# SEG.P.005 – Política de Segurança da Informação da ICPEdu Certificado Pessoal

CAIS | *Rede Nacional de Ensino e Pesquisa*

**Código: SEG.P.005** | **Versão: 1.0**

*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*

# DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de Segurança da Informação da ICPEdu Certificado Pessoal, a qual deve ser da ciência e observância de todas as entidades que integram a Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu).

Esta versão foi aprovada pela Diretoria Executiva da RNP e, juntamente com seus anexos, entra em vigor imediatamente após a sua aprovação e automaticamente revoga as versões anteriores.

O prazo de validade deste documento, incluindo seus anexos, e suas revisões devem ser realizadas a cada dois anos, considerando sua data de aprovação, ou a qualquer tempo diante de mudanças nos requisitos legais e direcionadores ou objetivos estratégicos da RNP.

**CICLO DE APROVAÇÃO**

| ***Elaboradores*** | ***Data*** |
|---|---|
| Cristiane Rodrigues, Edilson Lima, Yuri Alexandro, Luciano Rocha, Rick Lopes | 24/08/2021 |

| ***Revisores*** | ***Data*** |
|---|---|
| Camila Borges, Christian Lyra e Edilson Lima | 15/10/2021 |

| ***Aprovadores*** | ***Data*** |
|---|---|
| Comitê de Segurança da Informação da RNP | 06/12/2021 |

| ***Aprovadores Finais*** | ***Data*** |
|---|---|
| | |

**CONTROLE DE VERSÕES**

| Versão | Data | Responsável | Natureza das Modificações |
|---|---|---|---|
| 0.1 | 26/03/2021 | Cristiane Fernandez, Edilson Lima, Yuri Alexandro | 1ª versão do documento |

| | | | |
|---|---|---|---|
| 1.0 | 16/11/2021 | Luciano Rocha, Rick Lopes, Yuri Alexandro | Ajustes feitos para serviço ICPEdu Certificado Pessoal |

# SUMÁRIO

1. INTRODUÇÃO ..... 6
2. OBJETIVO ..... 6
3. ESCOPO ..... 6
4. TERMOS, DEFINIÇÕES E SIGLAS ..... 6
5. DEFINIÇÕES GERAIS ..... 9
5.1. GESTÃO DE SEGURANÇA ..... 9
5.2. GERENCIAMENTO DE RISCOS ..... 10
5.3. INVENTÁRIO DE ATIVOS ..... 11
5.4. PLANO DE CONTINUIDADE DE NEGÓCIO ..... 11
6. PROCEDIMENTOS RELATIVOS À SEGURANÇA DE PESSOAL ..... 11
6.1. DEFINIÇÃO ..... 11
6.2. OBJETIVOS ..... 12
6.3. DIRETRIZES ..... 12
6.4. DEVERES E RESPONSABILIDADES ..... 15
7. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO ..... 17
7.1. DEFINIÇÃO ..... 17
7.2. DIRETRIZES GERAIS ..... 17
8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO ..... 19
8.1. DEFINIÇÃO ..... 19
8.2. DIRETRIZES GERAIS ..... 19
8.3. DIRETRIZES ESPECÍFICAS ..... 20
9. REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS ..... 27
9.1. REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA ICPEDU CERTIFICADO PESSOAL ..... 27
9.2. CHAVES CRIPTOGRÁFICAS ..... 28
9.3. TRANSPORTE DE INFORMAÇÕES ..... 29
10. AUDITORIA E FISCALIZAÇÃO ..... 29
10.1. DIRETRIZES GERAIS ..... 29
11. GERENCIAMENTO DE RISCOS ..... 30
11.1. DEFINIÇÃO ..... 30
11.2. FASES PRINCIPAIS ..... 30
11.3. RISCOS RELACIONADOS ÀS ENTIDADES ..... 31
11.4. IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS ..... 31



*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*

**11.5. DIRETRIZES GERAIS ..... 31**

**12. TRATAMENTO DE VIOLAÇÕES ..... 32**

**12.1. DIRETRIZES GERAIS ..... 32**

# 1. INTRODUÇÃO

Esta política tem por finalidade estabelecer as diretrizes de segurança que deverão ser adotadas pelas entidades que integram da Infraestrutura de Chaves Públicas para Ensino e Pesquisa da RNP para emissão de certificado digital de uso pessoal (ICPEdu Certificado Pessoal). Tais diretrizes fundamentarão as normas e procedimentos de segurança a serem elaborados e implementados por parte de cada entidade, considerando as suas particularidades.

# 2. OBJETIVO

A Política de Segurança da ICPEdu Certificado Pessoal tem os seguintes objetivos específicos:

- Definir o escopo da segurança das entidades que compõem o serviço;
- Orientar todas as ações de segurança das entidades, a fim de reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos do serviço;
- Servir de referência para auditoria, apuração e avaliação de responsabilidades; e
- Orientar a formulação das Declarações de Práticas de Certificação - DPCs e Políticas de Certificação - PCs das autoridades certificadoras da ICPEdu.

# 3. ESCOPO

A Política de Segurança da ICPEdu Certificado Pessoal abrange os seguintes aspectos:

- Requisitos de segurança de pessoal;
- Requisitos de segurança física;
- Requisitos de segurança lógica; e
- Requisitos de segurança dos recursos criptográficos.

# 4. TERMOS, DEFINIÇÕES E SIGLAS

Devem ser considerados os conceitos abaixo no que se refere à Política de Segurança da ICPEdu Certificado Pessoal:

- **Ativo de informação** – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades da ICPEdu.

- **Ativos de TIC** – sistemas, serviços e aplicações (*software*), equipamentos computacionais e de telecomunicações (*hardware*).
- **Ativo de processamento** – patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos.
- **Autoridade certificadora (AC)** – responsável por receber os pedidos aprovados pela AR para processamento e assina os certificados. Além disso, gera e assina a Lista de Certificados Revogados e mantém um banco de dados com todos os certificados emitidos.
- **Autoridade de registro (AR)** – responsável pela validação da identidade do solicitante; autentica o assinante e aprova o pedido além de revogar ou suspender certificados. Tem um relacionamento direto com o solicitante.
- **CAIS** – Centro de Atendimento a Incidentes de Segurança, área responsável pela segurança da informação corporativa na RNP.
- **Controle de acesso** – conjunto de restrições ao acesso às informações de um sistema, estipuladas e exercidas pela DAGSer.
- **Colaborador** – força de trabalho corrente, sendo ela composta por celetistas, servidores cedidos, estagiários, aprendizes ou terceiros.
- **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.
- **DACS** – Diretoria Adjunta de CiberSegurança, área da RNP responsável pela segurança cibernética dos serviços.
- **DAGSer** – Diretoria Adjunta de Gestão de Serviços, área responsável pela gestão operacional dos serviços avançados ofertados pela RNP, dentre eles, a ICPEdu.
- **Direito de acesso** – é o grau de privilégio, ou tipo de restrição, para acesso a um ativo, associado a um cargo, pessoa ou processo.
- **DPC ou Declaração de Práticas de Certificação** – documento com força legal criado pela AC que define diretrizes relativas ao uso dos certificados, processos de identificação e autenticação, aspectos operacionais, aspectos de segurança física, lógica e de pessoal, procedimentos para continuidade da operação, divisão de responsabilidades, seguro, aceitação por usuários e termos de garantias quando um certificado é aceito, responsabilidade dos usuários ao aceitar certificados de outras pessoas, perfil dos certificados e lista de certificados revogados.
- **Entidades integrantes da ICPEdu Certificado Pessoal:** Instituições que executam alguma ação no âmbito do gerenciamento dos certificados digitais da ICPEdu

Certificado Pessoal, como emissão, distribuição, revogação, verificação das chaves criptográficas, criação e assinatura digital do certificado do titular, entre outras.

- **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplica a Política de Segurança da ICPEdu.
- **GAI** – Gerência de Atendimento Integrado, área da RNP responsável por recepcionar as requisições relacionadas à ICPEdu.
- **GPR** – Gerência de Processos e Riscos, área da RNP responsável pela gestão por processos, avaliação e tratamento de riscos corporativos.
- **ICPEdu** – Infraestrutura de Chaves Públicas para Pesquisa e Ensino.
- **Incidente de segurança** – qualquer evento ou ocorrência que se constitua numa ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo dos sistemas de informação das entidades integrantes da ICPEdu.
- **PC ou Política de Certificação** – documento que define os propósitos e regras aplicáveis a um conjunto de certificados.
- **PCN** – Plano de Continuidade de Negócio, documentação de procedimentos e informações desenvolvida, consolidada e mantida de forma que esteja pronta para uso caso ocorra um incidente, de forma a permitir que a organização mantenha suas atividades críticas em um nível aceitável previamente definido.
- **PRD** – Plano de Recuperação de Desastres, conjunto de políticas e procedimentos para permitir a recuperação ou continuação da infraestrutura de TI e sistemas vitais na sequência de um desastre de ordem intencional ou não-intencional.
- **Política de Segurança** – conjunto de diretrizes destinadas a orientar a proteção adequada dos ativos dos sistemas de informação das entidades que integram a ICPEdu.
- **Proteção dos ativos** – processo pelo qual os ativos dos sistemas de informação são classificados quanto ao seu grau de sensibilidade. Em particular, o meio físico de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.
- **Responsabilidade** – definida como o dever e obrigação de se responsabilizar pelas suas ações e de terceiros em relação a sua função, dever de prestar contas.
- **SEG.P.001** – Política Corporativa de Segurança da Informação da RNP, documento que define as diretrizes e responsabilidades de segurança da informação na organização para a preservação da confidencialidade, integridade, disponibilidade, autenticidade e demais requisitos das informações da RNP e, quando for o caso, de seus parceiros de negócio.



*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*

- **GR.POL.N.001** – Política de Gestão de Riscos, documento normativo da RNP que define os princípios, diretrizes e responsabilidades para identificar, avaliar, tratar, monitorar e comunicar os riscos que possam afetar os objetivos estratégicos, o negócio e a operação da RNP.
- **SEG.N.005** – Norma de Gestão de Acesso Lógico, documento que define as regras para a gestão do ciclo de vida dos acessos lógicos dos colaboradores, assegurando que os acessos sejam autorizados e rastreáveis.
- **SEG.N.010** – Norma de Gestão de Incidentes de Segurança da Informação, documento que estabelece as regras para assegurar o gerenciamento adequado dos incidentes de segurança da informação, minimizando o impacto e garantindo a continuidade dos negócios da RNP.
- **Senha fraca ou óbvia** – senha composta de caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras.
- **VPN –** *Virtual Private Network*, canal de comunicação segura criada através de um túnel lógico virtual criado entre duas redes distintas.

# 5. DEFINIÇÕES GERAIS

## 5.1. **Gestão de segurança**

5.1.1. A Política de Segurança da ICPEdu Certificado Pessoal se aplica a todos os recursos humanos, administrativos e tecnológicos que compõem o serviço ICPEdu – Certificado Pessoal.

5.1.1.1. A abrangência dos recursos citados refere-se tanto àqueles ligados às entidades em caráter permanente, quanto temporário.

5.1.2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada às entidades integrantes da ICPEdu Certificado Pessoal, garantindo que todos tenham ciência e a apliquem.

5.1.3. Todo o pessoal envolvido no contexto da ICPEdu Certificado Pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado nesta Política de Segurança.



*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*

5.1.4. Devem ser realizadas ações periódicas de conscientização sobre segurança da informação envolvendo todo o pessoal no contexto da operação da ICPEdu Certificado Pessoal, de acordo com as diretrizes da política SEG.P.001.

5.1.5. Os procedimentos de concessão, modificação, revisão ou revogação de privilégios para acesso à sistemas e informações deve seguir os requisitos previstos na norma SEG.N.005.

5.1.6. O CAIS é a área responsável por tratar e responder a incidentes de segurança envolvendo a ICPEdu Certificado Pessoal, conforme previsto na norma SEG.N.010.

5.1.6.1. Os procedimentos de resposta a incidentes de segurança da ICPEdu Certificado Pessoal devem prever a implementação de mecanismos e repositórios centralizados para registro de trilha, logs e notificações de incidentes de segurança.

5.1.7. Os processos de aquisição de bens e serviços, especialmente o de Tecnologia da Informação e Comunicação – TIC, envolvendo a ICPEdu Certificado Pessoal devem estar em conformidade com esta Política de Segurança.

5.1.8. No que se refere à segurança da informação, deve-se considerar não autorizado tudo aquilo que não esteja previamente alinhado pela DACS juntamente com o responsável da área de segurança da entidade pertencente à ICPEdu Certificado Pessoal.

5.1.9. A Política de Segurança da ICPEdu Certificado Pessoal deve ser revisada e atualizada periodicamente pela DAGSer, no máximo a cada 2 (dois) anos, ou conforme análise de riscos realizada anualmente ou ainda caso ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

## 5.2. **Gerenciamento de riscos**

5.2.1. O processo de gerenciamento de riscos de segurança da informação deve ser revisto pela DACS, em conjunto com a DAGSer, no máximo, a cada 12 (doze) meses, para prevenção contra riscos de segurança da informação, inclusive aqueles advindos de novas tecnologias, visando a elaboração e manutenção de planos de ação apropriados para proteção dos componentes ameaçados.



*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*

5.2.2. Todos os riscos identificados deverão ser reportados à GPR, a fim de serem registrados e monitorados no Painel de Riscos Corporativos da RNP, conforme disposto na GR.POL.N.001.

### 5.3. **Inventário de Ativos**

5.3.1. Todos os ativos das entidades integrantes que compõem a infraestrutura da ICPEdu Certificado Pessoal devem ser inventariados, classificados, permanentemente atualizados e possuírem um gestor responsável formalmente designado.

### 5.4. **Plano de Continuidade de Negócio**

5.4.1. Um PCN e seus respectivos procedimentos devem ser implementados e testados, pelo menos a cada 12 meses, para controle da resposta à interrupção dos serviços, aplicar soluções de continuidade de negócio, minimizar impactos e estabelecer uma comunicação eficaz com as partes envolvidas.

5.4.2. Todas as entidades que integram a ICPEdu Certificado Pessoal devem apresentar PRD e o Plano de Resposta a Incidentes, a serem aprovados pela RNP ou AC de nível imediatamente superior.

5.4.3. O Certificado da AC deve ser imediatamente revogado se um evento provocar a perda ou comprometimento de sua chave privada ou do seu meio de armazenamento.

5.4.4. Os procedimentos de revogação devem ser detalhados na respectiva DPC.

5.4.5. Todos os incidentes de segurança identificados pelas entidades integrantes da ICPEdu Certificado Pessoal devem ser imediatamente reportados ao CAIS/RNP, por meio obrigatoriamente seguro.

## 6. PROCEDIMENTOS RELATIVOS À SEGURANÇA DE PESSOAL

### 6.1. **Definição**

6.1.1. Conjunto de medidas e procedimentos de segurança a serem observados pelos colaboradores, necessário à proteção dos ativos da ICPEdu Certificado Pessoal.

## 6.2. **Objetivos**

6.2.1. Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos da ICPEdu Certificado Pessoal.

6.2.2. Prevenir e neutralizar as ações sobre pessoas que possam comprometer a segurança da ICPEdu Certificado Pessoal.

6.2.3. Orientar e capacitar os colaboradores das entidades integrantes envolvidos na realização de trabalhos diretamente relacionados à ICPEdu Certificado Pessoal, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham.

6.2.4. Orientar o processo de avaliação de todos os colaboradores das entidades integrantes que trabalhem na operação da ICPEdu Certificado Pessoal, mesmo em caso de funções desempenhadas por prestadores de serviço.

## 6.3. **Diretrizes**

### 6.3.1. Processo de Admissão

6.3.1.1. Devem ser adotados critérios específicos para o processo de seleção dos colaboradores das entidades integrantes envolvidos na operação da ICPEdu Certificado Pessoal, visando garantir a segurança e credibilidade dos serviços.

6.3.1.2. Nenhuma das entidades integrantes da ICPEdu Certificado Pessoal deve admitir estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

6.3.1.3. Todos os colaboradores que exercem atividades diretamente relacionadas com os processos de certificação devem assinar um termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todas as informações, ativos de informações e processos da ICPEdu Certificado Pessoal.

### 6.3.2. Atribuições das funções

6.3.2.1. Todas as atribuições de cada função devem ser claramente especificadas e relacionadas de acordo com a característica das

atividades desenvolvidas, a fim de se determinar o perfil necessário do colaborador, considerando os seguintes itens:

- a descrição sumária das tarefas inerentes à função;
- as necessidades de acesso a informações sensíveis;
- o grau de sensibilidade do setor onde a função é exercida;
- as necessidades de contato de serviço interno e/ou externo;
- as características de responsabilidade, decisão e iniciativas inerentes à função;
- a qualificação técnica necessária ao desempenho da função.

6.3.3. Processos de admissão

6.3.3.1. Deve-se avaliar o perfil e experiência profissional dos colaboradores que exercem atividades diretamente relacionadas com os processos de certificação, aliada ao conhecimento e comprometimento com a segurança da informação e as diretrizes contidas nesta Política.

6.3.3.2. As entrevistas devem ser realizadas por profissionais qualificados, designados pela DAGSer ou, no caso de demais entidades integrantes da ICPEdu Certificado Pessoal, pelos responsáveis pelo serviço.

6.3.4. Desempenho da função

6.3.4.1. O desempenho dos colaboradores deve ser acompanhado e avaliado periodicamente, com o propósito de detectar a necessidade de atualização técnica e de segurança.

6.3.4.2. As entidades integrantes da ICPEdu Certificado Pessoal devem dar aos respectivos colaboradores os devidos acessos às informações, mediante fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

6.3.5. Credenciais de segurança

6.3.5.1. Os colaboradores das entidades integrantes da ICPEdu Certificado Pessoal devem ser identificados por meio de uma credencial, habilitando-o a ter acesso devido às informações sensíveis, de acordo com a classificação do grau de sigilo da informação e,



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

consequentemente, com o grau de sigilo compatível ao cargo e/ou função a ser desempenhada.

6.3.5.2. As credenciais de segurança devem ser concedidas somente por colaboradores em nível superior competentes, ou por eles delegados, e se fundamentará na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise de necessidade do cargo ou função.

6.3.5.3. A validade da credencial de segurança do colaborador da entidade integrante da ICPEdu Certificado Pessoal deve ser revisada periodicamente pelos responsáveis do serviço, ou por eles delegados, fundamentada na necessidade de permissão correspondente ao exercício do cargo ou função.

6.3.6. Treinamento em segurança da informação

6.3.6.1. As entidades integrantes da ICPEdu Certificado Pessoal devem definir um processo pelo qual esta Política de Segurança, revisões, normas e demais procedimentos relativos ao tratamento de informações e dados sigilosos sejam apresentados aos colaboradores, com o propósito de instruir sobre a necessidade de seu cumprimento e desenvolver e manter uma efetiva conscientização de segurança.

6.3.6.2. As chefias imediatas devem assegurar formalmente que todos os colaboradores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

6.3.7. Processos de desligamento

6.3.7.1. As entidades integrantes da ICPEdu Certificado Pessoal devem vedar o acesso dos colaboradores desligados às áreas restritas de suas instalações físicas.

6.3.7.2. As credenciais de identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos do colaborador devem ser imediatamente revogados após decisão de desligamento.

6.3.7.3. As entidades integrantes da ICPEdu Certificado Pessoal devem garantir que os colaboradores, antes do eventual desligamento, firmem declaração de que não possuem qualquer tipo de ativos da



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

organização ou pendências junto às diversas unidades que compõem a entidade, devendo a autenticidade e veracidade da declaração ser verificada junto ao respectivo setor de Recursos Humanos ou outros setores necessários.

6.3.7.4. Deve ser realizada entrevista de desligamento para, dentre outros objetivos, orientar o profissional sobre a responsabilidade de manutenção do sigilo sobre dados ou sobre sistemas críticos aos quais teve acesso durante seu período de trabalho.

## 6.4. **Deveres e Responsabilidades**

### 6.4.1. Deveres dos colaboradores

6.4.1.1. Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.

6.4.1.2. Cumprir esta Política de Segurança e demais normativos relacionados, sob pena de serem aplicadas sanções administrativas e legais definidas na Seção 12 deste documento.

6.4.1.3. Utilizar os sistemas de informações relativos à ICPEdu Certificado Pessoal e os recursos a ela relacionados somente para os fins previstos para operação do serviço.

6.4.1.4. Cumprir as regras específicas de proteção estabelecidas para os ativos de informação.

6.4.1.5. Manter o caráter sigiloso das credenciais de acesso aos recursos e sistemas que integram a ICPEdu Certificado Pessoal.

6.4.1.6. Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso.

6.4.1.7. Responder por todo e qualquer acesso, aos recursos da ICPEdu, pelos efeitos desses acessos efetivados através de sua credencial de identificação ou com outro atributo para este fim utilizado.

6.4.1.8. Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente.

6.4.1.9. Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

6.4.2. Responsabilidade dos gestores

6.4.2.1. Gerenciar o cumprimento desta Política de Segurança por parte dos colaboradores sob sua gestão.

6.4.2.2. Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

6.4.2.3. Impedir o acesso de colaboradores desligados ou em processos de desligamento aos ativos de informações, fazendo valer os mecanismos definidos no processo de desligamento.

6.4.2.4. Proteger, em nível físico e lógico, os ativos de informação e de processamento das respectivas entidades participantes da ICPEdu Certificado Pessoal relacionados com sua área de atuação.

6.4.2.5. Garantir que o pessoal sob sua gestão compreenda e desempenhe a obrigação de proteger a informação das entidades.

6.4.2.6. Comunicar formalmente à respectiva área de gestão de tecnologia da informação as permissões de acesso aos ativos dos colaboradores sob sua supervisão.

6.4.2.7. Comunicar formalmente à respectiva área de gestão de tecnologia da informação a demissão, transferência de setor ou a ocorrência de processos administrativos, sindicâncias ou licenciamento de colaboradores, de modo a proceder o bloqueio das credenciais e inabilitação do acesso aos ativos.

6.4.3. Responsabilidades Gerais

6.4.3.1. As áreas que detém os ativos de processamento e de informação em cada entidade integrante da ICPEdu Certificado Pessoal são responsáveis por eles, devendo prover a sua proteção de acordo com esta Política de Segurança.

6.4.3.2. As entidades integrantes da ICPEdu Certificado Pessoal devem definir de forma clara todos os responsáveis pelos ativos de informação utilizados nos processos de certificação.

6.4.3.3. As entidades integrantes da ICPEdu Certificado Pessoal devem relacionar no PCN todos os ativos de informação utilizados nos processos de certificação.

6.4.4. Responsabilidades dos prestadores de serviços

6.4.4.1. As entidades integrantes da ICPEdu Certificado Pessoal devem prever em contrato clausulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança e respectivas normas e procedimentos.

# 7. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

## 7.1. **Definição**

7.1.1. Ambiente físico é aquele composto por todo o conjunto de ativos permanentes das entidades integrantes da ICPEdu Certificado Pessoal.

## 7.2. **Diretrizes Gerais**

7.2.1. As entidades integrantes da ICPEdu Certificado Pessoal devem definir as responsabilidades pela segurança física dos sistemas e atribuí-la, formalmente e de forma clara, aos colaboradores responsáveis na organização.

7.2.2. A localização das instalações e o sistema da AC Raiz, da AC PESSOA e demais ACs subsequentes da ICPEdu Certificado Pessoal não devem ser publicamente identificadas.

7.2.3. As entidades integrantes da ICPEdu Certificado Pessoal devem instalar sistemas de segurança para acesso físico, com objetivo de controlar e auditar o acesso aos sistemas de certificação.

7.2.4. Chaves, cartões ou outros dispositivos usados para conceder acesso físico, quando utilizados, devem ser inventariados – com informação atualizada sobre todos os colaboradores que os possuem –, e devem ser adotados controles de segurança reforçados sobre estes.

7.2.5. As chaves criptográficas da ICPEdu Certificado Pessoal deverão ser fisicamente protegidas contra acesso e uso não-autorizado, ou duplicação em quaisquer circunstâncias.

7.2.6. Chaves, cartões ou outros dispositivos usados para conceder acesso físico, quando perdidos, devem ser imediatamente comunicadas ao CAIS/RNP, que deve orientar medidas apropriadas para impedir acessos não autorizados.

7.2.7. Os sistemas de Autoridades Certificadoras devem estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de radiofrequência.

7.2.8. Recursos e instalações críticas ou sensíveis devem ser mantidas em áreas seguras, protegidas por perímetro de segurança definidos, com existência de barreiras e controles de segurança contra acesso não autorizado, danos ou interferências, de forma proporcional aos riscos identificados.

7.2.9. As entradas e saídas em áreas críticas, sensíveis ou de propósito específico, deverão ser monitoradas e acessos devem ser automaticamente registrados com data e hora definidas, devendo ser revisadas diariamente pela respectiva área responsável pela segurança da informação da entidade integrante da ICPEdu Certificado Pessoal.

7.2.10. As entidades integrantes da ICPEdu Certificado Pessoal devem restringir o acesso aos componentes da infraestrutura fundamentais ao funcionamento dos sistemas, como painéis de controle de energia, comunicações e cabeamento, somente ao pessoal autorizado.

7.2.11. As entidades integrantes da ICPEdu Certificado Pessoal devem utilizar sistemas de detecção de intrusão para monitorar e registrar os acessos físicos no ambiente onde estão hospedados os sistemas de certificação, devendo ser testados de forma regular, de forma a cobrir todos os ambientes acessíveis onde ocorrem processos críticos, com acionamento de alarme em caso de acessos não autorizados.

7.2.12. O inventário de todo o conjunto de ativos de processamento dos sistemas de certificação deve ser registrado e mantido atualizado por período mínimo de 30 dias.

7.2.13. Equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar só devem ter utilização permitida a partir de autorização formal e mediante supervisão.

7.2.14. As entidades integrantes da ICPEdu Certificado Pessoal devem garantir a utilização de identificação visível por parte dos colaboradores, assim como ter procedimentos de identificação e restrição de acesso a qualquer pessoa não identificada ou não acompanhada.



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

7.2.15. Visitantes devem obter acesso apenas a áreas específicas, mediante autorização prévia, com propósitos justificáveis, seguindo as instruções baseadas nos requisitos de segurança da área visitada.

7.2.16. As entidades integrantes da ICPEdu Certificado Pessoal devem garantir a supervisão sob os visitantes que circulam nas áreas de segurança, com o devido registro dos horários de entrada e saída, bem como dos locais de destino autorizados.

7.2.17. As entidades integrantes da ICPEdu Certificado Pessoal devem monitorar, em tempo real, os ambientes onde ocorrem os processos críticos de certificação, registrando imagens por meio de sistemas de Circuito Fechado de Televisão – CFTV.

# 8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

## 8.1. **Definição**

8.1.1. O ambiente lógico de uma entidade integrante da ICPEdu Certificado Pessoal é definido pelo conjunto de todos os ativos de informações daquela entidade.

## 8.2. **Diretrizes Gerais**

8.2.1. A proteção das informações deve ser elaborada de acordo com um sistema de classificação da informação, de acordo com o seu valor, nível de sigilo e criticidade.

8.2.2. Os dados, informações e sistemas de informação das entidades que integram a ICPEdu Certificado Pessoal devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

8.2.3. As entidades que integram a ICPEdu Certificado Pessoal devem registrar todas as violações de segurança da informação, armazenando e protegendo os registros de acordo com a sua classificação, e estabelecer processos de análise periódica com fins de ações corretivas, legais e de auditoria.

8.2.4. Os sistemas e recursos que suportam funções críticas para operação das entidades devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

8.2.5. As entidades integrantes da ICPEdu Certificado Pessoal devem, em intervalos de tempo previamente definidos, registrar e manter atualizado o inventário sistematizado de toda estrutura utilizadas na manipulação, armazenamento e transmissão dos ativos que compõem os sistemas de certificação.

## 8.3. **Diretrizes Específicas**

### 8.3.1. Sistemas de certificação

8.3.1.1. As entidades integrantes da ICPEdu Certificado Pessoal devem manter atualizadas todas as documentações referentes aos sistemas de certificação e identificar as necessidades de segurança para cada etapa do ciclo de vida dos sistemas.

8.3.1.2. As entidades integrantes da ICPEdu Certificado Pessoal devem ter uma Política de backup dos sistemas de certificação, realizar testes regulares de integridade das cópias de segurança e garantir a sua segurança.

8.3.1.3. Os sistemas de certificação devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. As entidades integrantes da ICPEdu Certificado Pessoal devem definir e registrar de forma clara o responsável pelas autorizações ou confirmações de autorização.

8.3.1.4. Os arquivos de logs devem ser definidos para permitir a recuperação nas situações de falhas, auditoria nas situações de violações e segurança e contabilização do uso de recursos. Os logs devem ser periodicamente analisados, conforme definidos pela DPC, para identificar tendências, falhas ou usos indevidos e protegidos de acordo com a sua classificação.

8.3.1.5. As entidades integrantes da ICPEdu Certificado Pessoal devem estabelecer e manter medidas e controles de segurança para verificação crítica dos dados e configurações de sistemas e dispositivos quanto à sua precisão, consistência e integridade.

8.3.1.6. As entidades integrantes da ICPEdu Certificado Pessoal devem realizar avaliações de segurança dos sistemas de certificação, incluindo-se testes de vulnerabilidade, antes de serem disponibilizados para produção. Vulnerabilidades do ambiente devem

ser avaliadas periodicamente e as recomendações de segurança devem ser adequadamente implementadas.

8.3.2. Máquinas servidoras

8.3.2.1. O acesso lógico ao ambiente ou serviços disponíveis em servidores deve ser controlado e protegido. As entidades integrantes da ICPEdu Certificado Pessoal devem periodicamente registrar, confirmar e revisar as devidas autorizações, definindo e registrando de forma clara o responsável pelas autorizações ou confirmações de autorização.

8.3.2.2. Os acessos lógicos aos servidores devem ser registrados em arquivos de log, os quais devem ser protegidos e analisados periodicamente, de modo a permitir a geração de trilhas de auditoria e rastreabilidade a partir dos registros. As entidades integrantes da ICPEdu Certificado Pessoal devem definir uma política de logs, descrevendo de forma precisa o tempo de retenção e as medidas de proteção associadas.

8.3.2.3. As entidades integrantes da ICPEdu Certificado Pessoal devem adotar procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração de sistemas operacionais e outros arquivos críticos dos servidores.

8.3.2.4. Os ativos devem ter sincronização uniforme de horário, de modo a permitir a correta rastreabilidade de eventos.

8.3.2.5. As entidades integrantes da ICPEdu Certificado Pessoal devem adotar medidas de proteção lógicas adicionais sempre que necessário, inclusive com técnicas criptográficas, a fim de evitar acessos não-autorizados às informações.

8.3.2.6. As versões dos sistemas operacionais dos servidores, assim como de outros softwares instalados nos ativos, devem ser mantidas atualizadas, em conformidade com as recomendações dos fabricantes.

8.3.2.7. Devem ser utilizados somente softwares homologados e autorizados pela RNP, a qual, por sua vez, deve realizar e manter os devidos controles de distribuição e instalação.



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

8.3.2.8. O acesso remoto aos ativos deve ser realizado adotando os mecanismos de segurança pré-definidos pela DAGSer, para evitar ameaças à integridade e sigilo do serviço.

8.3.3. Redes das entidades integrantes da ICPEdu Certificado Pessoal

8.3.3.1. O tráfego das informações no ambiente de rede deve ser protegido contra danos, perdas, acesso, uso ou exposição indevidos, incluindo vazamento imprevisto de emissão eletromagnética, conhecido como "Efeito Tempest".

8.3.3.2. Componentes críticos da rede local devem ser mantidos em salas protegidas e com acessos físicos e lógico controlados, devendo ser protegidos contra danos, furtos e outros incidentes.

8.3.3.3. As configurações de rede de todos os ativos de processamento devem ser averiguadas quando da sua instalação inicial, com fins de detecção e correção de vulnerabilidades inerentes à configuração padrão que possam estar ativos em sua primeira ativação, evitando a ocorrência de acessos indevidos e outros incidentes.

8.3.3.4. As entidades integrantes da ICPEdu Certificado Pessoal devem reforçar os níveis de proteção para serviços vulneráveis.

8.3.3.5. As entidades integrantes da ICPEdu Certificado Pessoal devem estabelecer uma política específica de gerência e utilização de senhas nos ativos e equipamentos envolvidos no processo de geração dos certificados.

8.3.3.6. Os acessos lógicos aos recursos de rede local de cada entidade integrante da ICPEdu Certificado Pessoal devem ser concedidos e mantidos pela área de administração de rede, baseados nas responsabilidades e tarefas de cada usuário, e realizados por meio de sistema de controle de acesso.

8.3.3.7. As entidades integrantes da ICPEdu Certificado Pessoal devem garantir que a utilização de qualquer mecanismo para realização de testes de qualquer natureza, entre eles monitoramento sobre dados, sistemas e dispositivos que compõem a rede, só sejam feitas a partir de autorização formal e mediante supervisão.

8.3.3.8. A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser previamente autorizados



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

pelas respectivas áreas de administração de rede ou de segurança da entidade integrante da ICPEdu Certificado Pessoal, e devem ser formalmente documentadas, de forma a permitir o registro histórico do diagrama topológico, da configuração e do inventário dos recursos.

8.3.3.9. As entidades integrantes da ICPEdu Certificado Pessoal devem estabelecer uma política de registros de log dos ativos do ambiente de rede, de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria, estabelecendo o período de análise periódica no menor tempo possível.

8.3.3.10. As entidades integrantes da ICPEdu Certificado Pessoal devem adotar proteções físicas e lógicas adicionais para recursos de rede considerados críticos, de modo a evitar acesso não-autorizado às informações, danos mecânicos e conexão não autorizada.

8.3.3.11. A alimentação elétrica para a rede local deve ser separada da rede convencional, devendo ser observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis.

8.3.3.12. O tráfego de informações deve ser monitorado por equipe autorizada, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

8.3.3.13. As entidades integrantes da ICPEdu Certificado Pessoal devem observar o cumprimento das questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades.

8.3.3.14. A guarda e o envio de informações sigilosas, corporativas ou que possam causar prejuízo à ICPEdu Certificado Pessoal devem ser feitas com a devida proteção adequada.

8.3.3.15. Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado.

8.3.3.16. As transações entre redes externas e a rede interna das entidades que integram a ICPEdu Certificado Pessoal devem ser protegidas através de mecanismos de segurança baseados em sistemas de proteção de acesso, tais como firewalls.



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

8.3.3.17. Os registros de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

8.3.3.18. As entidades integrantes da ICPEdu Certificado Pessoal devem adotar um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos.

8.3.3.19. Todos os recursos considerados críticos para o ambiente de rede devem possuir mecanismos de controle de acesso quando disponíveis.

8.3.3.20. A localização dos serviços baseados em sistemas de proteção de acesso deve ser resultante de uma análise de riscos, considerando os aspectos de requisitos de segurança definidos pelo serviço, objetivo do serviço, público-alvo, classificação da informação, forma de acesso, frequência de atualização do conteúdo, forma de administração do serviço e volume de tráfego.

8.3.3.21. Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a prover um nível adicional de segurança.

8.3.3.22. Sistemas que executam a função de certificação devem estar fisicamente isolados, a fim de minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação.

8.3.3.23. A chave de certificação das ACs da ICPEdu Certificado Pessoal deverá estar protegida de acesso não-autorizado, de modo a garantir seu sigilo e integridade.

8.3.3.24. A segurança das comunicações intra e inter rede entre os sistemas da ICPEdu Certificado Pessoal deverá ser garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações transmitidas.

8.3.3.25. Mecanismos de detecção de intrusão devem ser implantadas para monitorar as redes críticas envolvidas no processo de geração dos certificados, devendo o CAIS ser alertado sobre as tentativas de intrusão identificadas.

8.3.4. Controle de acesso lógico



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

8.3.4.1. Usuários e aplicações que necessitem ter acesso a recursos da ICPEdu Certificado Pessoal devem ser identificados e autenticados.

8.3.4.2. O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha.

8.3.4.3. Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário.

8.3.4.4. A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas.

8.3.4.5. O arquivo de senhas deve ser protegido com técnicas criptográficas apropriadas e acesso controlado.

8.3.4.6. As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções e considerando o princípio do privilégio mínimo.

8.3.4.7. As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada.

8.3.4.8. O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.

8.3.4.9. As entidades integrantes da ICPEdu Certificado Pessoal devem definir uma política de senhas que definam adequadamente o conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas.

8.3.4.10. A distribuição de senhas aos colaboradores das áreas de tecnologia da informação deve ser feita de forma segura, devendo a senha inicial, quando gerada pelo sistema, ser trocada no primeiro acesso.

8.3.4.11. O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar, sem exibi-la, e garantir, em casos de troca de uma senha bloqueada, a identificação positiva do usuário.

8.3.4.12. Devem ser adotados critérios para bloquear ou desativar usuários que não façam acesso ao sistema por algum período pré-definido, ou



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

que façam um número de tentativas sucessivas de acesso malsucedidas.

8.3.4.13. O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão.

8.3.4.14. O sistema de controle de acesso deve exibir, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão, o sistema deve exibir para o usuário informações sobre o último acesso.

8.3.4.15. Os logs do sistema de controle de acesso devem ser definidos de modo a auxiliar o tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas, devendo os logs ser periodicamente analisados.

8.3.4.16. Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

8.3.5. Proteção contra malwares

8.3.5.1. Os procedimentos de combate a malwares devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

8.3.6. Computação pessoal

8.3.6.1. As estações de trabalho, incluindo equipamentos portáteis ou *stand alone*, e as informações que carregam, devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

8.3.6.2. Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).

8.3.6.3. As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de backup, definidos em procedimento específico.

8.3.6.4. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à infraestrutura da ICPEdu Certificado Pessoal só devem ser



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

utilizadas em equipamentos das respectivas entidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados.

8.3.6.5. O acesso às informações deve atender aos requisitos de segurança, considerando o ambiente e forma de uso, pessoal ou coletivo, do equipamento.

8.3.6.6. Os colaboradores devem utilizar apenas softwares licenciados pelo fabricante nos equipamentos das entidades integrantes, observadas as normas de segurança da informação e legislação de propriedade intelectual de software.

8.3.6.7. A entidade deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

8.3.6.8. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável, devendo os relatórios impressos serem protegidos contra perda, reprodução e uso não-autorizado.

8.3.6.9. O inventário dos recursos deve ser mantido atualizado.

8.3.6.10. As entidades integrantes da ICPEdu Certificado Pessoal devem definir procedimentos formais para eliminação e descarte de mídias de forma segura quando estas não forem mais necessárias, com fins de minimizar os riscos.

# 9. REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS

## 9.1. **Requisitos gerais para sistema criptográfico da ICPEdu Certificado Pessoal**

9.1.1. O sistema criptográfico da ICPEdu Certificado Pessoal deve ser composto de:

9.1.1.1. Documentação normativa específica de criptografia aplicada na ICPEdu Certificado Pessoal;

9.1.1.2. Conjunto de requisitos criptográficos dos sistemas da ICPEdu Certificado Pessoal;

9.1.1.3. Projetos criptográficos desenvolvidos no âmbito da ICPEdu Certificado Pessoal;



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

9.1.1.4. Métodos para implementação de técnicas criptográficas na ICPEdu Certificado Pessoal;

9.1.1.5. Módulos implementados de hardware e software;

9.1.1.6. Definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico;

9.1.1.7. Procedimentos adotados para gerência das chaves criptográficas;

9.1.1.8. Métodos adotados para testes de robustez e detecção de violações das cifras.

9.1.2. Toda a documentação referente à definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados na ICPEdu Certificado Pessoal deve ser aprovada pela DAGSer.

9.1.3. Compete à AC Raiz da ICPEdu Certificado Pessoal acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados, com vistas a manter a segurança da infraestrutura.

9.1.4. Todo parâmetro crítico cuja exposição indevida comprometa a segurança do sistema criptográfico da ICPEdu Certificado Pessoal deve ser armazenado de forma cifrada.

9.1.5. Os aspectos relevantes relacionados à criptografia no âmbito da ICPEdu Certificado Pessoal devem ser detalhados em documentos específicos, aprovados pela DAGSer.

## 9.2. **Chaves criptográficas**

9.2.1. Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICPEdu Certificado Pessoal deverão ser executados pelo menor número necessário de responsáveis, assim como devem estar submetidos a mecanismos de controle definidos pela DAGSer.

9.2.2. Os responsáveis dos processos que envolvem as chaves criptográficas deverão ser formalmente designados, conforme as funções a serem desempenhadas e o correspondente grau de privilégios, assim como ter suas responsabilidades explicitamente definidas.

9.2.3. Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICPEdu Certificado Pessoal devem ser aprovados pela DAGSer.

9.2.4. Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da ICPEdu Certificado Pessoal devem estar explicitados nas práticas de certificação específicas.

### 9.3. **Transporte de informações**

9.3.1. O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICPEdu Certificado Pessoal devem ter a integridade e o sigilo assegurados por meio do emprego de soluções criptográficas específicas.

9.3.2. Deve-se adotar soluções baseadas em criptografia para realizar troca de informações sensíveis por meio de redes públicas entre as redes das entidades integrantes da ICPEdu Certificado Pessoal.

9.3.3. Estão habilitados a transportar e receber equipamentos de criptografia somente pessoas expressamente autorizadas pela DAGSer.

## 10.AUDITORIA E FISCALIZAÇÃO

### 10.1. **Diretrizes gerais**

10.1.1. A finalidade dos processos de auditoria e fiscalização deve ser a de verificar a capacidade das entidades integrantes da ICPEdu Certificado Pessoal em atender os requisitos de segurança desta Política de Segurança, de modo a facilitar a percepção e transmissão de confiança à comunidade de usuários.

10.1.2. O resultado das auditorias pré-operacionais deve ser condição necessária para o processo de credenciamento das entidades na ICPEdu Certificado Pessoal, da mesma forma que o resultado das auditorias operacionais e fiscalizações deve ser condição necessária para a manutenção da condição de entidade credenciada.

10.1.3. Auditorias regulares e periódicas devem ser realizadas nas entidades integrantes da ICPEdu Certificado Pessoal, inclusive de forma extraordinária quando necessária, conforme disposto no GR.POL.N.001.

# 11. GERENCIAMENTO DE RISCOS

## 11.1. Definição

11.1.1. Deve ter por objetivo a proteção da infraestrutura de certificação da ICPEdu Certificado Pessoal, por meio do levantamento dos riscos e posterior eliminação, redução ou transferência destes, conforme seja econômica e estrategicamente mais viável. Os pontos principais devem ser atendidos:

- identificação e classificação dos ativos;
- identificação das possíveis ameaças;
- identificação das possíveis vulnerabilidades;
- análise de riscos e;
- avaliação de riscos.

## 11.2. Fases principais

11.2.1. Identificação dos recursos a serem protegidos – hardware, rede, software, dados, informações pessoais, documentação, suprimentos;

11.2.2. Identificação dos riscos (ameaças) - que podem ser naturais, tais como tempestades, inundações, causadas por pessoas, tais como ataques, furtos, vandalismos, erros ou negligências ou de qualquer outro tipo, por exemplo, incêndios;

11.2.3. Análise dos riscos (vulnerabilidades e impactos) - identificação das vulnerabilidades e os impactos associados;

11.2.4. Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade de a ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;

11.2.5. Tratamento dos riscos (medidas a serem adotadas) - maneira de lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

11.2.6. Monitoramento da eficácia dos controles adotados para minimizar os riscos identificados;

11.2.7. Reavaliação periódica dos riscos em intervalos de tempo não superiores a 12 meses;



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

### 11.3. Riscos relacionados às entidades

11.3.1. Os riscos a serem avaliados para as entidades integrantes da ICPEdu Certificado Pessoal devem compreender minimamente, mas não limitado, aos seguintes:

| Ativos | Riscos |
|---|---|
| Dados e informação | Indisponibilidade, interrupção (perda), interceptação, modificação, fabricação, destruição. |
| Pessoas | Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, perda de conhecimento. |
| Rede | *Hacking*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço. |
| Hardware | Indisponibilidade, interceptação (furto ou roubo), falha. |
| Software e sistemas | Interrupção de serviço, interceptação, modificação, desenvolvimento, falha. |
| Recursos criptográficos | Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, *hardware* criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico. |

### 11.4. Implementação do Gerenciamento de Riscos

11.4.1. O gerenciamento de riscos nas entidades da ICPEdu Certificado Pessoal pode ser conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

### 11.5. Diretrizes gerais

11.5.1. Os riscos que não puderem ser eliminados devem ter seus controles documentados e ser levados ao conhecimento da DAGSer.

11.5.2. Um efetivo gerenciamento dos riscos deve permitir decidir se o custo de medida de proteção de um risco é mais alto que o custo das consequências do risco e os impactos da perda.

11.5.3. Convém a ciência e o envolvimento da alta gestão das entidades integrantes da ICPEdu Certificado Pessoal no apoio às medidas necessárias para o tratamento dos riscos.



CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

# 12.TRATAMENTO DE VIOLAÇÕES

## 12.1. **Diretrizes gerais**

12.1.1. Eventuais violações à esta política serão tratadas pela RNP junto à respectiva entidade integrante da ICPEdu Certificado Pessoal, priorizando ações que possibilitem a adequação à política antes de avaliar possíveis sanções.

12.1.2. Violações que, comprovadamente, exponham e afetem a ciberinfraestura do Sistema RNP, com prejuízo a sua operacionalidade, usabilidade, imagem ou que afete outros componentes do sistema, estarão sujeitas a medidas de mitigação emergenciais para reestabelecer a normalidade, as quais devem ser aplicadas enquanto durar a violação e comunicadas ao componente diretamente afetado.

12.1.3. O descumprimento reincidente da presente Política de Segurança, após esforços para a adequação, deverá ser apurado e avaliado por uma comissão interna, formada pela DAGSer e representantes internos da RNP previamente definidos, que apresentará seu parecer à Diretoria Executiva da RNP.

12.1.4. As sanções previstas em caso de descumprimento desta Política de Segurança poderão incluir a suspensão temporária ou descontinuidade de serviços, sem prejuízos a outras medidas administrativas ou legais cabíveis.

12.1.5. A RNP, por intermédio da DAGSer, deve conduzir todo o processo com transparência e idoneidade, mantendo os componentes diretamente envolvidos na violação informados e atualizados quanto ao andamento da apuração.



*CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada*