



**POLÍTICA DE SEGURANÇA**

**DA**

**AUTORIDADE CERTIFICADORA**

**DE DEFESA**

**(PS - AC DEFESA)**

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

## Sumário

<b>CONTROLE DE ALTERAÇÕES</b>	<b>4</b>
<b>TABELA DE SIGLAS E ACRÔNIMOS</b>	<b>5</b>
<b>1 INTRODUÇÃO</b>	<b>6</b>
<b>2 OBJETIVOS</b>	<b>6</b>
<b>3 ABRANGÊNCIA</b>	<b>6</b>
<b>4 TERMINOLOGIA</b>	<b>6</b>
<b>5 CONCEITOS DE DEFINIÇÕES</b>	<b>6</b>
<b>6 REGRAS GERAIS</b>	<b>7</b>
6.1 GESTÃO DE SEGURANÇA . . . . .	7
6.2 GERENCIAMENTO DE RISCOS . . . . .	8
6.3 INVENTÁRIO DE ATIVOS . . . . .	8
6.4 PLANO DE CONTINUIDADE DO NEGÓCIO . . . . .	9
<b>7 REQUISITOS DE SEGURANÇA DE PESSOAL</b>	<b>9</b>
7.1 DEFINIÇÃO . . . . .	9
7.2 OBJETIVOS . . . . .	9
7.3 DIRETRIZES . . . . .	9
7.3.1 O Processo de Admissão . . . . .	9
7.3.2 As Atribuições da Função . . . . .	10
7.3.3 Levantamento de Dados Pessoais . . . . .	10
7.3.4 A Entrevista de Admissão . . . . .	10
7.3.5 O Desempenho da Função . . . . .	11
7.3.6 A Credencial de Segurança . . . . .	11
7.3.7 Treinamento em Segurança da Informação . . . . .	11
7.3.8 Acompanhamento no Desempenho da Função . . . . .	11
7.3.9 O Processo de Desligamento . . . . .	12
7.3.10 O Processo de Liberação . . . . .	12
7.3.11 A Entrevista de Desligamento . . . . .	12
7.4 DEVERES E RESPONSABILIDADES . . . . .	12
7.4.1 Deveres dos integrantes ou servidores . . . . .	12
7.4.2 Responsabilidades das chefias . . . . .	13



7.4.3	Responsabilidades gerais . . . . .	13
7.4.4	Responsabilidades da Gerência de Segurança . . . . .	14
7.4.5	Responsabilidades dos prestadores de serviço . . . . .	14
7.5	SANÇÕES . . . . .	14
<b>8</b>	<b>REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO</b>	<b>15</b>
8.1	DEFINIÇÃO . . . . .	15
8.2	DIRETRIZES GERAIS . . . . .	15
<b>9</b>	<b>REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO</b>	<b>16</b>
9.1	DEFINIÇÃO . . . . .	16
9.2	DIRETRIZES GERAIS . . . . .	16
9.3	DIRETRIZES ESPECÍFICAS . . . . .	17
9.3.1	Sistemas . . . . .	17
9.3.2	Máquinas servidoras . . . . .	17
9.3.3	Redes da AC DEFESA . . . . .	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
<b>10</b>	<b>REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS</b>	<b>23</b>
10.1	REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA ICP- BRASIL . . . . .	23
10.2	CHAVES CRIPTOGRÁFICAS . . . . .	23
10.3	TRANSPORTE DAS INFORMAÇÕES . . . . .	24
<b>11</b>	<b>AUDITORIA E FISCALIZAÇÃO</b>	<b>24</b>
<b>12</b>	<b>GERENCIAMENTO DE RISCOS</b>	<b>25</b>
12.1	DEFINIÇÃO . . . . .	25
12.2	FASES PRINCIPAIS . . . . .	25
12.3	RISCOS RELACIONADOS ÀS ENTIDADES INTEGRANTES DA ICP- BRASIL . . . . .	26
12.4	CONSIDERAÇÕES GERAIS . . . . .	26
12.5	IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS . . . . .	26
<b>13</b>	<b>PLANO DE CONTINUIDADE DO NEGÓCIO</b>	<b>26</b>
13.1	DEFINIÇÃO . . . . .	26
13.2	DIRETRIZES GERAIS . . . . .	27
<b>14</b>	<b>DOCUMENTOS REFERENCIADOS</b>	<b>28</b>

## CONTROLE DE ALTERAÇÕES

Versão	Data	Motivo	Descrição da Alteração
1.0	23/06/2016	Versão Inicial	Versão inicial, de acordo com o DOC-ICP-02 - V.3.0
2.0	12/06/2023	Atualização	Atualizado de acordo com o DOC-ICP-02 - V.4.0

## TABELA DE SIGLAS E ACRÔNIMOS

<b>SIGLA</b>	<b>DESCRIÇÃO</b>
ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
CG ICP-BRASIL	Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira
CFTV	Circuito Fechado de Televisão
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Pública Brasileira
MD	Ministério da Defesa
PCN	Plano de Continuidade de Negócio
PS	Política de Segurança
TI	Tecnologia da Informação
VPN	Virtual Private Networks



## 1 INTRODUÇÃO

**1.1** Este documento tem por finalidade estabelecer as diretrizes de segurança adotadas pela Autoridade Certificadora de Defesa (AC DEFESA). Tais diretrizes fundamentam as normas e os procedimentos de segurança implementados pela AC DEFESA.

**1.2** Para cumprir a finalidade supracitada são estabelecidos os objetivos a seguir.

## 2 OBJETIVOS

**2.1** A Política de Segurança (PS) da AC DEFESA tem os seguintes objetivos específicos:

- a) definir o escopo da segurança da AC DEFESA;
- b) orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir 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

**3.1** A PS 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 DE DEFINIÇÕES

**5.1** Aplicam-se os conceitos abaixo no que se refere às PS da AC Defesa:

- a) **Ativo de Informação** - é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos da AC DEFESA;

- b) **Ativo de Processamento** - é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos da AC DEFESA, tanto os produzidos internamente quanto os adquiridos;
- c) **Controle de Acesso** - são restrições ao acesso aos dados e às informações de um sistema exercidas pela gerência de segurança da informação da AC DEFESA;
- d) **Custódia** - consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem concede o direito de facultar acesso a outros;
- e) **Direito de Acesso** - é o privilégio associado a um cargo, uma pessoa ou um processo para ter acesso a um ativo;
- f) **Ferramentas** - é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos pelos quais se aplica esta Política de Segurança;
- g) **Incidente de Segurança** - é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, à autenticidade, à confidencialidade ou à disponibilidade de qualquer ativo da AC DEFESA;
- h) **Política de Segurança** - é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação da AC DEFESA;
- 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 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 se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado em qualquer língua, dentre outras.

## 6 REGRAS GERAIS

### 6.1 GESTÃO DE SEGURANÇA

- 6.1.1 A PS da AC DEFESA aplica-se a todos os recursos humanos, administrativos e tecnológicos a ela relacionados. A abrangência dos recursos citados refere-se tanto àqueles ligados às entidades em caráter permanente quanto temporário.



- 6.1.2** Esta PS é comunicada a todo o pessoal envolvido e amplamente divulgada pela AC DEFESA, garantindo que todos tenham consciência dela e a pratiquem no âmbito da AC DEFESA.
- 6.1.3** Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado nesta PS.
- 6.1.4** Um programa de conscientização sobre segurança da informação é implementado por intermédio 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 DEFESA e suas entidades vinculadas. Especificamente, o pessoal envolvido ou que se relaciona com os usuários é informado sobre ataques típicos de engenharia social e como proceder e se proteger deles.
- 6.1.5** Os procedimentos são documentados e implementados para garantir que, quando o pessoal efetivo, contratado ou os prestadores de serviços sejam transferidos, re-manejados, promovidos, afastados ou demitidos, todos os privilégios de acesso aos sistemas, às informações e aos recursos sejam devidamente revistos, modificados ou revogados.
- 6.1.6** A AC DEFESA mantém mecanismo e repositório centralizado para manutenção de trilhas de auditoria, registros de eventos (*logs*) e demais notificações de incidentes. O responsável pela área de segurança deve ser acionado, assim que detectada qualquer tentativa de violação, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra ataques empreendidos contra esses mecanismo e repositório.
- 6.1.7** Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação (TI), estão em conformidade com esta PS.
- 6.1.8** É considerada proibida qualquer ação que não esteja explicitamente permitida na PS da AC DEFESA ou que não tenha sido previamente autorizada pelo responsável pela área de segurança da AC DEFESA.

## **6.2 GERENCIAMENTO DE RISCOS**

O processo de gerenciamento de riscos é revisto, no máximo a cada 12 (doze) meses, pela AC DEFESA, 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 DEFESA são inventariados, classificados, permanentemente atualizados pela própria entidade, e possuem gestor responsável formalmente designado.





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

- 6.4.1** Existe um Plano de Continuidade do Negócio - PCN implementado, o qual é testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.
- 6.4.2** A AC DEFESA possui, ainda, o Plano de Recuperação de Desastres e o Plano de Resposta a Incidentes, aprovados pela AC Raiz da ICP-Brasil.
- 6.4.3** O certificado da AC DEFESA será imediatamente revogado se um evento provocar a perda ou o comprometimento de sua chave privada ou de seu meio de armazenamento. Nesta situação, a AC DEFESA seguirá os procedimentos detalhados na sua Declaração de Práticas de Certificação (DPC).
- 6.4.4** Todos os incidentes serão reportados à AC Raiz imediatamente, a partir do momento em que for verificada sua ocorrência. Estes incidentes serão reportados de modo sigiloso às 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 e todos os empregados, necessário à proteção dos ativos da AC DEFESA.

### **7.2 OBJETIVOS**

- 7.2.1** Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso inapropriado dos ativos da AC DEFESA.
- 7.2.2** Prevenir e neutralizar as ações sobre as pessoas, que possam comprometer a segurança da AC DEFESA.
- 7.2.3** Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados à AC DEFESA, 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 DEFESA, 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, com o propósito de selecionar, para os quadros da AC DEFESA, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade da AC DEFESA.
- 7.3.1.2** A AC DEFESA não admitirá estagiários no exercício de atividades diretamente relacionadas aos processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.
- 7.3.1.3** O empregado, o funcionário ou o servidor assina um termo de compromisso, assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos da AC DEFESA.

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

As atribuições de cada função estão claramente relacionadas, de acordo com a característica das atividades desenvolvidas, a fim de determinar o perfil necessário do empregado ou servidor, 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 externo;
- e) as características de responsabilidade, decisão e iniciativa inerentes à função; e
- f) a qualificação técnica necessária ao desempenho da função.

### **7.3.3 Levantamento de Dados Pessoais**

É elaborada pesquisa do 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 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** É acompanhado e avaliado periodicamente o desempenho dos empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.
- 7.3.5.2** É dado aos integrantes, servidores ou prestadores de serviço da AC DEFESA 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 integrante, servidor ou prestador de serviço é identificado por intermédio de uma credencial, habilitando-o a ter acesso a informações sensíveis, de acordo com a classificação do grau de sigilo dessas informações e, conseqüentemente, com o grau de sigilo compatível ao cargo e à função desempenhada.
- 7.3.6.2** A Credencial de Segurança somente será concedida por autoridade competente, ou por ela delegada, e se fundamenta na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e da função.
- 7.3.6.3** O prazo de validade máximo de concessão a um indivíduo de uma credencial de segurança é de 1 (um) ano. Este prazo poderá ser prorrogado por igual período, quantas vezes forem necessárias, por ato da autoridade outorgante, enquanto exigir a necessidade do serviço.

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

Existe um processo pelo qual é apresentado aos integrantes da AC Defesa e aos prestadores de serviço esta PS e as normas e os procedimentos relativos ao trato de informações e dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

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

- 7.3.8.1** É realizado processo de avaliação de desempenho da função que documenta a observação do comportamento pessoal e funcional dos integrantes, servidores ou prestadores de serviço, sendo realizada por sua chefia imediata.
- 7.3.8.2** Constituem motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do integrante da AC DEFESA.
- 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 integrantes, servidores ou prestadores de serviço tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

### **7.3.9 O Processo de Desligamento**

**7.3.9.1** O acesso de ex-integrantes às instalações da AC DEFESA, quando necessário, é restrito às áreas de acesso público.

**7.3.9.2** Sua credencial, sua identificação, seu crachá, e seu acesso a equipamentos, mecanismos e acessos físicos e lógicos são revogados quando do seu desligamento.

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

O integrante ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a AC DEFESA, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias à veracidade das informações por ele prestadas.

### **7.3.11 A Entrevista de Desligamento**

Será realizada entrevista de desligamento para orientar o integrante ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência na AC DEFESA.

## **7.4 DEVERES E RESPONSABILIDADES**

### **7.4.1 Deveres dos integrantes ou servidores**

**7.4.1.1** São deveres dos integrantes ou servidores:

- a) preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos ativos de processamento e de informação;
- b) cumprir esta PS, sob pena de sofrer as sanções disciplinares e legais cabíveis;
- c) utilizar os Sistemas de Informações da AC DEFESA 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 DEFESA;
- f) não compartilhar, sob nenhuma forma, informações confidenciais com outros que não tenham a devida autorização de acesso e necessidade de conhecimento;
- g) responder por todo e qualquer acesso aos recursos da AC DEFESA, bem como pelos efeitos desses acessos efetivados por intermédio do seu código de identificação, ou outro atributo para esse fim utilizado;



- h) respeitar a proibição de não usar, inspecionar, copiar, armazenar programas de computador nem qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
- i) comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

#### **7.4.2 Responsabilidades das chefias**

##### **7.4.2.1 São responsabilidades das chefias:**

- a) gerenciar o cumprimento da PS, por parte de seus integrantes ou servidores;
- b) identificar os desvios praticados e adotar as medidas corretivas apropriadas;
- c) impedir o acesso de integrantes ou servidores demitidos ou demissionários, aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do integrante da AC DEFESA;
- d) proteger, em níveis físico e lógico, os ativos de informação e de processamento da AC DEFESA relacionados com a sua área de atuação;
- e) garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a informação e os ativos de informação da AC DEFESA;
- f) comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, quais os integrantes, servidores e prestadores de serviço, sob sua supervisão, podem acessar as informações da AC DEFESA;
- g) comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI quais os empregados, servidores e prestadores de serviço demitidos ou transferidos, para exclusão dos seus cadastros;
- h) comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

#### **7.4.3 Responsabilidades gerais**

##### **7.4.3.1 São responsabilidades gerais:**

- a) cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover a sua proteção de acordo com a política de classificação da informação da AC DEFESA;
- b) todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;
- c) todos os ativos de processamento das entidades devem estar relacionados no PCN.



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

##### **7.4.4.1 São responsabilidades da Gerência de Segurança:**

- a) estabelecer as regras de proteção dos ativos da AC DEFESA;
- b) decidir as medidas a serem tomadas no caso de violação das regras estabelecidas;
- c) revisar ao menos 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 PCN;
- f) executar as regras de proteção estabelecidas por esta PS;
- g) detectar, identificar, registrar e comunicar à AC Raiz as violações ou tentativas de acesso não autorizadas;
- h) definir e aplicar, para cada usuário de TI, restrições de acesso à rede, como horário autorizado, dias autorizados, entre outras;
- i) manter registros de atividades de usuários de TI (*logs*) por um período de tempo 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) excluir as contas inativas; e
- l) fornecer senhas de contas privilegiadas somente aos integrantes da AC DEFESA que necessitem efetivamente dos privilégios, mantendo-se os devidos registro e controle.

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

São previstas nos contratos cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta PS, 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 DEFESA.

### 8.2 DIRETRIZES GERAIS

- 8.2.1 As responsabilidades pela segurança física dos sistemas da AC DEFESA 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 DEFESA não são publicamente identificados.
- 8.2.3 Existem sistemas de segurança para acesso físico, 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 responsável 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 DEFESA. Ele toma as medidas apropriadas para prevenir acessos não autorizados.
- 8.2.7 Os sistemas da AC DEFESA estão localizados em área protegida (ambientes de nível 4) e afastada de fontes potentes de magnetismo ou interferência de rádio frequência.
- 8.2.8 Recursos e instalações críticas ou sensíveis são mantidos em área seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas são fisicamente protegidas de acesso não autorizado, dano ou interferência. A proteção fornecida é proporcional aos riscos identificados.
- 8.2.9 A entrada e a 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.
- 8.2.12** O inventário de todo o conjunto de ativos de processamento é registrado e mantido atualizado com periodicidade definida na DPC da AC DEFESA.
- 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 DEFESA todos utilizam crachá de identificação e devem informar à Gerência de Segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho desacompanhado.
- 8.2.15** Visitantes às instalações da AC DEFESA são supervisionados. 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 DEFESA 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 estão 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 aquele composto por todo o ativo de informações da AC DEFESA.

### **9.2 DIRETRIZES GERAIS**

- 9.2.1** A informação é protegida de acordo com o seu valor, sua sensibilidade e sua criticidade. Para tanto, a AC DEFESA possui um sistema de classificação da informação.
- 9.2.2** Os dados, as informações e os sistemas de informação da AC DEFESA 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. Os registros são protegidos e armazenados de acordo com a sua classificação.
- 9.2.4** Os sistemas e recursos que suportam funções críticas para operação da AC DEFESA asseguram a capacidade de recuperação nos prazos e condições definidos 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 em intervalos definidos na DPC da AC DEFESA.

## **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 disponíveis na AC DEFESA. 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.
- 9.3.1.3** Os arquivos de *logs* são criteriosamente definidos para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos. Os *logs* são periodicamente analisados, conforme definido na DPC, para identificar tendências, falhas ou usos indevidos. Os *logs* são 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 a suas precisão, consistência e integridade.
- 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 são adotadas.

### **9.3.2 Máquinas servidoras**

- 9.3.2.1** O acesso lógico ao ambiente ou aos serviços disponíveis em máquinas servidoras 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.



- 9.3.2.2** Os acessos lógicos são registrados em *logs*, que são analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas estão precisamente definidos.
- 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 e de outros arquivos críticos. Os eventos são armazenados em registros de eventos de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros.
- 9.3.2.4** As máquinas são sincronizadas para permitir o rastreamento de eventos.
- 9.3.2.5** Proteção lógica adicional (criptografia) é adotada, quando necessária, para evitar o acesso não autorizado às informações.
- 9.3.2.6** A versão do sistema operacional, assim como outros programas (*software*) básicos instalados em máquinas servidoras, são mantidos atualizados, em conformidade com as recomendações dos respectivos fabricantes.
- 9.3.2.7** São utilizados somente programas (*software*) autorizados pela AC DEFESA nos seus equipamentos. É realizado o controle de sua distribuição e de sua instalação.
- 9.3.2.8** O acesso remoto a máquinas servidoras é realizado adotando-se os mecanismos de segurança predefinidos para evitar ameaças à integridade e ao sigilo do serviço.
- 9.3.2.9** Os procedimentos de cópia de segurança (*backup*) e de recuperação são documentados, mantidos atualizados e regularmente testados, de modo a garantir a disponibilidade das informações.

### **9.3.3 Redes da AC DEFESA**

- 9.3.3.1** O tráfego de informações no ambiente de rede é protegido contra perdas e danos, bem como acesso, uso e 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.
- 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 nesses ativos em sua primeira ativação.



- 9.3.3.5** Serviços vulneráveis recebem nível de proteção adicional.
- 9.3.3.6** O uso de senhas é submetido a uma política específica para sua gerência e sua utilização.
- 9.3.3.7** O acesso lógico aos recursos da rede local é realizado por intermédio 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, é feita somente a partir de autorização formal e mediante supervisão.
- 9.3.3.9** A conexão com outros ambientes de rede e alterações internas em suas topologia e configuração são formalmente documentadas e mantidas, para permitir registro histórico, mediante 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 registros de eventos de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* são analisados periodicamente, com o menor intervalo possível.
- 9.3.3.11** São adotadas proteções físicas adicionais para os recursos de rede considerados críticos.
- 9.3.3.12** Proteção lógica adicional é adotada para evitar o acesso não autorizado às informações.
- 9.3.3.13** A infraestrutura de interligação lógica é protegida contra danos mecânicos e conexão não autorizada.
- 9.3.3.14** A alimentação elétrica para a rede local é separada da rede convencional, observando-se 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 à AC DEFESA são protegidas e não são enviadas para outras redes sem proteção adequada.
- 9.3.3.18** Todo serviço de rede não explicitamente autorizado 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 DEFESA.
- 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 máquinas servidoras, 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*) resulta 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 e 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 DEFESA e redes externas restringem-se somente àquelas que visem efetivar os processos.
- 9.3.3.26** As conexões de rede são ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, emprega-se controles de compensação, tais como o uso de (*proxies*) que são implementados para proteger os sistemas que executam a função de certificação contra possíveis ataques.
- 9.3.3.27** Sistemas que executam a função de certificação são isolados, para minimizar a exposição contra tentativas de comprometimento de sigilo, integridade e disponibilidade das funções de certificação.
- 9.3.3.28** A chave privada de certificação da AC DEFESA é protegida contra acesso desautorizado, para garantir seu sigilo e sua integridade.
- 9.3.3.29** A segurança das comunicações intra-rede e inter-rede entre os sistemas da AC DEFESA é garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas.
- 9.3.3.30** As ferramentas de detecção de intrusão são implantadas para monitorar as redes críticas, alertando 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 DEFESA são identificados e autenticados.
- 9.3.4.2** O sistema de controle de acesso mantém as habilitações atualizadas e registros que permitam contabilização do uso, auditoria e recuperação nas situações de falha.
- 9.3.4.3** Nenhum usuário tem permissão de obter os direitos de acesso de outro usuário.
- 9.3.4.4** O mecanismo que especifica os direitos de acesso de cada usuário ou aplicação é protegido contra modificações não autorizadas.
- 9.3.4.5** O arquivo de senhas é cifrado e seu acesso é 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 de forma adequada: conjunto de caracteres permitidos, tamanhos mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas, quando necessárias.
- 9.3.4.10** A distribuição de senhas aos usuários de TI (inicial ou não) 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 somente é executada após a identificação positiva do usuário. A senha digitada não é exibida.
- 9.3.4.12** São adotados critérios para bloquear ou desativar usuários de acordo com período predefinido sem acesso e tentativas sucessivas de acesso mal sucedidas.
- 9.3.4.13** O sistema de controle de acesso solicita nova autenticação após tempo de inatividade da sessão (*timeout*) adequado a cada aplicação.
- 9.3.4.14** O sistema de controle de acesso exibe, na tela inicial, mensagem informando que o serviço só pode ser acessado 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 e configurado para auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, a auditoria e a recuperação nas situações de falhas. Os *logs* são 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 protegidas contra danos ou perdas, bem como acesso, uso ou exposição indevidos.
- 9.3.5.2** Equipamentos que executam operações sensíveis recebem proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou seus componentes).
- 9.3.5.3** São adotadas medidas de segurança lógica referentes a combate a códigos maliciosos, *backup*, controle de acesso e uso de *software* não autorizado.
- 9.3.5.4** As informações armazenadas em meios eletrônicos são protegidas contra danos, furto ou roubo, devendo ser adotados procedimentos de *backup*, definidos em documento específico.
- 9.3.5.5** Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à AC DEFESA são utilizadas somente em equipamentos da AC DEFESA, onde foram geradas, ou naqueles por ela autorizados, com controles adequados.
- 9.3.5.6** O acesso às informações atende aos requisitos de segurança, considerando o ambiente e a forma de uso do equipamento (uso pessoal ou coletivo).
- 9.3.5.7** Os usuários de TI utilizam apenas *softwares* licenciados pelos fabricantes, nos equipamentos da AC DEFESA, observadas as normas da ICP-Brasil e legislação de *software*.
- 9.3.5.8** A AC DEFESA 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 autorizados.
- 9.3.5.10** O inventário dos recursos é mantido atualizado.
- 9.3.5.11** Os sistemas em uso solicitam nova autenticação após tempo de inatividade da sessão (*timeout*) adequado a cada aplicação.



**9.3.5.12** Toda e qualquer mídia deve ser eliminada de maneira segura, quando não mais for necessária. Procedimentos formais para a eliminação segura de mídia devem ser definidos, para minimizar os riscos.

### **9.3.6 Combate a vírus de computador**

Os procedimentos de combate a processos destrutivos (vírus, cavalos de troia e *worms*) são sistematizados e abrangem 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 DEFESA 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 destas.

**10.1.2** Toda a documentação referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados pela AC DEFESA 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 DEFESA 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 execução de processos que envolvam as chaves criptográficas utilizadas nos sistemas criptográficos da AC DEFESA 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 pela chefia competente, conforme as funções a serem desempenhadas e o correspondente grau de privilégio, assim como têm suas responsabilidades explicitamente definidas.
- 10.2.3** Os algoritmos de criação e de troca das chaves criptográficas utilizadas no sistema criptográfico da AC DEFESA são aprovados pelo CG ICP-Brasil.
- 10.2.4** Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da AC DEFESA estão explicitados nas Políticas de Certificado (PC) da AC DEFESA.

### **10.3 TRANSPORTE DAS INFORMAÇÕES**

- 10.3.1** O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da AC DEFESA têm a integridade, a autenticidade e o sigilo assegurados, por intermédio 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 intermédio de redes públicas, entre as redes da AC DEFESA.

## **11 AUDITORIA E FISCALIZAÇÃO**

**11.1** As atividades da AC DEFESA estão associadas ao conceito de confiança. Os processos de auditoria e fiscalização representam instrumentos que facilitam a percepção e a transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade da AC DEFESA 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 DEFESA, 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 DEFESA, pela AC Raiz ou por terceiros por ela 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, da frequência e da abrangência das auditorias, da identidade e da qualificação do auditor e dos demais temas correlacionados.





**11.4** Além de auditada, a AC DEFESA 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**

**12.1.1** Processo que visa à proteção dos serviços da AC DEFESA, por intermédio de aceitação, redução ou transferência dos riscos, conforme suas viabilidades econômica e estratégica. Os seguintes pontos principais são identificados:

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

### **12.2 FASES PRINCIPAIS**

**12.2.1** O gerenciamento de riscos consiste das seguintes fases principais:

- a) identificação dos recursos a serem protegidos: *hardware*, rede, *software*, dados, informações pessoais, documentação, suprimentos;
- b) identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismo, erros ou negligência) ou de qualquer outro tipo (incêndios);
- c) análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;
- d) 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;
- e) 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;
- f) monitoramento da eficácia dos controles adotados para minimizar os riscos identificados; e
- g) reavaliação periódica dos riscos em intervalos de tempo não superiores a 1 (um) ano.

## 12.3 RISCOS RELACIONADOS ÀS ENTIDADES INTEGRANTES DA ICP-BRASIL

Os riscos avaliados para a AC DEFESA 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), falha
<i>Software</i> e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento, falha
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, <i>hardware</i> criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico

## 12.4 CONSIDERAÇÕES GERAIS

**12.4.1** Os riscos que não atendam aos critérios mínimos de aceitação, após seu tratamento, têm seus controles documentados e são levados ao conhecimento da AC Raiz.

**12.4.1.1** Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo de suas consequências (impacto).

**12.4.1.2** É necessária a participação e o envolvimento da alta administração do Ministério da Defesa (MD) e das Forças Armadas para que o gerenciamento de riscos obtenha plena efetividade.

## 12.5 IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS

O gerenciamento de riscos da AC DEFESA pode ser conduzido de acordo com métodos padronizados ou proprietários, 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 DEFESA, 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 DEFESA, integrante da ICP-Brasil, possui um PCN e, ainda, um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres, que estabelece o tratamento adequado dos seguintes eventos de segurança:

- a) as condições para ativar o plano;
- b) procedimentos de emergência;
- c) procedimentos de *fallback*;
- d) procedimentos de restauração;
- e) cronograma para manutenção do plano;
- f) requisitos de conscientização e educação;
- g) responsabilidades individuais;
- h) objetivo de Tempo de Recuperação (RTO);
- i) testes regulares dos planos de contingência;
- j) plano para manter ou restaurar as operações de negócios da AC DEFESA de forma oportuna, após a interrupção ou falha de processos críticos de negócios;
- k) definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;
  - l) definição de interrupções aceitáveis do sistema e um tempo de recuperação;
- m) frequência para realização de cópias de *backup*;
- n) distância entre as instalações de recuperação (contingência) e o site principal da AC DEFESA; e
- o) procedimentos para proteger suas instalações após um desastre e antes de restaurar o ambiente seguro no local original ou remoto.

**13.2.2.1** No tratamento constante dos Planos acima, deve ser considerado:

- a) comprometimento da chave privada da AC DEFESA;
- b) invasão do sistema e da rede interna da AC DEFESA;
- c) incidente de segurança física e lógica;

- d) indisponibilidade da infraestrutura;
- e) fraudes ocorridas no registro do usuário, na emissão, na expedição, na distribuição, na revogação e no gerenciamento de certificados;
- f) comprometimento de controle de segurança em qualquer evento referenciado no PCN;
- g) notificação à comunidade de usuários, se for o caso;
- h) revogação dos certificados afetados, se for o caso;
- i) procedimentos para interrupção ou suspensão de serviços e investigação;
- j) análise e monitoramento de trilhas de auditoria; e
- k) relacionamento com o público e com meios de comunicação, se for o caso.

**13.2.3** Todo pessoal envolvido com o PCN recebe um treinamento específico para enfrentar estes incidentes.

## 14 DOCUMENTOS REFERENCIADOS

**14.1** Os documentos abaixo relacionados 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.

Ref.	Nome do documento	Código
[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