicial da identidade

A RNP pode optar por não emitir nenhum certificado a seu exclusivo critério.

3.2.1 Método para provar posse da chave privada

Os solicitantes são obrigados a provar a posse da Chave Privada correspondente à Chave Pública em uma solicitação de certificado assinando um CSR.

3.2.2 Autenticação da identidade da Organização e do Domínio

A RNP não emite certificados de Validação de Domínio (DV).

3.2.3 Autenticação da identidade individual

A RNP verifica as identidades individuais por meio de provedores de identidade confiáveis e assume que as informações de identidade fornecidas são precisas.

3.2.4 Informações do assinante não verificadas

Informações do solicitante não verificadas não são incluídas nos certificados RNP.

3.2.5 Validação de autoridade

A autoridade para solicitar um certificado é concedida a aplicativos de assinatura em uma análise caso a caso. Aplicativos de assinatura que recebem essa autoridade são considerados confiáveis.

3.2.6 Critérios para Interoperabilidade ou Certificação

A RNP proporciona interoperabilidade através de sua Lista de Serviços Confiáveis disponível em https://repositorio.icpedu.rnp.br/public/lsc.

3.3 Identificação e autenticação para solicitações de reemissão de chave

3.3.1 Identificação e autenticação para reemissão de chave rotineira

A RNP não permite rotinas de reemissão de chave.

3.3.2 Identificação e autenticação para reemissão de chave após revogação

Não aplicável.

3.4 Identificação e autenticação para solicitação de revogação

Os certificados de assinantes são irrevogáveis.

Identificação e autenticação não são necessárias quando a RNP está solicitando a revogação.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação de Certificado

4.1.1 Quem pode enviar uma solicitação de certificado

Aplicações de assinatura confiáveis podem enviar solicitações de emissão de certificado.

As aplicações de assinatura confiáveis DEVEM encaminhar um token de acesso de um provedor de identidade confiável válido do assinante.

A emissão dependerá da validação adequada e da conformidade com as políticas da RNP.

4.1.2 Processo de inscrição e responsabilidades

O processo de inscrição envolve as seguintes etapas, em nenhuma ordem específica:

- Gerar um par de chaves

- Enviar uma solicitação de certificado contendo todas as informações necessárias, incluindo a chave pública
- Concordar com o Acordo do Assinante relevante

4.2 Processamento da solicitação de certificado

4.2.1 Execução de funções de identificação e autenticação

A RNP executa todas as funções de identificação e autenticação de acordo com esta PC/DPC.

As informações do certificado são verificadas usando dados e documentos obtidos por meio de provedores de identidade confiáveis.

4.2.2 Aprovação ou rejeição de solicitações de certificado

A aprovação requer a conclusão bem-sucedida da validação do token de identidade, bem como a conformidade com todas as políticas da AC.

4.2.3 Tempo para processar solicitações de certificado

Nenhuma estipulação.

4.3 Emissão de certificado

4.3.1 Ações da AC durante a emissão de certificado

Em alto nível, os seguintes passos são tomados durante a emissão de um certificado de Assinante. Os processos automatizados da RNP confirmam que todos os nomes que aparecerão no Nome Comum e/ou na lista de SANs do certificado foram devidamente validados e controlados pelo Assinante que solicitou o certificado por meio do provedor de identidade confiável. O certificado é assinado por uma AC Subordinada em um MSC. Após a conclusão da emissão, o certificado é enviado como resposta à solicitação HTTP correspondente da API de emissão de certificados.

4.3.2 Notificação ao assinante pela AC da emissão do certificado

As entidades finais podem receber um e-mail notificando que o certificado foi emitido com sucesso.

4.4 Aceitação do certificado

4.4.1 Conduta que constitui aceitação do certificado

Nenhuma estipulação.

4.4.2 Publicação do certificado pela AC

Consulte a Seção 2.2 deste documento para informações sobre a publicação de certificados da AC Raiz e Subordinada.

4.4.3 Notificação da emissão do certificado pela AC para outras entidades

Consulte a Seção 4.4.2.

4.5 Uso do par de chaves e do certificado

4.5.1 Uso da chave privada e do certificado pelo assinante

O uso de Chaves Privadas e Certificados pelos Assinantes é regido pelo Termo de Uso da RNP.

4.5.2 Uso da chave pública e do certificado pela parte confiável

As Partes Confiáveis devem avaliar completamente o contexto em que confiam nos certificados e nas informações neles contidas e decidir até que ponto o risco de confiança é aceitável. Se o risco de confiar em um certificado for considerado inaceitável, as Partes Confiáveis não devem usar o certificado ou devem obter garantias adicionais antes de usar o certificado.

A RNP não garante que qualquer software utilizado pelas Partes Confiáveis para avaliar ou manusear certificados o faça de maneira adequada.

4.6 Renovação de certificado

Solicitações de renovação de certificado são tratadas como pedidos de novos certificados.

4.6.1 Circunstâncias para renovação de certificado

Nenhuma estipulação.

4.6.2 Quem pode solicitar a renovação

Nenhuma estipulação.

4.6.3 Processamento de solicitações de renovação de certificado

Nenhuma estipulação.

4.6.4 Notificação da emissão de um novo certificado ao assinante

Nenhuma estipulação.

4.6.5 Conduta que constitui aceitação de um certificado renovado

Nenhuma estipulação.

4.6.6 Publicação do certificado renovado pela AC

Nenhuma estipulação.

4.6.7 Notificação da emissão do certificado pela AC para outras entidades

Nenhuma estipulação.

4.7 Reemissão de chave do certificado

Solicitações de reemissão de chave de certificado são tratadas como pedidos de novos certificados.

4.7.1 Circunstâncias para reemissão de chave do certificado

Nenhuma estipulação.

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

Nenhuma estipulação.

4.7.3 Processamento de solicitações de reemissão de chave

Nenhuma estipulação.

4.7.4 Notificação da emissão de um novo certificado ao assinante

Nenhuma estipulação.

4.7.5 Conduta que constitui aceitação de um certificado reemitido

Nenhuma estipulação.

4.7.6 Publicação do certificado reemitido pela AC

Nenhuma estipulação.

4.7.7 Notificação da emissão do certificado pela AC para outras entidades

Nenhuma estipulação.

4.8 Modificação de certificado

Solicitações de modificação de certificado são tratadas como pedidos de novos certificados.

4.8.1 Circunstâncias para modificação de certificado

Nenhuma estipulação.

4.8.2 Quem pode solicitar a modificação de certificado

Nenhuma estipulação.

4.8.3 Processamento de solicitações de modificação de certificado

Nenhuma estipulação.

4.8.4 Notificação da emissão de um novo certificado ao assinante

Nenhuma estipulação.

4.8.5 Conduta que constitui aceitação de um certificado modificado

Nenhuma estipulação.

4.8.6 Publicação do certificado modificado pela AC

Nenhuma estipulação.

4.8.7 Notificação da emissão do certificado pela AC para outras entidades

Nenhuma estipulação.

4.9 Revogação e suspensão de certificado

4.9.1 Circunstâncias para revogação

A RNP não revoga Certificados na ICPEdu CertAU.

4.9.2 Quem pode solicitar a revogação

A RNP seguirá os Requisitos Básicos e revogará um certificado de AC de acordo com a Seção 4.9.1.2 dos Requisitos Básicos, marcando seu Root correspondente como não confiável na LSC da RNP.

4.9.3 Procedimento para solicitação de revogação

Questões relacionadas aos certificados da AC que possam resultar na sua revogação podem ser feitas por e-mail para atendimento@rnp.br, a RNP responderá a essas solicitações o mais rápido possível, embora uma investigação sobre a legitimidade da solicitação possa demorar mais tempo.

Uma investigação sobre se a revogação ou outra ação apropriada é justificada será baseada, pelo menos, nos seguintes critérios:

1. A natureza do problema alegado;
2. O número de relatórios de problemas de certificados recebidos sobre um determinado certificado ou assinante;
3. A entidade que fez a reclamação; e
4. Legislação relevante.

4.9.4 Período de carência para solicitação de revogação

Nenhuma estipulação.

4.9.5 Tempo para a AC processar a solicitação de revogação

Nenhuma estipulação.

4.9.6 Requisitos de verificação de revogação para partes confiáveis

As Partes Confiáveis devem verificar periodicamente a validade dos certificados raiz através da LSC da ICPEdu CertAU. O período em que a LSC é atualizada pode depender das necessidades da Parte Confiável. Partes Confiáveis que não puderem ou optarem por não atualizar sua versão local da LSC, mas decidirem confiar em um certificado de qualquer maneira, o fazem por sua própria conta e risco.

Consulte a Seção 4.5.2.

4.9.7 Frequência de emissão de CRLs (se aplicável)

Uma única CRL vazia é emitida quando a AC é criada. Certificados emitidos sob a ICPEdu CertAU são irrevogáveis e não requerem mecanismos de revogação.

4.9.8 Latência máxima para CRLs (se aplicável)

Nenhuma estipulação.

4.9.9 Disponibilidade de verificação de status/revogação online

Nenhuma estipulação.

4.9.10 Requisitos de verificação de revogação online

Nenhuma estipulação.

4.9.11 Outras formas de anúncios de revogação disponíveis

Nenhuma estipulação.

4.9.12 Requisitos especiais para comprometimento de chave

Nenhuma estipulação.

4.9.13 Circunstâncias para suspensão

A RNP não suspende certificados.

4.9.14 Quem pode solicitar a suspensão

Não aplicável.

4.9.15 Procedimento para solicitação de suspensão

Não aplicável.

4.9.16 Limites para o período de suspensão

Não aplicável.

4.10 Serviços de status de certificado

4.10.1 Características operacionais

Nenhuma estipulação.

4.10.2 Disponibilidade do serviço

Nenhuma estipulação.

4.10.3 Recursos opcionais

Nenhuma estipulação.

4.11 Fim da assinatura

A assinatura de um Assinante inicia ao final da autenticação e termina ao finalizar a assinatura do documento.

4.12 Escrow e recuperação de chave

4.12.1 Políticas e práticas de escrow e recuperação de chave

Não aplicável.

4.12.2 Políticas e práticas de encapsulação e recuperação de chave de sessão

Não aplicável.

5. CONTROLES DE GESTÃO, OPERACIONAIS E FÍSICOS

5.1 CONTROLES DE SEGURANÇA FÍSICA

5.1.1 Localização e construção do site

As Instalações Seguras de ICP da RNP estão localizadas no Brasil, assim como todas as Chaves Privadas das ACs da ICPEdu CertAU.

A RNP mantém pelo menos duas Instalações Seguras de ICP o tempo todo para garantir redundância.

As Instalações Seguras de ICP são construídas para prevenir a entrada não autorizada ou interferência.

As Instalações Seguras de ICP são monitoradas continuamente (24x7) para prevenir a entrada não autorizada ou interferência.

5.1.2 Acesso físico

O acesso físico às Instalações Seguras de ICP da RNP é restrito a funcionários, fornecedores e contratados autorizados da RNP, cujo acesso é

necessário para executar suas funções. As restrições de acesso são fortemente aplicadas por meio de mecanismos de autenticação multifator.

5.1.3 Energia e ar condicionado

Fontes de energia redundantes estão prontamente disponíveis em cada Instalação Segura de ICP e são projetadas para atender aos requisitos operacionais da RNP.

Os sistemas de ar condicionado em cada Instalação Segura de ICP são projetados para atender aos requisitos operacionais da RNP.

5.1.4 Exposição à água

As Instalações Seguras de ICP da RNP são projetadas para proteger a infraestrutura da RNP contra exposição/danos causados por água.

5.1.5 Prevenção e proteção contra incêndio

As Instalações Seguras de ICP da RNP são projetadas para prevenir incêndios e fornecer supressão, se necessário.

5.1.6 Armazenamento de mídia

As Instalações Seguras de ICP da RNP são projetadas para prevenir danos acidentais ou acesso não autorizado à mídia.

5.1.7 Descarte de resíduos

A RNP proíbe que qualquer mídia que contenha ou tenha contido dados sensíveis saia do controle organizacional de tal forma que ainda possa estar operacional ou conter dados recuperáveis. Tal mídia pode incluir documentos impressos ou dispositivos de armazenamento digital. Quando a mídia que contém informações sensíveis chega ao fim de sua vida útil, a mídia é apagada de forma segura ou destruída fisicamente de modo que a recuperação seja razoavelmente impossível.

Exceções onde a mídia deve ser transferida para outro local podem ser conduzidas por meio de cerimônias pré-aprovadas e devem ser devidamente documentadas.

5.1.8 Backup fora do local

A RNP mantém várias ACs diferentes que atuam como backups em várias Instalações Seguras de ICP. Todas as chaves privadas das ACs de backup são armazenadas em dispositivos que atendem aos critérios do FIPS 140-2 Nível 3 (ou superior).

5.2 Controles procedimentais

5.2.1 Papéis de confiança

Todas as pessoas, sejam funcionários ou não, que tenham a capacidade de impactar materialmente a operação dos sistemas e serviços da ICPEdu CertAU ou a capacidade de visualizar informações confidenciais da AC, devem fazê-lo enquanto designadas para atuar em um Papel de Confiança.

Papéis de Confiança incluem, mas não se limitam a:

- Administradores de ICP
    - Informação Confidencial: Acesso direto com base na necessidade de saber
    - Acesso ao Ambiente: Teste sim, produção sim
    - Autoridade de Tomada de Decisões na AC: Sim
- Equipe de ICP
    - Informação Confidencial: Visualização com base na necessidade de saber
    - Acesso ao Ambiente: Teste sim, produção não
    - Autoridade de Tomada de Decisões na AC: Sim
- Parceiros de ICP
    - Informação Confidencial: Visualização com base na necessidade de saber
    - Acesso ao Ambiente: Teste sim, produção não
    - Autoridade de Tomada de Decisões na AC: Não

- Equipe Não-PKI
    - Informação Confidencial: Visualização com base na necessidade de saber
    - Acesso ao Ambiente: Teste não, produção não
    - Autoridade de Tomada de Decisões na AC: Não

Cada Papel de Confiança requer um nível apropriado de treinamento e obrigação legal.

5.2.2 Número de Indivíduos Necessários por Tarefa

Diversas tarefas, como a geração de chaves e a entrada em áreas que contêm fisicamente sistemas operacionais da ICPEdu CertAU, requerem a presença de pelo menos duas pessoas em Papéis de Confiança.

5.2.3 Identificação e autenticação para cada papel

Qualquer pessoa que execute trabalho em um Papel de Confiança deve identificar-se e autenticar-se antes de acessar os sistemas ou informações confidenciais da ICPEdu CertAU.

5.2.4 Papéis que exigem separação de deveres

Consulte a Seção 6.6.1.

5.3 Controles de pessoal

5.3.1 Qualificações, experiência e requisitos de autorização

A gestão da RNP é responsável por garantir que os Contribuidores de Confiança sejam confiáveis e competentes, o que inclui ter qualificações e experiência adequadas.

A gestão da RNP assegura isso com práticas adequadas de entrevista, treinamento, e monitoramento e revisão regulares do desempenho dos Contribuidores de Confiança.

5.3.2 Procedimentos de verificação de antecedentes

Os Contribuidores de Confiança devem passar por uma aprovação da gestão da DAGSer.

5.3.3 Requisitos e Procedimentos de Treinamento

Os Contribuidores de Confiança devem ser treinados em tópicos relevantes para o papel que irão desempenhar.

Programas de treinamento são desenvolvidos para cada papel pela gestão da RNP e pelos Oficiais de Segurança.

5.3.4 Frequência e requisitos de reciclagem

O treinamento é oferecido sempre que mudanças na indústria ou nas operações exigirem, para que os contribuintes possam desempenhar suas funções de confiança com competência.

5.3.5 Frequência e sequência de rotação de funções

Nenhuma estipulação.

5.3.6 Sanções para ações não autorizadas

Serão tomadas medidas para proteger a RNP e seus Assinantes sempre que os Contribuidores de Confiança da RNP, seja por negligência ou intenção maliciosa, falharem em cumprir as políticas da RNP, incluindo esta PC/DPC.

As ações tomadas em resposta à não conformidade podem incluir demissão, remoção de papéis de confiança ou denúncia às autoridades legais.

Assim que a gestão tomar conhecimento da não conformidade, os Contribuidores de Confiança em questão serão removidos dos papéis de confiança até que uma revisão de suas ações seja concluída.

5.3.7 Controles para Contratados Independentes

Os contratados independentes que são designados para desempenhar Papéis de Confiança estão sujeitos aos deveres e requisitos especificados para tais papéis nesta PC/DPC. Isso inclui os descritos na Seção 5.3. As possíveis sanções para atividades não autorizadas por contratados independentes são descritas na Seção 5.3.6.

5.3.8 Documentação fornecida ao pessoal

Os Contribuidores de Confiança recebem toda a documentação necessária para desempenhar suas funções. Isso inclui, no mínimo, uma cópia da PC/DPC da RNP e da Política de Segurança da Informação.

5.4 Procedimentos de registro de auditoria

5.4.1 Tipos de eventos registrados

Os logs de auditoria são gerados para todos os eventos relacionados à segurança da AC (física e lógica) e à emissão de certificados. Os logs são gerados automaticamente sempre que possível. Quando é necessário registrar informações manualmente, os logs são mantidos em papel com a confirmação por escrito de uma testemunha e armazenados com segurança. Todos os logs de auditoria, eletrônicos ou não, devem ser retidos e disponibilizados para auditores de conformidade mediante solicitação.

No mínimo, cada registro de auditoria inclui:

- Data e hora da entrada;
- Identidade da pessoa (ou máquina) que fez a entrada; e
- Descrição da entrada.

5.4.2 Frequência de Processamento e Arquivamento de Logs de Auditoria

Nenhuma estipulação.

5.4.3 Período de Retenção dos Logs de Auditoria

Os logs de auditoria são mantidos por pelo menos dois (2) anos.

5.4.4 Proteção do Log de Auditoria

Os logs de auditoria, sejam de produção ou arquivados, são protegidos usando controles de acesso lógico e/ou físico.

5.4.5 Procedimentos de Backup dos Logs de Auditoria

A RNP faz cópias de backup regulares dos logs de auditoria.

5.4.6 Sistema de Acumulação de Logs de Auditoria (interno vs. externo)

Os dados de auditoria são gerados e relatados/registrados automaticamente por sistemas operacionais, aplicativos de software de AC e dispositivos de rede. Existem sistemas para garantir o relato e registro adequado dos dados de auditoria, e a falha de tais sistemas pode levar à suspensão dos serviços da AC até que o registro adequado dos logs de auditoria seja restaurado.

5.4.7 Notificação ao sujeito causador do evento

Nenhuma estipulação.

5.4.8 Avaliações de vulnerabilidade

Os logs de auditoria são monitorados por Contribuidores de Confiança, incluindo a equipe de operações e engenharia. Anomalias que indicam tentativas de violação da segurança da AC são relatadas e investigadas.

Varreduras de vulnerabilidades internas e externas ocorrem periodicamente, com periodicidade que pode depender de processos recentes, como a criação de uma nova AC, inclusão de ACs na LSC e vulnerabilidades relatadas.

Os Oficiais de Segurança da RNP realizam uma avaliação de risco sob demanda. Esta avaliação de risco:

1. Identifica ameaças internas e externas previsíveis que podem resultar em acesso não autorizado, divulgação, uso indevido, alteração ou destruição de qualquer Dado de Certificado ou Processos de Gestão de Certificados;
2. Avalia a probabilidade e o potencial de dano dessas ameaças, levando em consideração a sensibilidade dos Dados de Certificados e Processos de Gestão de Certificados; e
3. Avalia a suficiência das políticas, procedimentos, sistemas de informação, tecnologia e outras medidas que a AC tem em vigor para contrapor essas ameaças.

5.5 Arquivamento de registros

5.5.1 Tipos de registros arquivados

A RNP arquiva todos os logs de auditoria, cujo conteúdo é descrito na Seção 5.4.1. A RNP também arquiva outros documentos e informações críticos para entender a segurança histórica e o desempenho dos deveres da AC.

5.5.2 Período de retenção para o arquivo

Os registros arquivados são mantidos por pelo menos dois (2) anos.

5.5.3 Proteção do arquivo

Os arquivos são protegidos contra modificação ou destruição não autorizada por controles de segurança e ambientais robustos.

5.5.4 Procedimentos de backup do arquivo

Os arquivos são regularmente copiados para backup.

5.5.5 Requisitos para a marcação de tempo dos registros

Os registros são marcados com data e hora à medida que são criados.

Registros gerados por máquinas usam a hora do sistema, que é sincronizada automaticamente com fontes de tempo de terceiros. Máquinas sem acesso à rede têm a hora ajustada manualmente.

Registros manuais usam uma data e hora inserida manualmente, completa com o fuso horário em uso.

5.5.6 Sistema de coleta de arquivos (interno ou externo)

Nenhuma estipulação.

5.5.7 Procedimentos para obter e verificar informações do arquivo

Nenhuma estipulação.

5.6 Troca de chaves

Quando um certificado de AC está se aproximando da expiração, uma nova AC com uma chave privada distinta pode ser criada para substituí-lo.

5.7 Recuperação de comprometimento e desastre

5.7.1 Procedimentos de manuseio de incidentes e comprometimentos

A RNP criou e mantém procedimentos de resposta a incidentes para uma gama de situações potenciais de comprometimento e desastre. Tais situações incluem, mas não se limitam a, desastres naturais, incidentes de segurança e falhas de equipamentos.

5.7.2 Procedimentos de Recuperação se os Recursos de Computação, Software e/ou Dados forem Corrompidos

No caso de recursos de computação, software e/ou dados serem corrompidos ou danificados de outra forma, a RNP avaliará a situação, incluindo seu impacto na integridade e segurança da AC, e tomará as medidas apropriadas. As operações da AC podem ser suspensas até que a mitigação esteja completa. Os assinantes podem ser notificados se a corrupção ou dano tiver um impacto material no serviço fornecido a eles.

5.7.3 Procedimentos de Recuperação após Comprometimento de Chave

No caso de uma Chave Privada da AC da RNP ser comprometida ou suspeita de comprometimento, a RNP iniciará imediatamente uma investigação minuciosa. Evidências forenses serão coletadas e asseguradas o mais rápido possível. Se não for possível determinar com um alto grau de certeza que a chave privada em questão não foi comprometida, então as seguintes etapas podem ser tomadas na ordem que os Oficiais de Segurança da RNP considerarem mais apropriada:

- A RNP removerá o certificado da LSC ou o definirá como não confiável.
- A RNP notificará programas que dependem da integridade da chave em questão.
- A RNP notificará os Assinantes que dependem da integridade da chave em questão.

5.7.4 Capacidades de continuidade de negócios após um desastre

A RNP mantém várias instalações geograficamente diversas, cada uma das quais é capaz de operar os sistemas de AC da RNP independentemente. No caso de um desastre desabilitar completamente uma instalação, as operações da AC da RNP serão transferidas para outra instalação.

5.8 Terminação de AC ou RA

No caso de os serviços de AC da RNP serem encerrados:

- Todas as partes afetadas, incluindo programas e Assinantes, serão notificados com a maior antecedência possível.
- A RNP criará e revisará um plano de terminação.

Se existir uma entidade sucessora adequada, as seguintes etapas serão tomadas:

- Os registros, logs e outros documentos críticos serão transferidos para a organização sucessora de forma segura e em conformidade.
- Serão feitos arranjos para a continuação em conformidade das responsabilidades da AC.

Se não existir uma entidade sucessora adequada, as seguintes etapas serão tomadas:

- As Chaves Privadas da AC da RNP serão destruídas.
- Registros da AC, logs e outros documentos críticos serão transferidos para uma entidade terceirizada ou governamental com controles legais adequados para proteger as informações enquanto permitem seu uso em conformidade com as políticas relevantes e a lei.

6. CONTROLES DE SEGURANÇA TÉCNICA

6.1 Geração e instalação de pares de chaves

6.1.1 Geração de pares de chaves

As Chaves Privadas da AC da RNP são geradas por Módulos de Segurança de Hardware (MSCs) que atendem aos requisitos da Seção 6.2.1. Este

processo ocorre durante uma cerimônia que atende aos requisitos desta PC/DPC.

6.1.2 Entrega da chave privada ao assinante

Nenhuma estipulação.

6.1.3 Entrega da chave pública ao emissor do certificado

Consulte a Seção 4.3.1.

6.1.4 Entrega da chave pública da AC às partes confiantes

As Chaves Públicas da RNP são fornecidas às Partes Confiáveis pela LSC do ICPEdu CertAU, disponível em https://repositorio.icpedu.rnp.br/public/lsc.

6.1.5 Tamanhos das chaves

As Chaves Privadas RSA da AC Raiz da RNP têm, pelo menos, o tamanho de 4096 bits.

As Chaves Privadas RSA das ACs Subordinadas da RNP têm, pelo menos, o tamanho de 2048 bits.

6.1.6 Geração de parâmetros de chaves públicas e verificação de qualidade

A RNP usa MSCs que estão em conformidade com o FIPS 186, capazes de fornecer geração de números aleatórios e criação interna de chaves RSA de pelo menos 2048 bits.

6.1.7 Propósitos de uso das chaves (conforme o campo de uso de chave X.509 v3)

Consulte a Seção 7.

6.2 Proteção da Chave Privada e Controles de Engenharia de Módulo Criptográfico

6.2.1 Padrões e controles de módulo criptográfico

A RNP usa MSCs que atendem aos requisitos do FIPS 140-2 Nível 3 (ou superior).

6.2.2 Controle multipessoal (n de m) da chave privada

A RNP implementou mecanismos de segurança que exigem a atuação de várias pessoas em Papéis de Confiança para acessar as Chaves Privadas da AC da RNP, tanto física quanto logicamente.

6.2.3 Depósito de chave privada

A RNP não faz o depósito de Chaves Privadas da AC e não oferece esse serviço para Assinantes.

6.2.4 Backup de chave privada

A RNP não faz backup das chaves privadas.

6.2.5 Arquivamento de chave privada

A RNP não arquiva chaves privadas.

6.2.6 Transferência de chave privada para ou de um módulo criptográfico

As Chaves Privadas da AC da RNP são geradas dentro dos MSCs. Nenhuma cópia é feita para qualquer finalidade, incluindo backups.

As chaves privadas nunca existem em formato de texto claro fora dos MSCs.

6.2.7 Armazenamento de chave privada em módulo criptográfico

As Chaves Privadas da AC da RNP são armazenadas em MSCs que atendem aos requisitos descritos na Seção 6.2.1.

6.2.8 Ativação de Chaves Privadas

As Chaves Privadas da AC da RNP estão sempre armazenadas em MSCs e são ativadas usando os mecanismos fornecidos pelo fabricante do MSC.

6.2.9 Desativação de Chaves Privadas

As Chaves Privadas da AC da RNP estão sempre armazenadas em MSCs e são desativadas usando os mecanismos fornecidos pelo fabricante do MSC.

6.2.10 Destruição de Chaves Privadas

As Chaves Privadas da AC da RNP são destruídas por Contribuidores de Confiança usando um método de zeramento validado pelo FIPS 140-2 (ou superior) fornecido pelos MSCs que armazenam as chaves. Não é necessária a destruição física do MSC.

6.2.11 Capacidades do Módulo Criptográfico

Consulte a Seção 6.2.1.

6.3 Outros aspectos da gestão de pares de chaves

6.3.1 Arquivamento de chave pública

Consulte a Seção 5.5.

6.3.2 Períodos operacionais de certificados e períodos de uso de pares de chaves

Os períodos de validade dos certificados da AC Raiz, AC Subordinada e dos Assinantes da RNP são descritos na Seção 7 deste documento.

Os pares de chaves da AC Raiz e da AC Subordinada da RNP têm períodos de vida correspondentes aos seus certificados.

6.4 Dados de ativação

6.4.1 Geração e instalação de dados de ativação

Os dados de ativação usados para ativar as Chaves Privadas da AC da RNP são gerados durante uma cerimônia de chave. Os dados de ativação são então transferidos para a pessoa que os utilizará ou para o local onde serão armazenados.

6.4.2 Proteção dos dados de ativação

Os dados de ativação são protegidos contra divulgação não autorizada por meios lógicos e/ou físicos.

6.4.3 Outros aspectos dos dados de ativação

Sem estipulação.

6.5 Controles de segurança de computadores

6.5.1 Requisitos técnicos específicos de segurança de computadores

A infraestrutura e os sistemas da AC da RNP são adequadamente protegidos para evitar acesso ou modificação não autorizados ao software e aos dados da AC. O acesso aos sistemas é protegido por autenticação multifator sempre

que possível. As atualizações de segurança são aplicadas em tempo hábil. Varreduras de vulnerabilidades são realizadas regularmente.

6.5.2 Classificação de segurança de computadores

Sem estipulação.

6.6 Controles técnicos de ciclo de vida

6.6.1 Controles de desenvolvimento de sistemas

A RNP desenvolveu políticas e procedimentos para gerenciar efetivamente a aquisição e o desenvolvimento de seus sistemas de AC.

O hardware e o software da AC da RNP são dedicados exclusivamente a funções de AC.

A seleção de fornecedores inclui uma avaliação da reputação no mercado, capacidade de entregar um produto de qualidade, histórico de vulnerabilidades e a probabilidade de permanecer viável no futuro. As entregas de produtos físicos são recebidas por Contribuidores de Confiança e inspecionadas quanto a evidências de violação.

A RNP mantém um ambiente de teste de AC separado do ambiente de produção. O ambiente de teste simula razoavelmente o ambiente de produção, mas não tem acesso às Chaves Privadas da AC da RNP usadas em certificados confiáveis do ambiente de produção. O propósito deste ambiente de teste é permitir testes extensivos, mas seguros, de software e sistemas que são ou serão implantados no ambiente de produção da AC.

A RNP desenvolveu e mantém políticas e procedimentos adequados de controle de mudanças a serem seguidos sempre que os sistemas da AC são modificados. Mudanças nos sistemas da AC da RNP requerem revisão por Pessoal de Confiança qualificado que seja diferente da pessoa que solicitou a mudança. As solicitações de mudança são documentadas, assim como quaisquer revisões ou aprovações subsequentes necessárias.

Quando a RNP desenvolve software para ser usado nas operações da AC, políticas de desenvolvimento de software são implementadas e metodologias são seguidas para garantir a qualidade e integridade do software. Isso sempre inclui um requisito de revisão por pares das mudanças de código. Os privilégios de commit de código são concedidos apenas a colaboradores qualificados e confiáveis. Ninguém com a capacidade de implantar software nos sistemas do ICPEdu CertAU (por exemplo, Administradores de ICP) pode ter a capacidade de fazer commit de código de forma unilateral ao software central da AC. O inverso também é verdadeiro.

6.6.2 Controles de gestão de segurança

A RNP possui mecanismos para controlar e monitorar a configuração relacionada à segurança dos sistemas da AC. Equipamentos e softwares são instalados e configurados usando um processo de controle de mudanças documentado. A integridade do software é verificada após a implantação usando checksums.

6.6.3 Controles de segurança do ciclo de vida

Sem estipulação.

6.7 Controles de segurança de rede

A RNP implementa salvaguardas e controles razoáveis de segurança de rede para evitar o acesso não autorizado aos sistemas e à infraestrutura da AC. Firewalls e outros sistemas críticos da AC são configurados com base em uma política de lista de permissões de tráfego necessário sempre que possível.

As Chaves Privadas da AC Raiz da RNP são destruídas após a emissão dos artefatos necessários e das ACs Subordinadas ao final de sua cerimônia de criação.

6.8 Marcação de tempo

Consulte a Seção 5.5.5.

7. PERFIS DE CERTIFICADOS, CRL E OCSP

7.1 Perfil de Certificado

Todos os campos são especificados conforme o RFC 5280, incluindo campos e extensões não mencionados especificamente.

OIDs (Identificadores de Objetos) e extensões adicionais podem ser encontrados em https://repositorio.icpedu.rnp.br/.

Extensões não são marcadas como críticas, a menos que especificamente descritas como críticas aqui ou em seus documentos correspondentes.

Certificado da AC Raiz

Campo ou extensão	Valor
Número de Série	Deve ser único, com 64 bits
Nome Distinto do Emissor	C = BR, ST = DF, O = RNP, OU = DAGSer, CN = AC ICPEdu CertAU Raiz v<n> onde n é um inteiro representando a instância do certificado raiz da AC.
Nome Distinto do Assunto	Igual ao Nome Distinto do Emissor
Período de Validade	Sem estipulação

Restrições Básicas	Crítico. cA=True, pathLength diferente de 0 quando presente
Uso de Chave	Crítico. keyCertSign, cRLSign

Certificado da AC Subordinada

Campo ou extensão	Valor
Número de Série	Deve ser único, com 64 bits
Nome Distinto do Emissor	Derivado do certificado do Emissor
Nome Distinto do Assunto	CN=C = BR, ST = DF, O = RNP, OU = DAGSer, CN = AC ICPEdu CertAU v<n> onde n é um inteiro representando a instância do certificado da AC subordinada.
Período de Validade	Sem estipulação
Restrições Básicas	Crítico. cA=True, pathLength constraint 0
Uso de Chave	Crítico. keyCertSign, cRLSign
Políticas de Certificado	URI apontando para esta PC/DPC
Acesso a Informações da Autoridade	Contém URL de emissores da AC. URLs variam com base no Emissor.

Pontos de Distribuição de CRL	Contém uma URL de CRL. URL varia com base no Emissor.

Certificado do Assinante

Campo ou extensão	Valor
Número de Série	Deve ser único, com 64 bits
Nome Distinto do Emissor	Derivado do certificado do Emissor
Nome Distinto do Assunto	CN=Varia de acordo com a informação contida no token de acesso do provedor de identidade
Período de Validade	Sem estipulação
Restrições Básicas	Crítico. cA=False
Uso de Chave	Crítico. digitalSignature, nonRepudiation
Acesso a Informações da Autoridade	Contém URL de emissores da AC. URLs variam com base no Emissor.
Chave Pública do Assinante	RSA com módulo entre 2048 e 4096 bits.
Pontos de Distribuição de CRL	Contém uma URL de CRL. URL varia com base no Emissor.

7.1.1 Número(s) de versão

Todos os certificados usam a versão 3 do X.509.

7.1.2 Conteúdo e Extensões do Certificado; Aplicação do RFC 5280

Consulte a seção 7.1.

7.1.3 Identificadores de objeto de algoritmo

7.1.3.1 SubjectPublicKeyInfo

Sem estipulação.

7.1.3.2 Signature AlgorithmIdentifier

Nome	Identificador de objeto
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha512WithRSAEncryption	1.2.840.113549.1.1.13

7.1.4 Formas de nome

Sem estipulação.

7.1.5 Restrições de nome

Sem estipulação.

7.1.6 Identificador de objeto de política de certificado

Consulte a seção 7.1.

7.1.7 Uso da extensão de restrições de políticas

Não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Consulte a seção 7.1.

7.1.9 Semântica de processamento para a extensão crítica de Políticas de Certificado

Não aplicável.

7.2 Perfil de CRL

Para o status de quaisquer Certificados:

Campo ou Extensão	Valor
Versão	V2
Algoritmo de Assinatura	sha512WithRSAEncryption ou sha512WithRSAEncryption
ThisUpdate	A data e a hora em que a validade da lista de revogação de certificados começa
NextUpdate	Até ou além da data de expiração do Certificado da AC
RevokedCertificates	Não há certificados revogados
Número de CRL	1

7.2.1 Número(s) de versão

Consulte a seção 7.2.

7.2.2 Extensões de CRL e entradas de CRL

Sem estipulação.

7.3 Perfil de OCSP

A RNP não disponibiliza serviços de OCSP.

7.3.1 Número(s) de versão

Sem estipulação.

7.3.2 Extensões de OCSP

Sem estipulação.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

As auditorias de conformidade têm como objetivo garantir a conformidade de uma AC com seu PC e DPC e com os critérios de auditoria relevantes.

8.1 Frequência ou circunstâncias da avaliação

Sem estipulação.

8.2 Identidade/qualificações do auditor

As auditorias de conformidade da RNP são realizadas por um auditor qualificado. Um auditor qualificado significa uma pessoa natural, entidade legal ou grupo de pessoas naturais ou entidades legais que, coletivamente, possuam as seguintes qualificações e habilidades:

1. Independência em relação ao objeto da auditoria (que é a RNP);
2. Capacidade de conduzir uma auditoria que aborde os critérios relevantes especificados em um Esquema de Auditoria Elegível (consulte a Seção 8.4);
3. Emprega indivíduos que possuam proficiência na análise de tecnologia de Infraestrutura de Chave Pública, ferramentas e técnicas de segurança da informação, e auditoria de tecnologia da informação e segurança;
4. Vinculado por lei, regulamentação governamental ou código de ética profissional.

8.3 Relação do auditor com a entidade auditada

As auditorias da ICPEdu serão realizadas por avaliadores por meio de colaboradores do quadro da DAGSer ou por terceiros por ela autorizados.

8.4 Tópicos cobertos pela avaliação

As auditorias de conformidade abrangem a conformidade da RNP com a PC/DPC da RNP.

8.5 Ações tomadas como resultado de deficiências

O não cumprimento dos requisitos relevantes será documentado pelos auditores (internos ou externos), a RNP será informada, e a RNP garantirá que medidas sejam tomadas para resolver os problemas o mais rapidamente possível.

8.6 Comunicação dos resultados

Os resultados da auditoria são relatados à RNP e a qualquer outra entidade com direito aos resultados por lei, regulamentação ou acordo.

A RNP não é obrigada a divulgar publicamente qualquer achado de auditoria que não afete a opinião geral da auditoria.

8.7 Autoauditorias

A RNP realiza auditorias internas regulares.

9. OUTROS ASSUNTOS DE NEGÓCIOS E LEGAIS

9.1 Taxas

9.1.1 Taxas de emissão ou renovação de certificado

A RNP não cobra nenhuma taxa pela emissão de certificados.

9.1.2 Taxas de acesso a certificados

Sem estipulação.

9.1.3 Taxas de acesso a informações de revogação ou status

A RNP não cobra nenhuma taxa pela revogação de certificados ou pela verificação do status de validade de um certificado emitido.

9.1.4 Taxas por outros serviços

Sem estipulação.

9.1.5 Política de reembolso

A RNP não cobra nenhuma taxa, portanto, não oferece reembolsos.

9.2 Responsabilidade financeira

9.2.1 Cobertura de seguro

Sem estipulação.

9.2.2 Outros ativos

Sem estipulação.

9.2.3 Cobertura de seguro ou garantia para entidades finais

Sem estipulação.

9.3 Confidencialidade das informações comerciais

9.3.1 Âmbito das informações confidenciais

Sem estipulação.

9.3.2 Informações fora do âmbito das informações confidenciais

Sem estipulação.

9.3.3 Responsabilidade de proteger informações confidenciais

Os funcionários, agentes e contratados da RNP são responsáveis por proteger as informações confidenciais e são vinculados pelas políticas da RNP em relação ao tratamento de informações confidenciais ou são obrigados contratualmente a fazê-lo. Os funcionários recebem treinamento sobre como lidar com informações confidenciais.

9.4 Privacidade das informações pessoais

9.4.1 Plano de privacidade

A RNP segue a política de privacidade publicada em seu site (https://www.rnp.br/sobre-nos/privacidade/) ao lidar com informações pessoais.

9.4.2 Informações tratadas como privadas

A política de privacidade publicada no site da RNP (https://www.rnp.br/sobre-nos/privacidade/) identifica as informações que a RNP trata como privadas.

9.4.3 Informações não consideradas privadas

A política de privacidade publicada no site da RNP (https://www.rnp.br/sobre-nos/privacidade/) identifica as informações que a RNP não trata como privadas.

9.4.4 Responsabilidade de proteger informações privadas

Os funcionários e contratados da RNP estão sujeitos a políticas ou obrigações contratuais que exigem que cumpram com a política de privacidade da RNP (https://www.rnp.br/sobre-nos/privacidade/) ou com obrigações contratuais pelo menos tão protetoras das informações privadas quanto a política de privacidade da RNP.

9.4.5 Aviso e consentimento para uso de informações privadas

A RNP segue a política de privacidade publicada em seu site (https://www.rnp.br/sobre-nos/privacidade/) ao usar informações pessoais.

9.4.6 Divulgação em processo judicial ou administrativo

A RNP pode divulgar informações pessoais se obrigada a fazê-lo por ordem judicial ou outro processo legal obrigatório, desde que, se a RNP determinar que tal ordem judicial ou processo legal é inválido ou inconstitucional, a RNP fará esforços legais razoáveis para se opor à divulgação.

9.4.7 Outras circunstâncias de divulgação de informações

A RNP pode divulgar informações pessoais em outras circunstâncias que são descritas na política de privacidade publicada em seu site (https://www.rnp.br/sobre-nos/privacidade/).

9.5 Direitos de propriedade intelectual

A RNP e/ou seus parceiros de negócios possuem os direitos de propriedade intelectual nos serviços da RNP, incluindo os certificados, marcas registradas usadas na prestação dos serviços e esta PC/DPC. As informações sobre

certificados e revogações são propriedade da RNP. A RNP concede permissão para reproduzir e distribuir certificados de forma não exclusiva e isenta de royalties, desde que sejam reproduzidos e distribuídos na íntegra. As Chaves Privadas e Chaves Públicas permanecem como propriedade dos Assinantes que as possuem legitimamente.

Não obstante o exposto, o software de terceiros (incluindo software de código aberto) usado pela RNP para fornecer seus serviços é licenciado, não de propriedade, da RNP.

9.6 Declarações e garantias

9.6.1 Declarações e garantias da AC

Exceto conforme expressamente declarado nesta PC/DPC ou em um acordo separado com um Assinante, a RNP não faz nenhuma representação ou garantia em relação aos seus produtos ou serviços. A RNP declara e garante, na medida especificada nesta PC/DPC, que:

1. A RNP cumpre, em todos os aspectos formais e materiais, a PC/DPC da RNP,
2. Todos os certificados emitidos sob esta PC/DPC serão verificados de acordo com esta PC/DPC e atenderão aos requisitos mínimos aqui estabelecidos, e
3. A RNP manterá um repositório de informações públicas em seu site.

9.6.2 Declarações e garantias da RA

A RNP não utiliza serviços de RA de terceiros.

9.6.3 Declarações e garantias dos Assinantes

1. Cada Assinante garante à RNP e ao público em geral que é a pessoa legítima que é, ou será, o sujeito do certificado RNP emitido ao Assinante, e que o Assinante é o agente devidamente autorizado de tal registrante.

2. Cada Assinante garante à RNP e ao público em geral que o Assinante não obteve o controle do token de acesso do provedor de identidade resultante de uma apreensão das credenciais da pessoa ou seus dispositivos MFA.
3. Cada Assinante garante que todas as informações no certificado RNP emitido ao Assinante em relação ao Assinante ou ao seu nome de domínio são precisas, atuais, confiáveis, completas e não enganosas.
4. Cada Assinante garante que todas as informações fornecidas pelo Assinante através do seu token de acesso à RNP são precisas, atuais, completas, confiáveis, completas e não enganosas.

9.6.4 Declarações e garantias das partes confiantes

Cada Parte Confiável declara e garante que, antes de confiar em um certificado RNP, ela:

1. Obteve conhecimento suficiente sobre o uso de certificados digitais e ICP,
2. Estudou as limitações aplicáveis ao uso dos certificados e concorda com as limitações de responsabilidade da RNP relacionadas ao uso dos certificados,
3. Leu, compreendeu e concorda com esta PC/DPC,
4. Verificou tanto o certificado RNP quanto os certificados na cadeia de certificados,
5. Não usará um certificado RNP se o certificado estiver expirado ou revogado, e
6. Tomará todas as medidas razoáveis para minimizar o risco associado à confiança em uma assinatura digital, incluindo confiar apenas em um certificado RNP após considerar:

- A lei aplicável e os requisitos legais para identificação de uma parte, proteção da confidencialidade ou privacidade das informações e exequibilidade da transação;
- O uso pretendido do certificado conforme listado no certificado ou nesta PC/DPC,
- Os dados listados no certificado,
- O valor econômico da transação ou comunicação,

- A perda ou dano potencial que seria causado por uma identificação errônea ou uma perda de confidencialidade ou privacidade das informações na aplicação, transação ou comunicação,
- O histórico anterior de negociações da Parte Confiável com o Assinante,
- O entendimento da Parte Confiável sobre o comércio, incluindo experiência com métodos de comércio baseados em computadores, e
- Qualquer outro indicativo de confiabilidade ou não confiabilidade pertinente ao Assinante e/ou à aplicação, comunicação ou transação.

Qualquer confiança não autorizada em um certificado é por conta e risco da parte.

9.6.5 Declarações e garantias de outros participantes

Sem estipulação.

9.7 Isenção de garantias

Os certificados e serviços da RNP são fornecidos "como estão". A RNP isenta-se de todas e quaisquer garantias de qualquer tipo, expressas ou implícitas, incluindo e sem limitação a qualquer garantia implícita de título, não violação, comercialização ou adequação a um propósito específico, em conexão com qualquer serviço ou certificado da RNP.

9.8 Limitações de responsabilidade

A RNP não aceita qualquer responsabilidade por qualquer perda, dano, reivindicação ou honorários advocatícios em conexão com quaisquer certificados. A RNP não será responsável por quaisquer danos, honorários advocatícios ou recuperação, independentemente de tais danos serem diretos, consequentes, indiretos, incidentais, especiais, exemplares, punitivos ou compensatórios, mesmo que a RNP tenha sido avisada da possibilidade de tais danos. Esta limitação de responsabilidade se aplica independentemente da teoria da responsabilidade, ou seja, se a teoria da responsabilidade for baseada em contrato, garantia, indenização,

contribuição, responsabilidade civil, equidade, estatuto ou regulamento, direito comum ou qualquer outra fonte de direito, padrão de cuidado, categoria de reivindicação, noção de culpa ou responsabilidade, ou teoria de recuperação. Esta isenção destina-se a ser interpretada na extensão máxima permitida pela lei aplicável.

Sem renunciar ou limitar o exposto de qualquer maneira, a RNP não faz, e a RNP expressamente se isenta de qualquer garantia quanto ao seu direito de usar qualquer tecnologia, invenção, design técnico, processo ou método de negócio usado na emissão de certificados ou na prestação de qualquer serviço da RNP. Cada Assinante renuncia afirmativa e expressamente ao direito de responsabilizar a RNP de qualquer maneira, ou buscar indenização contra a RNP, por qualquer violação de direitos de propriedade intelectual, incluindo patentes, marcas registradas, segredos comerciais ou direitos autorais.

9.9 Indenizações

9.9.1 Indenização pela RNP

A RNP não fornece nenhuma indenização.

9.9.2 Indenização pelos Assinantes

Cada Assinante indenizará e isentará a RNP e seus diretores, executivos, funcionários, agentes, afiliados, terceiros e consultores de todas e quaisquer responsabilidades, reivindicações, demandas, danos, perdas, custos e despesas, incluindo honorários advocatícios, decorrentes de ou relacionados a: (i) qualquer falsa declaração ou omissão de fato material pelo Assinante à RNP, independentemente de tal falsa declaração ou omissão ter sido intencional, (ii) violação do Acordo do Assinante, (iii) qualquer comprometimento ou uso não autorizado de um certificado RNP ou da Chave Privada correspondente, ou (iv) uso indevido de um certificado RNP pelo Assinante. Se a lei aplicável proibir o Assinante de fornecer indenização pela negligência ou atos de outra parte, tal restrição, ou qualquer outra restrição exigida por lei para que esta disposição de indenização seja aplicável, será considerada parte desta disposição de indenização.

9.9.3 Indenização pelas Partes Confiáveis

Na medida permitida pela lei, cada Parte Confiável deverá indenizar a RNP, seus parceiros, entidades que tenham assinado ou emitido sub-ACs para a RNP e seus respectivos diretores, executivos, funcionários, agentes e contratados contra qualquer perda, dano ou despesa, incluindo honorários advocatícios razoáveis, relacionados à (i) violação da Parte Confiável de quaisquer termos de serviço aplicáveis aos serviços fornecidos pela RNP ou suas afiliadas e usados pela Parte Confiável, desta PC/DPC ou da lei aplicável; (ii) confiança não razoável em um certificado; ou (iii) falha em verificar o status do certificado antes do uso.

9.10 Vigência e rescisão

9.10.1 Vigência

Esta PC/DPC e quaisquer emendas a esta PC/DPC são eficazes quando publicados no repositório online da RNP e permanecem em vigor até serem substituídos por uma versão mais recente.

9.10.2 Rescisão

Esta PC/DPC e quaisquer emendas permanecem em vigor até serem substituídos por uma versão mais recente.

9.10.3 Efeito da rescisão e sobrevivência

A RNP comunicará as condições e o efeito da rescisão desta PC/DPC através do Repositório da RNP. A comunicação especificará quais disposições sobrevivem à rescisão. No mínimo, todas as responsabilidades relacionadas à proteção de informações confidenciais sobreviverão à rescisão. Todos os Termos de Uso permanecem em vigor pelo menos até que o certificado seja revogado ou expire, mesmo que esta PC/DPC seja rescindida.

9.11 Avisos e comunicações individuais com os participantes

A RNP aceita avisos relacionados a esta PC/DPC nos locais especificados na Seção 1.5.2 desta PC/DPC. Os avisos são considerados eficazes após o remetente receber um reconhecimento de recebimento válido e assinado digitalmente da RNP. Se um reconhecimento de recebimento não for recebido dentro de cinco dias, o remetente deve reenviar o aviso em papel para o endereço especificado na Seção 1.5.2 desta PC/DPC, usando um serviço de entrega que confirme a entrega ou via correio certificado ou registrado com porte pago e aviso de recebimento solicitado. A RNP pode permitir outras formas de aviso em seus Termos de Uso.

9.12 Emendas

9.12.1 Procedimento para emenda

Esta PC/DPC é revisada pelo menos anualmente e pode ser revisada com mais frequência. As emendas são feitas através da publicação de uma versão atualizada desta PC/DPC no repositório online. Controles estão em vigor que são projetados para garantir razoavelmente que esta PC/DPC não seja alterada e publicada sem a autorização prévia da RNP.

9.12.2 Mecanismo e período de notificação

A RNP publica revisões da PC/DPC em seu repositório. A RNP não garante ou define um período de notificação e comentários e pode fazer alterações nesta PC/DPC sem aviso prévio.

9.12.3 Circunstâncias nas quais o OID deve ser alterado

A RNP é a única responsável por determinar se uma emenda a esta PC/DPC requer uma alteração no OID.

9.13 Disposições de resolução de disputas

Qualquer reclamação, ação ou procedimento decorrente desta PC/DPC ou de qualquer produto ou serviço da RNP deve ser iniciado em um tribunal estadual ou federal localizado em São Paulo, Brasil, ressalvado ajuste diverso e específico entre as partes. A RNP pode buscar medidas cautelares ou judiciais em qualquer tribunal jurisdicional competente para qualquer lesão ou ameaça à lesão de direitos de propriedade intelectual ou outros que afetem o desempenho do seu trabalho.

9.14 Lei aplicável

As leis brasileiras governam a interpretação, construção e execução desta PC/DPC e todos os procedimentos relacionados aos produtos e serviços da RNP, incluindo reivindicações de responsabilidade civil e eventual regras sobre conflito de normas no direito internacional. A Convenção das Nações Unidas para a Venda Internacional de Mercadorias não se aplica a esta PC/DPC.

9.15 Conformidade com a lei aplicável

Esta PC/DPC está sujeita a todas as leis e regulamentos aplicáveis.

9.16 Disposições diversas

9.16.1 Acordo completo

A RNP exige que cada parte que utiliza seus produtos e serviços celebre um acordo que delineie os termos associados ao produto ou serviço. Se um acordo tiver disposições que diferem desta PC/DPC, então o acordo com essa parte prevalece, mas somente com relação a essa parte. Terceiros não podem confiar ou acionar para fazer cumprir tal acordo.

9.16.2 Cessão

Quaisquer entidades que operam sob esta PC/DPC não podem ceder seus direitos ou obrigações sem o consentimento prévio por escrito da RNP. A menos que especificado de outra forma em um contrato com uma parte, a RNP não fornece aviso de cessão.

9.16.3 Separabilidade

Se qualquer disposição desta PC/DPC for considerada inválida ou inexequível por um tribunal ou tribunal competente, o restante desta PC/DPC permanecerá válido e exequível. Cada disposição desta PC/DPC que prevê uma limitação de responsabilidade, isenção de garantia ou exclusão de danos é separável e independente de qualquer outra disposição.

9.16.4 Execução (honorários advocatícios e renúncia de direitos)

A RNP pode buscar indenização e honorários advocatícios de uma parte por danos, perdas e despesas relacionadas à conduta dessa parte. A falha da RNP em aplicar uma disposição desta PC/DPC não renuncia ao direito da RNP de aplicar a mesma disposição posteriormente ou o direito de aplicar qualquer outra disposição desta PC/DPC. Para ser eficaz, as renúncias devem ser por escrito e assinadas pela RNP.

9.16.5 Força Maior

A RNP não é responsável por qualquer atraso ou falha em cumprir uma obrigação sob esta PC/DPC na medida em que o atraso ou falha seja causado por um evento além do controle razoável da RNP.

9.17 Outras disposições

Sem estipulação.