RESOLUÇÃO N° 39, DE 18 DE ABRIL DE 2006.

Aprova a versão 2.0 da Política de Segurança da ICP-Brasil.

O COORDENADOR DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL, no uso das competências previstas nos incisos I, III, V e VI do art. 4° da Medida Provisória N° 2.200-2, de 24 de agosto de 2001.

RESOLVE:

Art. 1º Aprovar a versão 2.0 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL (DOC-ICP-02), em anexo.

Parágrafo único. A Política de Segurança da ICP-Brasil poderá ser revista e atualizada a qualquer tempo, caso se mostre necessário.

Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICP-Brasil nº 02, de 25 de setembro de 2001, nº 27, de 24 de outubro de 2003 e nº 32, de 21 de outubro de 2004 e convalidados os atos praticados durante suas vigências.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

ENYLSON FLÁVIO MARTINEZ CAMOLESI

ANEXO

POLÍTICA DE SEGURANÇA DA ICP-BRASIL
DOC-ICP-02 - Versão 2.0

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
DPC - Declaração de Práticas de Certificação
ICP-**Brasil** - Infra-Estrutura 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 deverão ser adotadas pelas entidades participantes da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil. Tais diretrizes fundamentarão as normas e procedimentos de segurança a serem elaborados e implementados por parte de cada entidade, considerando as suas particularidades.

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

2. OBJETIVOS

A Política de Segurança - PS da ICP-Brasil tem os seguintes objetivos específicos:

a) Definir o escopo da segurança das entidades;

b) Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades, para reduzir riscos e garantir a integridade, sigilo e 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 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 E DEFINIÇÕES

Aplicam-se os conceitos abaixo no que se refere à PS 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;

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, tanto os produzidos internamente quanto os adquiridos;

c) Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

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 PS da Informação das entidades;

g) Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo 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 das entidades;

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 – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

k) Senha Fraca ou Óbvia – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências 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 PS da ICP-Brasil se aplica a todos os recursos humanos, administrativos e tecnológicos pertencentes às entidades que a compõem. A abrangência dos recursos citados refere-se tanto àqueles ligados às entidades em caráter permanente quanto temporário.

6.1.2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada através das entidades, garantindo que todos tenham consciência da mesma e a pratiquem na organização.

6.1.3. Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.

6.1.4. Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles .

6.1.5. Os procedimentos deverão ser 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. Previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, *logs* e demais notificações de incidentes. Este mecanismo deverá ser incluído nas medidas a serem tomadas por um grupo encarregado de responder a este tipo de ataque, para prover uma defesa ativa e corretiva contra os mesmos.

6.1.7. Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, devem estar em conformidade com esta PS.

6.1.8. No que se refere a segurança da informação, deve-se considerar proibido, tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança da entidade pertencente à ICP-Brasil.

6.2. Gerenciamento de Riscos

O processo de gerenciamento de riscos deve ser revisto, no máximo a cada 18 (dezoito) meses, pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados

6.3. Inventário de ativos

Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado

6.4. Plano de Continuidade do Negócio

6.4.1. Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.

6.4.2. Todas as AC deverão apresentar planos de gerenciamento de incidentes e de ação de resposta a incidentes a serem aprovados pela AC Raiz ou AC de nível imediatamente superior;.

6.4.3. O certificado da AC deverá ser imediatamente revogado se um evento provocar a perda ou comprometimento de sua chave privada ou do seu meio de armazenamento. Nesta situação, a entidade deverá seguir os procedimentos detalhados na sua DPC.

6.4.4. Todos os incidentes deverão ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser 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 e todos os empregados, necessário à proteção dos ativos das entidades participantes da ICP-Brasil.

7.2. Objetivos

7.2.1. Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos das entidades participantes da ICP-Brasil.

7.2.2. Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança das entidades participantes da ICP-Brasil.

7.2.3. Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados às entidades participantes da ICP-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 nas entidades participantes da ICP-Brasil, mesmo em caso de funções desempenhadas por prestadores de serviço.

7.3. Diretrizes

7.3.1 O Processo de Admissão

7.3.1.1. Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.

7.3.1.2. Nenhuma entidade participante da ICP-Brasil 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 servidor assinará termo de compromisso assumindo 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

Relacionar claramente as atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se 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/ou externo;

e) as características de responsabilidade, decisão e iniciativa inerentes à função;

f) a qualificação técnica necessária ao desempenho da função.

7.3.3 O Levantamento de Dados Pessoais

Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil.

7.3.4 A Entrevista de Admissão

7.3.4.1. Deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.

7.3.4.2. Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.

7.3.5 O Desempenho da Função

7.3.5.1. Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.

7.3.5.2. Dar aos empregados ou servidores das entidades 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. Identificar o empregado por meio de uma credencial, habilitando-o a ter acesso a 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 a função a ser desempenhada.

7.3.6.2. A Credencial de Segurança somente será concedida por autoridade competente, ou por ela delegada, e se fundamentará 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. Será 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 for necessário, por ato da Autoridade Outorgante, enquanto exigir a necessidade do serviço.

7.3.7. Treinamento em Segurança da Informação

Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as normas e procedimentos relativos ao trato de informações e/ou 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 Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.

7.3.8.2 Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.

7.3.8.3 Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.

7.3.8.4 As chefias imediatas assegurarão que todos os empregados ou servidores 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-empregados às instalações, quando necessário, será restrito às áreas de acesso público.

7.3.9.2. Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.

7.3.10. O Processo de Liberação

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

7.3.11. A Entrevista de Desligamento

Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.

7.4. Deveres e Responsabilidades

7.4.1. Deveres dos empregados ou servidores

São deveres dos empregados ou servidores:

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 PS, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

c) utilizar os Sistemas de Informações das entidades 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 das entidades;

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 das entidades 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 ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

7.4.2. Responsabilidade das chefias

São responsabilidades das chefias:

a) gerenciar o cumprimento da PS, por parte de seus empregados ou servidores;

b) identificar os desvios praticados e adotar as medidas corretivas apropriadas;

c) impedir o acesso de empregados demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do empregado;

d) proteger, em nível físico e lógico, os ativos de informação e de processamento das entidades participantes da ICP-Brasil relacionados com sua área de atuação;

e) garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação das entidades;

f) comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, quais os empregados, servidores e prestadores de serviço, sob sua supervisão, que podem acessar as informações das entidades;

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 no cadastro dos usuários;

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

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 entidade;

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

São responsabilidades das Gerências de Segurança:

a) estabelecer as regras de proteção dos ativos das entidades participantes da ICP-Brasil;

b) decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;

c) revisar pelo 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 pela 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 Tecnologia da Informação - 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 superior a 6 (seis) 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;

l) fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.

7.4.5. Responsabilidades dos Prestadores de Serviço

Devem ser previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta PS 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 das entidades integrantes da ICP-Brasil.

8.2. Diretrizes Gerais

8.2.1. As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.

8.2.2. A localização das instalações e o sistema de certificação da AC Raiz e das AC não deverão ser publicamente identificados.

8.2.3. Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.

8.2.4. Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida.

8.2.5. Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

8.2.6. Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas ao responsável pela gerência de segurança da entidade. Ele deverá tomar as medidas apropriadas para prevenir acessos não autorizados.

8.2.7. Os sistemas de AC deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência.

8.2.8. Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.

8.2.9. A entrada e saída, nestas áreas ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.

8.2.10. O acesso aos componentes da infra-estrutura, atividade fundamental ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, deverá ser restrito ao pessoal autorizado.

8.2.11. Sistemas de detecção de intrusão deverão ser utilizados 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 deve ser registrado e mantido atualizado, no mínimo, mensalmente.

8.2.13. Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só devem ser utilizados a partir de autorização formal e mediante supervisão.

8.2.14. Nas instalações das entidades integrantes da ICP-Brasil, todos deverão utilizar alguma forma visível de identificação (por exemplo: crachá), e devem informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

8.2.15. Visitantes das áreas de segurança devem ser supervisionados. Suas horas de entrada e saída e o local de destino devem ser registrados. Essas pessoas devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada.

8.2.16. Os ambientes onde ocorrem os processos críticos das entidades integrantes da ICP-Brasil deverão ser 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 devem ser instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

1

9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

9.1. Definição

Ambiente lógico é composto por todo o ativo de informações das entidades.

9.2. Diretrizes gerais

9.2.1. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.

9.2.2. Os dados, as informações e os sistemas de informação das entidades e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

9.2.3. As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria. Os registros devem ser protegidos e armazenados de acordo com a sua classificação.

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

9.2.5. O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.

9.3. Diretrizes específicas

9.3.1. Sistemas

9.3.1.1. As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada e mantida atualizada.

9.3.1.2. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

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

9.3.1.4. Devem ser estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto a sua precisão, consistência e integridade.

9.3.1.5. Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente

devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.

9.3.2. Máquinas servidoras

9.3.2.1. O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

9.3.2.2. Os acessos lógicos devem ser registrados em *logs*, que devem ser analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas devem estar precisamente definidos.

9.3.2.3. Devem ser 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 devem ser armazenados em relatórios 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 devem estar sincronizadas para permitir o rastreamento de eventos.

9.3.2.5. Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não-autorizado às informações.

9.3.2.6. A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.

9.3.2.7. Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.

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

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

9.3.3. Redes das entidades da ICP-Brasil

9.3.3.1. O tráfego das informações no ambiente de rede deve ser 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 devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

9.3.3.3. Devem ser 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 deve ser 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 devem receber nível de proteção adicional.

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

9.3.3.7. O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser 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 devem ser utilizado à 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 devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.

9.3.3.10. Devem ser definidos relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* devem ser analisados periodicamente e o período de análise estabelecido deve ser o menor possível.

9.3.3.11. Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

9.3.3.12. Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações.

9.3.3.13. A infra-estrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.

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

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

9.3.3.16. Devem ser 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 às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.

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

9.3.3.19. Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.

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

9.3.3.21. Deve ser 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, deverão fazer uso de tal controle.

9.3.3.23. A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: requisitos de segurança definidos pelo serviço, objetivo do serviço, público alvo, classificação da informação, forma de acesso, freqüência de atualização do conteúdo, forma de administração do serviço e volume de tráfego.

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

9.3.3.25. Conexões entre as redes das entidades da ICP-Brasil e redes externas deverão estar restritas somente àquelas que visem efetivar os processos.

9.3.3.26. As conexões de rede devem ser ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, deve-se empregar controles de compensação, tais como o uso de *proxies* que deverão ser 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 deverão estar isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação.

9.3.3.28. A chave de certificação das AC deverá estar 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 das entidades da ICP-Brasil, deverá ser garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas.

9.3.3.30. As ferramentas de detecção de intrusos devem ser 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 das entidades da ICP-Brasil devem ser identificados e autenticados.

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

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

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

9.3.4.5. O arquivo de senhas deve ser criptografado e ter o acesso controlado.

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

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

9.3.4.9. As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas.

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

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

9.3.4.12. Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas.

9.3.4.13. O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).

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

9.3.4.15. O registro das atividades (*logs*) do sistema de controle de acesso deve ser 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 devem ser 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 devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

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

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

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

9.3.5.5. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da ICP-Brasil, só devem ser utilizadas em equipamentos das entidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados.

9.3.5.6. O acesso às informações deve atender 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 devem utilizar apenas *softwares* licenciados pelo fabricante nos equipamentos das entidades, observadas as normas da ICP-Brasil e legislação de *software.*

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

9.3.5.9. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado.

9.3.5.10. O inventário dos recursos deve ser mantido atualizado.

9.3.5.11. Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.5.12. As mídias devem ser eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias devem ser 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*) devem estar sistematizados e devem abranger 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 ICP-Brasil deve ser 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 a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados na ICP-Brasil, deve ser 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 infra-estrutura.

10.1.4. Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.

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

10.2. Chaves criptográficas

10.2.1. Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.

10.2.2. As pessoas, a que se refere o item anterior, deverão ser formalmente designadas pela chefia competente, conforme as funções a serem desempenhadas e o correspondente grau de privilégios, assim como terem suas responsabilidades explicitamente definidas.

10.2.3. Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.

10.2.4. Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da

ICP-Brasil devem estar explicitados nas políticas de certificado específicas.

10.3. Transporte das Informações

10.3.1. O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICP-Brasil devem ter a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

10.3.2. Deve-se adotar 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.

2

11. AUDITORIA E FISCALIZAÇÃO

11.1. As atividades das entidades integrantes da ICP-Brasil estão associadas ao conceito de confiança. Os processos de auditoria e fiscalização representam instrumentos que facilitam a percepção e transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade das entidades integrantes 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 das entidades na ICP-Brasil, da mesma forma que o resultado das auditorias operacionais e fiscalizações é item fundamental para a manutenção da condição de credenciada.

11.3. Deverão ser realizadas auditorias periódicas nas entidades integrantes da ICP-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, freqüência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

11.4. Além de auditadas, as entidades integrantes da ICP-Brasil podem ser fiscalizadas 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].

1

12. GERENCIAMENTO DE RISCOS

12.1. Definição

Processo que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser 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

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, vandalismos, erros ou negligências) 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) monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

g) reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses;

12.3. Riscos relacionados às entidades integrantes da ICP-Brasil

Os riscos a serem avaliados para as entidades integrantes da ICP-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	*Hacker*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço
Hardware	Indisponibilidade, interceptação (furto ou roubo), falha
Software e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento, falha
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, *hardware* criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico.

12.4. Considerações Gerais

12.4.1. Os riscos que não puderem ser eliminados devem ter seus controles documentados e devem ser 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 conseqüências do risco (impacto da perda).

12.4.3. É necessária a participação e o envolvimento da alta administração das entidades.

12.5. Implementação do Gerenciamento de Riscos

O gerenciamento de riscos nas entidades da ICP-Brasil pode ser 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 das entidades integrantes da ICP-Brasil, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

13.2. Diretrizes Gerais

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

13.2.2. Todas as AC integrantes da ICP-Brasil deverão apresentar um PCN que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

a) comprometimento da chave privada das entidades;

b) invasão do sistema e da rede interna da entidade;

c) incidentes de segurança física e lógica;

d) indisponibilidade da Infra-estrutura; e

e) fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados.

13.2.3. Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.

13.2.4. Um plano de ação de resposta a incidentes deverá ser estabelecido para todas as AC integrantes da ICP-Brasil. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:

a) comprometimento de controle de segurança em qualquer evento referenciado no PCN;

b) notificação à comunidade de usuários, se for o caso;

c) revogação dos certificados afetados, se for o caso;

d) procedimentos para interrupção ou suspensão de serviços e investigação;

e) análise e monitoramento de trilhas de auditoria; e

f) relacionamento com o público e com meios de comunicação, se for o caso.

114. 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.

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