

***Política de Segurança da  
Autoridade Certificadora  
SIC BRASIL  
(PS da AC SIC BRASIL).***

***Versão 2.0  
Maio de 2020***

---

## **ÍNDICE**

- 1. INTRODUÇÃO6
- 2. OBJETIVOS6
- 3. ABRANGÊNCIA6
- 4. TERMINOLOGIA6
- 5. CONCEITOS E DEFINIÇÕES6
- 6. REGRAS GERAIS7
  - 6.1. GESTÃO DE SEGURANÇA7
  - 6.2. GERENCIAMENTO DE RISCOS8
  - 6.3. INVENTÁRIO DE ATIVOS8
  - 6.4. PLANO DE CONTINUIDADE DO NEGÓCIO8
- 7. REQUISITOS DE SEGURANÇA DE PESSOAL9
  - 7.1. DEFINIÇÃO9
  - 7.2. OBJETIVOS9
  - 7.3. DIRETRIZES9
    - 7.3.1. O Processo de Admissão9
    - 7.3.2. As Atribuições da Função10
    - 7.3.3. O Levantamento de Dados Pessoais10
    - 7.3.4. A Entrevista de Admissão10
    - 7.3.5. O Desempenho da Função10
    - 7.3.6. A Credencial de Segurança11
    - 7.3.7. Treinamento em Segurança da Informação11
    - 7.3.8. Acompanhamento no Desempenho da Função11
    - 7.3.9. O Processo de Desligamento, Férias e Licença.11
    - 7.3.10. O Processo de Liberação11
    - 7.3.11. A Entrevista de Desligamento12
  - 7.4. DEVERES E RESPONSABILIDADES12
    - 7.4.1. Deveres dos funcionários ou prestadores de serviços12
    - 7.4.2. Responsabilidades dos cargos de chefias12
    - 7.4.3. Responsabilidades Gerais13
    - 7.4.4. Responsabilidades da Gerência de Segurança13
    - 7.4.5 Responsabilidades dos prestadores de serviço:14
  - 7.5 SANÇÕES14
- 8. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO14
  - 8.1. DEFINIÇÃO14
  - 8.2. DIRETRIZES GERAIS14

- 
- 9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO**16**
    - 9.1. DEFINIÇÃO**16**
    - 9.2. DIRETRIZES GERAIS**16**
    - 9.3. DIRETRIZES ESPECÍFICAS**16**
      - 9.3.1. Sistemas**16**
      - 9.3.2. Máquinas servidoras**17**
      - 9.3.3. Redes da AC SIC BRASIL**18**
      - 9.3.4. Controle de acesso lógico (baseado em senhas)**21**
      - 9.3.5. Computação pessoal**22**
      - 9.3.6. Combate a Vírus de Computador**23**
  - 10. REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS**23**
    - 10.1. REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA ICP-BRASIL**23**
    - 10.2. CHAVES CRIPTOGRÁFICAS**23**
    - 10.3. TRANSPORTE DAS INFORMAÇÕES**24**
  - 11. AUDITORIA E FISCALIZAÇÃO**24**
  - 12. GERENCIAMENTO DE RISCOS**25**
    - 12.1. DEFINIÇÃO**25**
    - 12.2. FASES PRINCIPAIS**25**
    - 12.3. RISCOS RELACIONADOS À AC SIC BRASIL**25**
    - 12.4. CONSIDERAÇÕES GERAIS**26**
    - 12.5. IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS**26**
  - 13. PLANO DE CONTINUIDADE DO NEGÓCIO**26**
    - 13.1. DEFINIÇÃO**26**
    - 13.2. DIRETRIZES GERAIS**26**
  - 14. DOCUMENTOS REFERENCIADOS**28**

---

**CONTROLE DE ALTERAÇÕES**

<b>Versão</b>	<b>Data</b>	<b>Resolução que aprova a alteração</b>	<b>Item Alterado</b>	<b>Descrição da Alteração</b>
2.0	17/04/2020	Resolução n. 151	Não se aplica	Criação da Política de Segurança da AR SIC.

---

## LISTA DE ACRÔNIMOS

**AC** - Autoridade Certificadora

**AC Raiz** - Autoridade Certificadora Raiz da ICP-Brasil

**ACT** – Autoridade Certificadora do Tempo

**AR** - Autoridades de Registro

**DPC** - Declaração de Práticas de Certificação

**ICP-Brasil** - infraestrutura de Chaves Públicas Brasileira

**CG** - Comitê Gestor

**PCN** - Plano de Continuidade de Negócio

**PS** - Política de Segurança

**TI** - Tecnologia da Informação

**CFTV** - Circuito Fechado de Televisão

**ABNT** – Associação Brasileira de Normas Técnicas

**VPN** - Virtual Private Networks

## 1. INTRODUÇÃO

1.1. Este documento tem por finalidade estabelecer as diretrizes de segurança que são adotadas pela Autoridade Certificadora **SIC BRASIL – AC SIC BRASIL** na Infraestrutura de Chaves Públicas Brasileira ICP-Brasil.

1.2. Para o cumprimento da finalidade supramencionada são estabelecidos os objetivos a seguir.

## 2. OBJETIVOS

A Política de Segurança da AC **SIC BRASIL** tem os seguintes objetivos:

- a) Definir o escopo da segurança das entidades;
- b) Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades reduzindo os riscos e garantindo a integridade, o sigilo e a disponibilidade das informações dos sistemas de informação e recursos;
- c) Permitir a adoção de soluções de segurança integradas;
- d) Servir de referência para auditoria, apuração e avaliação de responsabilidades.

## 3. ABRANGÊNCIA

A Política de Segurança abrange os seguintes aspectos:

- a) Requisitos de segurança humana;
- b) Requisitos de segurança física;
- c) Requisitos de segurança lógica;
- d) Requisitos de Segurança dos Recursos Criptográficos.

## 4. TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

## 5. CONCEITOS E DEFINIÇÕES

Aplicam-se os conceitos abaixo no que se refere à Política de Segurança das entidades:

**a) Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades vinculadas à AC **SIC BRASIL**;

**b) Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos

das entidades relacionadas à AC **SIC BRASIL**, tanto os produzidos internamente quanto os adquiridos;

**c) Controle de Acesso** – são restrições ao acesso às informações de um sistema exercidas pela gerência de segurança da informação das entidades relacionadas à AC **SIC BRASIL**;

**d) 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;

**e) Direito de Acesso** – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

**f) Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da informação das entidades vinculadas à AC **SIC BRASIL**;

**g) Incidente de Segurança** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da AC **SIC BRASIL** e das entidades integrantes da ICP-Brasil;

**h) Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação da AC **SIC BRASIL** e das entidades a ela vinculadas;

**i) Proteção dos Ativos** – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

**j) Responsabilidade** – são as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

**k) Senha Fraca ou Óbvia** – é aquela na qual utilizam-se 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.

## 6. REGRAS GERAIS

### 6.1. GESTÃO DE SEGURANÇA

**6.1.1.** A Política de Segurança da AC **SIC BRASIL** aplica-se a todos os recursos humanos, administrativos e tecnológicos pertencentes à AC **SIC BRASIL** e/ou as entidades que a compõem. A abrangência dos recursos citados refere-se tanto àqueles ligados às entidades em caráter permanente ou temporário.

**6.1.2.** Esta política é comunicada para todo o pessoal envolvido e largamente divulgada através da AC **SIC BRASIL** e as entidades à ela vinculadas, garantindo que todos tenham consciência da Política e a pratiquem na organização.

**6.1.3.** Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado na política de segurança.

**6.1.4.** Um programa de conscientização sobre segurança da informação é implementado através de treinamentos específicos, assegurando que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações da AC **SIC BRASIL** e suas entidades vinculadas. Especificamente, o pessoal envolvido ou que se relaciona com os usuários estão informados sobre ataques típicos de engenharia social e como se proteger deles.

**6.1.5.** Os procedimentos são documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

**6.1.6.** A AC **SIC BRASIL** mantém mecanismo e repositório centralizado para manutenção de trilhas, *logs* e demais notificações de incidentes. O Gerente de Segurança é acionado, uma vez que qualquer tentativa de violação seja detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra ataques empreendidos contra esses mecanismos.

**6.1.7.** Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, estão em conformidade com esta Política de Segurança.

**6.1.8.** É considerada proibida qualquer ação que não esteja explicitamente permitida na Política de Segurança da AC **SIC BRASIL** ou que não tenha sido previamente autorizada pelo Gerente de Segurança da AC **SIC BRASIL**.

## **6.2. GERENCIAMENTO DE RISCOS**

A AC **SIC BRASIL** implementa análises de risco periodicamente através de sua própria estrutura e de terceiros. O processo de gerenciamento de riscos é revisto, anualmente, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção dos componentes ameaçados.

## **6.3. INVENTÁRIO DE ATIVOS**

Todos os ativos da AC **SIC BRASIL** são inventariados, classificados, permanentemente atualizados, e possuem gestor responsável formalmente designado.

## **6.4. PLANO DE CONTINUIDADE DO NEGÓCIO**

**6.4.1.** O Plano de Continuidade do Negócio (PCN) da AC **SIC BRASIL** é testado pelo menos uma vez por ano, garantindo a continuidade dos serviços críticos ao negócio.

**6.4.2.** A AC **SIC BRASIL** possui Plano de Recuperação de Desastres e Plano de



Resposta a Incidentes aprovados pela AC Raiz ou AC de nível imediatamente superior.

**6.4.3.** O certificado da AC **SIC BRASIL** é imediatamente revogado, no caso de ocorrência de perda ou comprometimento de sua chave privada ou do seu meio de armazenamento, seguindo os procedimentos detalhados na DPC da AC **SIC BRASIL**.

**6.4.4.** Todos os incidentes são reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes são reportados de modo sigiloso a pessoas especialmente designadas para isso.

## 7. REQUISITOS DE SEGURANÇA DE PESSOAL

### 7.1. DEFINIÇÃO

Conjunto de medidas e procedimentos de segurança, a serem observados pelos prestadores de serviço por todos os funcionários, necessários à proteção dos ativos da AC **SIC BRASIL**.

### 7.2. OBJETIVOS

**7.2.1.** Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos da AC **SIC BRASIL**.

**7.2.2.** Prevenir e neutralizar as ações de pessoas que possam comprometer a segurança da AC **SIC BRASIL**.

**7.2.3.** Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados à AC **SIC BRASIL**, 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.

**7.2.4.** Orientar o processo de avaliação de todo o pessoal que trabalhe na AC **SIC BRASIL** e nas entidades a ela vinculadas, mesmo em caso de funções desempenhadas por prestadores de serviço.

### 7.3. DIRETRIZES

#### 7.3.1. O Processo de Admissão

**7.3.1.1.** São adotados critérios rígidos para o processo seletivo de candidatos em funções ligadas ao ciclo de vida dos certificados, com o propósito de selecionar para os quadros das entidades integrantes da AC **SIC BRASIL** pessoas reconhecidamente idôneas e sem antecedentes que possam vir a comprometer a segurança ou credibilidade da AC **SIC BRASIL**.

**7.3.1.2.** A AC **SIC BRASIL** não admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição,

revogação e gerenciamento de certificados.

**7.3.1.3.** O empregado, funcionário ou prestador de serviços assina um termo de compromisso assumindo o dever de cumprir a Política de Segurança da AC **SIC BRASIL** e o Acordo de Confidencialidade e Exclusividade de Propriedade das Informações da AC **SIC BRASIL**. Nesses documentos cada funcionário assume o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.

### **7.3.2. As Atribuições da Função**

As atribuições de cada função são relacionadas de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do funcionário ou prestador de serviço, considerando-se os seguintes itens:

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

### **7.3.3. O Levantamento de Dados Pessoais**

O levantamento de dados pessoais é elaborado através de pesquisado histórico da vida pública do candidato, com o propósito de levantamento de seu perfil, verificação de antecedentes e verificação de grau de instrução.

### **7.3.4. A Entrevista de Admissão**

**7.3.4.1.** É realizada, por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante o levantamento de dados pessoais do candidato.

**7.3.4.2.** São avaliadas, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato são apenas aquelas de caráter público.

### **7.3.5. O Desempenho da Função**

**7.3.5.1.** Periodicamente, o desempenho dos funcionários é acompanhado e avaliado com o propósito de detectar a necessidade de atualização técnica e de segurança.

**7.3.5.2.** É dado aos funcionários ou prestadores de serviços da AC **SIC BRASIL** acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

### **7.3.6. A Credencial de Segurança**

**7.3.6.1.** O funcionário é identificado por meio de uma credencial (crachá apropriado) que habilita o acesso às informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou à função a ser desempenhada.

**7.3.6.2.** A Credencial de Segurança somente é concedida pela área de Segurança e é fundamentada na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função.

**7.3.6.3.** É de um ano o prazo de Validade máximo de concessão a um indivíduo de uma credencial de segurança. Este prazo poderá ser prorrogado por igual período, quantas vezes forem necessárias, por ato da Gerência de Segurança, enquanto exigir a necessidade do serviço.

### **7.3.7. Treinamento em Segurança da Informação**

**7.3.7.1.** Nos treinamentos de segurança, a Política de Segurança e suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos são apresentadas aos funcionários e prestadores de serviço, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento.

**7.3.7.2.** Todo funcionário é treinado na ocasião de sua admissão na Instituição.

### **7.3.8. Acompanhamento no Desempenho da Função**

**7.3.8.1.** São realizados processos de avaliação de desempenho da função que documentam a observação do comportamento pessoal e funcional dos funcionários. A avaliação é realizada pela chefia imediata.

**7.3.8.2.** São registrados os atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do funcionário.

**7.3.8.3.** Os comportamentos incompatíveis ou que possam gerar comprometimentos à segurança são averiguados e comunicados à chefia imediata.

**7.3.8.4.** As chefias imediatas asseguram que todos os funcionários ou prestadores de serviços tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

### **7.3.9. O Processo de Desligamento, Férias e Licença.**

**7.3.9.1.** O acesso de ex-funcionários às instalações da AC **SIC BRASIL** é restrito às áreas de acesso público.

**7.3.9.2.** Sua credencial, sua identificação, seu crachá, o uso de equipamentos, mecanismos e acessos físicos e lógicos são revogados.

### **7.3.10. O Processo de Liberação**

O funcionário ou prestador de serviço assina, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que

compõem a AC **SIC BRASIL**.

### 7.3.11. A Entrevista de Desligamento

É realizada entrevista de desligamento para orientar o funcionário ou prestador de serviço sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência na AC **SIC BRASIL**.

## 7.4. DEVERES E RESPONSABILIDADES

### 7.4.1. Deveres dos funcionários ou prestadores de serviços

São deveres dos empregados ou prestadores de serviço:

- a) preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
- b) cumprir a política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- c) utilizar os sistemas de informações da AC **SIC BRASIL** e os recursos a ela relacionados somente para os fins previstos pela gerência de segurança;
- d) cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
- e) manter o caráter sigiloso da senha de acesso aos recursos e sistemas da AC **SIC BRASIL**;
- f) não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- g) responder, por todo e qualquer acesso, aos recursos da AC **SIC BRASIL** bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo para esse fim utilizado;
- h) 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;
- i) comunicar, imediatamente, ao seu superior imediato e/ou ao Gerente de Segurança o conhecimento de qualquer irregularidade ou desvio.

### 7.4.2. Responsabilidades dos cargos de chefias

A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

- a) gerenciar o cumprimento da Política de Segurança da AC **SIC BRASIL** por parte de seus funcionários e prestadores de serviços;
- b) identificar os desvios praticados e adotar as medidas corretivas apropriadas;

- c) impedir o acesso de funcionários demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do funcionário;
- d) proteger, no nível físico e lógico, os ativos de informação e de processamento da AC **SIC BRASIL** relacionados com a sua área de atuação;
- e) garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações da AC **SIC BRASIL**;
- f) comunicar formalmente à área de Segurança quais os funcionários e prestadores de serviço, sob sua supervisão, que podem acessar as informações da AC **SIC BRASIL**, seguindo as normas de classificação de informações e os perfis de cada cargo;
- g) comunicar formalmente ao Departamento Pessoal quais os funcionários e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários;
- h) comunicar formalmente ao Departamento Pessoal aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

#### **7.4.3. Responsabilidades Gerais**

São responsabilidades gerais:

- a) cada área que detém os ativos de processamento e de informação é responsável por eles, provendo a sua proteção de acordo com a política de classificação da informação da AC **SIC BRASIL**;
- b) todos os ativos de informações têm claramente definidos os responsáveis pelo seu uso;
- c) todos os ativos de processamento estão relacionados no Plano de Continuidade do Negócio - PCN;

#### **7.4.4. Responsabilidades da Gerência de Segurança**

São responsabilidades da Gerência de Segurança:

- a) estabelecer as regras de proteção dos ativos da AC **SIC BRASIL**;
- b) decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
- c) revisar, anualmente, as regras de proteção estabelecidas;
- d) restringir e controlar o acesso e os privilégios de usuários remotos e externos;
- e) elaborar e manter atualizado o Plano de Continuidade do Negócio - PCN;
- f) executar as regras de proteção estabelecidas pela Política de Segurança;
- g) detectar, identificar, registrar e comunicar à AC Raiz as violações ou tentativas relevantes e significativas de acesso não autorizadas;
- h) definir e aplicar, para cada usuário de TI, restrições de acesso à rede, como

horários autorizados, dias autorizados, entre outras;

- i) manter registros de atividades de usuários de TI (*logs*) por um período de no mínimo 7 (sete) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc);
- j) limitar o prazo de Validade das contas de prestadores de serviço ao período da contratação.
- k) verificar a exclusão das contas inativas.
- l) autorizar o fornecimento de senhas de contas privilegiadas somente aos funcionários que necessitem efetivamente dos privilégios segundo sua descrição de cargos, mantendo-se o devido registro e controle.

#### **7.4.5 Responsabilidades dos prestadores de serviço:**

São previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos.

### **7.5 SANÇÕES**

Sanções previstas pela legislação vigente.

## **8. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO**

### **8.1. DEFINIÇÃO**

Ambiente físico é aquele composto por todo o ativo permanente da AC **SIC BRASIL**.

### **8.2. DIRETRIZES GERAIS**

**8.2.1.** As responsabilidades pela segurança física dos sistemas da AC **SIC BRASIL** são definidas e atribuídas à Gerência de Segurança (ativos corporativos) e de Operações (Autoridade Certificadora).

**8.2.2.** A localização das instalações e o sistema de certificação da AC **SIC BRASIL** não são publicamente identificados.

**8.2.3.** Existem sistemas de segurança para acesso física, permitindo controlar e auditar o acesso aos sistemas de certificação.

**8.2.4.** São estabelecidos controles duplicados sobre o inventário e cartões/chaves de acesso. Uma lista atualizada do pessoal que possui cartões/chaves é mantida pela área de Segurança.

**8.2.5.** Chaves criptográficas são mantidas sob custódia da área de Criptografia e fisicamente protegidas contra acesso não autorizado, uso ou duplicação.



**8.2.6.** Perdas de cartões/chaves de acesso são imediatamente comunicadas ao responsável pela Gerência de Segurança da AC **SIC BRASIL**. Ele toma as medidas apropriadas para prevenir acessos não autorizados.

**8.2.7.** O sistema da AC está localizado em área protegida (ambiente de nível 4) e afastada de fontes potentes de magnetismo ou interferência de rádio frequência.

**8.2.8.** Recursos e instalações críticas ou sensíveis devem ser fisicamente protegidos de acesso não autorizado, dano, ou interferência, com barreiras de segurança e controle de acesso. A proteção deve ser proporcional aos riscos identificados. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

**8.2.9.** A entrada e saída, nestas áreas ou partes dedicadas, são automaticamente registradas com data e hora definidas e são revisadas periodicamente pelo responsável pela Gerência de Segurança e mantidas em local adequado e sob sigilo.

**8.2.10.** O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal das áreas de Segurança e Infraestrutura.

**8.2.11.** São utilizados sistemas de detecção de intrusão para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.

**8.2.12.** O inventário de todo o conjunto de ativos de processamento é registrado e mantido atualizado, mensalmente.

**8.2.13.** Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só são utilizados a partir de autorização formal da área de Segurança e mediante supervisão.

**8.2.14.** Nas instalações da AC **SIC BRASIL** todos utilizam crachá de identificação e devem informar à Gerência de Segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não-acompanhado.

**8.2.15.** Visitantes as instalações da AC **SIC BRASIL** são supervisionadas. Suas horas de entrada e saída e o local de destino são registrados. Essas pessoas têm acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos seguem instruções baseadas nos requisitos de segurança da área visitada.

**8.2.16.** Os ambientes onde ocorrem os processos críticos da AC **SIC BRASIL** são monitorados, em tempo real, com as imagens registradas por meio de sistemas de Circuito Fechado de Televisão - CFTV.

**8.2.17.** Sistemas de detecção de intrusos foram instalados e são testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis nos ambientes onde ocorrem processos críticos. As áreas não ocupadas possuem um sistema de alarme que permanece sempre ativado, desligando-se quando o sistema de controle de acesso identifica a entrada de alguém autorizado.

---

## 9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

### 9.1. DEFINIÇÃO

Ambiente lógico é composto por todo o ativo de informações da AC **SIC BRASIL**.

### 9.2. DIRETRIZES GERAIS

**9.2.1.** A informação é protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, a AC **SIC BRASIL** possui um sistema de classificação da informação.

**9.2.2.** Os dados, as informações e os sistemas de informação da AC **SIC BRASIL** e sob sua guarda são protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

**9.2.3.** As violações de segurança são registradas e esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

Cada tipo de registro é analisado com forma e periodicidade própria de acordo com sua natureza, procedimento este realizado tanto pela área de Segurança como de Operações. Os registros são protegidos e armazenados de acordo com a sua classificação e mantidos sob custódia da área de Segurança.

Os tipos de registros mantidos pela AC **SIC BRASIL** englobam:

- registros de sistemas operacionais – *login*, *logout*, acesso a arquivos do sistema, dentre outros. Tais registros devem ser avaliados semanalmente.
- registros de aplicativos – registros de transações realizadas por servidores Web, Bancos de Dados. Tais registros devem ser avaliados semanalmente.
- registros de firewall e roteadores - pacotes e conexões aceitas e rejeitadas. Tais registros devem ser avaliados semanalmente.
- registros do sistema de detecção de invasão – tentativas de invasão da rede externa para a rede interna e vice-versa. Tais registros devem ser avaliados *online* permanentemente.

**9.2.4.** Os sistemas e recursos que suportam funções críticas para operação da AC **SIC BRASIL** asseguram a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

**9.2.5.** O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, está registrado e é mantido atualizado mensalmente.

### 9.3. DIRETRIZES ESPECÍFICAS

#### 9.3.1. Sistemas

**9.3.1.1.** As necessidades de segurança são identificadas para cada etapa do ciclo



de vida dos sistemas AC **SIC BRASIL**. A documentação dos sistemas é mantida atualizada. A cópia de segurança é testada e mantida atualizada.

**9.3.1.2.** Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado.

As autorizações devem ser realizadas segundo sua criticidade:

- usuários só poderão ter acesso a sistemas uma vez que tenham autorização do Departamento Pessoal, com o devido consentimento da Área de Segurança.
- exceções só poderão ser autorizadas pelo Gerente de Segurança ou por seu substituto em caso de impedimento.

**9.3.1.3.** Os arquivos de *logs* são criteriosamente definidos para permitir recuperação nas situações de falhas, auditorias nas situações de violações de segurança e contabilização do uso de recursos. Os *logs* são periodicamente analisados, no máximo semanalmente, para identificar tendências, falhas ou usos indevidos. O *log* do sistema de detecção de invasão é avaliado preferencialmente *online* e imediatamente após a constatação do início de um incidente. Os *logs* devem ser protegidos e armazenados de acordo com sua classificação.

**9.3.1.4.** São estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto à sua precisão, consistência e integridade.

**9.3.1.4.1.** É gerado periodicamente um *hash* dos seguintes componentes do sistema:

- arquivos críticos do sistema operacional;
- arquivos críticos das aplicações;
- arquivos que contenham informações classificadas estáticas.

Quaisquer alterações ou tentativas de alteração realizadas em tais arquivos, observadas nas auditorias de *log*, devem ser registradas e investigadas.

**9.3.1.5.** Os sistemas são avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente são avaliadas periodicamente e as recomendações de segurança adotadas.

## **9.3.2. Máquinas servidoras**

**9.3.2.1.** O acesso lógico ao ambiente ou serviços disponíveis em servidores é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. Todas as exceções devem ser aprovadas pelo Gerente de Segurança.

**9.3.2.2.** Os acessos lógicos são registrados em *logs*, que são analisados semanalmente. Tais arquivos de *log* são armazenados em servidor específico. O tempo de retenção desses *logs* é de pelo menos 2 (dois) meses. Neste servidor o

sistema de controle de acesso aos *logs* é feito através de mecanismos nativos do sistema operacional.

**9.3.2.3.** São adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do sistema operacional. Existem medidas preventivas, como procedimentos detectivos que permitam a identificação de qualquer anomalia. Os eventos são armazenados em relatórios de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros. Todos os registros são mantidos pela área de Segurança em local seguro e centralizado.

**9.3.2.4.** As máquinas são sincronizadas para permitir o rastreamento de eventos.

**9.3.2.5.** Proteção lógica adicional (criptografia) é adotada para evitar o acesso não-autorizado às informações, segundo classificações de segurança definidas para as informações.

**9.3.2.6.** A versão do sistema operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, são mantidos atualizados, em conformidade com as recomendações dos fabricantes.

**9.3.2.7.** São utilizados somente *softwares* autorizados pela AC **SIC BRASIL** nos seus equipamentos. É realizado o controle da distribuição e instalação dos mesmos.

**9.3.2.8.** O acesso remoto a máquinas servidoras é realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço.

**9.3.2.9.** Os procedimentos de cópia de segurança (*backup*) e de recuperação estão documentados, atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações.

### **9.3.3. Redes da AC SIC BRASIL**

**9.3.3.1.** O tráfego das informações no ambiente de rede é protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o “Efeito *Tempest*”.

**9.3.3.2.** Componentes críticos da rede local são mantidos em salas protegidas e com acesso físico e lógico controlado, sendo protegidos contra danos, furtos, roubos e intempéries. Os servidores devem ser mantidos no mesmo nível das informações que eles armazenam. Todos os servidores da rede local estão em *racks* adequados.

**9.3.3.3.** São adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.

**9.3.3.4.** A configuração de todos os ativos de processamento é averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nestes ativos em sua primeira ativação.

**9.3.3.5.** Serviços vulneráveis são eliminados ou trocados por similares mais

seguros.

**9.3.3.6.** O uso de senhas é submetido a uma política específica para sua gerência e utilização.

**9.3.3.7.** O acesso lógico aos recursos da rede local é realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário.

**9.3.3.8.** A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só ocorrem a partir de autorização formal e mediante supervisão.

**9.3.3.9.** A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração são formalmente documentadas e mantidas, de forma a permitir registro histórico, e tem a autorização da administração da rede e da Gerência de Segurança. O diagrama topológico, a configuração e o inventário dos recursos são mantidos atualizados.

**9.3.3.10.** São definidos relatórios de segurança (*logs*) periódicos de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Tais relatórios são disponibilizados e armazenados de maneira segura. As anormalidades identificadas nestes relatórios são tratadas segundo a sua severidade. Entre elas, incluem-se:

- ataques externos e internos;
- utilização indevida de recursos;
- falhas de subsistemas.

**9.3.3.11.** São adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

**9.3.3.12.** A AC **SIC BRASIL** adota proteção lógica adicional para evitar o acesso não autorizado às informações.

**9.3.3.13.** A infraestrutura de interligação lógica está protegida contra danos mecânicos e conexão não autorizada.

**9.3.3.14.** A alimentação elétrica para a rede local é separada da rede convencional, sendo observadas as recomendações dos fabricantes dos equipamentos utilizados assim como as normas ABNT aplicáveis.

**9.3.3.15.** O tráfego de informações é monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

**9.3.3.16.** São observadas as questões envolvendo propriedade intelectual quando da cópia de *software* ou arquivos de outras localidades.

**9.3.3.17.** Informações sigilosas, corporativas ou que possam causar prejuízo a terceiros estão protegidas e não são enviadas para outras redes, sem proteção adequada.

**9.3.3.18.** Todo serviço de rede não explicitamente autorizado pela AC **SIC BRASIL** é bloqueado ou desabilitado.

**9.3.3.19.** Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) são utilizados para proteger as transações entre redes externas e a rede interna da AC **SIC BRASIL**.

**9.3.3.20.** Os registros de eventos são analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

**9.3.3.21.** É adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos.

**9.3.3.22.** Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, fazem uso de tal controle.

**9.3.3.23.** A localização dos serviços baseados em sistemas de proteção de acesso (firewall) é resultante de uma análise de riscos. No mínimo os seguintes aspectos são considerados:

- 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;
- volume de tráfego.

**9.3.3.24.** Ambientes de rede considerados críticos são isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

**9.3.3.25.** Conexões entre as redes da AC **SIC BRASIL** e redes externas estão restritas somente àquelas que visem efetivar os processos necessários à operação da AC **SIC BRASIL**.

**9.3.3.26.** As conexões de rede da AC **SIC BRASIL** são ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, a AC **SIC BRASIL** emprega controles de compensação, tais como o uso de *proxies* que são implementados pela AC **SIC BRASIL** para proteger os sistemas que executam a função de certificação contra possíveis ataques.

**9.3.3.27.** Sistemas que executam a função de certificação estão isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade de tais funções.

**9.3.3.28.** A chave de certificação da AC **SIC BRASIL** está protegida de acesso desautorizado, para garantir seu sigilo e integridade.

**9.3.3.29.** A segurança das comunicações intra-rede e inter-rede entre os sistemas da AC **SIC BRASIL** é garantida pelo uso de mecanismos que asseguram o sigilo e a integridade das informações trafegadas.

**9.3.3.30.** As ferramentas de detecção de intrusos são implantadas para monitorar

as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão.

#### **9.3.4. Controle de acesso lógico (baseado em senhas)**

**9.3.4.1.** Usuários e aplicações que necessitem ter acesso a recursos da AC **SIC BRASIL** são identificados e autenticados.

**9.3.4.2.** O sistema de controle de acesso mantém as habilitações atualizadas e registros que permitem a contabilização do uso, auditoria e recuperação nas situações de falha.

**9.3.4.3.** Não é permitido a nenhum usuário obter direitos de acesso de outro usuário.

**9.3.4.4.** A informação que especifica os direitos de acesso de cada usuário ou aplicação é protegida contra modificações não autorizadas.

**9.3.4.5.** O arquivo de senhas é criptografado e o seu acesso controlado.

**9.3.4.6.** As autorizações são definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

**9.3.4.7.** As senhas são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada.

**9.3.4.8.** O sistema de controle de acesso possui mecanismos que impedem a geração de senhas fracas ou óbvias.

**9.3.4.9.** As seguintes características das senhas são definidas:

- O conjunto de caracteres permitidos deve incluir letras (maiúsculas e minúsculas), números e caracteres especiais;
- Tamanho mínimo é de 8 caracteres;
- Não existe tamanho máximo;
- O prazo de Validade máximo é de 90 dias;
- As trocas são realizadas através dos mecanismos nativos dos sistemas operacionais;
- Restrições específicas para cada ambiente, aplicação ou plataforma poderão ser adotadas, se necessárias.

**9.3.4.10.** A distribuição de senhas (iniciais ou não) aos usuários de TI é feita de forma segura. A senha inicial, quando gerada pelo sistema, é trocada, pelo usuário de TI, no primeiro acesso.

**9.3.4.11.** O sistema de controle de acesso permite ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só é executada após a identificação positiva do usuário. A senha digitada não é exibida.

**9.3.4.12.** Os usuários são bloqueados após 45 dias sem acesso e/ou 3 tentativas sucessivas de acesso mal sucedidas.

**9.3.4.13.** O sistema de controle de acesso solicita nova autenticação após 20 minutos de inatividade da sessão (*time-out*).

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

**9.3.4.15.** O registro das atividades (*logs*) do sistema de controle de acesso é definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *logs* devem ser periodicamente analisados.

**9.3.4.16.** Os usuários e administradores do sistema de controle de acesso são formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

### **9.3.5. Computação pessoal**

**9.3.5.1.** As estações de trabalho, incluindo equipamentos portáteis ou *stand alone* e informações, são protegidos contra danos ou perdas, bem como uso ou exposições indevidos.

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

**9.3.5.3.** São adotadas medidas de segurança lógica referentes ao combate a vírus, *backup*, controle de acesso e uso de *software* não autorizado.

**9.3.5.4.** As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de *backup*, definidos em documento específico.

**9.3.5.5.** Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo as entidades da ICP-Brasil, só são utilizadas em equipamentos da AC **SIC BRASIL** onde foram geradas ou naqueles equipamentos por ela autorizados, com controles adequados.

**9.3.5.6.** O acesso às informações atende aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo).

**9.3.5.7.** Os usuários de TI utilizam apenas *softwares* licenciados pelo fabricante nos equipamentos da AC **SIC BRASIL**, observadas as normas da ICP-Brasil e legislação de *software*.

**9.3.5.8.** A AC **SIC BRASIL** estabelece os aspectos de controle, distribuição e instalação de *softwares* utilizados.

**9.3.5.9.** A impressão de documentos sigilosos é feita sob supervisão do responsável. Os relatórios impressos são protegidos contra perda, reprodução e uso não autorizado.

**9.3.5.10.** O inventário dos recursos é mantido atualizado.

**9.3.5.11.** Os sistemas em uso solicitam nova autenticação após 20 minutos de



inatividade da sessão (*time-out*).

**9.3.5.12.** As mídias são eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias são definidos, para minimizar os riscos.

### **9.3.6. Combate a Vírus de Computador**

Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e *worms*) são sistematizados e englobam máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

## **10. REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS**

### **10.1. REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA ICP-BRASIL**

**10.1.1.** O sistema criptográfico da AC **SIC BRASIL** é entendido como sendo um sistema composto de documentação normativa específica de criptografia aplicada na ICP-Brasil, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas.

**10.1.2.** Toda a documentação referente à definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados pela AC **SIC BRASIL** é aprovada pela AC Raiz.

**10.1.3.** Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, com vistas a manter a segurança da infraestrutura.

**10.1.4.** Todo parâmetro crítico cuja exposição indevida comprometa a segurança do sistema criptográfico da AC **SIC BRASIL** é armazenado cifrado.

**10.1.5.** Os aspectos relevantes relacionados à criptografia no âmbito da ICP-Brasil, são detalhados em documentos específicos, aprovados pela AC Raiz.

### **10.2. CHAVES CRIPTOGRÁFICAS**

**10.2.1.** A manipulação das chaves criptográficas utilizadas nos sistemas criptográficos da AC **SIC BRASIL** é restrita a um número mínimo e essencial de pessoas, assim como está submetida a mecanismos de controle considerados adequados pelo CG ICP-Brasil.

**10.2.2.** As pessoas, às quais se refere o item anterior, são formalmente designadas pelo Gerente de Criptografia, conforme as funções a serem desempenhadas e o correspondente grau de privilégios, assim como ter suas responsabilidades

explicitamente definidas.

**10.2.3.** Os algoritmos de criação e de troca das chaves criptográficas utilizadas no sistema criptográfico da AC **SIC BRASIL** são aprovados pelo CG ICP-Brasil.

**10.2.4.** Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da AC **SIC BRASIL** estão explicitados nas Políticas de Certificado implementadas da AC **SIC BRASIL**.

### **10.3. TRANSPORTE DAS INFORMAÇÕES**

**10.3.1.** O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da AC **SIC BRASIL** tem a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

**10.3.2.** São adotados recursos de VPN (*Virtual Private Networks* – redes privadas virtuais), baseadas em criptografia, para a troca de informações sensíveis, por meio de redes públicas, entre as redes das entidades da ICP-Brasil que pertençam a uma mesma organização.

**10.3.3.** Estão habilitados a transportar e receber os equipamentos de criptografia os Gerentes de Criptografia junto com qualquer outro funcionário de confiança da AC **SIC BRASIL**.

## **11. AUDITORIA E FISCALIZAÇÃO**

**11.1.** As atividades da AC **SIC BRASIL** estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade da AC **SIC BRASIL** em atender aos requisitos da ICP-Brasil.

**11.2.** O resultado das auditorias pré-operacionais é um item fundamental a ser considerado no processo de credenciamento da AC **SIC BRASIL**, da mesma forma que o resultado das auditorias operacionais e fiscalizações é item fundamental para a manutenção da condição de credenciada.

**11.3.** São realizadas auditorias periódicas na AC **SIC BRASIL**, pela AC Raiz ou por terceiros por ele autorizados, conforme o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [1]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

**11.4.** Além de auditadas, a AC **SIC BRASIL** pode ser fiscalizada pela AC Raiz a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].



## 12. GERENCIAMENTO DE RISCOS

### 12.1. DEFINIÇÃO

Processo que visa à proteção dos serviços da AC **SIC BRASIL**, por meio da eliminação, redução ou transferência dos riscos. Os seguintes pontos principais são identificados:

- O que deve ser protegido;
- Análise de riscos (contra quem ou contra o que deve ser protegido);
- Avaliação de riscos (análise da relação custo/benefício).

### 12.2. FASES PRINCIPAIS

O gerenciamento de riscos consiste das seguintes fases principais:

- Identificação dos recursos a serem protegidos – *hardwares*, rede, *software*, dados, informações pessoais, documentação, suprimentos;
- Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);
- Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;
- Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;
- Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;
- Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;
- Reavaliação periódica dos riscos em intervalos de tempo não superiores a 1 (um) ano;

### 12.3. RISCOS RELACIONADOS À AC SIC BRASIL

Os riscos avaliados para a AC **SIC BRASIL** compreendem, dentre outros, os seguintes:

SEGMENTO	RISCOS
Dados e Informação	Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição.
Pessoas	Omissão, erro, negligência, imprudência, imperícia,

	desídia, sabotagem, perda de conhecimento.
Rede	<i>Hacker</i> , acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço.
<i>Hardware</i>	Indisponibilidade, interceptação (furto ou roubo) ou falha.
<i>Software</i> e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento ou falha.
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, <i>hardware</i> criptográfico, algoritmos (desenvolvimento e utilização) ou material criptográfico.

## 12.4. CONSIDERAÇÕES GERAIS

**12.4.1.** Os riscos que não podem ser eliminados têm seus controles documentados e são levados ao conhecimento da AC Raiz.

**12.4.2.** Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das consequências do risco (impacto da perda).

**12.4.3.** É necessária a participação e o envolvimento da alta administração da AC SIC BRASIL.

## 12.5. IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS

O gerenciamento de riscos na AC SIC BRASIL é conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

## 13. PLANO DE CONTINUIDADE DO NEGÓCIO

### 13.1. DEFINIÇÃO

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos da AC SIC BRASIL, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

### 13.2. DIRETRIZES GERAIS

**13.2.1.** Sistemas e dispositivos redundantes estão disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

**13.2.2.** A AC **SIC BRASIL** apresenta um PCN e, ainda, um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres, que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

- As condições para ativar o plano;
- Procedimentos de emergência;
- Procedimentos de *fallback*;
- Procedimentos de restauração;
- Cronograma para manutenção do plano;
- Requisitos de conscientização e educação;
- Responsabilidades individuais;
- Objetivo de Tempo de Recuperação (RTO);
- Testes regulares dos planos de contingência;
- O plano para manter ou restaurar as operações de negócios da AC de forma oportuna, após a interrupção ou falha de processos críticos de negócios;
- Definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;
- Definição de interrupções aceitáveis do sistema e um tempo de recuperação;
- Frequência para realização de cópias de backup;
- Distância entre as instalações de recuperação e o site principal da AC; e
- Procedimentos para proteger suas instalações após um desastre e antes de restaurar o ambiente seguro no local original ou remoto.

No tratamento constante nos Planos acima deve ser considerado:

- comprometimento da chave privada das entidades;
- invasão do sistema e da rede interna da entidade;
- incidentes de segurança física e lógica;
- indisponibilidade da Infraestrutura;
- fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e
- no gerenciamento de certificados;
- comprometimento de controle de segurança em qualquer evento referenciado no PCN;
- notificação à comunidade de usuários, se for o caso;
- revogação dos certificados afetados, se for o caso;
- procedimentos para interrupção ou suspensão de serviços e investigação;

- análise e monitoramento de trilhas de auditoria; e
- com o público e com meios de comunicação, se for o caso.

**13.2.3.** Todo pessoal envolvido com o Plano de Continuidade do Negócio recebe um treinamento específico para poder enfrentar estes incidentes.

**13.2.4.** A AC **SIC BRASIL** possui um plano de ação de resposta a incidentes. Este plano prevê o tratamento adequado dos seguintes eventos:

- Comprometimento de controle de segurança em qualquer evento referenciado no Plano de Continuidade do Negócio;
- Notificação à comunidade de usuários, se for o caso;
- Revogação dos certificados afetados, se for o caso;
- Procedimentos para interrupção ou suspensão de serviços e investigação;
- Análise e monitoramento de trilhas de auditoria; e
- Relacionamento com o público e com meios de comunicação, se for o caso.

## 14. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

<i>REF.</i>	<i>NOME DO DOCUMENTOS</i>	<i>CÓDIGO</i>
[1]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09