Presidência da República
Casa Civil da Presidência da República

PARTE III

POLÍTICA DE SEGURANÇA DA ICP-BRASIL

19 DE JUNHO DE 2001

1- INTRODUÇÃO

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, ou seja, Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras integrantes (AC), Autoridades de Registro (AR) e Repositórios. É composto por fundamentos que darão origem a normas e procedimentos de segurança, considerando as particularidades de cada entidade.

O detalhamento das Políticas de Segurança da Informação específicas de cada entidade participante da ICP-Brasil é de responsabilidade do Comitê Gestor da ICP-Brasil (CG ICP-Brasil).

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

2- OBJETIVOS

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

2.1.1- Definir o escopo da segurança das entidades;

2.1.2- Orientar, por meio de suas diretrizes todas as ações de segurança das entidades, para reduzir riscos e garantir a integridade, autenticidade, irretratabilidade, sigilo e disponibilidade das informações, dos sistemas de informação e recursos;

2.1.3- Permitir a adoção de soluções de segurança integradas;

2.1.4- Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3- ABRANGÊNCIA

3.1- A Política de Segurança abrange os seguintes aspectos:

3.1.1- Requisitos de Segurança Humana;

3.1.2- Requisitos de Segurança Física;

3.1.3- Requisitos de Segurança Lógica;

3.1.4- Requisitos de Segurança dos Recursos Criptográficos.

4- TERMINOLOGIA

4.1- A terminologia usada nestas regras e diretrizes de segurança devem ser interpretadas da seguinte forma:

4.1.1- Deve-se - Quando usado este termo, é estabelecido um requerimento mandatório, ou seja, é obrigatório atender ao que é determinado;

4.1.2- Recomenda-se - Quando usado este termo, é estabelecido um requerimento não mandatório.

4.1.3- Sugere-se - Quando usado este termo, é estabelecido um requerimento opcional.

5- CONCEITOS E DEFINIÇÕES

5.1- Conceitos

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

5.1.1.1- **Ativo de Informação** – é o patrimônio composto por todos os dados e informações gerados e manipulados durante a execução dos sistemas e processos das entidades;

5.1.1.2- **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.

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

5.1.1.4- **Custódia** – define-se a como a 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;

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

5.1.1.6- **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades;

5.1.1.7- **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

5.1.1.8- **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;

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

6- REGRAS E DIRETRIZES GERAIS

6.1- Gestão de Segurança

6.1.1- A Política de Segurança Geral 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 aqueles ligados as 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 para garantir que todas as pessoas 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 política de segurança;

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. Especificamente, o pessoal envolvido ou que realiza a interface com os usuários deve estar informado sobre ataques típicos de engenharia social 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 revistos, modificados ou revogados de acordo;

6.1.6- Um mecanismo ou procedimento deverá ser estabelecido para ativar e manter trilhas ou logs de segurança sobre vulnerabilidades e ataques reportados por fontes confiáveis e desenvolvidas medidas de controle e correção imediatas. Este mecanismo ou procedimento 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- A Política de Segurança Geral ICP-Brasil deverá ser considerada como subsídio essencial para confecção de processos de aquisição de bens e serviços de Tecnologia da Informação - TI;

6.1.8- A Política de Segurança Geral ICP-Brasil deve ser revisada e atualizada periodicamente pelo CG ICP-Brasil , ou no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

6.2- Gerenciamento de Riscos

6.2.1- Os recursos da infra-estrutura das entidades (tais como algoritmos de criptografia e seus parâmetros chave, segurança física, sistemas de segurança, sistemas de operação etc.), devem ser revistos anualmente

pela AC Raiz, para prevenção contra riscos advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados;

6.2.2- Deverão ser realizadas auditorias periódicas gerenciadas pela AC Raiz ou credenciados;

6.3- Plano de Continuidade de Negócio

6.3.1- Um plano de continuidade do negócio deve ser implementado e testado periodicamente, para garantir a continuidade dos serviços críticos, na ocorrência de um desastre ou falha dos sistemas de computação;

6.3.2- O pessoal da equipe de recuperação deve receber um treinamento adequado para poder enfrentar estes incidentes;

6.3.3- Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

6.3.4- Um plano de gerenciamento de incidentes deve ser desenvolvido e aprovado pela AC Raiz. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

6.3.4.1- Comprometimento da chave privada das entidades;

6.3.4.2- Invasão do sistema e da rede interna da entidade;

6.3.4.3- Vulnerabilidades na segurança física e lógica;

6.3.4.4- Indisponibilidade da Infra-estrutura; e

6.3.4.5- Fraudes ocorridas no registro do usuário, e emissão e revogação de certificados.

6.3.5- Um plano de ação de resposta a incidentes deverá ser estabelecido. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:

6.3.5.1- Comprometimento do controle de segurança de qualquer processo;

6.3.5.2- Notificação à comunidade de usuários (se aplicável);

6.3.5.3- Revogação dos certificados afetados (se aplicável);

6.3.5.4- Procedimentos para interrupção de serviços e investigação;

6.3.5.5- Análise e monitoramento de trilhas de auditoria; e

6.3.5.6- Relacionamento com o público e com a mídia (se aplicável).

6.3.6- 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, neste caso, todos os certificados assinados usando esta chave privada deverão ser revogados;

6.3.7- Todos os incidentes deverão ser reportados à AC Raiz no máximo em 24 (vinte e quatro) horas.

7- REQUISITOS DE SEGURANÇA DE PESSOAL

7.1- Definição:

7.1.1.1- Conjunto de medidas e procedimentos de segurança, a serem observados pelos contratados, terceirizados e todos os funcionários, necessárias à salvaguarda de dados e/ou conhecimentos sensíveis e classificados ao cumprimento da missão das entidades.

7.2- Objetivos:

7.2.1- Reduzir os riscos de erros humanos, roubo, fraude ou uso não apropriado das facilidades das entidades;

7.2.2- Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança das entidades;

7.2.3- Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados às entidades da ICP-Brasil, assim como o pessoal em desempenho de funções de apoio, tais como manutenção das instalações físicas, a adotarem medidas de proteção compatíveis com a natureza da função que desempenham ou que desempenharam;

7.2.4- Orientar o processo de avaliação de todo o pessoal que trabalhe nas entidades mesmo em caso de funções terceirizadas.

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 evitar a incorporação aos quadros das entidades de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade das entidades.

7.3.1.2- Não devem ser admitidos estagiários em nenhuma entidade da ICP-Brasil.

7.3.2- As Atribuições da Função:

7.3.2.1- 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:

7.3.2.1.1- A descrição sumária das tarefas inerentes a função;

7.3.2.1.2- As necessidades de acesso a informações sensíveis;

7.3.2.1.3- O grau de sensibilidade do setor onde a função é exercida;

7.3.2.1.4- As necessidades de contato de serviço internos e/ou externos;

7.3.2.1.5- As características de responsabilidade, decisão e iniciativa inerentes à função;

7.3.2.1.6- O histórico do desempenho nos aspectos técnico e funcional se aplicável ao funcionário.

7.3.3- O Levantamento de Dados Pessoais:

7.3.3.1- Deve ser elaborado uma pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de perfil, devendo ainda serem observados os ambientes social, familiar e funcional.

7.3.4- A entrevista de admissão:

7.3.4.1- Deve ser realizada por profissional legalmente qualificado, que tem 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 vinculadas na entrevista do candidato só deverão ser aquelas de caráter ostensivo.

7.3.5- Avaliação Psicológica:

7.3.5.1- Deve ser realizada por profissional legalmente qualificado, e tem o propósito de avaliar o candidato e de traçar o seu perfil relativo ao equilíbrio emocional, o ajuste da personalidade e a existência de atributos pessoais exigidos para o cargo e/ou função a ser desempenhada.

7.3.6- O Desempenho da Função:

7.3.6.1- Acompanhar o desempenho e avaliar periodicamente os funcionários com o propósito de detectar a necessidade de atualização técnica e de segurança;

7.3.6.2- Habilitar os funcionários das entidades no acesso às informações, mediante a realização de instruções e orientações sobre as medidas e procedimentos de segurança.

7.3.7- A Credencial de Segurança:

7.3.7.1- Certificar o funcionário por meio de uma credencial, habilitando-o a ter acesso às informações sensíveis, de acordo com a classificação do grau de sigilo da informação e a conseqüente relação com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada;

7.3.7.2- 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.

7.3.8- Treinamento em Segurança em Informação:

7.3.8.1- Deve ser definido um processo pelo qual serão apresentadas aos funcionários as normas e procedimentos da Política de Segurança da Informação relativos ao trato de conhecimentos e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva mentalidade de segurança, assim como instruir o seu fiel cumprimento.

7.3.9- Acompanhamento no Desempenho da Função:

7.3.9.1- Recomenda-se a realização de processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos funcionários, a ser realizada pela chefia imediata do mesmo;

7.3.9.2- Deverão ser motivo de registro, atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do funcionário;

7.3.9.3- Os comportamentos inadequados, ou que possam gerar comprometimentos, deverão ser averiguados ou comunicados à chefia imediata;

7.3.9.4- As chefias imediatas deverão se assegurar de que todos os funcionários tenham conhecimento e compreensão das medidas e procedimentos de segurança prescritos nas Normas e Instruções de Segurança em vigor.

7.3.10- O Processo de Desligamento:

7.3.10.1- Deverá ser assegurada a salvaguarda dos assuntos sigilosos após o desligamento dos funcionários das entidades, através de contrato específico assinado no processo de admissão;

7.3.10.2- Será restrito o acesso de ex-funcionários às instalações onde sejam produzidas, manuseadas, tratadas ou armazenadas informações sigilosas;

7.3.10.3- Sua credencial, identificação, crachá, equipamentos, mecanismos e acessos lógicos devem ser revogados.

7.3.11- O Processo de Liberação:

7.3.11.1- Deve ser aplicado, antes do desligamento, um certificado de nada consta das diversas unidades que compõem a unidade AC.

7.3.12- A Entrevista de Desligamento:

7.3.12.1- Deverá ser formalizada uma entrevista de desligamento para orientar o funcionário 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;

7.3.12.2- Deverá ser elaborado um texto adequadamente fundamentado, com informações que identifiquem o motivo de desligamento e o grau de satisfação do funcionário em relação ao órgão;

7.3.12.3- Sempre que possível será esclarecido na entrevista que a organização reconhece os serviços relevantes prestados e a competência dedicada pelo funcionário, possibilitando assim manter novos e periódicos contatos futuros;

7.3.12.4- Deve ser previsto, no contrato inicial, uma cláusula que determine que o funcionário, quando desligado, mantenha sigilo sobre todos os ativos de informações e de processos das entidades.

7.4- Responsabilidades

7.4.1- Responsabilidades dos funcionários:

7.4.1.1- Todos são responsáveis pelas informações de que fazem uso e pelos respectivos recursos de processamento de informações;

7.4.1.2- As responsabilidades devem ser classificadas em função da posição hierárquica do funcionário dentro da organização;

7.4.1.3- Todos os funcionários que acessem ativos de informação das entidades são responsáveis pela integridade dos mesmos;

7.4.1.4- Todos os funcionários são responsáveis pelo cumprimento da política de segurança. O não cumprimento ou a recusa em fazê-lo sujeita o funcionário às sanções disciplinares ou legais cabíveis;

7.4.1.5- Os Sistemas de Informações das entidades e os recursos a ela relacionados somente poderão ser utilizados para os fins previstos pela Gerência de Segurança;

7.4.1.6- Cumprir as regras específicas de proteção aos ativos de informação estabelecidas;

7.4.1.7- Manter o caráter sigiloso da senha de acesso aos recursos e sistemas das entidades;

7.4.1.8- Manter o caráter sigiloso dos dados das entidades participantes da ICP-Brasil aos quais tiver acesso;

7.4.1.9- Informações confidenciais não devem ser compartilhadas, sob qualquer forma, com outros que não tenham a devida autorização de acesso;

7.4.1.10- 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;

7.4.1.11- Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da lei de direitos autorais (copyright).

7.4.2- Responsabilidades das Chefias:

7.4.2.1- Gerenciar o cumprimento da política de segurança, por parte de seus funcionários;

7.4.2.2- Identificar os desvios praticados e iniciar as medidas corretivas apropriadas;

7.4.2.3- Impedir o acesso de funcionários demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do funcionário;

7.4.2.4- 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;

7.4.2.5- Comunicar à unidade que efetua a concessão de privilégios a funcionários, quais os empregados e prestadores de serviço, sob sua supervisão, que podem acessar as informações das entidades;

7.4.2.6- Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação das entidades;

7.4.2.7- Comunicar à unidade que efetua a concessão de privilégios a funcionários, quais os empregados e prestadores de serviço

demitidos e transferidos e quais estejam respondendo a processos e sindicâncias, bem como o resultado apurado, para exclusão do usuário do cadastro;

7.4.3- Responsabilidades Gerais:

7.4.3.1- Cada área que detém recursos de informação é responsável pelos ativos de informações que use em suas atividades;

7.4.3.2- Todos os ativos de informações deverão ter responsáveis pelo seu uso claramente definidos;

7.4.3.3- Todos os ativos de computação das entidades são considerados como ativos desta e, portanto, devem receber a proteção adequada conforme a importância para os negócios;

7.4.3.4- Todos os ativos de computação das entidades devem receber classificação quanto à preservação e proteção.

7.4.4- Responsabilidades da Gerência de Segurança:

7.4.4.1- Estabelecimento das regras de proteção dos ativos das entidades;

7.4.4.2 - Acompanhamento do cumprimento das regras estabelecidas;

7.4.4.3 - Decisão quanto às linhas de ação a serem tomadas no caso de violação das regras estabelecidas;

7.4.4.4 - Responder pelos danos causados em decorrência de ausência ou inadequação das regras;

7.4.4.5 - Revisar periodicamente as regras de proteção estabelecidas;

7.4.4.6- Restringir e controlar o acesso e os privilégios de usuários remotos e externos;

7.4.4.7- Elaborar e manter o Plano de Contingências das entidades;

7.4.4.8- Implementar e administrar as regras de proteção estabelecidas pela Política de Segurança;

7.4.4.9- Detectar, identificar, registrar e comunicar a AC Raiz as violações ou tentativas de acesso não autorizados;

7.4.4.10- Implementar, para cada usuário, restrições de acesso à Rede como horário autorizado, dias autorizados, entre outras;

7.4.4.11- Manter registros de atividades de usuários na Rede (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, 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.);

7.4.4.12- Limitar o prazo de validade das contas de prestadores de serviço;

7.4.4.13- Suspender contas de acesso inativas;

7.4.4.14- Fornecer senhas de contas privilegiadas somente aos funcionários que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.

7.4.5- Responsabilidades dos terceirizados

7.4.5.1- Deve ser assinado um contrato, que contemple as diretrizes e recomendações de segurança especificadas no presente item, abrangendo todos os contratados nesta modalidade (consultores, funcionários ou empresas terceirizadas), para atuar nas entidades participantes da ICP-Brasil, em todos os níveis.

7.5- Sanções

7.5.1- Sanções previstas pela legislação vigente.

8 – REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

Ambiente físico é aquele composto por todo o ativo de processamento das entidades.

- As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e associados a indivíduos definidos e identificados na organização;

- A localização e o sistema de certificação da AC Raiz e das AC não deverão ser publicamente identificados;

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

- 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;

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

- 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;

- Os sistemas de AC deverão estar localizados em área afastada de fontes potentes de magnetismo ou interferência de rádio freqüência;

- Sistemas que realizam as funções de certificação e identificação deverão estar localizados em uma área dedicada exclusivamente para isso, visando facilitar a execução dos procedimentos de controle de acesso físico;

- 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;

- Acesso aos componentes da infra-estrutura essencial ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, deverão ser restritos a pessoal autorizado;

- Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização;

- O inventário de todo o conjunto de ativos de processamento deve estar registrado e ser atualizado periodicamente nos menores intervalos de tempo possíveis.

9- REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

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

9.1- Diretrizes gerais

9.1.1- A informação é um patrimônio e deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser classificada de acordo com a legislação em vigor;

9.1.2- 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;

9.1.3- As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter preventivo e corretivo, legais e de auditoria. Os registros devem ser protegidos de modo adequado;

9.1.4- 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;

9.1.5- O inventário de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e ser atualizado periodicamente nos menores intervalos de tempo possíveis.

9.2- Diretrizes específicas

9.2.1- Sistemas

9.2.1.1- 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;

9.2.1.2- 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;

9.2.1.3- 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 analisadas para identificar tendências, falhas ou uso indevido. Os logs devem ser protegidos;

9.2.1.4- Devem ser estabelecidas e mantidas medidas de segurança para verificação crítica dos dados quanto a sua precisão, consistência e integridade;

9.2.1.5- 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.

9.2.2- Máquinas servidoras

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

9.2.2.2- 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 definidas;

9.2.2.3- Os procedimentos de backup e recuperação devem estar documentados, atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade dos dados e aplicações;

9.2.2.4- 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;

9.2.2.5- As máquinas devem estar sincronizadas para permitir o rastreamento de eventos. Nas AC e AC Raiz devem ser utilizados selos temporais;

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

9.2.2.7- A versão do Sistema Operacional, assim como outros softwares básicos instalados em máquinas servidoras, devem ser mantidas atualizadas, em conformidade com as recomendações dos fornecedores;

9.2.2.8- Devem ser utilizados somente softwares autorizados nos equipamentos. Recomenda-se a realização do controle, distribuição e instalação dos mesmos;

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

9.2.2.10- Os procedimentos de cópia de segurança e de recuperação devem estar documentados, atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.

9.2.3- Redes das Entidades da ICP-Brasil

9.2.3.1- O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

9.2.3.2- Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso controlado e devem ser protegidos contra danos, furtos e roubos;

9.2.3.3- As facilidades de segurança disponíveis de forma nativa nos ativos de processamento da rede devem ser adotadas;

9.2.3.4- 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 encontram-se esses ativos em sua primeira ativação;

9.2.3.5- Serviços vulneráveis devem receber nível de proteção adicional;

9.2.3.4- O uso de senhas deve estar submetido a uma política específica para sua gerência e utilização;

9.2.3.5- 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;

9.2.3.6- A utilização de qualquer mecanismo capaz de realizar testes de monitoração sobre os dados da rede só deve ocorrer com a autorização e a supervisão adequadas;

9.2.3.7- A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração, devem ter a autorização da administração da rede e da gerência de segurança. A topologia, configuração e inventário dos recursos devem ser mantidos atualizados;

9.2.3.8- 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;

9.2.3.9- A produção de documentos sigilosos em mídias utilizadas em equipamentos de redes, tais como papel para impressão ou CD-R, deve ser feita em dispositivos protegidos ou sob supervisão do responsável;

9.2.3.10- Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos;

9.2.3.11- Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações;

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

9.2.3.13- 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;

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

9.2.3.15- Devem ser observadas as questões envolvendo direitos autorais quando da cópia de software ou arquivos de outras localidades;

9.2.3.16- Informações sigilosas, corporativas ou que possam causar prejuízo às entidades, não devem estar disponíveis ou ser enviadas para redes inseguras sem a proteção adequada;

9.2.3.17- Todo serviço de rede não explicitamente autorizado deve ser bloqueado;

9.2.3.18- Os serviços de rede, cuja implementação admitem proteção adicional, devem sofrer as modificações pertinentes em sua configuração;

9.2.3.19- Mecanismos de segurança baseados em sistemas de firewall devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade;

9.2.3.20- Os registros de eventos devem ser analisados, periodicamente, no menor prazo possível e em intervalos de tempo adequados;

9.2.3.21- Deve ser adotado um padrão de segurança para todos tipos de equipamentos servidores, considerando aspectos físicos e lógicos;

9.2.3.22- Deve ser adotado um padrão de segurança para o desenvolvimento de sistemas que façam uso de tecnologias utilizadas na Internet, visando a proteção das informações, recursos e a reputação das entidades. As informações tornadas disponíveis devem ser precisas e estar atualizadas;

9.2.3.23- Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle;

9.2.3.24- A localização dos serviços com relação ao 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;

9.2.3.25- Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;

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

9.2.3.27- As conexões de rede devem ser ativadas na seguinte ordem: 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, por exemplo, o uso de proxies, que deverão ser implementados para proteger os sistemas que executam a função de certificação contra possíveis ataques;

9.2.3.28- 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;

9.2.3.29- A chave de certificação das AC deverá estar protegida de acesso desautorizado, para garantir seu sigilo e integridade;

9.2.3.30- 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;

9.2.3.31- 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.

9.2.4- Controle de acesso lógico (baseado em senhas)

9.2.4.1- Usuários e aplicações que necessitem ter acesso a recursos das entidades da ICP-Brasil devem ser identificados e autenticados;

9.2.4.2- 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;

9.2.4.3- Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário;

9.2.4.4- A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não-autorizadas;

9.2.4.5- O arquivo de senhas deve ser criptografado e ter o acesso controlado;

9.2.4.6- As autorizações devem ser definidas de acordo com a necessidade de condução das tarefas (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a condução de tarefas);

9.2.4.7- As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada;

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

9.2.4.9- As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho, tempo de vida, forma de troca e restrições específicas;

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

9.2.4.11- 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;

9.2.4.12- Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso malsucedidas;

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

9.2.4.14- 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;

9.2.4.15- 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;

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

9.2.5- Computação pessoal

9.2.5.1- As estações de trabalho, notebooks e informações devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

9.2.5.2- Equipamentos instalados em locais não protegidos ou 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);

9.2.5.3- Medidas de segurança lógica referentes a combate a vírus, backup, controle de acesso e uso de software não autorizado devem ser adotadas;

9.2.5.4- Os meios magnéticos devem ser protegidos contra danos, furtos ou roubos, devendo ser adotados procedimentos de backup em documento específico;

9.2.5.6- Informações sigilosas, corporativas ou cuja divulgação desautorizada 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;

9.2.5.7- O acesso às informações deve atender às necessidades de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo);

9.2.5.8- Os usuários devem utilizar apenas softwares autorizados nos equipamentos das entidades, de acordo com os aspectos de controle, distribuição e instalação de software definidos nos documentos normativos da ICP-Brasil;

9.2.5.9- 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;

9.2.5.10- O inventário dos recursos deve ser mantido atualizado.

9.2.6- Combate a Vírus de computador

9.2.6.1- Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e worms) devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho 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 pelos seguintes elementos: 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- Recomenda-se que todos os sistemas criptográficos implementados na ICP-Brasil sejam de origem nacional;

10.1.3- A expressão “solução criptográfica”, citada no parágrafo anterior, deve ser interpretada como referindo-se a todos os requisitos que caracterizam os componentes da solução (hardware e software) com especial atenção para os algoritmos criptográficos. Com igual cuidado, deve-se tratar os demais algoritmos necessários para gerar parâmetros críticos para a execução dos primeiros;

10.1.4- Recomenda-se que a implementação do sistema, tanto no que se refere ao hardware e ao software sejam realizados por fabricantes nacionais;

10.1.5- Toda a documentação, referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados na ICP-Brasil, deve ser aprovada pelo CG ICP-Brasil ;

10.1.6- A robustez do sistema criptográfico deve ser periodicamente testada por entidades competentes na área de criptografia. A periodicidade a que se refere este item não deve ser superior a 2 (dois) anos;

10.1.7- Os testes necessários para satisfazer o item anterior devem estar previamente definidos em documento normativo específico e de caráter oficial aprovado pelo CG ICP-Brasil;

10.1.8- Na impossibilidade de satisfazer na íntegra o uso de soluções nacionais, deve-se buscar compor a solução de tal modo que seus elementos constituintes possam ser substituídos por soluções nacionais quando estas estiverem disponíveis e tecnologicamente confiáveis, desde de que tais substituições não comprometam a robustez da solução global;

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

10.1.10- Os aspectos relevantes relacionados à criptografia no âmbito da ICP-Brasil devem ser detalhados em documentos específico, aprovado pelo CG ICP-Brasil ;

10.1.11- Recomenda-se consulta às normas técnicas da ABNT, relacionadas com a Segurança da Informação, quando da realização de trabalhos a criptografia de dados no âmbito da ICP-Brasil.

10.2- Chaves criptográficas

10.2.1- A manipulação das chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverá ser restrita a um número mínimo e essencial de pessoas assim como deve estar submetida 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 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- Recomenda-se o uso de redes virtuais privadas baseadas em criptografia para a comunicação entre redes internas entidades da ICP-Brasil que pertençam a uma mesma organização.

11- AUDITORIA

11.1- Introdução

11.1.1- As atividades das entidades integrantes da ICP-Brasil estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários.

11.2- Objetivo da Auditoria

11.2.1- Verificar a capacidade da AC Raiz, demais AC, AR e repositórios em atender os requisitos da ICP-Brasil. O resultado da auditoria é um item fundamental a ser considerado no processo de licenciamento das AC para a ICP-Brasil, assim como, para a manutenção da condição de licenciada.

11.3- Abrangência

11.3.1- A auditoria deve abordar os aspectos relativos ao ambiente de operação e ciclo de vida de certificados. Os seguintes tópicos devem ser verificados :

11.3.2- Ambiente de operação

- Segurança da operação;
- Segurança de pessoal;
- Segurança física;
- Segurança lógica;
- Segurança de telecomunicações;
- Segurança de recursos criptográficos;
- Plano de contingência.

11.3.3- Ciclo de vida do certificado

- Solicitação;
- Validação;
- Emissão;
- Uso;
- Revogação.

11.4- Documentos de Referência

11.4.1- A auditoria deve ser realizada tendo como orientação básica os seguintes documentos da ICP-Brasil e padrões :

11.4.1.1- Documentação normativa da ICP-Brasil;
11.4.1.2- Documentação normativa específica para auditoria definida pelo CG ICP-Brasil.

11.5- Identidade e qualificação do Auditor

11.5.1- A auditoria da AC Raiz e das AC licenciadas deve ser realizada por entidade previamente credenciada pelo CG ICP-Brasil, atendendo aos seguintes requisitos mínimos :

11.5.1.1- corpo técnico com comprovada experiência nas áreas de segurança da informação (ambientes físico e lógico), criptografia, infra-estrutura de chaves pública e sistemas críticos;

11.5.1.2- experiência em serviços de auditoria dessa mesma natureza e referências de outros serviços de auditoria similares;

11.5.1.3- utilização de padrões internacionais (como exemplo: ISO 17799) ou padrão similar como referência de melhores práticas e procedimentos.

11.6- O resultado da auditoria pode sugerir as seguintes ações:

11.6.1- Suspender temporariamente os serviços nas AC da ICP-Brasil até correção dos problemas;

11.6.2- Revogar o certificado das AC da ICP-Brasil;

11.6.3- Substituir / treinar pessoal;

11.6.4- Aumentar a freqüência das auditorias;

11.6.5- Encaminhar o relatório final da auditoria, com sugestões e conclusões para o CG ICP-Brasil e AC Raiz.

11.7- Freqüência das Auditorias

11.7.1- O processo de auditoria deve ser realizado nas seguintes situações e respectivas freqüências:

11.7.1.1- Licenciamento inicial – antes do licenciamento e da entrada em produção;

11.7.1.2- Auditoria periódica (anual) – para manter o licenciamento;

11.7.1.3- Por determinação do CG ICP-Brasil ou da AC Raiz, a qualquer tempo.

12- GERENCIAMENTO DE RISCOS

12.1- Introdução

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

- o que deve ser protegido;
- contra quem ou contra o quê deve ser protegido;
- análise da relação custo x benefício.

12.2- Fases Principais

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

12.2.1.1- Identificação dos recursos a serem protegidos – “hardware”, rede, “software”, dados, informações pessoais, documentação, suprimentos;

12.2.1.2- 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);

12.2.1.3- Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

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

12.2.1.5- 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;

12.2.1.6- Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

12.2.1.7- Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses.

12.3- Riscos relacionados às entidades integrantes da ICP-Brasil

12.3.1- Para as entidades da ICP-Brasil os seguintes riscos devem ser avaliados :

Segmento	Riscos
Dados e Informação	Interrupção (perda), interceptação, modificação, fabricação, destruição
Pessoas	Omissão, erro, empregado descontente, sabotagem, perda de conhecimento
Rede	Hacker, acesso, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço
Hardware	Indisponibilidade, interceptação (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 estar documentados e devem ser levados ao conhecimento da AC-Raiz e do CG ICP-Brasil;

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

12.5.1- 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