Política de Segurança
da Autoridade Certificadora
DOCCLOUD

PS - AC DOCCLOUD RFB

Versão 1.0

Outubro 2015

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Responsável	Descrição	Item alterado	Versão	Data
Compliance	Versão Inicial		1.0	02/10/2015

1 INTRODUÇÃO

1.1 Esta Política de Segurança tem por finalidade estabelecer e informar as diretrizes de segurança que são adotadas pela AC DOCCLOUD RFB, integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Tais diretrizes fundamentam as normas e procedimentos de segurança elaborados e implementados pela AC DOCCLOUD RFB.

2 OBJETIVOS

A Política de Segurança (PS) da AC DOCCLOUD RFB tem os seguintes objetivos específicos:

a) Definir o escopo da segurança da AC DOCCLOUD RFB;

b) Orientar, por meio de suas diretrizes, todas as ações de segurança da AC DOCCLOUD RFB, 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 dessa Política de Segurança serão interpretadas de forma que todas as suas determinações sejam consideradas obrigatórias, indispensáveis e cogentes.

5 CONCEITOS E DEFINIÇÕES

Aplicam-se os conceitos abaixo:

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

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

d) **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros. 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 da AC DOCCLOUD RFB;

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 da AC DOCCLOUD RFB;

h) **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação da AC DOCCLOUD RFB;

i) **Proteção dos Ativos** – é o processo pelo qual os ativos da AC DOCCLOUD RFB recebem classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação recebe 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, sequências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras.

6 REGRAS GERAIS

6.1 GESTÃO DE SEGURANÇA

6.1.1 A PS da AC DOCCLOUD RFB se aplica a todos os recursos humanos, administrativos e tecnológicos pertencentes às entidades que a compõem. A abrangência dos recursos citados refere-se àqueles ligados às Autoridades de Registro, postos de atendimento e provisórios tanto em caráter permanente quanto temporário.

6.1.2 Esta política foi comunicada para todo o pessoal envolvido e largamente divulgada através da AC DOCCLOUD RFB, garantindo que todos os envolvidos tenham consciência da mesma e de suas atualizações e a pratiquem na organização.

6.1.3 Todo o pessoal recebeu e recebe as informações atualizadas necessárias para cumprir adequadamente o que está determinado na PS e no DOC – ICP 02.

6.1.4 Um programa de conscientização sobre segurança da informação foi implementado para assegurar que todo o pessoal foi informado e entendeu as informações sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações da AC DOCCLOUD RFB. Especialmente, o pessoal envolvido ou que se relaciona com os usuários foi devidamente treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.

6.1.5 Os procedimentos foram implementados e documentados 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 possam ser devidamente revistos, modificados ou revogados.

6.1.6 A AC DOCCLOUD RFB possui um repositório centralizado e um mecanismo para ativação e manutenção de trilhas, *logs* e demais notificações de incidentes. Este mecanismo está 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, estão em conformidade com esta PS.

6.1.8 No que se refere a segurança da informação, é considerado proibido, tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança da AC DOCCLOUD RFB.

6.2 GERENCIAMENTO DE RISCOS

O processo de gerenciamento de riscos da AC DOCCLOUD RFB é sempre revisto, a cada prazo máximo de 18 (dezoito) meses, pela própria AC DOCCLOUD RFB, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando a execução de plano de ação apropriado para proteção aos componentes ameaçados.

6.3 INVENTÁRIO DE ATIVOS

Todos os ativos da AC DOCCLOUD RFB foram e estão inventariados e classificados, e são permanentemente atualizados pela própria AC DOCCLOUD RFB, e possuem um gestor responsável e formalmente designado.

6.4 PLANO DE CONTINUIDADE DO NEGÓCIO

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

6.4.2 A AC DOCCLOUD RFB possui planos de gerenciamento de incidentes e de ação de resposta a incidentes aprovados pela AC Raiz ou AC de nível imediatamente superior.

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

6.4.4 Todos os incidentes serão reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes serão sempre 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, que são observados pelos prestadores de serviço e todos os empregados da AC DOCCLOUD RFB, necessário à proteção dos ativos AC DOCCLOUD RFB.

7.2 OBJETIVOS

7.2.1 Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos AC DOCCLOUD RFB.

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 a AC DOCCLOUD RFB 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 na AC DOCCLOUD RFB, mesmo em caso de funções desempenhadas por prestadores de serviço.

7.3 DIRETRIZES

7.3.1 O PROCESSO DE ADMISSÃO

7.3.1 A AC DOCCLOUD RFB adota critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros da AC DOCCLOUD RFB, integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade AC DOCCLOUD RFB.

7.3.2 A AC DOCCLOUD RFB não admite estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

7.3.3 Todo o empregado, funcionário ou servidor assina no ato da contratação 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

A AC DOCCLOUD mantém relação clara das atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar o perfil necessário do empregado ou servidor, considerando-se os seguintes itens:

a) a descrição sumária das tarefas inerentes à função;

b) as necessidades de acesso a informações sensíveis;

c) o grau de sensibilidade do setor onde a função é exercida;

d) as necessidades de contato de serviço interno e/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

No ato da admissão é 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 A AC DOCCLOUD RFB realiza entrevista de admissão através de 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 A AC DOCCLOUD RFB avalia, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato são somente aquelas de caráter público.

7.3.5 O DESEMPENHO DA FUNÇÃO

7.3.5.1 A AC DOCCLOUD RFB acompanha o desempenho e avalia periodicamente os seus empregados e/ou servidores, e de suas AR (s) vinculadas, com o propósito de detectar a necessidade de atualização técnica e de segurança.

7.3.5.2 A AC DOCCLOUD RFB dá aos seus empregados ou servidores e de suas AR (s) vinculadas 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 A AC DOCCLOUD RFB identifica o empregado selecionado 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, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada.

7.3.6.2 A Credencial de Segurança somente é concedida por autoridade competente da AC DOCCLOUD RFB, 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 da AC DOCCLOUD RFB. 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

A AC DOCCLOUD RFB possui um processo definido pelo qual esta PS é apresentada aos empregados, servidores e prestadores de serviço, junto às 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 A AC DOCCLOUD RFB realiza processo de avaliação de desempenho da função que documenta a observação do comportamento pessoal e funcional dos empregados, realizada pela chefia imediata dos mesmos.

7.3.8.2 A AC DOCCLOUD RFB mantém registrados quaisquer 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, são sempre averiguados e comunicados à chefia imediata.

7.3.8.4 As chefias imediatas da AC DOCCLOUD RFB asseguram 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 da AC DOCCLOUD RFB às instalações, quando necessário, é sempre restrito às áreas de acesso público.

7.3.9.2 Ato contínuo a demissão é revogada a credencial do empregado demitido, sua identificação e crachá, e proibido o uso de equipamentos, mecanismos e acessos físicos e lógicos.

7.3.10 O PROCESSO DE LIBERAÇÃO

Ocorrendo demissão, o empregado ou servidor da AC DOCCLOUD RFB firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a AC DOCCLOUD RFB, sendo esse requisito sempre checado junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.

7.3.11 A ENTREVISTA DE DESLIGAMENTO

Ocorrendo demissão, a AC DOCCLOUD RFB sempre realiza entrevista de desligamento e orienta 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 na AC DOCCLOUD RFB.

7.4 DEVERES E RESPONSABILIDADES

7.4.1 DEVERES DOS EMPREGADOS OU SERVIDORES DA AC DOCCLOUD RFB

São deveres dos empregados ou servidores da AC DOCCLOUD RFB:

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 AC DOCCLOUD RFB e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança;

d) cumprir as regras específicas de proteção estabelecidas aos ativos de informação;

e) manter o caráter sigiloso da senha de acesso aos recursos e sistemas da AC DOCCLOUD RFB;

f) não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;

g) responder, por todo e qualquer acesso, aos recursos da AC DOCCLOUD RFB 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 DA AC DOCCLOUD RFB

São responsabilidades das chefias da AC DOCCLOUD RFB:

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 AC DOCCLOUD RFB, 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 AC DOCCLOUD RFB;

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 AC DOCCLOUD RFB;

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 DA AC DOCCLOUD RFB

São responsabilidades gerais da AC DOCCLOUD RFB:

a) cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover, e provê, a sua proteção de acordo com a política de classificação da informação da AC DOCCLOUD RFB;

b) todos os ativos de informações deverão ter, e têm, claramente definidos os responsáveis pelo seu uso;

c) todos os ativos de processamento AC DOCCLOUD RFB devem estar, e estão, relacionados no PCN.

7.4.4 RESPONSABILIDADES DA GERÊNCIA DE SEGURANÇA DA AC DOCCLOUD RFB

São responsabilidades das Gerências de Segurança da AC DOCCLOUD RFB:

a) estabelecer as regras de proteção dos ativos AC DOCCLOUD RFB 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 contém 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 DA AC DOCCLOUD RFB

São 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 da AC DOCCLOUD RFB.

8.2 DIRETRIZES GERAIS

8.2.1 As responsabilidades pela segurança física dos sistemas AC DOCCLOUD RFB são definidas e atribuídas a indivíduos claramente identificados na organização.

8.2.2 A localização das instalações e o sistema de certificação da AC Raiz e da AC DOCCLOUD RFB não serão publicamente identificados.

8.2.3 Os sistemas de segurança para acesso físico da AC DOCCLOUD RFB são instalados para controlar e auditar o acesso aos sistemas de certificação.

8.2.4 Os controles duplicados sobre o inventário e cartões/chaves de acesso são estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves é mantida atualizada.

8.2.5 As chaves criptográficas sob custódia do responsável são fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

8.2.6 As 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 da AC DOCCLOUD RFB estão localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio frequência.

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

8.2.9 A entrada e saída, nestas áreas ou partes dedicadas, são sempre automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação da AC DOCCLOUD RFB e mantidas em local adequado e sob sigilo.

8.2.10 O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas AC DOCCLOUD RFB, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal autorizado.

8.2.11 Os sistemas de detecção de intrusão são implementados e 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 é sempre registrado e mantido atualizado, no mínimo, mensalmente.

8.2.13 Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, somente é utilizado a partir de autorização formal e mediante supervisão.

8.2.14 Nas instalações AC DOCCLOUD RFB, todos utilizam alguma forma visível de identificação (por exemplo: crachá), e são obrigados a informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

8.2.15 Os visitantes das áreas de segurança são sempre supervisionados. Suas horas de entrada e saída e o local de destino sempre são registrados. Essas pessoas somente obtém acesso às áreas específicas, com propósitos autorizados, e esses acessos devem seguir obrigatoriamente instruções baseadas nos requisitos de segurança da área visitada da AC DOCCLOUD RFB.

8.2.16 Os ambientes onde ocorrem os processos críticos AC DOCCLOUD RFB integrantes da ICP-Brasil são monitorados, em tempo real, com as imagens registradas por meio de sistemas de Circuito Fechado de Televisão - CFTV.

8.2.17 Os sistemas de detecção de intrusos são 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 possuem um sistema de alarme que permanece sempre ativado.

9 REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

9.1 DEFINIÇÃO

Ambiente lógico é composto por todo o ativo de informações da AC DOCCLOUD RFB.

9.2 DIRETRIZES GERAIS

9.2.1 A informação da AC DOCCLOUD RFB é protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, foi elaborado um sistema de classificação da informação.

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

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

9.2.4 Os sistemas e recursos que suportam funções críticas para operação AC DOCCLOUD RFB, asseguram a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

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

9.3 DIRETRIZES ESPECÍFICAS

9.3.1 SISTEMAS

9.3.1.1 As necessidades de segurança foram identificadas para cada etapa do ciclo de vida dos sistemas disponíveis da AC DOCCLOUD RFB. A documentação dos sistemas é mantida atualizada. A cópia de segurança foi testada e é mantida atualizada.

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

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

9.3.1.4 Foram estabelecidas e são mantidas pela AC DOCCLOUD RFB 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 foram avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente são avaliadas periodicamente e as recomendações de segurança sempre são adotadas.

9.3.2 MÁQUINAS SERVIDORAS

9.3.2.1 O acesso lógico, ao ambiente ou serviços disponíveis em servidores, sempre é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização está claramente definido e registrado.

9.3.2.2 Os acessos lógicos são registrados em *logs*, e analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas estão definidos.

9.3.2.3 A AC DOCCLOUD RFB adota procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos são armazenados em 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 estão sincronizadas para permitir o rastreamento de eventos.

9.3.2.5 Existe proteção lógica adicional (criptografia) 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 são mantidos atualizados, em conformidade com as recomendações dos fabricantes.

9.3.2.7 A AC DOCCLOUD RFB utiliza 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 sempre é 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 sempre estão documentados, são mantidos atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações.

9.3.3 REDES DA AC DOCCLOUD RFB

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

9.3.3.2 Os componentes críticos da rede local são mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

9.3.3.3 Foram 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 foi averiguada quando da sua instalação inicial, para que fossem detectadas e corrigidas eventuais vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.

9.3.3.5 Serviços vulneráveis receberam nível de proteção adicional.

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

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

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

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

9.3.3.10 A AC DOCCLOUD RFB define relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* são analisados periodicamente e o período de análise estabelecido é o menor possível.

9.3.3.11 A AC DOCCLOUD RFB adota proteções físicas adicionais para os recursos de rede considerados críticos.

9.3.3.12 A AC DOCCLOUD RFB adota proteção lógica adicional para evitar o acesso não-autorizado às informações.

9.3.3.13 A infraestrutura de interligação lógica da AC DOCCLOUD RFB está protegida contra danos mecânicos e conexão não autorizada.

9.3.3.14 A alimentação elétrica para a rede local da AC DOCCLOUD RFB está separada da rede convencional, estando observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis.

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

9.3.3.16 A AC DOCCLOUD RFB observa as questões envolvendo propriedade intelectual quando da cópia de *software* ou arquivos de outras localidades.

9.3.3.17 As informações sigilosas da AC DOCCLOUD RFB, corporativas ou que possam causar prejuízo às entidades estão protegidas e não são enviadas para outras redes, sem proteção adequada.

9.3.3.18 Todo serviço de rede não explicitamente autorizado pela AC DOCCLOUD RFB é bloqueado ou desabilitado.

9.3.3.19 A AC DOCCLOUD RFB utiliza mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) para proteger as transações entre redes externas e a rede interna da AC DOCCLOUD RFB.

9.3.3.20 Os registros de eventos são analisados pelos técnicos da AC DOCCLOUD RFB periodicamente, no menor prazo possível e em intervalos de tempo adequados.

9.3.3.21 A AC DOCCLOUD RFB adota um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos.

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

9.3.3.23 A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) é resultante de uma análise de riscos criteriosa feita pela AC DOCCLOUD RFB. No mínimo, os seguintes aspectos são considerados: (i) requisitos de segurança definidos pelo serviço, (ii) objetivo do serviço, (iii) público alvo, (iv) classificação da informação, (v) forma de acesso, (vi) frequência de atualização do conteúdo, (vii) forma de administração do serviço e (viii) volume de tráfego.

9.3.3.24 Os ambientes de rede da AC DOCCLOUD RFB considerados críticos são isolados de outros ambientes de rede da AC DOCCLOUD RFB, de modo a garantir um nível adicional de segurança.

9.3.3.25 As conexões entre as redes da AC DOCCLOUD RFB e as redes externas estão restritas somente àquelas que visem efetivar os processos.

9.3.3.26 As conexões de rede da AC DOCCLOUD RFB são ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, a AC DOCCLOUD RFB emprega controles de compensação, tais como

o uso de *proxies* que são implementados pela AC DOCCLOUD RFB para proteger os sistemas que executam a função de certificação contra possíveis ataques.

9.3.3.27 Os sistemas da AC DOCCLOUD RFB que executam a função de certificação estão 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 da AC DOCCLOUD RFB está protegida de acesso desautorizado, para garantir seu sigilo e integridade.

9.3.3.29 A segurança das comunicações intra-rede e inter-rede, entre os sistemas da AC DOCCLOUD RFB está garantida pelo uso de mecanismos que asseguram o sigilo e a integridade das informações trafegadas.

9.3.3.30 A AC DOCCLOUD RFB implantou e utiliza ferramentas de detecção de intrusos 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 Todos os usuários e aplicações que necessitem ter acesso a recursos da AC DOCCLOUD RFB são identificados e autenticados.

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

9.3.4.3 Nenhum usuário é 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 possui proteção contra modificações não autorizadas.

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

9.3.4.6 A AC DOCCLOUD RFB define as autorizações de acordo com a necessidade de desempenho das funções (acesso motivado) e considera o princípio dos privilégios mínimos (possui acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

9.3.4.7 As senhas são individuais, secretas, intransferíveis e protegidas pela AC DOCCLOUD RFB com grau de segurança compatível com a informação associada.

9.3.4.8 A AC DOCCLOUD RFB possui e utiliza um sistema de controle de acesso com mecanismos que impedem a geração de senhas fracas ou óbvias.

9.3.4.9 As seguintes características das senhas estão definidas de forma adequada pela AC DOCCLOUD RFB: (i) conjunto de caracteres permitidos, (ii) tamanho mínimo e máximo, (iii) prazo de validade máximo, (iv) forma de troca e (v) restrições específicas.

9.3.4.10 A AC DOCCLOUD RFB distribui, sempre de forma segura, as senhas aos usuários de TI (inicial ou não). A senha inicial, quando gerada pelo sistema, é sempre trocada, obrigatoriamente, pelo usuário de TI, no primeiro acesso.

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

9.3.4.12 A AC DOCCLOUD RFB adota 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 A AC DOCCLOUD RFB possui e utiliza um sistema de controle de acesso que solicita nova autenticação após certo tempo de inatividade da sessão (*time-out*).

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

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

9.3.4.16 Os usuários e administradores do sistema de controle de acesso da AC DOCCLOUD RFB são conscientizados, de maneira formal e expressa, de suas responsabilidades, mediante assinatura de termo de compromisso.

9.3.5 COMPUTAÇÃO PESSOAL

9.3.5.1 Todas as estações de trabalho da AC DOCCLOUD RFB, incluindo equipamentos portáteis ou *stand alone*, e informações são protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

9.3.5.2 Os equipamentos da AC DOCCLOUD RFB que executam operações sensíveis recebem proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).

9.3.5.3 A AC DOCCLOUD RFB adota 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 da AC DOCCLOUD RFB armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, e sempre são 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, são utilizadas somente em equipamentos da AC DOCCLOUD RFB onde foram geradas ou naqueles por ela autorizadas, e sempre com controles adequados.

9.3.5.6 O acesso às informações da AC DOCCLOUD RFB 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 da AC DOCCLOUD RFB utilizam apenas *softwares* licenciados pelo fabricante nos equipamentos da AC DOCCLOUD RFB, observadas as normas da ICP-Brasil e legislação de *software.*

9.3.5.8 A AC DOCCLOUD RFB estabeleceu aspectos de controle, distribuição e instalação de *softwares* utilizados.

9.3.5.9 A impressão de documentos sigilosos pela AC DOCCLOUD RFB sempre é feita sob supervisão do responsável. Os relatórios impressos são protegidos contra perda, reprodução e uso não-autorizado.

9.3.5.10 O inventário dos recursos da AC DOCCLOUD RFB é mantido atualizado.

9.3.5.11 Os sistemas em uso da AC DOCCLOUD RFB solicitam nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.5.12 As mídias são eliminadas de forma segura, quando não forem mais necessárias. A AC DOCCLOUD RFB tem definidos procedimentos formais para a eliminação segura das mídias, para minimizar os riscos.

9.3.6 COMBATE A VÍRUS DE COMPUTADOR

A AC DOCCLOUD RFB sistematizou os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e *worms*), que abrangem máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

10 REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS

10.1 REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA ICP-BRASIL

10.1.1 O sistema criptográfico da AC DOCCLOUD RFB é 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, com adoção de procedimentos para gerência das chaves criptográficas, e de métodos para testes de robustez das cifras e de detecção de violações dessas.

10.1.2 Toda a documentação, referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados pela AC DOCCLOUD RFB, foram aprovadas pela AC Raiz.

10.1.3 Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, com vistas a manter a segurança da infraestrutura, cujas atualizações são sempre implementadas e cumpridas pela AC DOCCLOUD RFB.

10.1.4 Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da AC DOCCLOUD RFB, é sempre armazenado cifrado.

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

10.2 CHAVES CRIPTOGRÁFICAS

10.2.1 Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da AC DOCCLOUD RFB são sempre executados por um número mínimo e essencial de pessoas, assim como foram submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.

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

10.2.3 Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da AC DOCCLOUD RFB estão aprovados pelo CG ICP-Brasil.

10.2.4 Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da AC DOCCLOUD RFB (ICP-Brasil) estão 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 AC DOCCLOUD RFB tem a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

10.3.2 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, a AC DOCCLOUD RFB adota recursos de VPN (*Virtual Private Networks* – redes privadas virtuais), baseadas em criptografia.

11 AUDITORIA E FISCALIZAÇÃO

11.1 As atividades da AC DOCCLOUD RFB 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 sempre foi, ainda é, e sempre será o de verificar a capacidade da AC DOCCLOUD RFB em atender aos requisitos da ICP-Brasil.

11.2 O resultado das auditorias pré-operacionais foi um item fundamental considerado no processo de credenciamento da AC DOCCLOUD RFB, da mesma forma que o resultado das auditorias operacionais e fiscalizações futuras será item fundamental para a manutenção da condição de credenciada da AC DOCCLOUD RFB.

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

11.4 Além de auditadas, a AC DOCCLOUD RFB poderá via a ser fiscalizada pela AC Raiz a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO AC DOCCLOUD RFB INTEGRANTES DA ICP-BRASIL [2].

12 GERENCIAMENTO DE RISCOS

12.1 DEFINIÇÃO

Gerenciamento de riscos é um processo que visa a proteção dos serviços da AC DOCCLOUD RFB, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. A AC DOCCLOUD RFB identifica os seguintes pontos:

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 de 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 de chaves criptográficas, *hardware* criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico

12.4 CONSIDERAÇÕES GERAIS

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

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

12.4.3 É necessária a participação e o envolvimento da alta administração da AC DOCCLOUD RFB.

12.5 IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS

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

13 PLANO DE CONTINUIDADE DO NEGÓCIO

13.1 DEFINIÇÃO

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

13.2 DIRETRIZES GERAIS

13.2.1 A AC DOCCLOUD RFB possui sistemas e dispositivos redundantes que estão sempre disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

13.2.2 A AC DOCCLOUD RFB possui e apresentou um Plano de Continuidade de Negócios – PCN, que estabelece, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

a) comprometimento da chave privada da AC DOCCLOUD RFB;

b) invasão do sistema e da rede interna da AC DOCCLOUD RFB;

c) incidentes de segurança física e lógica;

d) indisponibilidade da Infraestrutura; 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 recebeu um treinamento específico para poder enfrentar estes incidentes.

13.2.4 Um plano de ação de resposta a incidentes está estabelecido para a AC DOCCLOUD RFB. Este plano prevê, 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 os meios de comunicação, se for o caso.

14 DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio

http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

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

SIGLAS

AC	Autoridade Certificadora
ACT	Autoridade de Carimbo do Tempo
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
CG	Comitê Gestor
PCN	Plano de Continuidade de Negócio
PS	Política de Segurança
TI	Tecnologia da Informação
CFTV	Circuito Fechado de Televisão
ABNT	Associação Brasileira de Normas Técnicas
VPN	*Virtual Private Networks*

Política de Segurança da ICP-Brasil - DOC-ICP-02 – V 3.0.

Infraestrutura de Chaves Públicas Brasileira.