Infraestrutura de Chaves Públicas Brasileira

MAPA DE PROCESSOS IDENTIFICADOS NA ICP-BRASIL

ADE-ICP - 08.E
Versão 4.1

Posição em 04.08.2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Motivação
04/08/2021 Versão 4.1	Inclusão e atualização de controles relativos à identificação por videoconferência, atualização dos controles relativos aos PSBios, atualização de controles relativos ao Sistema de Carimbos do Tempo na ICP-Brasil e atualizações motivadas pelo Decreto nº 10.139, de 28 de novembro de 2019.
14/10/2019 Versão 4.0	Inclusão de processos relativos às Autoridades de Carimbo do Tempo – ACTs e Prestadores de Serviço de Confiança – PSCs. Atualização de controles motivada pela Resolução nº 151, de 30 de maio de 2019.
15/03/2017 Versão 3.0	Inclusão de processos e atualização de controles relativos aos Prestadores de Serviço Biométrico – PSBios, sincronização com a Fonte Confiável do Tempo – FCT e certificados do tipo A CF e-SAT.
01/09/2016 Versão 2.0	Inclusão da identificação numérica dos controles e da referência normativa correspondente, citando o DOC-ICP e o respectivo item.
18/11/2009 Versão 1.0	Criação documento pela Instrução Normativa nº 07, de 18 de novembro de 2009.

1 Os processos nas ACs– Autoridades Certificadoras estão assim distribuídos:

1.1 Manter credenciamento de AC, composto pelos subprocessos:

1.1.1 Manter requisitos de manutenção de credenciamento

10101001	Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 do DOC-ICP-03.	DOC-ICP-03, item 2.1.
10101002	A AC deve comunicar, desde logo, à AC-Raiz e à AC a que está subordinada qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores.	DOC-ICP-03, item 3.1.a.i.
10101003	A AC deve comunicar, desde logo, à AC-Raiz e à AC a que está subordinada o indício ou fraude comprovada na emissão de certificado por requerente que apresente documento ou informação falsa, no dia útil imediatamente subsequente à confirmação do ato, na forma estabelecida no ADE-ICP-03.H.	DOC-ICP-03, item 3.1.a.iv.
10101004	A entidade credenciada para desenvolver as atividades de AC deverá manter os titulares dos certificados informados acerca de eventual sucessão de AC ou AR operacionalmente vinculadas.	DOC-ICP-03, item 3.1.c.
10101005	A entidade credenciada para desenvolver as atividades de AC deverá encaminhar à AC Raiz, dentro do prazo estabelecido no Plano Anual de Auditoria Operacional, definido no DOC-ICP-08, cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculadas.	DOC-ICP-03, item 3.1.d.
10101006	Todas as Autoridades Certificadoras (AC) que emitem certificados digitais para usuário final deverão enviar semanalmente ao Instituto Nacional de Tecnologia da Informação – ITI, toda segunda-feira da semana seguinte à respectiva emissão, os certificados emitidos, as biometrias atreladas a cada certificado e informações sobre suas emissões.	Instrução Normativa nº 05/2019, Art. 1º.
10101007	A entidade credenciada para desenvolver as atividades de AC deve manter a conformidade com suas respectivas DPC, PCs, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust.*	DOC-ICP-05, item 8.4.1.
10101008	Caso ocorra uma ou mais das hipóteses previstas no item 4.1.2 do DOC-ICP-03, a AC deve ser descredenciada.	DOC-ICP-03, item 4.1.2.

1.1.2 Manter condições fisco-tributárias e econômico-financeiras

10102001	A AC deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.	DOC-ICP-03, Anexo I, item 2.
10102002	A AC deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos à sua qualificação econômico-financeira: a)Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente. b)Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.	DOC-ICP-03, item 2.1.c e Anexo I, item 3.

1.1.3 Manter contrato de seguro

10103001	A AC deve manter contrato de seguro de cobertura de responsabilidade civil vigente decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo.	DOC-ICP-05, item 4.1.2.2.t.

1.1.4 Manter histórico de agentes de registro

10104001	A AR deve enviar à AC a relação atualizada dos Agentes de Registro em atividade, seus perfis qualificados e suas necessidades de acesso a informações do gerenciamento de ciclo de vida dos certificados. A AC deve manter essa informação atualizada, organizada e consolidada, inclusive com o histórico das alterações realizadas, à disposição do ITI	DOC-ICP-03.01, item 2.1.3.

	para os procedimentos de auditoria e fiscalização.	
10104002	As ACs ou seus respectivos PSSs devem encaminhar semanalmente ao ITI seus arquivos de manutenção do Cadastro de Agentes de Registro.	Instrução Normativa nº 11/2020, item 4 do anexo.
10104003	As ACs deverão manter acesso em seus sistemas de emissão de certificado digitais (Sistema de AR) somente dos agentes de registros relacionados na lista disponibilizada no sítio do ITI, devendo revogar os acessos daqueles agentes de registro que deixarem de figurar na relação.	Instrução Normativa 11/2020, Art. 5º.

1.1.5 Manter e cumprir Política de Segurança – PS de AC

10105001	Todos os empregados devem possuir conhecimento da Política de Segurança – PS da AC que a deve divulgar.	DOC-ICP-02, item 6.1.2.
10105002	Os empregados, as chefias e os prestadores de serviços devem conhecer os deveres e as responsabilidades definidos na PS.	DOC-ICP-02, item 7.4.1 a 7.4.5.
10105003	A AC responsável tornará disponível para todo o seu pessoal e para o pessoal das ARs vinculadas, pelo menos: a) Sua DPC; b) As PCs que implementa; c) A PS; d) Documentação operacional relativa a suas atividades; e e) Contratos, normas e políticas relevantes para suas atividades.	DOC-ICP-05, item 5.3.8.1.

1.1.6 Comunicar mudanças operacionais e violação de normas

10106001	A AC deve comunicar formalmente e imediatamente as mudanças operacionais ocorridas em seu ambiente de certificação e qualquer violação de normas da ICP-Brasil.	DOC-ICP-03, item 3.1.a.
10106002	Para encaminhar os dados biométricos de um suposto fraudador, as ACs farão uso do procedimento previsto no item 3.1 do DOC-ICP-05.02.	DOC-ICP-05.03, item 2.6.5.

1.1.7 Regularizar não conformidades identificadas

10107001	A entidade auditada deve cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não conformidades	DOC-ICP-08, item 9.1.

	com a legislação ou com as políticas, normas, práticas e regras estabelecidas.	

1.2 Credenciar e manter entidades operacionalmente vinculadas, composto pelos subprocessos:

1.2.1 Auditar entidades operacionalmente vinculadas

10201001	Deverão ser realizadas auditorias nas entidades integrantes da ICP-Brasil conforme frequência estabelecida no DOC-ICP-08 em todas as entidades operacionalmente vinculadas à AC sob avaliação.	DOC-ICP-02, item 11.3.
10201002	As ACs devem encaminhar à AC RAIZ, no prazo estabelecido no Plano Anual de Auditoria Operacional, definido no documento CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL– DOC-ICP-08, cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculadas.	DOC-ICP-03, item 3.1.d.
10201003	As ACs devem encaminhar à AC RAIZ relatórios de auditorias realizadas nas entidades que lhe sejam operacionalmente vinculadas até 30 (trinta) dias após sua conclusão.	DOC-ICP-03, item 3.1.e.
10201004	A equipe de auditoria contratada pela AC para realizar auditoria em seu âmbito ou cadeia deve ser totalmente independente da entidade auditada, aplicando-se no que couber, as regras de suspeição e impedimentos estabelecidas nos artigos 134 e 135 do Código de Processo Civil.	DOC-ICP-08, item 7.1.
10201005	Os auditores contratados pela AC para realizar auditoria em seu âmbito devem firmar declaração, sob as penas da lei, de que não se enquadram em quaisquer das causas de impedimento tratadas no DOC-ICP-08.	DOC-ICP-08, item 7.3.
10201006	As fiscalizações e auditorias devem verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust.*	DOC-ICP-05, item 8.4.1.
10201007	Os serviços de auditoria devem ser executados diretamente pela entidade de auditoria credenciada junto à ICP-Brasil, vedada a subcontratação total ou parcial de serviços.	DOC-ICP-08, item 6.1.6.

1.2.2 Observar procedimentos de extinção de entidades operacionalmente vinculadas

10202001	As ACs devem comunicar à AC RAIZ, por intermédio da cadeia de hierarquia, a desvinculação de AC, de PSBio, AR ou PSS credenciado sob sua responsabilidade.	DOC-ICP-03, item 3.1.a.ii.
10202002	Caso ocorra uma ou mais das hipóteses previstas no item 4 do DOC-ICP-03, para encerramento de AC, AR ou PSS vinculado, as ACs devem proceder o descredenciamento, conforme o caso, da AC, AR ou PSS vinculado.	DOC-ICP-03, item 4.1.1.
10202003	Nos descredenciamentos de AC, AR e PSS, as ACs às quais se vinculam devem executar os procedimentos previstos no item 4 da DOC-ICP-03.	DOC-ICP-03, itens 4.1, 4.2 e 4.4.
10202004	As ACs devem executar os procedimentos descritos em suas DPC em relação ao disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, que trata da notificação aos usuários, transferência de guarda de seus dados e registros de arquivos quando da extinção ou encerramento dos serviços da AC responsável, de uma AR, PSS ou PSBio a ela vinculados.	DOC-ICP-05, item 4.11.

1.2.3 Observar procedimentos de credenciamento de entidades operacionalmente vinculadas

10203001	As ACs devem observar os critérios a serem atendidos pelos candidatos a credenciamento na ICP-Brasil sob sua vinculação.	DOC-ICP-03, itens 2.1, 2.1.1, 2.1.2, 2.1.4 e 2.1.5.
10203002	O pedido inicial de credenciamento deverá ser encaminhado à AC Raiz por intermédio da cadeia de certificação à qual a candidata ao credenciamento se encontrar operacionalmente vinculada, inciando-se a tramitação pela AC, ou candidato a AC de nível imediatamente superior à interessada e, a partir daí, respeitando-se a hierarquia da cadeia, até chegar à AC Raiz.	DOC-ICP-03, item 2.2.1.2.

1.2.4 Manter credenciamento de entidades operacionalmente vinculadas

10204001	Qualquer alteração em atos constitutivos, estatuto, contrato social ou	DOC-ICP-03,

	administradores seus ou de seus vinculados; desvinculação de AC, de PSBio, de AR ou de PSS credenciados; ou ainda violação das diretrizes e normas técnicas da ICP-Brasil cometidas pela própria ou pelas ACs, ARs ou PSSs, PSBios ou PSCs que lhe sejam operacionalmente vinculados devem ser comunicadas ao ITI.	itens 3.1.a.i, 3.1.a.ii, 3.1.a.iii, 3.1.b, 3.2.1.a e 3.2.1.b.
10204002	Em caso de alteração de endereço da AR, o fato deve ser previamente reportado à AC responsável, que enviará ao ITI formulário de credenciamento ADE-ICP-03B com os dados atualizados.	DOC-ICP-03.01, item 1.7.
10204003	O PSS deve observar a DPC, as PCs e a PS da AC, ou a DPCT, a PCT e PS da ACT ou a DPPSC e PS do PSC a que estiver vinculado.	DOC-ICP-03, item 3.4.b.
10204004	A AC responde solidariamente pelos atos das entidades de sua cadeia de certificação: ACs subordinadas, AR e PSS.	DOC-ICP-05, item 4.1.2.1.2.

1.3 Executar fases do ciclo de vida de certificados digitais, composto pelos subprocessos:

1.3.1 Registrar solicitação

10301001	Os certificados admitidos no âmbito da ICP-Brasil devem manter conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.	DOC-ICP-04 item 7.1.
10301002	O padrão de formato para solicitação de certificados às ACs emitentes deve ser PKCS#10.	DOC-ICP-01.01 item 2.
10301003	A solicitação de geração de novo par de chaves antes da expiração do atual, quando por meio eletrônico, só é permitida para titulares pessoa física, limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular.	DOC-ICP-05, item 3.3.2.b.
10301004	A solicitação por meio eletrônico de geração de novo par de chaves para pessoas físicas deve ser assinada digitalmente com o uso de certificado vigente de, pelo menos, mesmo nível de segurança.	DOC-ICP-05, item 3.3.2.
10301005	A solicitação de revogação de certificados digitais deve ser efetuada somente por pessoa autorizada.	DOC-ICP-05 item 4.9.2.
10301006	As circunstâncias para solicitação de revogação devem ser somente as previstas nas normas.	DOC-ICP-05 item 4.9.1.
10301007	O solicitante da revogação de um certificado deve ser identificado.	DOC-ICP-05

		item 4.9.3.2.a.
10301008	A solicitação de revogação de certificado deve conter justificativa documentada e armazenada.	DOC-ICP-05 item 4.9.3.2.b e 4.9.3.2.c.
10301009	Na solicitação por meio eletrônico de geração de novo par de chaves para pessoas físicas assinada digitalmente com o uso de certificado do tipo A1 a confirmação do respectivo cadastro deve ser realizada por meio de videoconferência.	DOC-ICP-05, item 3.3.2.d.

1.3.2 Tratar validação

10302001	Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3.	DOC-ICP-05 item 3.2.8.2.
10302002	A confirmação da identidade de um indivíduo deverá ser realizada mediante a presença física ou por meio de videoconferência, do interessado, com base em documentos de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.	DOC-ICP-05 item 3.2.3.
10302003	Na autenticação da identidade de um indivíduo, os documentos digitais de que trata o item 3.2.3.1 do DOC ICP-05 deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado.	DOC-ICP-05 item 3.2.3.1.2.
10302004	Na autenticação da identidade de um indivíduo, os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados por agente de registro distinto do que realizou a etapa de identificação.	DOC-ICP-05 item 3.2.3.1.3.a.
10302005	Para identificação de um indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto no item 3.2.9.3 do DOC-ICP-05.	DOC-ICP-05 item 3.2.3.1.5.
10302006	O sistema de certificação da AC deve registrar eletronicamente em arquivo de auditoria todos os eventos relacionados a validação e aprovação das solicitações de certificados, bem como as solicitações de revogação.	DOC-ICP-05 item 5.4.1.6.

10302007	Na DPC deverão ser detalhados a forma, os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados digitais.	DOC-ICP-05 item 3.2.
10302008	Na DPC devem ser definidos os procedimentos empregados pelas AR vinculadas a uma AC para a identificação e cadastramento iniciais de um indivíduo na ICP-Brasil.	DOC-ICP-05 item 3.2.3.
10302009	A DPC deve estabelecer os processos de identificação e confirmação do cadastro do solicitante utilizados na geração de um certificado.	DOC-ICP-05 item 3.3.1.
10302010	A identificação por meio de videoconferência deve assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.	DOC-ICP-05 item 3.2.3.
10302011	Para certificados de equipamento ou aplicação que utilizem URL, a AC poderá implementar mecanismos automatizado de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e a identificação do solicitante, seja pessoa física ou jurídica.	DOC-ICP-05 item 3.2.2.1.

1.3.3 Processar solicitação de certificado

10303001	O acesso ao aplicativo que faz interface entre a AR e o sistema de certificação da AC só será permitido mediante a autenticação por meio de certificado digital do tipo A3 de agente de registro formalmente autorizado por autoridade competente.	DOC-ICP-03.01 item 4.2.1.a.
10303002	O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve permitir acesso somente a partir de equipamentos autenticados.	DOC-ICP-03.01 item 4.2.1.b.
10303003	O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve possuir mecanismo de *timeout* de sessão de acordo com a análise de risco da AC	DOC-ICP-03.01 item 4.2.1.c.
10303004	A AR deve encaminhar as solicitações de emissão ou de revogação de certificados à AC utilizando VPN, SSL ou outra tecnologia de igual ou superior nível de segurança.	DOC-ICP-03.01 item 5.

1.3.4 Emitir certificados

10304001	O padrão de formato para entrega de certificados emitidos pela AC deve ser o PKCS#7.	DOC-ICP-01.01, item 2.
10304002	O algoritmo criptográfico e tamanho das chaves para geração de chaves assimétricas de AC devem seguir o previsto no DOC-ICP-01-01, item 2.	DOC-ICP-01.01, item 2.
10304003	O algoritmo criptográfico e tamanho das chaves para geração de chaves assimétricas de usuário final devem seguir o previsto no DOC-ICP-01-01, item 2.	DOC-ICP-01.01, item 2.
10304004	O algoritmo criptográfico para assinatura de certificado de AC deve seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.
10304005	O algoritmo criptográfico para assinatura de certificado de usuário final deve seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.
10304006	O algoritmo simétrico para guarda da chave privada da entidade titular e de seu *backup* deve seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.
10304007	O módulo criptográfico de geração e armazenamento de chaves assimétricas de usuário final deve atender ao padrão previsto no DOC-ICP-01.01, item 3.	DOC-ICP-01.01, item 3.
10304008	O módulo criptográfico de geração e armazenamento de chaves assimétricas de AC deve atender ao padrão previsto no DOC-ICP-01.01, item 3.	DOC-ICP-01.01, item 3.
10304009	A chave privada da AC deve trafegar cifrada entre o dispositivo gerador e a mídia utilizada para seu armazenamento.	DOC-ICP-04, item 6.1.1.5.
10304010	As mídias armazenadoras de chaves criptográficas devem atender aos requisitos mínimos de acordo com o tipo de certificado, conforme tabela 4 referenciada no item 6.1.1.4 do DOC-ICP-04.	DOC-ICP-04, item 6.1.1.4
10304011	A chave privada da AC deve ser utilizada apenas para assinatura de certificados por ela emitidos e de sua LCR.	DOC-ICP-05, item 6.1.7.2.
10304012	A extensão "*Key Usage*", deve ser configurada conforme o disposto no item 7.1.2.7 do DOC-ICP-04.	DOC-ICP-04, item 7.1.2.2.b.
10304013	Propósito de uso em certificados de sigilo podem ter somente os bits de "*keyEncipherment*" e "*dataEncipherment*" ativados, sendo os restantes	DOC-ICP-04, item 7.1.2.7.g.

	obrigatoriamente desativados.	
10304014	As Políticas de Certificado deve identificar quem é o agente de recuperação (*escrow*), qual forma que a chave é recuperada (por exemplo, inclui o texto em claro, encriptado, por divisão de chaves) e quais são os controles de segurança do sistema de recuperação.	DOC-ICP-04, item 6.2.3.
10304015	A AC não deve manter cópia de segurança (*backup*) de chave privada de titular de certificado de assinatura digital por ela emitido. Salvo nos casos em que esta é credenciada como PSC.	DOC-ICP-04, item 6.2.4.2.
10304016	Cópia de segurança de chave privada, em qualquer caso, deve ser protegida com um nível de segurança não inferior àquele definido para a chave original.	DOC-ICP-04, item 6.2.4.3.
10304017	O arquivamento de chave privada na AC, quando for o caso, deve ser condizente com o especificado em sua respectiva Política de Certificado.	DOC-ICP-04, item 6.2.5.
10304018	As ACs emissoras de certificados de assinatura digital e LCR devem armazenar permanentemente as chaves públicas e as LCR para uso futuro.	DOC-ICP-04, item 6.3.1.
10304019	As ACs não devem emitir certificados com validade superior ao período máximo definido na ICP-Brasil.	DOC-ICP-04, item 6.3.2.3.
10304020	Os certificados emitidos pela AC deve implementar a versão 3 definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.	DOC-ICP-04 item 7.1.1.
10304021	Os certificados ICP-Brasil emitidos para usuários finais devem contemplar as extensões de certificados definidas como obrigatórias.	DOC-ICP-04 item 7.1.2.
10304022	Em certificados ICP-Brasil, o nome do titular do certificado, constante do campo *Subject*, deve adotar o *Distinguished Name* (DN) do padrão ITU X.500/ISO 9594.	DOC-ICP-04 item 7.1.4.
10304023	Chaves privadas de AC devem trafegar cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.	DOC-ICP-05 item 6.2.
10304024	O controle múltiplo ("n" de "m") para utilização da chave privada da AC deve requerer pelo menos 2 (dois) detentores de partição de chave formalmente designados.	DOC-ICP-05 item 6.2.2.
10304025	A AC deve manter cópia de segurança de sua própria chave privada com armazenamento cifrado, protegido e nível de segurança não inferior àquele definido para a chave original.	DOC-ICP-05 item 6.2.4.2 e 6.2.4.4.
10304026	O arquivamento das chaves privadas de sigilo, quando cabível, devem	DOC-ICP-05,

	manter o nível de segurança não inferior àquele definido para a chave original. Não devem ser arquivadas chaves privadas de assinatura digital.	item 6.2.5.1.
10304027	O método de ativação e desativação de chave privada da AC deve atender ao estabelecido em sua respectiva DPC.	DOC-ICP-05, itens 6.2.8 e 6.2.9.
10304028	Os certificados ICP-Brasil de AC devem contemplar as extensões de certificados definidas como obrigatórias.	DOC-ICP-05 item 7.1.2.
10304029	Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.	DOC-ICP-04, item 1.1.8.
10304030	A DPC deve especificar os propósitos para os quais poderão ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC responsável, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes. Cada PC implementada deve especificar os propósitos específicos aplicáveis.	DOC-ICP-05, item 6.1.7.1.
10304031	Com exceção das chaves privadas vinculadas a certificados do tipo A CF-e-SAT, OM-BR, T3 e T4, que não podem possuir cópia de segurança, qualquer titular de certificado dos demais tipos poderá, a seu critério, manter cópia de segurança de sua própria chave privada.	DOC-ICP-04, item 6.2.4.1.
10304032	O algoritmo criptográfico para assinatura de pedidos e respostas de carimbo do tempo devem seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.
10304033	A função *hash* para assinatura de pedidos e respostas de carimbo do tempo devem seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.
10304034	Nos certificados de equipamento de carimbo do Tempo de ACT (T3 e T4) credenciada na ICP-Brasil é obrigatória a utilização da seguinte extensão: “Key Usage”, crítica: somente os bits digitalSignature e nonRepudiation devem estar ativado; “*Extended Key Usage*", crítica: deve conter somente o propósito *timeStamping* com OID 1.3.6.1.5.5.7.3.8. Esse OID não deve ser empregado em qualquer outro tipo de certificado.	DOC-ICP-04, item 7.1.2.7c.
10304035	A AC/PSS deve manter em base de dados a relação entre dados biográficos dos requerentes de certificados digitais e seus respectivos IDNs (Identificador de Registro Biométrico).	DOC-ICP-05.03, item 2.5.1.

10304036	A AC/PSS deve manter as imagens das biometrias coletadas (impressão digital e face) em arquivo.	DOC-ICP-05.03, item 2.5.3.
10304037	A AC/PSS deve garantir a segregação entre dados biográficos e dados biométricos, além de tratar adequadamente a segurança contra acesso e divulgação não autorizadas.	DOC-ICP-05.03, item 2.5.2.
10304038	É vedado o uso de nomes nos certificados que violem os direitos de propriedade intelectual de terceiros.	DOC-ICP-05 item 3.1.4.2.

1.3.5 Emitir LCR

10305001	A frequência para emissão de LCR deve atender ao estabelecido em sua respectiva DPC, não podendo ultrapassar 6 (seis) horas para certificados de usuários finais, 45 (quarenta e cinco) dias para certificados de AC e no máximo 90 (noventa) dias para certificados da AC-RAIZ.	DOC-ICP-05 itens 4.9.7.2 e 4.9.7.3 DOC-ICP-01, item 4.4.7.
10305002	A LCR gerada pela AC deve implementar a versão 2 do padrão ITU X.509, de acordo com o estabelecido na RFC 5280.	DOC-ICP-05, item 7.2.1.
10305003	As ACs que disponibilizam verificação da situação de certificado por meio do protocolo OCSP (*On-line Certificate Status Protocol*) devem manter conformidade com o padrão estabelecido.	DOC-ICP-05, item 4.9.9.
10305004	Antes de publicadas, todas as LCRs geradas pela AC devem ser checadas quanto à consistência de seu conteúdo.	DOC-ICP-05, item 6.6.4.
10305005	O algoritmo criptográfico para assinatura de Listas de Certificado Revogados e Respostas OCSP devem seguir o previsto no DOC-ICP-01.01, item 2.	DOC-ICP-01.01, item 2.

1.3.6 Tratar revogação

10306001	Certificados digitais devem ser revogados quando caracterizadas as circunstâncias definidas no item 4.9.1 do DOC-ICP-05.	DOC-ICP-05, item 4.9.1.
10306002	O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previsto pela ICP-Brasil é de 24 (vinte e quatro) horas.	DOC-ICP-05, item 4.9.3.3.

10306003	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. Nessa situação, a entidade deverá seguir os procedimentos detalhados na sua DPC.	DOC-ICP-02, item 6.4.3.
10306004	Solicitações de revogação de certificados devem ser registradas.	DOC-ICP-05, item 3.4.

1.3.7 Gerenciar IDN

10307001	É proibida a divulgação da chave simétrica, sendo que essa deve estar armazenada, com propriedade de não exportável, dentro dos HSM de cada AC recebedora da mesma.	DOC-ICP-05.03, item 1.3.2.
10307002	O IDN (Identificador de Registro Biométrico) será gerado a partir do CPF da pessoa física, de forma a não existir dois IDNs para um mesmo CPF e nem tão pouco dois CPFs com mesmo IDN. Em hipótese alguma, uma AC/PSS deve transmitir a chave gerada para o PSBio contratado.	DOC-ICP-05.03, item 1.4.1.
10307003	A geração do IDN utilizará criptografia simétrica com chave armazenada em HSM e deverá seguir a forma definida no DOC-ICP-05.04.	DOC-ICP-05.03, item 1.4.2 e item 1.4.4.
10307004	A AC responsável pelo registro/IDN, ao receber uma notificação de irregularidade deve repassá-la ao seu PSBio. Nesta situação, o IDN deve ser removido da base biométrica de produção e os procedimentos de fraude devem ser realizados conforme DOC-ICP-05.02.	DOC-ICP-05.03, item 2.6.6.
10307005	É responsabilidade da AC que gerou um cadastro (IDN) a análise e resolução de notificações de exceção (conflitos biométricos identificados pela Rede PSBio) relacionada àquele cadastro.	DOC-ICP-05.03, item 2.6.2.
10307006	O procedimento de substituição da chave criptográfica simétrica, incluindo a indexação dos IDNs recalculados, deve ser executado num prazo máximo de 15 (quinze) dias, de maneira sincronizada entre as entidades e PSBios, de forma a não causar indisponibilidades no sistema.	DOC-ICP-05.04, item 4.
10307007	Após a reindexação das bases de dados, os PSBios deverão excluir permanentemente qualquer informação indexada pelo IDN gerado a partir da chave criptográfica simétrica anterior, devendo as entidades manter em seus registros a associação entre IDN antigo e o novo.	DOC-ICP-05.04, item 4.

10307008	As exceções (suspeitas de irregularidades e duplicidades dos registros) devem ser prontamente comunicadas para as entidades biométricas credenciadas, se for o caso, disponibilizando essas informações para a AC que solicitou o cadastramento, para os devidos encaminhamentos.	DOC-ICP-05.03, item 3.5.2.

1.4 Manter Publicação, composto pelos subprocessos:

1.4.1 Manter DPC, PC e PS

10401001	As alterações nas DPC, PC e PS devem ser autorizadas pela AC RAIZ.	DOC-ICP-03, item 3.1.b; DOC-ICP-04, item 9.12.1; DOC-ICP-05, item 9.12.1.
10401002	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve observar requisitos e estrutura do DOC-ICP-04/DOC-ICP-05 (RFC 2527)	DOC-ICP-04, item 1.1.2; DOC-ICP-05, item 1.1.2.
10401003	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 1.2 o tipo de certificado, o nome da instituição e o OID atribuído para a respectiva PC ou DPC, conforme o caso.	DOC-ICP-05, item 1.2, DOC-ICP-04, item 1.2.
10401004	Toda PC e DP C elaborada no âmbito da ICP-Brasil deve indicar no item 1.3 informações das entidades envolvidas e no item 1.4 a usabilidade do certificado.	DOC-ICP-05, item 1.3 e item 1.4, DOC-ICP-04, item 1.3 e item 1.4.
10401005	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 6.1 a descrição dos requisitos e os procedimentos para geração e instalação do par de chaves referentes ao certificado que define.	DOC-ICP-05, item 6.1, DOC-ICP-04 item 6.1.
10401006	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 7 a descrição de perfis do certificado que define.	DOC-ICP-05, item 7,

		DOC-ICP-04 item 7.
10401007	Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 4.1.2 as obrigações gerais conforme estabelecido no DOC-ICP-05.	DOC-ICP-05, item 4.1.2.
10401008	Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 3 os requisitos de identificação e autenticação.	DOC-ICP-05, item 3.
10401009	Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 4 os requisitos operacionais do ciclo de vida do certificado.	DOC-ICP-05, item 4.
10401010	Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 5 os controles operacionais, de gerenciamento e de instalações.	DOC-ICP-05, item 5.
10401011	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 6 os Controles Técnicos de Segurança.	DOC-ICP-05, item 6, DOC-ICP-04, item 6.
10401012	Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 7 os perfis de certificados, LCR e OCSP.	DOC-ICP-04, item 7, DOC-ICP-05, item 7.
10401013	A PC deve descrever todos os requisitos e procedimentos aplicáveis ao processo de geração de uma cópia de segurança da chave privada de um certificado.	DOC-ICP-04, item 6.2.4.4.

1.4.2 Manter Repositório

10402001	As informações a serem publicadas pela AC responsável pela DPC devem estar disponíveis, no mínimo, por 99,5% do mês, 24 horas por dia, 7 dias por semana.	DOC-ICP-05, item 2.2.1.
10402002	A AC deve manter em seu repositório, localizado no endereço da página web indicado na sua DPC, as informações descritas no item 2.2.2 do DOC-ICP-05.	DOC-ICP-05, item 2.2.2.

1.4.3 Manter publicação de LCR

10403001	A frequência de publicação de LCR e certificado da AC deve assegurar a	DOC-ICP-05,

	disponibilização sempre atualizada de seus conteúdos.	item 2.3.
10403002	A AC deve implementar recursos necessários para a segurança dos dados armazenados em seus respectivos repositórios.	DOC-ICP-05, itens 2.4.

1.5 Manter sítio de contingência, composto pelos subprocessos:

1.5.1 Manter integridade dos dados

10501001	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.	DOC-ICP-02 item 10.3.1.
10501002	Recurso de VPN (*Virtual Private Networks* - redes privadas virtuais), baseada em criptografia, para troca de informações sensíveis, por meio de redes públicas, deve ser adotada para a troca de informações entre o sítio principal e o sítio de contingência	DOC-ICP-02 item 10.3.2.
10501003	Uma segunda cópia de todo o material arquivado deverá ser armazenada em local externo à AC responsável, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.	DOC-ICP-05 item 5.5.4.1.
10501004	A AC deve verificar a integridade das cópias de segurança armazenadas no sítio de contingência, no mínimo, a cada 6 (seis) meses.	DOC-ICP-05 item 5.5.4.3.

1.5.2 Ativar sítio de contingência

10502001	A instalação de *backup* (sítio de contingência) deve entrar em operação em condições idênticas ao principal em no máximo 48 (quarenta e oito) horas quando ocorrer sinistro que torne inoperante a instalação principal.	DOC-ICP-05 item 5.1.8.
10502002	Os procedimentos de ativação do sítio de contingência devem ser regularmente testados, de modo a garantir a disponibilidade.	DOC-ICP-02 item 9.3.2.9.

1.5.3 Ativar retorno ao sítio principal

10503001	Os procedimentos de retorno do sítio de contingência para o sítio principal devem ser regularmente testados, de modo a garantir a disponibilidade.	DOC-ICP-02 item 9.3.2.9.

10503002	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.	DOC-ICP-02 item 9.2.4.

1.5.4 Manter infraestrutura

10504001	Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.	DOC-ICP-02 item 13.2.1.
10504002	Os controles estabelecidos no processo “Manter Infraestrutura" devem ser aplicados sob o contexto do sítio de contingência, para que opere em condições idênticas as instalações principais.	DOC-ICP-05 item 5.1.8.

1.5.5 Manter segurança lógica

10505001	Os controles estabelecidos no processo “Manter Segurança Lógica" devem ser aplicados sob o contexto do sítio de contingência.	DOC-ICP-05 item 5.1.8.

1.6 Manter segurança da informação, composto pelos subprocessos:

1.6.1 Manter inventário de ativos

10601001	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
10601002	O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.	DOC-ICP-02, item 8.2.12 e 9.3.5.10.
10601003	O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.	DOC-ICP-02, item 9.2.5.

1.6.2 Manter análise de risco e Plano de Continuidade do Negócio - PCN

10602001	Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.	DOC-ICP-02, item 6.4.1.
10602002	Todas as AC devem apresentar Plano de Recuperação de Desastre e Plano de Resposta a Incidentes a serem aprovados pela AC Raiz ou AC de nível imediatamente superior.	DOC-ICP-02, item 6.4.2 e 13.2.2.
10602003	Todos os incidentes devem ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.	DOC-ICP-02, item 6.4.4.
10602004	Todos os ativos de processamento das entidades devem estar relacionados no PCN.	DOC-ICP-02, item 7.4.3.c.
10602005	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.	DOC-ICP-02, item 13.2.3.
10602006	A AC responsável deve descrever os procedimentos de notificação e recuperação a serem utilizados nos seguintes casos: a) quando os recursos computacionais, *software* ou dados estiverem corrompidos ou houver suspeita de corrupção; b) na circunstância de revogação de certificados; c) na circunstância de comprometimento da chave privada da AC responsável; d) após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.	DOC-ICP-05, item 5.7.2 a 5.7.4.
10602007	Em um processo de gerenciamento de riscos, que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, os seguintes pontos principais devem ser identificados: a) o que deve ser protegido; b) a análise de riscos (contra quem ou contra o quê deve ser protegido); c) avaliação de riscos (análise da relação custo/benefício).	DOC-ICP-02, item 12.1.
10602008	A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: a) requisitos de segurança definidos pelo serviço; b) objetivo do serviço, público-alvo; c) classificação da informação; d) forma de acesso; e) frequência de atualização do conteúdo; f) forma de administração do serviço e volume de tráfego.	DOC-ICP-02, item 9.3.3.23.

10602009	O processo de gerenciamento de riscos deve ser revisto anualmente pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.	DOC-ICP-02, item 6.2.

1.6.3 Manter documentos armazenados e classificados

10603001	Toda a documentação fornecida ao pessoal deve estar classificada segundo a política de classificação de informação definida pela AC e deve ser mantida atualizada.	DOC-ICP-05, item 5.3.8.2.
10603002	A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.	DOC-ICP-02, item 9.2.1.
10603003	Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.	DOC-ICP-05, item 9.4.2.
10603004	Os registros devem ser protegidos e armazenados de acordo com a sua classificação, conforme a PS da ICP-Brasil.	DOC-ICP-05, item 5.5.3.
10603005	Os dossiês dos titulares devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado.	DOC-ICP-05, item 5.5.2.b.
10603006	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.	DOC-ICP-02, item 9.3.5.9.
10603007	As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias.	DOC-ICP-05, item 5.5.4.2.
10603008	Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs da ICP-BRASIL.	DOC-ICP-05, item 3.2.8.3.
10603009	As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica.	DOC-ICP-05, item 5.5.2.a.
10603010	No caso de certificados A CF-e-SAT ou OM-BR deve ser mantida toda a documentação eletrônica utilizada no processo de validação e confirmação da identificação do equipamento SAT ou objeto metrológico acreditado	DOC-ICP-05, item 3.2.8.3.1.

	pelo INMETRO, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL.	
10603011	As demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.	DOC-ICP-05, item 5.5.2.c.

1.7 Manter sistemas aplicativos, composto pelos subprocessos

1.7.1 Manter sistemas de informação

10701001	As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.	DOC-ICP-02 item 9.3.1.1.
10701002	A documentação dos sistemas deve ser mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
10701003	A cópia de segurança deve ser testada e mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
10701004	Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.	DOC-ICP-02 item 9.3.1.5.
10701005	As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.	DOC-ICP-02 item 9.3.1.5.
10701006	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.5.11.
10701007	A coleta de dados biométricos é de responsabilidade da AC/PSS e de sua rede de Autoridades de Registro.	DOC-ICP-05.03, item 2.2.
10701008	Todos os arquivos gerados pelas coletas das biometrias devem conter trilha de auditoria em relação a data, horário e local da coleta e o registro do equipamento de coleta, conforme DOC-ICP-05.	DOC-ICP-05.03, item 2.3.

1.7.2 Manter sistema de AC

10702001	O aplicativo que faz a interface entre a AR e AC deve possuir registro em *log* de auditoria dos eventos citados no item 5.4.1 do DOC-ICP-05.	DOC-ICP-03.01 item 4.2.1.d.
10702002	O aplicativo que faz a interface entre a AR e AC deve possuir histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões	DOC-ICP-03.01 item 4.2.1.e.

	concedidas ou revogadas	
10702003	O aplicativo que faz a interface entre a AR e AC deve possuir mecanismo para revogação automática dos certificados digitais.	DOC-ICP-03.01 item 4.2.1.f.
10702004	Para atendimento do previsto noDOC-ICP-05 para Geração e Instalação do Par de Chaves, esse aplicativo deve: a) ter sido desenvolvido com documentação formal; b) ter mecanismos para controle de versões; c) ter documentação dos testes realizados em cada versão; d) ter documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si; e) ter aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção.	DOC-ICP-03.01 item 4.2.2.
10702005	A AR deve encaminhar as solicitações de emissão ou de revogação de certificados à AC utilizando VPN (*Virtual Private Network* - Rede Privativa Virtual), SSL (*Secure Socket Layer* - Protocolo de Comunicação Seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.	DOC-ICP-03.01 item 5.
10702006	Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.	DOC-ICP-02 item 10.2.3.
10702007	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.4.13.
10702008	A DPC deve observar que quando um evento for registrado pelo conjunto de sistemas de auditoria da AC responsável, nenhuma notificação deverá ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.	DOC-ICP-05 item 5.4.7.
10702009	A AC, quando cabível, deve definir a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”, requerido para a utilização das chaves privadas. A DPC deve estabelecer a exigência de controle múltiplo para a utilização da chave privada da AC responsável. Pelo menos 2 (dois) detentores de partição de chave, formalmente designados pela AC, deverão ser requeridos para a utilização de sua chave privada.	DOC-ICP-05 item 6.2.2.
10702010	Os dados de ativação da chave privada da AC responsável serão únicos e aleatórios.	DOC-ICP-05, item 6.4.1.1.
10702011	Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.	DOC-ICP-05, item 6.4.1.2.

10702012	A geração do par de chaves da AC responsável será realizada *off-line*, para impedir acesso remoto não autorizado.	DOC-ICP-05, item 6.5.1.1.
10702013	Cada computador servidor da AC responsável, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, deverá implementar, entre outras, as seguintes características: a) controle de acesso aos serviços e perfis da AC; b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC; c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações; d) geração e armazenamento de registros de auditoria da AC; e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e f) mecanismos para cópias de segurança (*backup*).	DOC-ICP-05, item 6.5.1.3.
10702014	Os processos de projeto e desenvolvimento conduzidos pela AC deverão prover documentação suficiente para suportar avaliações externas de segurança dos componentes da AC.	DOC-ICP-05, item 6.6.1.2.
10702015	Devem ser descritas na DPC as ferramentas e os procedimentos empregados pela AC responsável e pelas ARs vinculadas para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.	DOC-ICP-05, item 6.6.2.1.
10702016	Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação e a contínua manutenção do sistema de certificação da AC.	DOC-ICP-05, item 6.6.2.2.

1.7.3 Manter bases de dados

10703001	Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.	DOC-ICP-02, item 10.1.4.
10703002	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.	DOC-ICP-02, item 10.3.1.
10703003	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.	DOC-ICP-02, item 9.2.2.
10703004	Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras	DOC-ICP-02, item 9.3.3.17.

	redes, sem proteção adequada.	
10703005	As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.	DOC-ICP-02, item 9.3.5.4.
10703006	Devem ser estabelecidos os formatos e padrões de data e hora contidos em cada tipo de registro.	DOC-ICP-05, item 5.5.5.
10703007	Proteção lógica adicional (criptografia) e senhas devem ser adotados para evitar o acesso não autorizado às informações. O arquivo de senhas deve ser criptografado e ter acesso controlado.	DOC-ICP-02, item 9.3.2.5 e item 9.3.4.5.

1.8 Manter segurança lógica e rede, composto pelos subprocessos:

1.8.1 Manter sistemas básicos

10801001	Os equipamentos utilizados nos processos de certificação digital devem possuir Homologação da ICP-Brasil ou Certificação INMETRO.	DOC-ICP-01.01, item 3.
10801002	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.	DOC-ICP-02, item 9.3.2.3.
10801003	As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.	DOC-ICP-02, item 9.3.2.4.
10801004	A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.	DOC-ICP-02, item 9.3.2.6.
10801005	Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.	DOC-ICP-02, item 9.3.2.7.
10801006	Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.	DOC-ICP-02, item 9.3.3.3.
10801007	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses	DOC-ICP-02, item 9.3.3.4.

	ativos em sua primeira ativação.	
10801008	As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.	DOC-ICP-05, item 6.7.1.4.

1.8.2 Manter equipamentos protegidos de ameaças

10802001	O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o "Efeito *Tempest*".	DOC-ICP-02, item 9.3.3.1.
10802002	Mecanismos de segurança baseados em sistemas de proteção (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.	DOC-ICP-02, item 9.3.3.19.
10802003	A ativação da rede deve respeitar a ordem prevista no DOC-ICP-02, item 9.3.3.26. Os sistemas de certificação devem ser dispostos em segmentos de rede que devem ser isolados por meios diversos, como por exemplo: a) utilizando virtual "*lans*" (*vlan*); b) utilizando de *firewall*; c)utilizando artifícios de roteamento.	DOC-ICP-02, itens 9.3.3.26 e 9.3.3.27.
10802004	Nos computadores pessoais, devem ser adotadas medidas para combate de vírus, realização de *backups*, controle de acesso e uso de *software* não autorizado.	DOC-ICP-02, item 9.3.5.3.
10802005	Em todos os equipamentos devem ser sistematizados procedimentos para combate a processos destrutivos (vírus, "*worms*" e cavalos-de-tróia).	DOC-ICP-02, item 9.3.6.
10802006	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.	DOC-ICP-02, item 9.3.3.30.
10802007	Devem ser definido procedimentos formais para a eliminação segura de mídias desnecessárias.	DOC-ICP-02, item 9.3.5.12.

1.8.3 Manter *logs* e trilhas de auditoria

10803001	A AC deverá registrar em arquivos de auditoria todos os eventos	DOC-ICP-05

	relacionados à segurança do seu sistema de certificação. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria: a) iniciação e desligamento do sistema de certificação; b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC; c) mudanças na configuração da AC ou nas suas chaves; d) mudanças nas políticas de criação de certificados; e) tentativas de acesso (*login*) e de saída do sistema (*logoff*); f) tentativas não autorizadas de acesso aos arquivos de sistema; g) geração de chaves próprias da AC ou de chaves de seus usuários finais; h) emissão e revogação de certificados; i) geração de LCR; j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves; k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e l) operações de escrita nesse repositório, quando aplicável.	item 5.4.1.1.
10803002	Informações de segurança não geradas pelo sistema de certificação devem ser registradas.	DOC-ICP-05, item 5.4.1.2.
10803003	Registrar e avaliar periodicamente violações de segurança.	DOC-ICP-02, item 9.2.3.
10803004	Definir, analisar periodicamente e proteger devidamente arquivos de *logs* de sistemas.	DOC-ICP-02, item 9.3.1.3.
10803005	Solicitações de revogação de certificados devem ser registradas.	DOC-ICP-05, item 3.4.
10803006	Para os sistemas de controle de acesso lógico, os registros de atividades (*logs*) devem ser analisados periodicamente.	DOC-ICP-02, item 9.3.4.15.
10803007	Manter os equipamentos sincronizados com a FCT (Fonte Confiável do Tempo).	DOC-ICP-03.01, item 4.1.2.j.

1.8.4 Manter cópias de segurança e restauração

10804001	Devem ser descritos os procedimentos para recuperação de recursos computacionais corrompidos.	DOC-ICP-05, item 5.7.2.
10804002	Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.	DOC-ICP-02, item 9.3.2.9.

1.8.5 Manter controle de acesso a rede

10805001	A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.	DOC-ICP-02, item 9.3.3.9.
10805002	Devem ser implementados mecanismos de *firewall* em equipamentos de utilização específica, configurados exclusivamente para tal função. Os *firewalls* deverão ser dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC.	DOC-ICP-05, item 6.7.2.1.
10805003	As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, diária e todas as ações tomadas em decorrência desse exame deverão ser documentadas.	DOC-ICP-05, item 6.7.4.
10805004	Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, deverão estar localizados e operar em ambientes de nível, no mínimo, 4.	DOC-ICP-05, item 6.7.1.3.
10805005	Nos ambientes de rede, registrar e avaliar periodicamente eventos de segurança.	DOC-ICP-02, item 9.3.3.10.
10805006	O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.	DOC-ICP-02, item 9.3.3.15.

1.8.6 Manter controle de acesso lógico

10806001	Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.	DOC-ICP-02, item 9.3.2.2.
10806002	A AC deverá implementar um padrão de utilização de “senhas fortes”, definido na sua PS e em conformidade com a PS da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.	DOC-ICP-05, item 5.2.3.3.

10806003	Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.	DOC-ICP-02, item 9.3.1.2.
10806004	O responsável pela autorização ou confirmação da autorização de acesso lógico a sistemas e servidores deve ser claramente definido e registrado.	DOC-ICP-02, item 9.3.2.1.
10806005	O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido.	DOC-ICP-02, item 9.3.2.1.
10806006	As autorizações de acesso lógico das máquinas servidoras devem ser revistas, confirmadas e registradas continuamente.	DOC-ICP-02, item 9.3.2.1.
10806007	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.	DOC-ICP-02, item 9.3.3.7.
10806008	O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.	DOC-ICP-02, item 9.3.4.8.

1.9 Manter infraestrutura, composto pelos subprocessos:

1.9.1 Manter equipamentos de computação

10901001	Módulo criptográfico para geração de chaves assimétricas de usuário final e armazenamento da chave privada de titular de certificado deve ser homologado pela ICP-Brasil ou possuir certificação INMETRO.	DOC-ICP-01.01, item 3.
10901002	Módulo criptográfico para geração de chaves assimétricas de AC e armazenamento da chave privada de AC deve possuir certificação padrão NSH-2, ter sido homologado pela ICP-Brasil ou possuir certificação INMETRO.	DOC-ICP-01.01, item 3.

1.9.2 Manter controle de acesso físico

10902001	Acesso aos componentes de infraestrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.	DOC-ICP-02, item 8.2.10.
10902002	Todas as passagens entre os níveis de acesso, bem como os ambientes de nível 4 e o ambiente do sistema de monitoração devem possuir sistemas de CTFV, 24x7.	DOC-ICP-05, item 5.1.2.2.1 e 5.1.2.2.6.
10902003	O uso de equipamentos não autorizados nas instalações da AC só podem ser utilizados após autorização formal e sob supervisão.	DOC-ICP-02, item 8.2.13.

10902004	Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).	DOC-ICP-02, item 8.2.14.
10902005	Acesso de visitantes aos ambientes da AC devem ser registrados e supervisionados.	DOC-ICP-02, item 8.2.15.
10902006	Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente deverão ser monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.	DOC-ICP-05, item 5.1.2.2.3.
10902007	O ambiente de nível 4 deve possuir alarme de detecção de movimento permanentemente ativo enquanto não for satisfeito o critério de acesso ao ambiente.	DOC-ICP-02, item 8.2.17, DOC-ICP-05, item 5.1.2.2.4.
10902008	A estrutura inteiriça do ambiente de nível 4, construída na forma de célula estanque, deverá prover proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.	DOC-ICP-05, item 5.1.4.
10902009	Não deverá haver identificação pública externa das instalações e, internamente, não deverão ser admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações deverão ser segregadas em compartimentos fechados e fisicamente protegidos.	DOC-ICP-05, item 5.1.1.1. DOC-ICP-02, item 8.2.2.
10902010	Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.	DOC-ICP-02, item 8.2.3. DOC-ICP-05, item 5.1.2.
10902011	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.	DOC-ICP-02, item 8.2.4.
10902012	Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.	DOC-ICP-02, item 8.2.5.
10902013	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.	DOC-ICP-02, item 8.2.6.

10902014	Os sistemas de AC e ACT deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio frequência.	DOC-ICP-02, item 8.2.7.
10902015	Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.	DOC-ICP-02, item 8.2.8 e DOC-ICP-05, item 5.1.2.
10902016	A entrada e saída, de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.	DOC-ICP-02, item 8.2.9.
10902017	Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.	DOC-ICP-02, item 9.3.3.11.
10902018	A infraestrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.	DOC-ICP-02, item 9.3.3.13.
10902019	Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries	DOC-ICP-02, item9.3.3.2.
10902020	A chave de certificação das AC (ativação da AC) deve estar protegida fisicamente de acesso desautorizado, para garantir seu sigilo e integridade.	DOC-ICP-02, item 9.3.3.28.
10902021	Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).	DOC-ICP-02, item 9.3.5.2.
10902022	A AC deve possuir pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC, e mais 2 (dois) níveis relativos à proteção da chave privada da AC.	DOC-ICP-05, item 5.1.2.1.1.
10902023	As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.	DOC-ICP-05, item 5.1.2.1.10.
10902024	A Autoridade Certificadora deve possuir um cofre (quinto nível) com capacidade de armazenar chaves criptográficas, materiais de ativação, suas cópias e equipamentos criptográficos.	DOC-ICP-05, item 5.1.2.1.12.

10902025	Para garantir a segurança do material armazenado, o cofre ou o gabinete deverá ser feito em aço ou material de resistência equivalente e possuir tranca com chave.	DOC-ICP-05, item 5.1.2.1.13.
10902026	O sexto nível - ou nível 6 - deve consistir de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos deve dispor de fechadura individual. Os dados de ativação da chave privada da AC deverão ser armazenados nesses depósitos.	DOC-ICP-05, item 5.1.2.1.14.
10902027	O primeiro nível - ou nível 1 - deverá situar-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo deverá ser identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC deverão transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC deverá ser executado nesse nível.	DOC-ICP-05, item 5.1.2.1.2.
10902028	O segundo nível - ou nível 2 - será interno ao primeiro e deverá requerer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico, e o uso de crachá.	DOC-ICP-05, item 5.1.2.1.4.
10902029	Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e supervisão.	DOC-ICP-05, item 5.1.2.1.3.
10902030	O terceiro nível - ou nível 3 - deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais deverá estar localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não deverão ter permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não poderão permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.	DOC-ICP-05, item 5.1.2.1.5.
10902031	No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.	DOC-ICP-05, item 5.1.2.1.6.

10902032 0.1.1.1	Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC, não serão admitidos a partir do nível 3.	DOC-ICP-05, item 5.1.2.1.7.
10902033	No quarto nível - ou nível 4 -, interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação da AC, tais como a emissão e revogação de certificados e a emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado.	DOC-ICP-05, item 5.1.2.1.8.
10902034	No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 - que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.	DOC-ICP-05, item 5.1.2.1.9.
10902035	As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 7 (sete) anos. Elas deverão ser testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas deverão ser armazenadas em ambiente de terceiro nível.	DOC-ICP-05, item 5.1.2.2.2.
10902036	O sistema de notificação de alarmes deverá utilizar pelo menos 2 (dois) meios de notificação: sonoro e visual.	DOC-ICP-05, item 5.1.2.2.5.
10902037	O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, deverão ser permanentemente monitorados e estar localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, deverão ser monitoradas por câmeras de vídeo cujo posicionamento deverá permitir o acompanhamento das ações.	DOC-ICP-05, item 5.1.2.2.6.
10902038	Mecanismos específicos deverão ser implantados pela AC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de	DOC-ICP-05, item 5.1.2.4.1.

	todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.	
10902039	Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.	DOC-ICP-02, item 8.2.11.
10902040	Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, deverão ser monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a recuperação de senhas digitadas nos controles de acesso.	DOC-ICP-05, item 5.1.2.2.1.

1.9.3 Manter ar-condicionado

10903001	O sistema de ar-condicionado deve possuir redundância.	DOC-ICP-05, item 5.1.3.10.
10903002	O sistema de climatização deve atender às condições ambientais estabelecidas na Norma NBR 11515.	DOC-ICP-05, item 5.1.3.7. e 5.1.6.
10903003	A temperatura dos ambientes atendida pelo sistema de climatização deve ser permanentemente monitorada por sistema de notificação e alarme.	DOC-ICP-05, item 5.1.3.8.
10903004	O sistema de ar-condicionado em ambiente de nível 4 deve ser interno.	DOC-ICP-05, item 5.1.3.9.

1.9.4 Manter energia elétrica

10904001	A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.	DOC-ICP-02, item 9.3.3.14.
10904002	A energia elétrica para a infraestrutura da AC deve possuir sistemas e dispositivos que garantam o fornecimento ininterrupto.	DOC-ICP-05, item 5.1.3.1.
10904003	Todos os cabos elétricos devem estar protegidos por tubulações ou dutos apropriados.	DOC-ICP-05, item 5.1.3.2.
10904004	Sistema de aterramento deve ser implantado.	DOC-ICP-05, item 5.1.3.1.

10904005	Tubulações, dutos, calhas, quadros e caixas - de passagem, distribuição e terminações - devem ser construídos de forma a facilitar vistorias e a detecção de tentativas de violações.	DOC-ICP-05, item 5.1.3.3.
10904006	Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados.	DC-ICP-05, item 5.1.3.3.
10904007	Todos os cabos devem ser catalogados e vistoriados no mínimo a cada 6 (seis) meses.	DOC-ICP-05, item 5.1.3.4.
10904008	Deve ser mantida atualizada a topologia de rede de cabos.	DOC-ICP-05, item 5.1.3.5.
10904009	Instalações elétricas provisórias, fiações expostas e conexões inadequadas não devem ser admitidas.	DOC-ICP-05, item 5.1.3.6.

1.9.5 Manter sistema de combate a incêndio

10905001	Sistema de prevenção contra incêndio nos ambientes da AC devem possuir alarme preventivo antes da fumaça visível, acionado somente com a presença de partículas que caracterizam o sobreaquecimento de materiais.	DOC-ICP-05 item 5.1.5.1.
10905002	Sala-cofre de nível 4 (quatro) deve possuir sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás.	DOC-ICP-05, item 5.1.5.3.
10905003	As portas de acesso à sala-cofre deverão constituir eclusas, onde uma porta só deverá se abrir quando a anterior estiver fechada.	DOC-ICP-05, item 5.1.5.3.
10905004	Em caso de incêndio nas instalações da AC, o aumento da temperatura interna da sala-cofre de nível 4 (quatro), não deverá exceder 50 graus Celsius, e a sala deverá suportar esta condição por, no mínimo, 1 (uma) hora (NBR 15247).	DOC-ICP-05, item 5.1.5.4.

1.10 Manter recursos humanos, composto pelos subprocessos:

1.10.1 Admitir pessoas

11001001	Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.	DOC-ICP-02, item 7.3.1.1.

11001002	Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.	DOC-ICP-02, item 7.3.1.2.
11001003	A entrevista de admissão deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados durante a pesquisa para a sua admissão.	DOC-ICP-02, item 7.3.4.1.
11001004	Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.	DOC-ICP-02, item 7.3.4.2.
11001005	Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL. A AC responsável poderá definir requisitos adicionais para a contratação.	DOC-ICP-05, item 5.3.7.
11001006	Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil, verificação de antecedentes e verificação de grau de instrução.	DOC-ICP-02, item 7.3.3.

1.10.2 Manter capacitação de pessoas

11002001	Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na Política de Segurança.	DOC-ICP-02, item 6.1.3.
11002002	Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.	DOC-ICP-02, item 6.1.4.
11002003	Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.	DOC-ICP-02, item 7.3.7.
11002004	Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá	DOC-ICP-05, item 5.3.3.

	receber treinamento documentado, suficiente para o domínio dos seguintes temas: a) princípios e mecanismos de segurança da AC e das ARs vinculadas; b) sistema de certificação em uso na AC; c) procedimentos de recuperação de desastres e de continuidade do negócio; d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2 e 3.2.3 e 3.2.7; e e) outros assuntos relativos a atividades sob sua responsabilidade.	
11002005	Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC ou das ARs.	DOC-ICP-05, item 5.3.4.
11002006	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar os incidentes descritos no DOC-ICP-02.	DOC-ICP-02, item 13.2.3.
11002007	Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, com carga horária mínima de 16 horas, sobre os seguintes temas: a) princípios e mecanismos de segurança da AR; b) sistema de certificação em uso na AC; c) procedimentos de recuperação de desastres e de continuidade do negócio; d) reconhecimento de assinaturas e validade dos documentos apresentados; e) outros assuntos relativos a atividades sob sua responsabilidade.	DOC-ICP-03.01, item 2.3.1.
11002008	Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.	DOC-ICP-02, item 7.3.5.2.

1.10.3 Manter habilitação de pessoas

11003001	Todo empregado da AC responsável terá sua identidade e perfil verificados antes de: a) Ser incluído em uma lista de acesso às instalações da AC; b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC; c) Receber um certificado para executar suas atividades operacionais na AC; e d) Receber uma conta no sistema de certificação da AC.	DOC-ICP-05, item 5.2.3.1.
11003002	Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.	DOC-ICP-02, item 10.2.1.

11003003	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.	DOC-ICP-02, item 10.2.2.
11003004	O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.	DOC-ICP-02, item 7.3.1.3.
11003005	Todos os empregados da AC deverão estar identificados por uma credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo máximo de 1 (um) ano de validade. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário.	DOC-ICP-02, item 7.3.6.
11003006	As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidas e atribuídas a indivíduos claramente identificados na organização.	DOC-ICP-02, item 8.2.1.
11003007	Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.	DOC-ICP-02, item 9.3.4.16.
11003008	Somente após o recebimento da solicitação de habilitação do agente de registro e das declarações previstas, a AC pode incluí-lo nas bases de dados e conceder as permissões de acesso no sistema de certificação, sendo necessária para isso prévia autorização documentada do Gerente da AC ou do responsável por ele designado.	DOC-ICP-03.01, item 2.2.4.
11003009	A AC deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o seu sistema de certificação sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.	DOC-ICP-05, item 5.2.1.1.
11003010	A AC deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.	DOC-ICP-05, item 5.2.1.2.
11003011	O tipo e o nível de acesso serão determinados, em documento formal, com	DOC-ICP-05,

	base nas necessidades de cada perfil. Todos os operadores do sistema de certificação da AC deverão receber treinamento específico antes de obter qualquer tipo de acesso.	item 5.2.1.3.
11003012	Todas as tarefas executadas no ambiente onde estiver localizado o equipamento de certificação da AC deverão requerer a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC poderão ser executadas por um único empregado.	DOC-ICP-05, item 5.2.2.2.
11003013	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
11003014	A AC deve descrever os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC responsável e nas ARs a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.	DOC-ICP-05, item 5.2.

1.10.4 Avaliar desempenho

11004001	Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.	DOC-ICP-02, item 7.3.5.1.
11004002	Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.	DOC-ICP-02, item 7.3.8.1.
11004003	Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.	DOC-ICP-02, item 7.3.8.2.
11004004	Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.	DOC-ICP-02, item 7.3.8.3.
11004005	As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.	DOC-ICP-02, item 7.3.8.4.

1.10.5 Suspender, movimentar e desligar pessoas

11005001	Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.	DOC-ICP-02, item 6.1.5.
11005002	O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público. Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.	DOC-ICP-02, item 7.3.9.
11005003	Quando um empregado se desligar da AC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.	DOC-ICP-05, item 5.2.1.4.
11005004	O empregado ou servidor firmará, antes do desligamento, declaração de que não possui nenhum tipo de pendência junto às diversas unidades que compõem a entidade, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.	DOC-ICP-02, item 7.3.10.
11005005	Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.	DOC-ICP-02, item 7.3.11.
11005006	Pode ser definida uma política a ser adotada pela AC responsável e pelas ARs vinculadas para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.	DOC-ICP-05, item 5.3.5.
11005007	Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC responsável ou de uma AR vinculada, a AC deverá, de imediato, suspender o acesso dessa pessoa ao seu sistema de certificação, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis. O processo administrativo referido acima deverá conter, no mínimo, os seguintes itens: a) relato da ocorrência com "*modus operandis*"; b) identificação dos envolvidos; c) eventuais prejuízos causados; d) punições aplicadas, se for o caso; e e) conclusões. Concluído o processo administrativo, a AC responsável deverá encaminhar suas conclusões à AC Raiz.	DOC-ICP-05, item 5.3.6.1, 5.3.6.2 e 5.3.6.3

11005008	As punições passíveis de aplicação, em decorrência de processo administrativo, são: a) advertência; b) suspensão por prazo determinado; ou c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.	DOC-ICP-05, item 5.3.6.4.
11005009	Quando o Agente de Registro é suspenso ou desligado de suas atividades, a AR imediatamente providencia a revogação de suas permissões de acesso ao sistema de certificação da AC e permissões de acesso físico e lógico aos equipamentos e mecanismos inerentes à atividade de Agente de Registro. Esses processos são documentados e esses documentos são arquivados no dossiê do Agente de Registro.	DOC-ICP-03.01, item 2.5 e item 2.2.2.a.

2 Os processos nas Autoridades de Registro - ARs estão assim distribuídos:

2.1 Manter credenciamento de AR, composto pelos subprocessos:

2.1.1 Manter requisitos de manutenção de credenciamento

20101001	Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 do DOC-ICP-03.	DOC-ICP-03, item 2.1.
20101002	Qualquer alteração nos atos constitutivos, estatuto, contrato social ou administradores nas AR devem ser comunicados à AC a que está operacionalmente vinculada.	DOC-ICP-03, item 3.2.1.a.i.
20101003	A AR deve manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL, bem como Princípios e Critérios *WebTrust* para AR.	DOC-ICP-05 item 4.1.2.4.e.
20101004	Caso ocorra uma ou mais das hipóteses previstas no item 4.2.1 do DOC-ICP-03, a AR deve ser descredenciada.	DOC-ICP-03, item 4.2.1.

2.1.2 Manter condições fisco-tributárias e econômico-financeiras

20102001	A AR deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede	DOC-ICP-03, Anexo II, item 2.

	do candidato, ou outra equivalente, na forma da lei; e d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.	
20102002	A AR deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos à sua qualificação econômico-financeira: a) Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente. b) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.	DOC-ICP-03, item 2.1.c e Anexo II, item 3.

2.1.3 Manter contrato de seguro

20103001	AR cuja a empresa tenha sido criada a menos de um ano e entidades sem fins lucrativos devem manter vigente apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 200.000,00 (duzentos mil reais).	DOC-ICP-03, Anexo II, itens 3.2.e e 3.2.f.

2.1.4 Manter histórico de agentes de registro

20104001	A AR deve enviar à AC a relação atualizada dos Agentes de Registro em atividade, seus perfis qualificados e suas necessidades de acesso a informações do gerenciamento de ciclo de vida dos certificados.	DOC-ICP-03.01, item 2.1.3.
20104002	Apenas Agentes de Registro relacionados na Lista disponibilizada no sítio do ITI podem ter acesso aos sistemas de emissão de certificado.	Instrução Normativa 11/2020, Art. 5º.

2.1.5 Comunicar alterações operacionais e violação de normas

20105001	Qualquer alteração em atos constitutivos, estatuto, contrato social ou administradores nas ARs devem ser comunicados à AC a que está operacionalmente vinculada.	DOC-ICP-03, item 3.2.1.a.i.
20105002	Violações, que a AR tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil por parte de seus funcionários, devem ser comunicados à AC	DOC-ICP-03, item 3.2.1.a.ii.

	a que está operacionalmente vinculada.	

2.1.6 Regularizar não conformidades identificadas

20106001	A entidade auditada deve cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas.	DOC-ICP-08, item 9.1.

2.1.7 Manter procedimentos para extinção de AR

20107001	No caso de extinção, A AR deve observar os requisitos e procedimentos estabelecidos pela AC a qual esteja vinculada.	DOC-ICP-05, item 4.11.
20107002	Disponibilizar relatório descrevendo todos os procedimentos de descredenciamento adotados para avaliação pela auditoria operacional, no prazo máximo de 60 (sessenta) dias.	DOC-ICP-03, item 4.2.2.4.b.v.

2.2 Atender solicitação de certificados, composto pelos subprocessos:

2.2.1 Identificar solicitante

20201001	O processo de identificação e confirmação do cadastro inicial do solicitante na ICP-Brasil deve ser realizado mediante a presença física do interessado ou por meio de videoconferência.	DOC-ICP-05 item 3.2.3.
20201002	Documentos obrigatórios de identificação, em suas versões originais, podendo ser física ou digital, por meio de barramento ou aplicação oficial, devem ser apresentados para a identificação da pessoa e realizada a coleta de biometria.	DOC-ICP-05 item 3.2.3.1.
20201003	A identidade do indivíduo deve ser confirmada.	DOC-ICP-05 item 3.2.a.i.
20201004	A identidade da organização deve ser confirmada.	DOC-ICP-05 item 3.2.a.ii.
20201005	Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação.	DOC-ICP-05 item 3.2.8.4.1
20201006	A solicitação de certificados do tipo A CF-e-SAT e OM-BR deve ser	DOC-ICP-05

	validada.	item 3.2.9.2 e item 3.2.9.5.
20201007	Na modalidade presencial a coleta de dados biométricos deve ser feita de forma assistida (acompanhada) por um Agente de Registro (AGR).	DOC-ICP-05.03, item 2.1.
20201008	A fotografia frontal da face deve seguir os parâmetros mínimos previstos DOC-ICP-05.03, item 2.4.1.	DOC-ICP-05.03, item 2.4.1.
20201009	A impressão digital deve seguir os parâmetros mínimos previstos DOC-ICP-05.03, item 2.4.2.	DOC-ICP-05.03, item 2.4.2.
10302010	Os processos de identificação e confirmação do cadastro do solicitante por meio de videoconferência devem assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico, observando os requisitos apresentados no DOC-ICP-05.05.	DOC-ICP-05 item 3.3.2.
20201011	Na modalidade remota por videoconferência a coleta de dados biométricos deverá ser realizada pela captura de face (*frame*) do requerente durante a videoconferência de forma assistida e, opcionalmente, pela coleta das impressões digitais do requerente de forma não assistida e assíncrona à videoconferência, para execução do batimento biométrico junto a uma base oficial nacional ou PSBio.	DOC-ICP-05.03, item 2.1.
10302012	A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional admitidas regulamentadas na ICP-Brasil.	DOC-ICP-05 item 3.2.3.1.8.
10302013	Os órgãos e conselhos de classe profissional credenciados como AR na ICP-Brasil, poderão realizar a identificação dos profissionais solicitantes sujeitos a registro perante o respectivo órgão ou conselho de classe.	DOC-ICP-05 item 3.2.9.6.
10302014	Solicitações de certificados digitais realizadas através do Balcão Único para Abertura de Empresas devem atender os critérios definidos no item 3.2.9.7 do DOC-ICP-05.	DOC-ICP-05 item 3.2.9.7.
10302015	Solicitações de certificado a ser emitido em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverão observar os requisitos definidos no item 3.2.9.8 do DOC-ICP-05.	DOC-ICP-05 item 3.2.9.8.

2.2.2 Confrontar dados da solicitação

20202001	Os dados da solicitação de certificado devem ser conferidos com os	DOC-ICP-05

	documentos originais apresentados.	item 3.2.b.
20202002	Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados por Agente de Registro distinto do que realizou a etapa de identificação.	DOC-ICP-05 item 3.2.3.1.3.a.
20202003	Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos.	DOC-ICP-05 item 3.2.3.1.2.
20202004	Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados na sede da AR ou AR própria da AC.	DOC-ICP-05 item 3.2.3.1.3.b.
20202005	O certificado emitido cuja verificação não ocorra antes do início de validade deve ser revogado automaticamente.	DOC-ICP-05 item 3.2.3.1.3.c.
20202006	Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinada digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3.	DOC-ICP-05 item 3.2.8.2.
20202007	Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou indivíduo.	DOC-ICP-05 item 3.2.8.3.

2.2.3 Assinar Termo de Titularidade

20203001	O termo de titularidade deve ser assinado digitalmente pelo candidato a titular ou responsável pelo uso do certificado.	DOC-ICP-05 item 3.2.2.1.3.”d”.
20203002	A AC deve descrever em detalhes os requisitos e procedimentos que devem ser adotados para assinatura do termo de titularidade.	DOC-ICP-05 item 4.1.”c”.

2.2.4 Armazenar documentos

20204001	O armazenamento definitivo dos dossiês de titulares de certificado, digitalizados ou eletrônicos, deve ser feito: a) no ponto definitivo da AC à qual a AR está vinculada; ou b) na AC emissora para os casos de certificados A CF-e-SAT ou OM-BR.	DOC-ICP-03.01 item 6.2.3.
20204002	Os documentos digitalizados cujas cópias devam constar no dossiê do titular do certificado devem ser assinados digitalmente com uso de certificado ICP-Brasil e arquivados no ponto de centralização da AC à qual a AR está vinculada ou na AC emissora para os casos de certificados	DOC-ICP-03.01 item 6.2.2.a e 6.2.3.

	A CF-e-SAT ou OM-BR.	
20204003	Todos os arquivos que compõem um dossiê do titular do certificado devem ser organizados de forma a permitir sua recuperação conjunta, para fins de fiscalização e auditoria.	DOC-ICP-03.01 item 6.2.2.c.
20204004	O diretório ou sistema onde são armazenados os documentos digitalizados do dossiê do titular do certificado deve ser protegido contra leitura e gravação, dando permissão de acesso somente aos Agentes de Registro vinculados ou responsáveis designados formalmente para trabalhar com os documentos.	DOC-ICP-03.01 item 6.2.2.d.
20204005	Procedimentos de cópias e recuperação dos documentos digitalizados em caso de sinistro devem ser especificados.	DOC-ICP-03.01 item 6.2.2.e.
20204006	A AC deve ser capaz de determinar facilmente e a qualquer momento o local onde se encontra cada dossiê de titular de certificado que se encontra sob sua guarda.	DOC-ICP-03.01 item 6.2.5.
20204007	O ponto de centralização da AC deve ser informado ao ITI, bem como qualquer alteração que venha ser feita.	DOC-ICP-03.01 item 6.2.6.
20204008	A remessa ou transmissão do dossiê para o local de armazenamento definitivo deve ser feita por meio seguro, no prazo máximo de 7 (sete) dias corridos, a partir da geração do dossiê.	DOC-ICP-03.01 item 6.2.4.

2.3 Atender solicitação de revogação de certificados, composto pelos subprocessos:

2.3.1 Identificar solicitante

20301001	A identificação deverá ser realizada mediante a presença física do interessado ou por meio de videoconferência.	DOC-ICP-05 item 3.2.3.
20301002	Documentos obrigatórios de identificação, em suas versões originais, podendo ser física ou digital, por meio de barramento ou aplicação oficial, devem ser apresentados para a identificação e realizada a coleta de biometria.	DOC-ICP-05 item 3.2.3.1.
20301003	A identidade do indivíduo deve ser confirmada.	DOC-ICP-05 item 3.2.a.i.
20301004	A identidade da organização deve ser confirmada.	DOC-ICP-05 item 3.2.a.ii.
20301005	Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação.	DOC-ICP-05 item 3.2.8.4.1.

2.3.2 Revogar certificados

20302001	A revogação de certificado será solicitada por uma das pessoas ou entidades elencadas no item "Quem pode solicitar revogação" do DOC-ICP-05, o qual deverá ser identificada.	DOC-ICP-05 itens 4.9.2."a" e 4.9.3.2 "a".
20302002	As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas.	DOC-ICP-05 item 4.9.3.2. "b".
20302003	A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 da DPC e deve estabelecer prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado poderá ser solicitada sem cobrança de tarifa pela AC.	DOC-ICP-05 item 4.9.4.1.

2.4 Manter segurança da informação, composto pelos subprocessos:

2.4.1 Manter inventário de ativos

20401001	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
20401002	O inventário de todos os ativos da AR, relacionando equipamentos e softwares, deve ser mensalmente atualizado.	DOC-ICP-02, item 6.3 e item 8.2.12, DOC-ICP-03.01, item 6.1.5.
20401003	O inventário de ativos deve manter histórico das alterações e ser assinado pelo responsável pela AR.	DOC-ICP-03.01, item 6.1.4.

2.4.2 Manter análise de risco e Plano de Continuidade do Negócio - PCN

20402001	Um Plano de Continuidade de Negócios (PCN) deve ser implementado e testado pelo menos uma vez por ano.	DOC-ICP-02, item 6.4.1, item 13, DOC-ICP-03.01, item 6.1.3, DOC-ICP-05, item 5.7.1.
20402002	Todos os incidentes devem ser reportados à AC Raiz imediatamente, a	DOC-ICP-02,

	partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.	item 6.4.4.
20402003	Todos os ativos de processamento das entidades devem estar relacionados no PCN.	DOC-ICP-02, item 7.4.3.c.
20402004	O processo de gerenciamento de risco deve ser revisto anualmente.	DOC-ICP-02, item 6.2 e 12.
10602005	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.	DOC-ICP-02, item 13.2.3.

2.4.3 Manter documentos armazenados e classificados

20403001	Sistema de classificação da informação deve ser elaborado para proteger as informações de acordo com o seu valor, sensibilidade e criticidade.	DOC-ICP-02, item 9.2.1.
20403002	A AC deve possuir dossiê contendo os documentos relacionados no item 6.1.2 do DOC-ICP-03-01.	DOC-ICP-03.01, item 6.1.1.
20403003	A AR deve possuir, também, cópia do PCN.	DOC-ICP-03.01, item 6.1.3.
20403004	Dossiês dos titulares de certificados e dos Agentes de Registro devem ser enviados à AC vinculada, inclusive os antigos, e guardados preferencialmente, em ambiente computacional protegido, com acesso permitido somente aos Agentes de Registro vinculados ou responsáveis designados formalmente para trabalhar com os documentos.	DOC-ICP-03.01, item 6.2.1.
20403005	Caso a AC opte pela substituição da guarda física dos dossiês de Agente de Registro e de titulares de certificados por digitalização dos mesmos, os documentos cujas cópias devam constar nos dossiês devem ser digitalizados e assinados digitalmente com certificado ICP-Brasil.	DOC-ICP-03.01, item 6.2.2.a.
20403006	Todos os arquivos digitais que compõem os dossiês devem ser organizados de forma a permitir sua recuperação conjunta e devem ter proteção contra leitura e gravação, com permissão de acesso somente aos Agentes de Registro vinculados ou responsáveis formalmente designados.	DOC-ICP-03.01, item 6.2.2.c e 6.2.2.d.
20403007	Os dossiês de titulares de certificados, digitalizados ou eletrônicos, devem ser armazenados: a) no ponto de centralização da AC à qual a AR está vinculada; ou b) na AC emissora para os casos de certificados ACF-e-SAT ou OM-BR.	DOC-ICP-03.01, item 6.2.3.
20403008	A remessa ou transmissão do dossiê para o local de armazenamento definitivo deve ser feita por meio seguro no prazo máximo de 7 (sete) dias	DOC-ICP-03.01, item 6.2.4.

	corridos, da data de geração do dossiê.	
20403009	O Ponto de Centralização da AC deve ser informado ao ITI, bem como qualquer alteração que venha a ser feita posteriormente.	DOC-ICP-03.01, item 6.2.6.
20403010	Todos os documentos em papel que contenham informações classificadas como sensíveis devem ser destruídos, de forma a tornar irrecuperável a informação neles contida, antes de ir para o lixo.	DOC-ICP-03.01, item 6.2.7.

2.5 Manter sistemas aplicativos, composto pelos subprocessos

2.5.1 Manter sistemas de informação

20501001	As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.	DOC-ICP-02 item 9.3.1.1.
20501002	A documentação dos sistemas deve ser mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
20501003	A cópia de segurança deve ser testada e mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
20501004	Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.	DOC-ICP-02 item 9.3.1.5.
20501005	As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.	DOC-ICP-02 item 9.3.1.5.
20501006	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.5.11.
20501007	O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve possuir, no mínimo, as características de segurança descritas no item 4.2.1 do DOC – ICP- 03.01	DOC-ICP-03.01, item 4.2.1.
20501008	Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.	DOC-ICP-02 item 10.2.3.

2.5.2 Manter bases de dados

20502001	Todo parâmetro crítico, cuja exposição indevida comprometa a segurança	DOC-ICP-02,

	do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.	item 10.1.4.
20502002	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.	DOC-ICP-02, item 10.3.1.
20502003	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.	DOC-ICP-02, item 9.2.2.
20502004	Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.	DOC-ICP-02, item 9.3.3.17.
20502005	As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.	DOC-ICP-02, item 9.3.5.4.
20502006	Proteção lógica adicional (criptografia) e senhas devem ser adotados para evitar o acesso não autorizado às informações. O arquivo de senhas deve ser criptografado e ter acesso controlado.	DOC-ICP-02, item 9.3.2.5 e 9.3.4.5.

2.6 Manter segurança lógica e rede, composto pelos subprocessos:

2.6.1 Manter sistemas básicos

20601001	Os Agentes de Registro devem utilizar apenas *softwares* licenciados pelo fabricante nos equipamentos das entidades, observadas as normas da ICP-Brasil e legislação de *software*.	DOC-ICP-02, item 9.3.5.7 e 9.3.5.8.
20601002	A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.	DOC-ICP-02, item 9.3.2.6.
20601003	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.	DOC-ICP-02, item 9.3.2.3.
20601004	As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.	DOC-ICP-02, item 9.3.2.4.

20601005	Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.	DOC-ICP-02, item 9.3.3.3.
20601006	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.

2.6.2 Manter equipamentos protegidos de ameaças

20602001	Os usuários que necessitam de acesso aos equipamentos e recursos da AR devem ser identificados e autenticados.	DOC-ICP-02, itens 9.3.4.1 e 9.3.4.3 DOC-ICP-03.01 item 4.1.2.a.
20602002	O sistema de controle de acesso aos equipamentos e recursos da AR devem manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha.	DOC-ICP-02, item 9.3.4.2.
20602003	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.	DOC-ICP-02, item 9.3.3.27.
20602004	Mecanismos de segurança baseados em sistemas de proteção (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.	DOC-ICP-02, item 9.3.3.19.
20602005	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.	DOC-ICP-02, item 9.3.3.30.
20602006	Autorizações de acesso de cada usuário aos equipamentos e recursos da AR devem ser definidas de acordo com a função exercida e protegido contra modificações não autorizadas.	DOC-ICP-02, item 9.3.4.4 e item 9.3.4.6.
20602007	As senhas devem ser protegidas com grau de segurança compatível com a informação associada.	DOC-ICP-02, item 9.3.4.7 a 9.3.4.13, DOC-ICP-03.01, itens 4.1.2.b e 4.1.2.c.
20602008	Os procedimentos de combate a processos destrutivos (antivírus, antitrojan e antispyware) devem estar sistematizados e abranger todos os	DOC-ICP-02, item 9.3.5.3 e

	equipamentos de computação.	9.3.6, DOC-ICP-03.01, item 4.1.1 e 4.1.2.d.
20602009	Todas as estações de trabalho da AR devem possuir *firewall* ativado, com permissões de acesso mínimas necessárias às atividades.	DOC-ICP-03.01, item 4.1.2.e.
20602010	Estações de trabalho devem possuir proteção de tela acionada no máximo após dois minutos de inatividade, com exigência de nova autenticação para desbloqueio.	DOC-ICP-02, item 9.3.4.13, DOC-ICP-03.01, item 4.1.2.f.
20602011	O sistema operacional deve ser mantido atualizado com aplicação de correções necessárias (*patches*, *hotfix*, etc).	DOC-ICP-03.01, item 4.1.2.g.
20602012	A entidade deve utilizar apenas *softwares* licenciados e necessários para a realização das atividades do AGR.	DOC-ICP-03.01, item 4.1.2.h.
20602013	Estações de trabalho devem impedir *login* remoto, via outro equipamento ligado à rede de computadores utilizadas pela AR, exceto para as atividades de suporte remoto.	DOC-ICP-03.01, item 4.1.2.i.
20602014	As mídias, quando não forem mais necessárias, devem ser eliminadas de forma segura e os procedimentos para eliminação segura devem estar formalizados.	DOC-ICP-02, item 9.3.5.12.

2.6.3 Manter *logs* e trilhas de auditoria

20603001	Os *logs* de auditoria do sistema operacional devem registrar os acessos aos equipamentos e devem ficar armazenados localmente para avaliação pela auditoria operacional ou equipe de segurança.	DOC-ICP-02, item 9.2.3 e item 9.3.4.15, DOC-ICP-03.01, item 4.1.3.
20603002	Os *logs* de auditoria do sistema operacional devem ser analisados em caso de suspeitas quanto a acessos não autorizados ou para dirimir dúvidas que possam surgir sobre a utilização dos equipamentos.	DOC-ICP-03.01, item 4.1.4.
20603003	Para os sistemas de controle de acesso lógico, os registros de atividades (*logs*) devem ser analisados periodicamente	DOC-ICP-02, item 9.3.4.15.
20603004	Manter os equipamentos sincronizados com a FCT (Fonte Confiável do Tempo).	DOC-ICP-03.01, item 4.1.2.j.

2.6.4 Manter cópias de segurança e restauração

20604001	Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.	DOC-ICP-02, item 9.3.2.9.

2.6.5 Manter controle de acesso a rede

20605001	A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.	DOC-ICP-02, item 9.3.3.9.
20605002	Nos ambientes de rede, registrar e avaliar periodicamente eventos de segurança.	DOC-ICP-02, item 9.3.3.10.
20605003	O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.	DOC-ICP-02, item 9.3.3.15.

2.6.6 Manter controle de acesso lógico

20606001	Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.	DOC-ICP-02, item 9.3.2.2.
20606002	O ambiente operacional dos sistemas deve ser monitorado.	DOC-ICP-02, item 9.3.2.3.
20606003	Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.	DOC-ICP-02, item 9.3.1.2.
20606004	O responsável pela autorização ou confirmação da autorização de acesso lógico a sistemas e servidores deve ser claramente definido e registrado.	DOC-ICP-02, item 9.3.2.1.
20606005	O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido.	DOC-ICP-02, item 9.3.2.1.
20606006	As autorizações de acesso lógico das máquinas servidoras devem ser revistas, confirmadas e registradas continuamente.	DOC-ICP-02, item 9.3.2.1.
20606007	O Agente de Registro não deve possuir perfil de administrador ou senha	DOC-ICP-03.01,

	root dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções. O Agente de Registro somente deve receber acesso aos serviços e aplicações que tenham sido especificamente autorizados a usar.	item 4.1.5.
20606008	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.	DOC-ICP-02, item 9.3.3.7.
20606009	O arquivo de senhas deve ser criptografado e ter o acesso controlado.	DOC-ICP-02, item 9.3.4.5.
20606010	O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.	DOC-ICP-02, item 9.3.4.8.

2.6.7 Cumprir Política de Segurança de AC

20607001	Empregados ou servidores devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado.	DOC-ICP-02, item 7.4.1.
20607002	A chefia ou responsável pela AR devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado.	DOC-ICP-02, item 7.4.2 e item 7.4.3.
20607003	A gerência de segurança da AR devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado.	DOC-ICP-02, item 7.4.4.
20607004	Contrato com prestadores de serviço deve contemplar cláusula que responsabilize a prestadora quanto ao cumprimento da PS, normas e procedimentos.	DOC-ICP-02, item 7.4.5.

2.7 Manter infraestrutura, composto pelos subprocessos:

2.7.1 Manter equipamentos de computação

20701001	Módulo criptográfico para geração de chaves assimétricas de usuário final e armazenamento da chave privada de titular de certificado deve ser homologado pela ICP-Brasil ou possuir certificação INMETRO.	DOC-ICP-01.01, item 3.
20701002	As estações de trabalho de AR, incluindo equipamentos portáteis, devem estar protegidas contra ameaças e ações não autorizadas, bem como contra acesso, uso ou exposição indevidos.	DOC-ICP-03.01, item 4.1.1.

20701003	As estações de trabalho da AR deverão conter apenas aplicações e serviços que sejam suficientes e necessários para atividades corporativas.	DOC-ICP-03.01, item 4.1.1.3.
20701004	As estações de trabalho da AR, incluindo equipamentos portáteis, devem receber, no mínimo, as configurações de segurança descritas no item 4.1.2 do DOC – ICP- 03.01.	DOC-ICP-03.01, item 4.1.2.

2.7.2 Manter controle de acesso físico

20702001	Acesso aos componentes de infraestrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.	DOC-ICP-02, item 8.2.10.
20702002	O uso de equipamentos não autorizados nas instalações da AR só podem ser utilizados após autorização formal e sob supervisão.	DOC-ICP-02, item 8.2.13.
20702003	Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).	DOC-ICP-02, item 8.2.14.
20702004	Acesso de visitantes às áreas de segurança devem ser registrados e supervisionados.	DOC-ICP-02, item 8.2.15.
20702005	Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.	DOC-ICP-02, item 8.2.3, e
20702006	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.	DOC-ICP-02, item 8.2.4.
20702007	Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.	DOC-ICP-02, item 8.2.5.
20702008	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.	DOC-ICP-02, item 8.2.6.
20702009	Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.	DOC-ICP-02, item 8.2.8 .

20702010	A entrada e saída, de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.	DOC-ICP-02, item 8.2.9.
20702011	Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.	DOC-ICP-02, item 9.3.3.11.
20702012	A infraestrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.	DOC-ICP-02, item 9.3.3.13.
20702013	Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries	DOC-ICP-02, item9.3.3.2.
20702014	Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).	DOC-ICP-02, item 9.3.5.2.
20702015	Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.	DOC-ICP-02, item 8.2.11.

2.7.3 Manter energia elétrica

20703010	A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.	DOC-ICP-02, item 9.3.3.14.

2.8 Manter recursos humanos, composto pelos subprocessos:

2.8.1 Admitir pessoas

20801001	Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.	DOC-ICP-02, item 7.3.1.1.
20801002	Nenhuma entidade participante da ICP-Brasil admitirá estagiários no	DOC-ICP-02,

	exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.	item 7.3.1.2.
20801003	Os Agentes de Registro devem ser funcionários ou servidores da própria organização credenciada ou candidata ao credenciamento como AR junto à ICP-Brasil.	DOC-ICP-03.01, item 2.1.2, DOC-ICP-02.
20801004	Entrevista de Admissão dos Agentes de Registro deve ser realizada e formalizada documentalmente por profissional qualificado.	DOC-ICP-02, item 7.3.4.
20801005	Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.	DOC-ICP-02, item 7.3.4.2.
20801006	Pesquisa do histórico de empregos anteriores, da vida pública com o propósito de levantamento de perfil, verificação de antecedentes e verificação do grau de instrução deve ser realizado para os candidatos a Agente de Registro.	DOC-ICP-02, item 7.3.3, DOC-ICP-03.01, item 2.2.1.d.
20801007	Termos de compromisso e das condições do perfil que ocuparão devem ser registrados em contrato ou termo de responsabilidade dos Agentes de Registro.	DOC-ICP-05, item 5.3.
20801008	Comprovante de residência deve ser apresentado no processo de admissão de Agentes de Registro.	DOC-ICP-03.01, item 2.2.1.e, DOC-ICP-05, item 5.3.2.1.d.
20801009	Antecedentes criminais dos Agentes de Registro devem ser verificados no processo de admissão.	DOC-ICP-03.01, item 2.2.1.b, DOC-ICP-05, item 5.3.2.1.a.
20801010	Situação de crédito dos Agentes de Registro devem ser verificados no processo de admissão.	DOC-ICP-03.01, item 2.2.1.c, DOC-ICP-05, item 5.3.2.1.b.

2.8.2 Manter capacitação de pessoas

20802001	Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, com carga horária mínima de 16 (dezesseis) horas, sobre os temas descritos no item 2.3.1 do DOC-ICP-03.01.	DOC-ICP-03.01, item 2.3.
20802002	Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão,	DOC-ICP-05, item 5.3.3.

	expedição, distribuição, revogação e gerenciamento de certificados deverá receber treinamento documentado, suficiente para o domínio dos seguintes temas: a) princípios e mecanismos de segurança da AC e das ARs vinculadas; b) sistema de certificação em uso na AC; c) procedimentos de recuperação de desastres e de continuidade do negócio; d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2 e 3.2.3 e 3.2.7; e e) outros assuntos relativos a atividades sob sua responsabilidade.	
20802003	Todo Agente de Registro deve manter-se atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC ou da AR.	DOC-ICP-05, item 5.3.4.
20802004	Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, em reconhecimento de assinaturas (grafotecnia) e validade dos documentos apresentados.	DOC-ICP-03.01, item 2.3.1.d.
20802005	Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, referente ao sistema de certificação em uso na AC.	DOC-ICP-03.01, item 2.3.1.b.
20802006	Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.	DOC-ICP-02, item 7.3.5.2.
20802007	Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na Política de Segurança.	DOC-ICP-02, item 6.1.3.
20802008	Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.	DOC-ICP-02, item 6.1.4.
20802009	Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.	DOC-ICP-02, item 7.3.7.
20802010	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar os incidentes descritos no DOC-ICP-02.	DOC-ICP-02, item 13.2.3.

2.8.3 Manter habilitação de pessoas

20803001	A habilitação e desabilitação (se for o caso) do Agente de Registro no sistema de certificação da AC deve ser formalizada e confirmada.	DOC-ICP-03.01, itens 2.2.1.j e 2.2.2.
20803002	O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.	DOC-ICP-02, item 7.3.1.3.
20803003	Todos os empregados da AR deverão estar identificados por uma credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo máximo de 1 (um) ano de validade. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário.	DOC-ICP-02, item 7.3.6.
20803004	As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.	DOC-ICP-02, item 8.2.1.
20803005	Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.	DOC-ICP-02, item 9.3.4.16.
20803006	Somente após o recebimento da solicitação de habilitação do Agente de Registro e das declarações previstas, a AC pode incluí-lo nas bases de dados e conceder as permissões de acesso no sistema de certificação, sendo necessária para isso prévia autorização documentada do Gerente da AC ou do responsável por ele designado.	DOC-ICP-03.01, item 2.2.4.
20803007	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.

2.8.4 Avaliar desempenho

20804001	O acompanhamento de desempenho das funções e avaliação anual dos	DOC-ICP-03.01,

	Agentes de Registro devem ser realizados.	item 2.4.1 DOC-ICP-02, item 7.3.5.1 e 7.3.8.
20804002	Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.	DOC-ICP-02, item 7.3.8.1.
20804003	Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.	DOC-ICP-02, item 7.3.8.2.

2.8.5 Suspender, movimentar e desligar pessoas

20805001	Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.	DOC-ICP-02, item 6.1.5.
20805002	O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público, sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.	DOC-ICP-02, item 7.3.9.
20805003	Declaração, antes do desligamento, de que não possui nenhum tipo de pendência junto às diversas unidades que compõem a entidade deve ser firmada pelo empregado ou servidor.	DOC-ICP-02, item 7.3.10.
20805004	Credenciais, identificações e acessos físicos e lógicos de Agentes de Registro desligados ou suspensos devem ser revogados.	DOC-ICP-02, item 7.3.9.
20805005	Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.	DOC-ICP-02, item 7.3.11.
20805006	Na eventualidade de ação não autorizada por Agente de Registro, real ou suspeita, deve-se suspender o acesso dessa pessoa ao sistema de certificação e instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.	DOC-ICP-05, item 5.3.6.1.
20805007	No caso de desligamento do Agente de Registro, seu dossiê deve conter: a) confirmação da AC quanto à desabilitação do Agente de Registro no sistema de certificação e no CAR; b) declaração assinada pelo Agente de	DOC-ICP-03.01, item 2.2.2.

	Registro de que não possui pendências; e c) resultado da entrevista de desligamento, com a assinatura do entrevistador.	

2.8.6 Manter dossiê de Agentes de Registro

20806001	Os documentos de cada Agente de Registro que esteja atuando ou que já atuou em AR deve ser armazenados em um dossiê.	DOC-ICP-03.01, item 2.2.1.
20806002	Os documentos que compõem os dossiês dos Agentes de Registro devem ser enviados à AC vinculada, inclusive os antigos, e guardados preferencialmente, em ambiente computacional protegido, com acesso permitido somente aos Agentes de Registro vinculados ou responsáveis designados formalmente para trabalhar com os documentos.	DOC-ICP-03.01, item 6.2.1.
20806003	Os dossiês de todos os Agentes de Registro da AR devem ficar em um mesmo ponto de centralização da AC, que deverá ser informado ao ITI.	DOC-ICP-03.01, item 2.2.5.
20806004	Verificações de antecedentes criminais dos Agentes de Registro devem ser renovadas bianualmente.	DOC-ICP-03.01, item 2.4.2.
20806005	Verificações da situação de crédito dos Agentes de Registro devem ser renovadas bianualmente.	DOC-ICP-03.01, item 2.4.2.

3 Os processos nas ACT - Autoridades de Carimbo do Tempo estão assim distribuídos:

3.1 Manter credenciamento de ACT, composto pelos subprocessos:

3.1.1 Manter requisitos de manutenção de credenciamento

30101001	Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 do DOC-ICP-03.	DOC-ICP-03, item 2.1.
30101002	A ACT credenciada deve comunicar, desde logo, à AC Raiz qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores.	DOC-ICP-03, item 3.3.a.i.
30101003	A ACT credenciada deve comunicar, desde logo, à AC Raiz a desvinculação de PSSs credenciados.	DOC-ICP-03, item 3.3.a.ii.
30101004	A entidade credenciada para desenvolver as atividades de ACT deverá encaminhar à AC Raiz relatórios de auditorias realizadas nas suas instalações técnicas, até 30 (trinta) dias após a conclusão das mesmas.	DOC-ICP-03, item 3.3.c.
30101005	A entidade credenciada para desenvolver as atividades de ACT deverá registrar alterações na sua infraestrutura de *hardware*, *software* ou procedimental relacionada diretamente com a atividade de AC, AR, PSS ou PSBio.	DOC-ICP-03, item 3.3.d.
30101006	A ACT deve informar à EAT, mensalmente, a quantidade de carimbos do tempo emitidos.	DOC-ICP-12 item 4.2.3.s.
30101007	Caso ocorra uma ou mais das hipóteses previstas no item 4.3.2 do DOC-ICP-03, a ACT deve ser descredenciada.	DOC-ICP-03, item 4.3.2.

3.1.2 Manter condições fisco-tributárias e econômico-financeiras

30102001	A ACT deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular	DOC-ICP-03, Anexo IV, item 2.

	no cumprimento dos encargos sociais instituídos por lei.	
30102002	A ACT deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos à sua qualificação econômico-financeira: a) Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente. b) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.	DOC-ICP-03, item 2.1.c e Anexo IV, item 3.

3.1.3 Manter contrato de seguro

30103001	A ACT deve manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades.	DOC-ICP-12, item 4.1.2.2.q.
30103002	A ACT deve informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada.	DOC-ICP-12, item 4.1.2.2.r.

3.1.4 Manter e cumprir Política de Segurança de ACT

30104001	Todos os empregados devem possuir conhecimento da PS da ACT, que a deve divulgar.	DOC-ICP-02, item 6.1.2.
30104002	Os empregados, as chefias e os prestadores de serviços devem conhecer os deveres e as responsabilidades definidas na PS.	DOC-ICP-02, item 7.4.1 a 7.4.5.

3.1.5 Comunicar mudanças operacionais e violação de normas

30105001	A ACT deve comunicar à AC Raiz imediatamente as mudanças operacionais ocorridas em seu ambiente e qualquer violação de normas da ICP-Brasil.	DOC-ICP-03, item 3.3.a.
30105002	A ACT credenciada deve comunicar, desde logo, à AC Raiz a violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, cometida pelos PSSs que lhe sejam operacionalmente vinculados.	DOC-ICP-03, item 3.3.a.iii.

3.1.6 Regularizar não conformidades identificadas

30106001	A entidade auditada deve cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas.	DOC-ICP-08, item 9.1.

3.2 Credenciar e manter entidades operacionalmente vinculadas, composto pelos subprocessos:

3.2.1 Auditar entidades operacionalmente vinculadas

30201001	Deverão ser realizadas auditorias nas entidades integrantes da ICP-Brasil conforme frequência estabelecida no DOC-ICP-08.	DOC-ICP-02, item 11.3.
30201002	As ACTs devem encaminhar à AC Raiz relatórios de auditorias realizadas nas suas instalações técnicas, até 30 (trinta) dias após a conclusão das mesmas.	DOC-ICP-03, item 3.3.c.
30201003	A equipe de auditoria deve ser totalmente independente da entidade auditada, aplicando-se no que couber, as regras de suspeição e impedimentos estabelecidas nos artigos 134 e 135 do Código de Processo Civil.	DOC-ICP-08, item 7.1.
30201004	Os auditores que realizarão a auditoria devem firmar declaração, sob as penas da lei, de que não se enquadram em quaisquer das causas de impedimento tratadas no DOC-ICP-08.	DOC-ICP-08, item 7.3.
30201005	Os serviços de auditoria devem ser executados diretamente pela entidade de auditoria credenciada junto à ICP-Brasil, vedada a subcontratação total ou parcial de serviços.	DOC-ICP-08, item 6.1.6.
30201006	As fiscalizações e auditorias realizadas nas ACTs da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades estão em conformidade com suas respectivas DPCTs, PCTs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil.	DOC-ICP-12, item 8.4.1.
30201007	A ACT é responsável pela realização de auditorias anuais das entidades operacionalmente a ela vinculadas, para fins de manutenção de credenciamento.	DOC-ICP-12, item 8.4.4.

3.2.2 Observar procedimentos de extinção de entidades operacionalmente vinculadas

30202001	As ACTs devem comunicar, desde logo, à AC RAIZ a desvinculação de PSS credenciado sob sua responsabilidade.	DOC-ICP-03, item 3.3.a.ii.
30202002	Caso ocorra uma ou mais das hipóteses previstas no item 4 da DOC-ICP-03, para encerramento de ACT, ou PSS vinculado, as ACTs devem proceder o descredenciamento, conforme o caso, da ACT ou PSS vinculado.	DOC-ICP-03, item 4.3.2.
30202003	Nos descredenciamentos de ACT ou PSS, as ACTs ao qual se vinculam devem executar os procedimentos previstos no item 4 do DOC-ICP-03.	DOC-ICP-03, item 4.3.3, e item 4.4.
30202004	As ACT devem executar os procedimentos descrito em suas DPCTs em relação a extinção dos serviços de ACT ou PSS.	DOC-ICP-12, item 5.8.1.

3.2.3 Observar procedimentos de credenciamento de entidades operacionalmente vinculadas

30203001	As ACTs devem observar os critérios a serem atendidos pelos candidatos a credenciamento na ICP-Brasil sob sua vinculação.	DOC-ICP-03, itens 2.1, 2.1.3 e 2.1.4.
30203002	As solicitações dos candidatos ao credenciamento como PSS na ICP-Brasil devem ser encaminhadas à ACT ou candidato a ACT a que o candidato a PSS esteja operacionalmente vinculado, por meio do formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS.	DOC-ICP-03, item 2.2.5.1.1.
30203003	A ACT ou candidato a ACT que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz, a qual será protocolada perante o Protocolo Geral da AC Raiz.	DOC-ICP-03, item 2.2.5.1.2 e 2.2.5.1.3.

3.2.4 Manter credenciamento de entidades operacionalmente vinculadas

30204001	Qualquer alteração em atos constitutivos, estatuto, contrato social ou administradores seus ou de seus vinculados; desvinculação de PSS credenciados; ou ainda violação das diretrizes e normas técnicas da ICP-Brasil cometidas pela própria ou pelos PSSs que lhe sejam operacionalmente vinculados devem ser comunicadas ao ITI.	DOC-ICP-03, item 3.3.a e item 3.4.a.
30204002	O PSS deve observar a DPC, as PCs e a PS da AC, ou a DPCT, as PCTs e PS da ACT ou a DPPSC e PS do PSC a que estiver vinculado.	DOC-ICP-03, item 3.4.b.

30204003	A ACT responde solidariamente pelos atos dos PSSs por ela contratados.	DOC-ICP-12, item 4.1.2.1.2.

3.3 Executar fases do ciclo de vida do carimbo do tempo, composto pelos subprocessos:

3.3.1 Manter a sincronia do tempo

30301001	A disseminação da escala de tempo da ICP-Brasil para as entidades que compõem a rede de carimbo do tempo da ICP-Brasil é realizada pela EAT, que utiliza mecanismos para garantir o sincronismo dos relógios dos equipamentos e a rastreabilidade do tempo informado até a fonte confiável do tempo.	DOC-ICP-11 item 2.4.1.
30301002	Os recursos usados para auditoria e sincronismo dos relógios dos equipamentos que compõem a Rede de Carimbo do Tempo da ICP-Brasil devem seguir o disposto do DOC-ICP-11.01.	DOC-ICP-11 item 2.4.2.
30301003	Os relógios dos SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo.	DOC-ICP-11 item 1.3.
30301004	Os equipamentos que compõem a Rede de Carimbo do Tempo da ICP-Brasil somente receberão os respectivos alvarás se estiverem adequadamente sincronizados.	DOC-ICP-11 item 2.4.3.
30301005	Os alvarás devem ser assinados com certificado digital ICP-Brasil, que garante a autoria desses documentos.	DOC-ICP-11 item 2.4.4.
30301006	O relógio interno do SCT deve estar sincronizado com a FCT (Fonte Confiável do Tempo).	DOC-ICP-12, item 6.5.3.2.
30301007	Os relógios dos SCTs devem estar protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, para evitar que sejam descalibrados. Qualquer modificação ocorrida nestes relógios deverá ser registrada e detectada.	DOC-ICP-12 item 6.7.5.3.

3.3.2 Tratar solicitação de um carimbo do tempo

30302001	A ACT deve definir as formas de lhe solicitar um carimbo do tempo: presencial ou remota.	DOC-ICP-11 item 2.5.1.
30302002	Na solicitação presencial um subscritor deve comparecer em uma ACT	DOC-ICP-11

	para que o documento seja submetido ao Sistema de Carimbo do Tempo – SCT. Ao receber o carimbo do SCT, esse é repassado ao subscritor.	item 2.5.1.1.
30302003	Na solicitação remota, feita a partir de redes de comunicação privadas ou internet, a ACT deve dispor de servidores atuando como interface de acesso ao SCT.	DOC-ICP-11 item 2.5.1.2.
30302004	A ACT é responsável pela implementação, segurança e suporte dos servidores de acesso ao SCT e pelo fornecimento e atualização dos aplicativos que sejam necessários para utilização do serviço.	DOC-ICP-11 item 2.5.2.
30302005	O formato das solicitações e respostas de carimbo do tempo e os protocolos utilizados para o seu transporte devem atender ao disposto na RFC 3161.	DOC-ICP-11 item 2.5.3.
30302006	Os procedimentos detalhados para solicitação e recebimento de carimbos do tempo devem constar nas Declarações de Práticas de Carimbo do Tempo da ACT.	DOC-ICP-11 item 2.5.4.
30302007	Cada ACT pode emitir carimbos do tempo para uso próprio ou por solicitação de terceiros, com base em diferentes Políticas de Carimbo do tempo que especificam o uso desses carimbos e a comunidade a que se aplicam.	DOC-ICP-11 item 2.7.1.

3.3.3 Tratar verificação de um carimbo do tempo

30303001	O subscritor e a terceira parte devem verificar a identidade da ACT e do Sistema de Carimbo do Tempo – SCT. Também devem ser verificados os certificados digitais e o respeito à política sob a qual o carimbo foi emitido.	DOC-ICP-11 item 2.6.1.
30303002	Os procedimentos detalhados para verificação de carimbos do tempo devem constar das Declarações de Práticas de Carimbo do Tempo e das Políticas de Carimbo do tempo (PCT).	DOC-ICP-11 item 2.6.2.
30303003	Somente são aceitos na ICP-Brasil carimbos do tempo emitidos por Sistema de Carimbo do Tempo – SCT com alvarás de sincronismo fornecidos por Sistemas de Auditoria e Sincronismo.	DOC-ICP-11 item 2.7.2.

3.4 Manter publicações, composto pelos subprocessos:

3.4.1 Manter DPCT, PCT e PS

30401001	As alterações nas DPCT, PCT e PS devem ser submetidas à aprovação da AC Raiz.	DOC-ICP-03, item 3.3.b; DOC-ICP-12, item 9.12.1; DOC-ICP-13, item 9.12.1.1.
30401002	Toda DPCT e PCT elaborada no âmbito da ICP-Brasil deve observar requisitos e estrutura do DOC-ICP-12/DOC-ICP-13 (RFC 3628 e 3161).	DOC-ICP-12, item 1.1.6; DOC-ICP-13, item 1.1.6.
30401003	Toda DPCT e PCT elaborada no âmbito da ICP-Brasil deve indicar no item 1.2 o nome da instituição e o OID atribuído para a respectiva DPCT ou PCT, conforme o caso.	DOC-ICP-12, item 1.2, DOC-ICP-13, item 1.2.
30401004	Toda DPCT e PCT elaborada no âmbito da ICP-Brasil deve indicar as informações das entidades envolvidas e a aplicabilidade dos carimbos do tempo emitidos.	DOC-ICP-12, item 1.3, DOC-ICP-13, item 1.5.
30401005	Toda PCT elaborada no âmbito da ICP-Brasil deve indicar as características dos carimbos que serão emitidos, contendo, no mínimo, a exatidão ou precisão mínima do tempo registrado no carimbo e a unidade utilizada no campo *genTime* do carimbo do tempo.	DOC-ICP-13, item 1.4.
30401006	Toda DPCT elaborada no âmbito da ICP-Brasil deve indicar as obrigações gerais conforme estabelecido no DOC-ICP-12.	DOC-ICP-12, item 4.1.2.
30401007	Toda DPCT elaborada no âmbito da ICP-Brasil deve indicar no item 3 os requisitos de identificação e autenticação dos solicitantes de carimbo do tempo.	DOC-ICP-12, item 3.
30401008	Toda DPCT e PCT elaborada no âmbito da ICP-Brasil deve indicar os requisitos operacionais referentes à emissão de um carimbo do tempo.	DOC-ICP-12, item 4 e DOC-ICP-13, item 2.

30401009	Toda DPCT elaborada no âmbito da ICP-Brasil deve indicar no item 5 os controles de segurança física, procedimental e pessoal.	DOC-ICP-12, item 5.
30401010	Toda DPCT elaborada no âmbito da ICP-Brasil deve indicar no item 6 os Controles Técnicos de Segurança.	DOC-ICP-12, item 6.
30401011	Toda DPCT elaborada no âmbito da ICP-Brasil deve indicar no item 7 os Perfis dos Carimbos do Tempo.	DOC-ICP-12, item 7.

3.4.2 Manter publicação de informações da ACT

30402001	ACT deve publicar em sua página *web* a DPCT, a PCT e as condições gerais mediante as quais são prestados os serviços de carimbo do tempo.	DOC-ICP-12, item 4.1.2.2.j.
30402002	A ACT deve publicar em sua página *web* a exatidão do carimbo do tempo com relação ao UTC.	DOC-ICP-12, item 2.1.2.e.
30402003	A ACT deve publicar em sua página *web* os algoritmos de *hash* que poderão ser utilizados pelos subscritores e o algoritmo de *hash* utilizado pela ACT	DOC-ICP-12, item 2.1.2.f.
30402004	A ACT deve publicar em sua página *web* a relação, regularmente atualizada, dos Prestadores de Serviço vinculados.	DOC-ICP-12, item 2.1.2.g.

3.4.3 Manter publicação dos certificados dos SCT

30403001	A ACT deve publicar em sua página *web* os certificados dos SCT que opera.	DOC-ICP-12, item 2.1.2.a.

3.5 Manter segurança da informação, composto pelos subprocessos:

3.5.1 Manter inventário de ativos

30501001	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
30501002	O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.	DOC-ICP-02, item 8.2.12 e

		9.3.5.10.
30501003	O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.	DOC-ICP-02, item 9.2.5.

3.5.2 Manter análise de risco e Plano de Continuidade do Negócio - PCN

30502001	Todas as ACs e ACTs integrantes da ICP-Brasil deverão apresentar um PCN e, ainda, um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres, que estabelecerá, no mínimo, o tratamento adequado dos eventos de segurança descritos no DOC-ICP-02, item 13.2.2.	DOC-ICP-02, item 13.2.2.
30502002	Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.	DOC-ICP-02, item 6.4.1 e DOC-ICP-12, item 2.1.1.p.
30502003	Todos os incidentes devem ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.	DOC-ICP-02, item 6.4.4.
30502004	Todos os ativos de processamento das entidades devem estar relacionados no PCN.	DOC-ICP-02, item 7.4.3.c.
30502005	Em um processo de gerenciamento de riscos, que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, os seguintes pontos principais devem ser identificados: a) o que deve ser protegido; b) a análise de riscos (contra quem ou contra o quê deve ser protegido); c) avaliação de riscos (análise da relação custo/benefício).	DOC-ICP-02, item 12.1.
30502006	A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: a) requisitos de segurança definidos pelo serviço; b) objetivo do serviço, público-alvo; c) classificação da informação; d) forma de acesso; e) frequência de atualização do conteúdo; f) forma de administração do serviço e volume de tráfego.	DOC-ICP-02, item 9.3.3.23.

30502007	O processo de gerenciamento de riscos deve ser revisto anualmente pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.	DOC-ICP-02, item 6.2.

3.5.3 Manter documentos armazenados e classificados

30503001	Toda a documentação fornecida ao pessoal deve estar classificada segundo a política de classificação de informação definida pela ACT e deve ser mantida atualizada.	DOC-ICP-12, item 5.3.8.2.
30503002	A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.	DOC-ICP-02, item 9.2.1.
30503003	Os registros devem ser protegidos e armazenados de acordo com a sua classificação, conforme a PS da ICP-Brasil.	DOC-ICP-12, item 5.5.3.
30503004	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.	DOC-ICP-02, item 9.3.5.9.
30503005	As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias, devendo a integridade ser verificada, no mínimo, a cada 6 (seis) meses.	DOC-ICP-12, item 5.5.4.2 e 5.5.4.3.

3.6 Manter sistemas aplicativos, composto pelos subprocessos

3.6.1 Manter sistemas de informação

30601001	As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.	DOC-ICP-02 item 9.3.1.1.
30601002	A documentação dos sistemas deve ser mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
30601003	A cópia de segurança deve ser testada e mantida atualizada.	DOC-ICP-02 item 9.3.1.1.

30601004	Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.	DOC-ICP-02 item 9.3.1.5.
30601005	As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.	DOC-ICP-02 item 9.3.1.5.
30601006	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.5.11.
30601007	Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.	DOC-ICP-02 item 10.2.3.

3.6.2 Manter bases de dados

30602001	Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.	DOC-ICP-02, item 10.1.4.
30602002	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.	DOC-ICP-02, item 10.3.1.
30602003	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.	DOC-ICP-02, item 9.2.2.
30602004	Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.	DOC-ICP-02, item 9.3.3.17.
30602005	As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.	DOC-ICP-02, item 9.3.5.4.
30602006	Devem ser estabelecidos os formatos e padrões de data e hora contidos em cada tipo de registro.	DOC-ICP-12, item 5.5.5.
30602007	Proteção lógica adicional (criptografia) e senhas devem ser adotados para evitar o acesso não autorizado às informações. O arquivo de senhas deve ser criptografado e ter acesso controlado.	DOC-ICP-02, item 9.3.2.5 e item 9.3.4.5.

3.7 Manter segurança lógica e rede, composto pelos subprocessos:

3.7.1 Manter sistemas básicos

30701001	Os aplicativos e equipamentos utilizados nos processos de certificação digital devem possuir certificado de homologação da ICP-Brasil ou Certificação INMETRO.	DOC-ICP-01.01, item 3.
30701002	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.	DOC-ICP-02, item 9.3.2.3.
30701003	As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.	DOC-ICP-02, item 9.3.2.4.
30701004	A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.	DOC-ICP-02, item 9.3.2.6.
30701005	Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.	DOC-ICP-02, item 9.3.2.7.
30701006	Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.	DOC-ICP-02, item 9.3.3.3.
30701007	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.

3.7.2 Manter equipamentos protegidos de ameaças

30702001	O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o "*Efeito Tempest*".	DOC-ICP-02, item 9.3.3.1.
30702002	Mecanismos de segurança baseados em sistemas de proteção (*firewall*)	DOC-ICP-02,

	devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.	item 9.3.3.19.
30702003	A ativação da rede deve respeitar a ordem prevista no DOC-ICP-02, item 9.3.3.26. Os sistemas de certificação devem ser dispostos em segmentos de rede que devem ser isolados por meios diversos, como por exemplo: a) utilizando virtual "lans" (vlan); b) utilizando de *firewall*; c) utilizando artifícios de roteamento.	DOC-ICP-02, itens 9.3.3.26 e 9.3.3.27.
30702004	Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.	DOC-ICP-02, itens 9.3.3.2.
30702005	Ativos de processamento da rede, a exemplo de "*switches*" e roteadores, quando possuírem recursos básicos de segurança como acesso mediante senhas e outros, devem ser configurados para utilizá-los, visando reforçar seus controles de segurança.	DOC-ICP-02, itens 9.3.3.3.
30702006	Nos computadores pessoais, devem ser adotadas medidas para combate de vírus, realização de *backups*, controle de acesso e uso de *software* não autorizado.	DOC-ICP-02, item 9.3.5.3.
30702007	Em todos os equipamentos devem ser sistematizados procedimentos para combate a processos destrutivos (virus, "*worms"* e cavalos-de-tróia).	DOC-ICP-02, item 9.3.6 e DOC-ICP-12, item 6.10.5.2.
30702008	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.	DOC-ICP-02, item 9.3.3.30.
30702009	Definir procedimentos formais para a eliminação segura de mídias desnecessárias.	DOC-ICP-02, item 9.3.5.12.

3.7.3 Manter *logs* e trilhas de auditoria

30703001	Informações de segurança não geradas pelo sistema de certificação devem ser registradas.	DOC-ICP-12, item 5.4.1.2.
30703002	Registrar as violações de segurança e avaliar esses registros periodicamente	DOC-ICP-02, item 9.2.3.

30703003	Definir, analisar periodicamente e proteger devidamente arquivos de *logs* de sistemas.	DOC-ICP-02, item 9.3.1.3.
30703004	Para os sistemas de controle de acesso lógico, os registros de atividades (*logs*) devem ser analisados periodicamente.	DOC-ICP-02, item 9.3.4.15.

3.7.4 Manter cópias de segurança e restauração

30704001	A ACT deve descrever na DPCT os procedimentos para recuperação de recursos computacionais corrompidos.	DOC-ICP-12, item 5.7.2.
30704002	Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.	DOC-ICP-02, item 9.3.2.9.

3.7.5 Manter controle de acesso a rede

30705001	A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.	DOC-ICP-02, item 9.3.3.9.
30705002	Devem ser implementados mecanismos de *firewall* em equipamentos de utilização específica, configurados exclusivamente para tal função. Os *firewalls* deverão ser dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à ACT.	DOC-ICP-12, item 6.7.2.1.
30705003	As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, semanal e todas as ações tomadas em decorrência desse exame deverão ser documentadas.	DOC-ICP-12, item 6.7.4.
30705004	Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, deverão estar localizados e operar em ambientes de nível, no mínimo, 3.	DOC-ICP-12, item 6.7.1.2.

30705005	Nos ambientes de rede, registrar e avaliar periodicamente eventos de segurança.	DOC-ICP-02, item 9.3.3.10.
30705006	O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.	DOC-ICP-02, item 9.3.3.15.

3.7.6 Manter controle de acesso lógico

30706001	Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.	DOC-ICP-02, item 9.3.2.2.
30706002	O ambiente operacional dos sistemas deve ser monitorado.	DOC-ICP-02, item 9.3.2.3.
30706003	A ACT deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a PS da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.	DOC-ICP-12, item 5.2.3.3.
30706004	Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.	DOC-ICP-02, item 9.3.1.2.
30706005	O responsável pela autorização ou confirmação da autorização de acesso lógico a sistemas e servidores deve ser claramente definido e registrado.	DOC-ICP-02, item 9.3.2.1.
30706006	O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido.	DOC-ICP-02, item 9.3.2.1.
30706007	As autorizações de acesso lógico das máquinas servidoras devem ser revistas, confirmadas e registradas continuamente.	DOC-ICP-02, item 9.3.2.1.
30706008	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.	DOC-ICP-02, item 9.3.3.7.
30706009	O arquivo de senhas deve ser criptografado e ter o acesso controlado.	DOC-ICP-02, item 9.3.4.5.
30706010	O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.	DOC-ICP-02, item 9.3.4.8.

3.8 Manter infraestrutura, composto pelos subprocessos:

3.8.1 Manter equipamentos de computação

30801001	Materiais criptográficos, tais como, chaves, suas cópias e equipamentos criptográficos devem ser armazenados em ambiente de nível 4, interior ao ambiente de nível 3.	DOC-ICP-12, item 5.1.2.1.15.
30801002	Preferentemente, *no-breaks*, geradores e outros componentes da infraestrutura física deverão estar abrigados no nível 2, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção.	DOC-ICP-12, item 5.1.2.1.6.

3.8.2 Manter controle de acesso físico

30802001	Acesso aos componentes de infraestrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.	DOC-ICP-02, item 8.2.10.
30802002	A segurança de todos os ambientes da ACT deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana).	DOC-ICP-12, item 5.1.2.2.1.
30802003	O uso de equipamentos nas instalações da ACT só pode ser realizado após a autorização formal e sob supervisão.	DOC-ICP-02, item 8.2.13.
30802004	Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).	DOC-ICP-02, item 8.2.14.
30802005	Acesso de visitantes aos ambientes da ACT deve ser registrado e supervisionado.	DOC-ICP-02, item 8.2.15.
30802006	Devem ser instalados e testados regularmente sistemas de detecção de intrusos de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.	DOC-ICP-02, item 8.2.17.
30802007	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.	DOC-ICP-02, item 8.2.4.
30802008	Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.	DOC-ICP-02, item 8.2.5.

30802009	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.	DOC-ICP-02, item 8.2.6.
30802010	Os sistemas de AC e ACT deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio frequência.	DOC-ICP-02, item 8.2.7.
30802011	Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.	DOC-ICP-02, item 8.2.8 e DOC-ICP-12, item 5.1.2.
30802012	A entrada e saída, de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.	DOC-ICP-02, item 8.2.9.
30802013	Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.	DOC-ICP-02, item 9.3.3.11.
30802014	A infraestrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.	DOC-ICP-02, item 9.3.3.13.
30802015	Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.	DOC-ICP-02, item 9.3.3.2 .
30802016	Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).	DOC-ICP-02, item 9.3.5.2.
30802017	A ACT deve registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação como os registros de acessos físicos.	DOC-ICP-12, item 5.4.1.2.
30802018	A ACT deve possuir pelo menos 3 (três) níveis de acesso físico aos diversos ambientes da ACT, e mais 1 (um) nível relativo à proteção do SCT.	DOC-ICP-12, item 5.1.2.1.1.
30802019	Para garantir a segurança do material armazenado, o cofre ou o gabinete	DOC-ICP-12,

	deverá ser feito em aço ou material de resistência equivalente e possuir tranca com chave.	item 5.1.2.1.16.
30802020	O cofre ou gabinete que abrigará os SCTs deverá ser trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança da ACT.	DOC-ICP-12, item 5.1.2.1.17.
30802021	O primeiro nível – ou nível 1 – deverá situar-se após a primeira barreira de acesso às instalações da ACT. O ambiente de nível 1 das ACTs da ICP-Brasil desempenha a função de interface com o cliente que deseja utilizar o serviço de carimbo do tempo e necessita comparecer pessoalmente à ACT.	DOC-ICP-12, item 5.1.2.1.2.
30802022	O segundo nível – ou nível 2 – será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.	DOC-ICP-12, item 5.1.2.1.3.
30802023	O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-12, item 5.1.2.1.4.
30802024	O acesso ao nível 2 deverá ser permitido apenas a pessoas que trabalhem diretamente com as atividades de carimbo do tempo ou ao pessoal responsável pela manutenção de sistemas e equipamentos da ACT, como administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT ou do possível ambiente que esta compartilhe não deverão acessar este nível.	DOC-ICP-12, item 5.1.2.1.5.
30802025	Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e supervisão.	DOC-ICP-12, item 5.1.2.1.7.
30802026	O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da ACT. Qualquer atividade relativa à emissão de carimbos do tempo deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.	DOC-ICP-12, item 5.1.2.1.8.
30802027	No terceiro nível deverão ser controladas tanto as entradas quanto as	DOC-ICP-12,

	saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha.	item 5.1.2.1.9.
30802028	As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-12, item 5.1.2.1.10.
30802029	Caso o ambiente de nível 3 possua forro ou piso falsos, devem ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior.	DOC-ICP-12, item 5.1.2.1.11.
30802030	Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deve ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.	DOC-ICP-12, item 5.1.2.2.12.
30802031	O ambiente de nível 3 deverá ser dotado, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 2.	DOC-ICP-12, item 5.1.2.2.3 e 5.1.2.2.4.
30802032	Caso a ACT se situe dentro de um *datacenter*, com requisitos de segurança julgados adequados pela AC-Raiz, poderá ser dispensada a existência de um ambiente de Nível 3 específico para a ACT.	DOC-ICP-12, item 5.1.2.1.14.
30802033	O quarto nível, ou nível 4, interior ao ambiente de nível 3, deverá compreender pelo menos 2 cofres ou gabinetes reforçados trancados, que abrigarão, separadamente os SCT e equipamentos criptográficos; outros materiais criptográficos, tais como cartões, chaves, dados de ativação e suas cópias.	DOC-ICP-12, item 5.1.2.1.15.
30802034	Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.	DOC-ICP-02, item 8.2.11.

3.8.3 Manter ar-condicionado

30803001	O sistema de ar-condicionado deve possuir redundância.	DOC-ICP-12, item 5.1.3.9.
30803002	O sistema de climatização deve atender às condições ambientais estabelecidas na Norma NBR 11515.	DOC-ICP-12, item 5.1.3.7. e 5.1.6.
30803003	A temperatura dos ambientes atendida pelo sistema de climatização deve ser permanentemente monitorada.	DOC-ICP-12, item 5.1.3.8.

3.8.4 Manter energia elétrica

30804001	A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.	DOC-ICP-02, item 9.3.3.14.
30804002	A energia elétrica para a infraestrutura da ACT deve possuir sistemas e dispositivos que garantam o fornecimento ininterrupto.	DOC-ICP-12, item 5.1.3.1.
30804003	Todos os cabos elétricos devem estar protegidos por tubulações ou dutos apropriados.	DOC-ICP-12, item 5.1.3.2.
30804004	Sistema de aterramento deve ser implantado.	DOC-ICP-12, item 5.1.3.1.
30804005	Tubulações, dutos, calhas, quadros e caixas - de passagem, distribuição e terminações - devem ser construídos de forma a facilitar vistorias e a detecção de tentativas de violações.	DOC-ICP-12, item 5.1.3.3.
30804006	Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados.	DC-ICP-12, item 5.1.3.3.
30804007	Todos os cabos devem ser catalogados e vistoriados no mínimo a cada 6 (seis) meses.	DOC-ICP-12, item 5.1.3.4.
30804008	Deve ser mantida atualizada a topologia de rede de cabos.	DOC-ICP-12, item 5.1.3.5.
30804009	Instalações elétricas provisórias, fiações expostas e conexões inadequadas não devem ser admitidas.	DOC-ICP-12, item 5.1.3.6.

3.8.5 Manter sistema de combate a incêndio

30805001	Nas instalações da ACT não será permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.	DOC-ICP-12 item 5.1.5.1.
30805002	No interior do ambiente nível 3 devem existir extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de *sprinklers* no prédio, o ambiente de nível 3 da ACT não deverá possuir saídas de água, para evitar danos aos equipamentos.	DOC-ICP-12, item 5.1.5.2.
30805003	O ambiente de nível 3 deve possuir sistema de prevenção contra incêndios, que acione alarmes preventivos uma vez detectada fumaça no ambiente.	DOC-ICP-12, item 5.1.5.3.
30805004	Nos demais ambientes da ACT deverão existir extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio.	DOC-ICP-12, item 5.1.5.4.
30805005	Mecanismos específicos deverão ser implantados pela ACT para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.	DOC-ICP-12, item 5.1.5.5.

3.9 Manter recursos humanos, composto pelos subprocessos:

3.9.1 Admitir pessoas

30901001	Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.	DOC-ICP-02, item 7.3.1.1.
30901002	Nenhuma entidade participante da ICP-Brasil deve admitir estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.	DOC-ICP-02, item 7.3.1.2.

30901003	A entrevista de admissão deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.	DOC-ICP-02, item 7.3.4.1.
30901004	Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.	DOC-ICP-02, item 7.3.4.2.
30901005	Todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL. A ACT responsável poderá definir requisitos adicionais para a contratação.	DOC-ICP-12, item 5.3.7.
30901006	Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil.	DOC-ICP-02, item 7.3.3.
30901007	O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.	DOC-ICP-02, item 7.3.1.3.

3.9.2 Manter capacitação de pessoas

30902001	Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.	DOC-ICP-02, item 6.1.3.
30902002	Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.	DOC-ICP-02, item 6.1.4.
30902003	Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.	DOC-ICP-02, item 7.3.7.
30902004	Todos os empregados da ACT deverão receber treinamento específico antes de obter qualquer tipo de acesso.	DOC-ICP-12, item 5.2.1.3.

30902005	Todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da ACT.	DOC-ICP-12, item 5.3.4.
30902006	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar os incidentes descritos no DOC-ICP-02.	DOC-ICP-02, item 13.2.3.
30902007	Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.	DOC-ICP-02, item 7.3.5.2.

3.9.3 Manter habilitação de pessoas

30903001	Todo empregado da ACT responsável terá sua identidade e perfil verificados antes de: a) ser incluído em uma lista de acesso físico às instalações da ACT; b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis da ACT; c) ser incluído em uma lista para acesso lógico aos SCTs da ACT	DOC-ICP-12, item 5.2.3.1.
30903002	Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.	DOC-ICP-02, item 10.2.1.
30903003	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.	DOC-ICP-02, item 10.2.2.
30903004	Todos os empregados da ACT deverão estar identificados por uma credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo máximo de 1 (um) ano de validade. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário.	DOC-ICP-02, item 7.3.6.
30903005	As responsabilidades pela segurança física dos sistemas das entidades	DOC-ICP-02,

	deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.	item 8.2.1.
30903006	Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.	DOC-ICP-02, item 9.3.4.16.
30903007	A ACT deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o SCT sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.	DOC-ICP-12, item 5.2.1.1.
30903008	A ACT deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação: administrador do sistema, operador de sistema e auditor de sistema.	DOC-ICP-12, item 5.2.1.2.
30903009	O tipo e o nível de acesso dos operadores do sistema de certificação da ACT serão determinados, em documento formal, com base nas necessidades de cada perfil.	DOC-ICP-12, item 5.2.1.3.
30903010	Todas as tarefas executadas no cofre ou gabinete onde se localizam os SCT deverão requerer a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. As demais tarefas da ACT poderão ser executadas por um único empregado.	DOC-ICP-12, item 5.2.2.2.
30903011	A AC deve designar formalmente o responsável por inventariar, classificador, permanentemente atualizar seus ativos.	DOC-ICP-02, item 6.3.
30903012	A ACT deve descrever os requisitos para a caracterização e o reconhecimento de perfis qualificados na ACT responsável e nos PSSs a ela vinculados, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.	DOC-ICP-12, item 5.2.

3.9.4 Avaliar desempenho

30904001	Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.	DOC-ICP-02, item 7.3.5.1.
30904002	Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.	DOC-ICP-02, item 7.3.8.1.

30904003	Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.	DOC-ICP-02, item 7.3.8.2.
30904004	Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.	DOC-ICP-02, item 7.3.8.3.
30904005	As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.	DOC-ICP-02, item 7.3.8.4.

3.9.5 Suspender, movimentar e desligar pessoas

30905001	Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.	DOC-ICP-02, item 6.1.5.
30905002	O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público. Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.	DOC-ICP-02, item 7.3.9.
30905003	Quando um empregado se desligar da ACT, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da ACT, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à ACT no ato de seu desligamento.	DOC-ICP-12, item 5.2.1.4.
30905004	O empregado ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a entidade, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.	DOC-ICP-02, item 7.3.10.
30905005	Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.	DOC-ICP-02, item 7.3.11.
30905006	A ACT pode definir uma política a ser adotada pela ACT responsável e	DOC-ICP-12,

	pelos PSSs vinculados para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.	item 5.3.5.
30905007	Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT responsável ou de um PSS vinculado, a ACT deverá, de imediato, suspender o acesso dessa pessoa aos SCT, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.	DOC-ICP-12, item 5.3.6.1.
30905008	As punições passíveis de aplicação, em decorrência de processo administrativo, são: a) advertência; b) suspensão por prazo determinado; ou c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.	DOC-ICP-12, item 5.3.6.4.

4 Os processos nos PSBio – Prestadores de Serviço Biométrico estão assim distribuídos:

4.1 Manter credenciamento de PSBio, composto pelos subprocessos:

4.1.1 Manter requisitos de manutenção de credenciamento

40101001	Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 do DOC-ICP-03.	DOC-ICP-03, item 2.1.
40101002	Os PSBios deverão ser entidades com capacidade técnica para realizar a identificação e a verificação biométrica do requerente de um certificado digital em um ou mais bancos/sistemas de dados biométrico da ICP-Brasil.	DOC-ICP-03, item 1.2.d.
40101003	Os candidatos ao credenciamento como PSBios devem apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS, ter sede administrativa localizada no território nacional e ter instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de identificação biométrica, localizadas no território nacional, ou contratar PSS que as possua.	DOC-ICP-03, item 2.1.5.
40101004	As solicitações dos candidatos ao credenciamento como PSBio na ICP-Brasil serão encaminhadas ao ITI, por intermédio da cadeia hierárquica, mediante a apresentação dos documentos relacionados no DOC-ICP-03, item 2.2.6.1.1.	DOC-ICP-03, item 2.2.6.1.1.
40101005	Ao protocolar a solicitação de credenciamento, o candidato a PSBIO deve estar em conformidade com todos os requisitos exigidos pelas resoluções	DOC-ICP-03, item 2.2.6.2.1.

	do CG da ICP-Brasil relacionados à atividade de prestador de serviços biométricos e pronto para ser auditado, conforme os critérios e procedimentos para realização de auditoria nas entidades da ICP-Brasil dispostos no DOC-ICP-08.	
40101006	A entidade credenciada para desenvolver as atividades de PSBio deverá, via cadeia hierárquica, encaminhar ao ITI, relatórios de auditorias em até 30 (trinta) dias após a conclusão das mesmas.	DOC-ICP-03, item 3.5.b.
40101007	A entidade credenciada para desenvolver as atividades de PSBio deverá, observar o DOC-ICP-05.03 e a PS aplicável.	DOC-ICP-03, item 3.5.c.
40101008	A entidade credenciada para desenvolver as atividades de PSBio deve manter conformidade com os Requisitos Mínimos de Segurança PSBio na ICP-Brasil, DOC-ICP-03.02.	DOC-ICP-03.02, item 01.
40101009	Caso ocorra uma ou mais das hipóteses previstas no item 4.5.1 do DOC-ICP-03 o PSBio deve ser descredenciado.	DOC-ICP-03, item 4.5.1.

4.1.2 Manter condições fisco-tributárias e econômico-financeiras

40102001	O PSBio deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.	DOC-ICP-03, Anexo V, item 2.
40102002	O PSBio deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos à sua qualificação econômico-financeira: a) Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente. b) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), atestando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.	DOC-ICP-03, item 2.1.c e Anexo V, item 3.

4.1.3 Manter contrato de seguro

40103001	PSBio cuja a empresa tenha sido criada a menos de um ano deve manter vigente apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 2.000.000,00 (dois milhões de reais).	DOC-ICP-03, Anexo V, item 3.2.e.

4.1.4 Manter e cumprir a Política de Segurança - PS do PSBio

40104001	Todos os empregados devem possuir conhecimento da PS do PSBio que a deve divulgar.	DOC-ICP-02, item 6.1.2 e DOC-ICP-03.02, item 1.
40104002	Os empregados, as chefias e os prestadores de serviços devem conhecer os deveres e as responsabilidades definidas na PS.	DOC-ICP-02, item 7.4.1 a 7.4.5.

4.1.5 Comunicar mudanças operacionais e violação de normas

40105001	A entidade credenciada para desenvolver as atividades de PSBio deverá, via cadeia hierárquica, comunicar ao ITI qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores.	DOC-ICP-03, item 3.5.a.i.
40105002	O PSBio deve comunicar formalmente e imediatamente as mudanças operacionais ocorridas em seu ambiente de certificação e qualquer violação de normas da ICP-Brasil.	DOC-ICP-03, item 3.5.a.

4.1.6 Regularizar não conformidades identificadas

40106001	A entidade auditada deve cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas.	DOC-ICP-08, item 9.1.

4.2 Executar Fases do Ciclo Biométrico, composto pelos subprocessos:

4.2.1 Manter base biométrica

40201001	A base biométrica ICP-Brasil, sob responsabilidade dos PSBios credenciados, será anônima. Esse anonimato é garantido pelo fato dos registros biométricos estarem associados ao Identificador de Registro Biométrico (IDN) único para cada pessoa, não sendo possível ao PSBio relacionar esse identificador a nenhum dado biográfico da pessoa.	DOC-ICP-05.03, item 1.3.1.
40201002	O PSBio deve garantir a segregação entre a base biométrica local da AC/PSS e a base biométrica do PSBio, mantendo o anonimato da base no PSBio.	DOC-ICP-05.03, item 1.3.3.
40201003	A fotografia frontal da face deve seguir os parâmetros mínimos previstos DOC-ICP-05.03, item 2.4.1.	DOC-ICP-05.03, item 2.4.
40201004	A impressão digital deve seguir os parâmetros mínimos previstos DOC-ICP-05.03, item 2.4.2.	DOC-ICP-05.03, item 2.4.
40201005	O PSBio deve armazenar os registros biométricos de impressão digital e face, tendo cada registro vinculado ao IDN (Identificador de Registro Biométrico).	DOC-ICP-05.03, item 3.4.1.1.
40201006	O PSBio deve ser capaz de realizar a identificação (1:N) biométrico de impressão digital e face por meio do seu IDN.	DOC-ICP-05.03, item 3.4.1.2.
40201007	O PSBio deve ser capaz de fazer a verificação (1:1) biométrica de impressão digital e face de um registro por meio de seu IDN.	DOC-ICP-05.03, item 3.4.1.3.
40201008	As operações biométricas devem utilizar posições de dedos conhecidas, ou seja, cada dedo será comparado apenas com os dedos cadastrados para a mesma posição.	DOC-ICP-05.03, item 3.4.1.4.
40201009	Para garantir que determinados dados biométricos não existem na Rede PSBio com outro IDN, deve ser realizada comparação através de dedos, para aqueles registros em que isso for possível, e por face, nos registros onde não existirem dedos disponíveis para identificação. No caso de emissão primária com batimento biométrico em base de identificação oficial, fica dispensada essa comparação de face (1:N).	DOC-ICP-05.03, item 4.4.4.
40201010	O PSBio deve ser capaz de identificar as irregularidades e duplicidades dos registros e prontamente realizar as comunicações para as entidades biométricas credenciadas, se for o caso, publicando essas informações para a AC/PSS que solicitou o cadastramento, para os devidos encaminhamentos.	DOC-ICP-05.03, item 3.5.2.
40201011	O sistema utilizado para realizar as identificações dos requerentes de um	DOC-ICP-05.03,

	certificado digital deve ter, no mínimo, a acurácia definida no DOC 05.03, item 3.6.3.	item 3.6.3.
40201012	O procedimento de substituição da chave criptográfica simétrica, incluindo a indexação dos IDNs recalculados, deve ser executado num prazo máximo de 15 (quinze) dias, de maneira sincronizada entre as entidades e PSBios, de forma a não causar indisponibilidades no sistema.	DOC-ICP-05.04, item 4.
40201013	Após a reindexação das bases de dados, os PSBios deverão excluir permanentemente qualquer informação indexada pelo IDN gerado a partir da chave criptográfica simétrica anterior, devendo a AC manter em seus registros a associação entre IDN antigo e o novo.	DOC-ICP-05.04, item 4.

4.2.2 Gerenciar transações biométricas

40202001	O PSBio deve receber e processar cada transação separadamente, por ordem cronológica de solicitação, independentemente de qual entidade (ACs ou outros PSBios), devendo preservar as trilhas de auditoria para comprovação de horário de chegada e saída das transações.	DOC-ICP-05.03, item 3.3.2.
40202002	As requisições para os serviços de HUB devem seguir o padrão assíncrono, ou seja, todas as respostas devem ser retornadas pelo HUB que recebeu a solicitação quando o mesmo tiver a informação disponível.	DOC-ICP-05.03, item 3.7.4.
40202003	As requisições para os serviços de HUB devem utilizar o método POST, e seguir as especificações previstas no DOC-ICP-05.03, item 5.2.8.	DOC-ICP-05.03, item 5.2.8.
40202004	As requisições devem utilizar autenticação dupla com certificado ICP-Brasil, e a identificação do PSBio deve ser feita por meio do certificado enviado pelo lado cliente (quem originou a requisição). O FQDN (*Fully Qualified Domain Name*) do PSBio deve estar presente no CN (*Common name*) do certificado.	DOC-ICP-05.03, item 3.3.3 e item 3.3.5.
40202005	O PSBio deve possuir uma interface para receber as transações de remoção de um IDN da base biométrica por parte de suas ACs. devendo remover o IDN da mesma e repassar a transação aos demais PSBios para que estes possam remover o registro de seus *caches*, se for o caso.	DOC-ICP-05.03, item 3.11.
40202006	As exceções (suspeitas de irregularidades e duplicidades dos registros) devem ser prontamente comunicadas para as entidades biométricas credenciadas, se for o caso, disponibilizando essas informações para a AC que solicitou o cadastramento, para os devidos encaminhamentos.	DOC-ICP-05.03, item 3.5.2.
40202007	Sempre que uma AC responsável pelo IDN confirmar uma fraude, deve informar ao PSBio a necessidade de remoção do IDN da base e o PSBio deverá fazer a propagação da mensagem de remoção à Rede PSBio.	DOC-ICP-05.03, item 2.6.6.

40202008	O cadastramento de um novo IDN deve passar por uma série de etapas para garantir a unicidade das biometrias na Rede PSBio, além de verificar base de fraudadores conhecidos.	DOC-ICP-05.03, item 4.4.1.
40202009	Em horários agendados de hora em hora, o PSBio deve consultar as operações que estiverem pendentes junto a outros PSBios e deve ainda solicitar o reenvio destas transações e adicioná-las à fila de processamento.	DOC-ICP-05.03, item 3.10.4.
40202010	É obrigatório que transações da AC e de outros PSBios sejam tratadas com igual prioridade.	DOC-ICP-05.03, item 3.5.4.
40202011	Não é autorizado ao PSBio guardar qualquer tipo de dado biográfico de indivíduos.	DOC-ICP-05.03, item 3.4.1.5.
40202012	Na consulta ao sistema da AC para verificar se existe cadastro biométrico na Base Local da AC, caso o CPF ainda não esteja cadastrado na Base Local da AC, deve ser realizada uma coleta de cadastro (ENR) seguindo o descrito no item 4.1.2 do DOC-ICP-05.03. Caso o CPF já exista na Base Local da AC, deverá ser realizada uma verificação (VER).	DOC-ICP-05.03, item 4.1.
40202013	As transações de verificação devem ser executadas com prioridade sobre transações de identificação.	DOC-ICP-05.03, item 4.4.3.2.
40202014	A atualização de dados é possível apenas para cadastros pertencentes ao PSBio. Não haverá atualização de cadastros de outro PSBio, e em caso de correção o IDN deverá ser removido e novo cadastro ser efetivado.	DOC-ICP-05.03, item 4.4.2.1.
40202015	O processo de atualização deve incluir a verificação utilizando biometrias preexistentes e identificação de biometrias novas na Rede PSBio para garantir que não são pertencentes a fraudador ou outro IDN.	DOC-ICP-05.03, item 4.4.2.2.
40202016	As transações de atualização, devem ser precedidas de uma transação de verificação, que valide pelo menos uma das biometrias do registro existente.	DOC-ICP-05.03, item 5.1.1.2.1.4.
40202017	Durante o processo de atualização, os dados biométricos enviados na transação devem sobrepor os já existentes e, caso alguma biometria não seja enviada, os dados anteriores devem ser mantidos. Deve ser realizado o processo de busca 1:N em todas as novas biometrias enviadas na transação.	DOC-ICP-05.03, item 5.1.1.2.1.5.
40202018	Uma transação biométrica de atualização deve formatar os dados mencionados em formato ANSI/NIST, seguindo o formato definido no DOC-ICP-05.03, item 5.1.1.2.1.6.	DOC-ICP-05.03, item 5.1.1.2.1.6.
40202019	Qualquer transação biométrica que falhar em sua execução deve enviar uma resposta de erro em formato ANSI/NIST, seguindo o formato definido no DOC-ICP-05.03, item 5.1.1.8.	DOC-ICP-05.03, item 5.1.1.8.

4.2.3 Manter HUB Biométrico e Serviço de Diretório

40203001	O HUB biométrico, que deve ser disponibilizado pelo PSBio, deve ter interface de comunicação e formato de transação que faça uso dos padrões especificados no DOC-ICP-05.03.	DOC-ICP-05.03, item 3.7.1 e item 3.7.2.
40203002	O PSBio deve verificar a qualidade das biometrias recebidas das suas ACs e de outros PSBIOs, confirmando que as coletas foram realizadas dentro dos padrões mínimos de qualidade estabelecidos no DOC-ICP-05.03.	DOC-ICP-05.03, item 3.7.3.
40203003	As requisições para os serviços de HUB devem seguir o padrão assíncrono. O modelo assíncrono implementado deve seguir o conceito "PULL", ou seja, quem recebeu a requisição é responsável por gerar e entregar a requisição de resposta.	DOC-ICP-05.03, item 3.7.4.
40203004	Em geral, o HUB retorna os erros de forma assíncrona. Em algumas situações específicas, o erro é gerado em tempo de execução da requisição. Em ambos os casos, devem ser seguidas as definições previstas no DOC-ICP-05.03.	DOC-ICP-05.03, item 3.7.5.
40203005	O serviço deve retornar um código de sucesso ou erro conforme os padrões HTTP definidos no item 3.7.5.1 do DOC-ICP-05.03.	DOC-ICP-05.03, item 3.7.5.1.
40203006	Em caso de recebimento erros no envio de uma transação, o PSBio de origem não deve incluir a transação na lista de pendências até que o problema seja sanado.	DOC-ICP-05.03, item 3.7.5.2
40203007	O serviço de diretório síncrono deve ser oferecido por cada um dos HUBs/PSBio como um mecanismo rápido de consultas, ou seja, todas as respostas devem ser retornadas na mesma requisição/resposta.	DOC-ICP-05.03, item 3.8.1 e item 3.8.2.
40203008	O serviço de diretório deve prover quatro operações básicas: a. consulta de IDN; b. listagem de operações pendentes; c. requisição de reenvio de operações pendentes; d. Listar os IDNs de seus registros.	DOC-ICP-05.03, item 3.8.3.
40203009	O PSBio deve manter um *cache* de IDN para as consultas das ACs.	DOC-ICP-05.03, item 3.8.5
40203010	O serviço de listagem de operações pendentes será realizado através de *GET* no *endpoint* descrito no arquivo *swagger* disponível no Repositório da AC Raiz.	DOC-ICP-05.03, item 3.8.6.
40203011	O serviço de requisição de reenvio de operações pendentes será realizado através de *POST* no *endpoint* descrito no arquivo *swagger* disponível no Repositório da AC Raiz.	DOC-ICP-05.03, item 3.8.7.

40203012	Devem ser implementados mecanismos de tratamento de pendências para permitir a solicitação de reenvio de transações assíncronas que podem não ter sido recebidas ou processadas por outros PSBios, por falhas de rede ou falhas de *software*.	DOC-ICP-05.03, item 3.9.
40203013	Para evitar excesso de tráfego de dados, a operação de listagem pendências retornará no máximo 1.000 registros. Caso o PSBio possua uma fila maior que 1.000 registros para tratar, deve fazer o tratamento dos primeiros 1.000 registros pendentes antes de solicitar nova listagem de pendências.	DOC-ICP-05.03, item 3.10.3.
40203014	Ao retornar de uma falha o PSBio deve consultar as operações que estiverem pendentes junto a outros PSBios e deve ainda solicitar o reenvio destas transações e adicioná-las à fila de processamento.	DOC-ICP-05.03, item 3.10.4.
40203015	Os PSBios que implementam o *cache* devem possuir mecanismo previsto no DOC-ICP-05.03, item 3.12.2, para garantir a consistência e a manutenção do conteúdo de *cache*.	DOC-ICP-05.03, item 3.12.2.
40203016	A base de fraudadores será mantida atualizada através da consulta ao sistema SAF, conforme DOC-ICP-05.02, no mínimo uma vez por dia.	DOC-ICP-05.03, item 3.13.1 e item 3.8.2.
40203017	A cada novo registro de fraudador confirmado presente no SAF, deve ser executada uma busca 1:N na base do PSBio. Em caso de conflito, devem ser identificadas as transações (TCNs) que foram processadas com base naqueles dados, e a AC de origem deve ser notificada para providências de fraude.	DOC-ICP-05.03, item 3.8.3.

4.3 Manter segurança da informação, composto pelos subprocessos:

4.3.1 Manter inventário de ativos

40301001	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
40301002	O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.	DOC-ICP-02, item 8.2.12 e 9.3.5.10.
40301003	O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.	DOC-ICP-02, item 9.2.5.

40301004	Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos *softwares*, deverão estar inventariados com informações que permitam a identificação inequívoca.	DOC-ICP-03.02, item 3.1.1.3.h.

4.3.2 Manter análise de risco e Plano de Continuidade do Negócio - PCN

40302001	Um Plano de Continuidade do Negócio – PCN deverá ser implementado e testado no PSBio, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.	DOC-ICP-03.02, item 10 e DOC-ICP-02, item 6.4.1.
40302002	Todos os incidentes deverão ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.	DOC-ICP-02, item 6.4.4.
40302003	Todos os ativos de processamento das entidades devem estar relacionados no PCN.	DOC-ICP-02, item 7.4.3.c.
40302004	Todo pessoal envolvido com o Plano de Continuidade de Negócio deve receber um treinamento específico para poder enfrentar estes incidentes.	DOC-ICP-02, item 13.2.3.
40302005	Em um processo de gerenciamento de riscos, que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, os seguintes pontos principais devem ser identificados: a) o que deve ser protegido; b) a análise de riscos (contra quem ou contra o quê deve ser protegido); c) avaliação de riscos (análise da relação custo/benefício).	DOC-ICP-02, item 12.1.
40302006	A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: a) requisitos de segurança definidos pelo serviço; b) objetivo do serviço, público-alvo; c) classificação da informação; d) forma de acesso; e) frequência de atualização do conteúdo; f) forma de administração do serviço e volume de tráfego.	DOC-ICP-02, item 9.3.3.23.
40302007	O processo de gerenciamento de riscos deve ser revisto anualmente pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.	DOC-ICP-02, item 6.2.

4.3.3 Manter documentos armazenados e classificados

40303001	A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.	DOC-ICP-02, item 9.2.1.
40303002	Toda informação gerada e custodiada pelo PSBio deverá ser classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação.	DOC-ICP-03.02, item 7.1.
40303003	A classificação da informação no PSBio deverá ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada;	DOC-ICP-03.02, item 7.2.
40303004	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.	DOC-ICP-02, item 9.3.5.9.
40303005	Todo pessoal envolvido nos projetos coordenados pelo PSBio, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.	DOC-ICP-03.02, item 2.3.
40303006	O termo de sigilo da informação deverá conter cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos da ICP-Brasil.	DOC-ICP-03.02, item 2.4.
40303007	Aplicar-se-á o termo de sigilo de informações a quaisquer outras entidades que porventura tenham acesso as informações internas e de terceiros originárias dos projetos coordenados pelo PSBio.	DOC-ICP-03.02, item 2.5.
40303008	Todo material crítico inservível, descartável ou não mais utilizável deverá ter tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção deverá ter seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do PSBio.	DOC-ICP-03.02, item 3.1.1.3.g.
40303009	O PSBio deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.	DOC-ICP-03.02, item 8.3.

4.4 Manter sistemas aplicativos, composto pelos subprocessos

4.4.1 Manter sistemas de informação

40401001	As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.	DOC-ICP-02 item 9.3.1.1.

40401002	A documentação dos sistemas deve ser mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
40401003	A cópia de segurança deve ser testada e mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
40401004	Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.	DOC-ICP-02 item 9.3.1.5.
40401005	As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.	DOC-ICP-02 item 9.3.1.5.
40401006	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.5.11.

4.4.2 Manter bases de dados

40402001	Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.	DOC-ICP-02, item 10.1.4.
40402002	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.	DOC-ICP-02, item 10.3.1.
40402003	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.	DOC-ICP-02, item 9.2.2.
40402004	Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.	DOC-ICP-02, item 9.3.3.17.
40402005	As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.	DOC-ICP-02, item 9.3.5.4.
40402006	Proteção lógica adicional (criptografia) e senhas devem ser adotados para evitar o acesso não autorizado às informações. O arquivo de senhas deve ser criptografado e ter acesso controlado.	DOC-ICP-02, item 9.3.2.5 e item 9.3.4.5.

4.5 Manter segurança lógica e rede, composto pelos subprocessos:

4.5.1 Manter sistemas básicos

40501001	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.	DOC-ICP-02, item 9.3.2.3.
40501002	As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.	DOC-ICP-02, item 9.3.2.4.
40501003	A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.	DOC-ICP-02, item 9.3.2.6.
40501004	Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.	DOC-ICP-02, item 9.3.2.7.
40501005	Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.	DOC-ICP-02, item 9.3.3.3.
40501006	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.

4.5.2 Manter equipamentos protegidos de ameaças

40502001	O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o "*Efeito Tempest*".	DOC-ICP-02, item 9.3.3.1.
40502002	Mecanismos de segurança baseados em sistemas de proteção (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.	DOC-ICP-02, item 9.3.3.19.
40502003	A ativação da rede deve respeitar a ordem prevista no DOC-ICP-02, item 9.3.3.26. Os sistemas de certificação devem ser dispostos em segmentos	DOC-ICP-02, itens 9.3.3.26 e

	de rede que devem ser isolados por meios diversos, como por exemplo: a) utilizando virtual "lans" (vlan);b) utilizando de *firewall*; c)utilizando artifícios de roteamento.	9.3.3.27.
40502004	Ativos de processamento da rede, a exemplo de "*switches*" e roteadores, quando possuírem recursos básicos de segurança como acesso mediante senhas e outros, devem ser configurados para utilizá-los, visando reforçar seus controles de segurança.	DOC-ICP-02, itens 9.3.3.3 e 9.3.3.4.
40502005	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.
40502006	Nos computadores pessoais, devem ser adotadas medidas para combate de vírus, realização de *backups*, controle de acesso e uso de *software* não autorizado.	DOC-ICP-02, item 9.3.5.3.
40502007	Em todos os equipamentos devem ser sistematizados procedimentos para combate a processos destrutivos (vírus, "*worms"* e cavalos-de-tróia).	DOC-ICP-02, item 9.3.6.
40502008	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.	DOC-ICP-02, item 9.3.3.30.
40502009	Definir procedimentos formais para a eliminação segura de mídias desnecessárias.	DOC-ICP-02, item 9.3.5.12.
40502010	Os *softwares* dos sistemas operacionais, os antivírus e aplicativos de segurança devem ser mantidos atualizados.	DOC-ICP-03.02, item 4.8.

4.5.3 Manter *logs* e trilhas de auditoria

40503001	Todo equipamento do PSBio deverá ter *log* ativo e seu horário sincronizado com uma fonte confiável de tempo.	DOC-ICP-03.02, item 4.6.
40503002	As informações como *log*, trilhas de auditoria (das transações e coletas biométricas), registros de acesso (físico e lógico) e imagens deverão ter cópia de segurança cujo armazenamento será de 7 anos.	DOC-ICP-03.02, item 4.7.
40503003	Todos os registros de eventos (*logs*, trilhas de auditorias e imagens) deverão ser analisados, no mínimo, mensalmente e um relatório deverá ser gerado com assinatura do responsável pelo PSBio. Todos os registros da transação biométrica por parte do PSBio deverão ser guardados por um período de 7 anos.	DOC-ICP-03.02, item 11.

40503004	A hora utilizada pelo PSBio será fornecida pela AC RAIZ, por meio do serviço *Network Time Protocol* - NTP, descrito pela RFC 5905.	DOC-ICP-07.01, item 1.
40503005	O PSBio deve obter a hora UTC do serviço disponibilizado pelo ITI para sincronizar seus servidores de tempo.	DOC-ICP-07.01, item 1.1.
40503006	Registrar e avaliar periodicamente violações de segurança.	DOC-ICP-02, item 9.2.3.
40503007	Definir, analisar periodicamente e proteger devidamente arquivos de *logs* de sistemas.	DOC-ICP-02, item 9.3.1.3.
40503008	Para os sistemas de controle de acesso lógico, os registros de atividades (*logs*) devem ser analisados periodicamente.	DOC-ICP-02, item 9.3.4.15.

4.5.4 Manter cópias de segurança e restauração

40504001	O PSBio deverá, em sua Política de Segurança da Informação, definir como será realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado *backup*.	DOC-ICP-03.02, item 8.1.
40504002	A salvaguarda de ativos da informação deverá ter descrita as formas de execução dos seguintes processos: i. Procedimentos de *backup*; ii. Indicações de uso dos métodos de *backup*; iii. Tabela de temporalidade; iv. Local e restrições de armazenamento e salvaguarda em função da fase de uso; v. Tipos de mídia; vi. Controles ambientais do armazenamento; vii. Controles de segurança; viii. Teste de restauração de *backup*.	DOC-ICP-03.02, item 8.2.
40504003	Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.	DOC-ICP-02, item 9.3.2.9.

4.5.5 Manter controle de acesso a rede

40505001	Os PSBios devem enviar ao ITI a topologia de rede de comunicação com as AC/PSS e demais PSBios que compõe o Sistema Biométrico da ICP-Brasil.	DOC-ICP-05.03, item 3.1.2.

40505002	A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.	DOC-ICP-02, item 9.3.3.9.
40505003	O tráfego das informações no ambiente de rede deverá ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos.	DOC-ICP-03.02, item 5.1.
40505004	Não poderão ser admitidos acessos do mundo externo a rede interna do PSBio. As tentativas de acessos externos deverão ser inibidas e monitoradas por meio de aplicativos que criem barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão.	DOC-ICP-03.02, item 5.2.
40505005	Deverão ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada 3 (três) meses. Os testes na rede deverão ser documentados e as vulnerabilidades detectadas corrigidas.	DOC-ICP-03.02, item 5.3.
40505006	Nos ambientes de rede, registrar e avaliar periodicamente eventos de segurança.	DOC-ICP-02, item 9.3.3.10.
40505007	O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.	DOC-ICP-02, item 9.3.3.15,

4.5.6 Manter controle de acesso lógico

40506001	Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.	DOC-ICP-02, item 9.3.2.2.
40506002	O ambiente operacional dos sistemas deve ser monitorado.	DOC-ICP-02, item 9.3.2.3.
40506003	Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.	DOC-ICP-02, item 9.3.1.2.
40506004	O responsável pela autorização ou confirmação da autorização de acesso lógico a sistemas e servidores deve ser claramente definido e registrado.	DOC-ICP-02, item 9.3.2.1.
40506005	O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido.	DOC-ICP-02, item 9.3.2.1.
40506006	As autorizações de acesso lógico das máquinas servidoras devem ser revistas, confirmadas e registradas continuamente.	DOC-ICP-02, item 9.3.2.1.
40506007	O acesso lógico aos recursos da rede local deve ser realizado por meio de	DOC-ICP-02,

	sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede baseado nas responsabilidades e tarefas de cada usuário.	item 9.3.3.7.
40506008	O arquivo de senhas deve ser criptografado e ter o acesso controlado.	DOC-ICP-02, item 9.3.4.5.
40506009	O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.	DOC-ICP-02, item 9.3.4.8.
40506010	O acesso lógico ao ambiente computacional do PSBio se dará, no mínimo, mediante usuário individual e senha, que deverá ser trocada periodicamente.	DOC-ICP-03.02, item 4.1.
40506011	Todos os equipamentos do parque computacional deverão ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas.	DOC-ICP-03.02, item 4.2.
40506012	Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa.	DOC-ICP-03.02, item 4.3.
40506013	O PSBio deverá ter explícita a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários deverão estar cadastrados em perfis de acesso que permitam privilégio mínimo para realização de suas atividades.	DOC-ICP-03.02, item 4.4.
40506014	Os usuários especiais (a exemplo do *root* e do administrador) de sistemas operacionais, de banco de dados e de aplicações em geral devem ter suas senhas segregadas de forma que o acesso lógico a esses ambientes se dê por, pelo menos, duas pessoas autorizadas.	DOC-ICP-03.02, item 4.5.

4.6 Manter infraestrutura, composto pelos subprocessos:

4.6.1 Manter nível de serviço

40601001	O PSBio deve possuir desempenho, escalabilidade e disponibilidade, com SLA mínimo de 99,5% (resguardadas as janelas programadas de manutenção) ao mês, para atender toda a demanda da ICP-Brasil.	DOC-ICP-05.03, item 3.6.1.
40601002	O PSBio deve manter um ambiente segregado de homologação para os testes, com as ACs e PSBios, de tecnologia e interconexão necessários para operação do sistema e atendimento às normas da ICP-Brasil, com SLA mínimo de 95,5% ao mês.	DOC-ICP-05.03, item 3.6.2.

4.6.2 Manter controle de acesso físico

40602001	Acesso aos componentes de infraestrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.	DOC-ICP-02, item 8.2.10.
40602002	Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).	DOC-ICP-02, item 8.2.14.
40602003	O ambiente físico do PSBio deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos.	DOC-ICP-03.02, item 3.1.1.3.a.
40602004	O PSBio deverá conter imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente.	DOC-ICP-03.02, item 3.1.1.3.b.
40602005	É mandatório o sincronismo de data e hora entre os mecanismos de segurança física garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem.	DOC-ICP-03.02, item 3.1.1.3.c.
40602006	Todos que transitam no ambiente físico do PSBio deverão portar crachás de identificação, inclusive os visitantes.	DOC-ICP-03.02, item 3.1.1.3.d.
40602007	Só é permitido o trânsito de material de terceiros pelos ambientes físicos do PSBio mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação.	DOC-ICP-03.02, item 3.1.1.3.e.
40602008	Em caso de inoperância dos sistemas automáticos, o controle de acesso físico deverá ser realizado provisoriamente por meio de um livro de registro onde constará quem acessou, a data, hora e o motivo do acesso.	DOC-ICP-03.02, item 3.1.1.3.i.
40602009	Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.	DOC-ICP-02, item 8.2.3
40602010	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.	DOC-ICP-02, item 8.2.4.
40602011	Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.	DOC-ICP-02, item 8.2.5.
40602012	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.	DOC-ICP-02, item 8.2.6.
40602013	A entrada e saída de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da	DOC-ICP-02, item 8.2.9.

	informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.	
40602014	Acesso de visitantes as áreas de segurança devem ser registrados e supervisionados.	DOC-ICP-02, item 8.2.15.
40602015	Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.	DOC-ICP-02, item 9.3.3.11.
40602016	O PSBio deve manter pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSBio.	DOC-ICP-03.02, item 3.1.1.1.
40602017	O primeiro nível – ou nível 1 – deverá situar-se após a primeira barreira de acesso às instalações do PSBio. O ambiente de nível 1 dos PSBio da ICP-Brasil desempenha a função de interface com cliente ou fornecedores que necessitam comparecer ao PSBio.	DOC-ICP-03.02, item 3.1.1.1.1.
40602018	O segundo nível – ou nível 2 – será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSBio. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.	DOC-ICP-03.02, item 3.1.1.1.2.
40602019	O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-03.02, item 3.1.1.1.2.a.
40602020	O acesso ao nível 2 deverá ser permitido apenas a pessoas que trabalhem diretamente com as atividades de serviços biométricos ou ao pessoal responsável pela manutenção de sistemas e equipamentos do PSBio, como administradores de rede e técnicos de suporte de informática. Demais funcionários do PSBio ou do possível ambiente que esta compartilhe não deverão acessar este nível.	DOC-ICP-03.02, item 3.1.1.1.2.b.
40602021	Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações do PSBio, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.	DOC-ICP-03.02, item 3.1.1.1.2.d.
40602022	O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação do PSBio. Qualquer atividade relativa à Transação Biométrica Digital deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.	DOC-ICP-03.02, item 3.1.1.1.3.
40602023	No terceiro nível deverão ser controladas tanto as entradas quanto as	DOC-ICP-03.02,

	saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha.	item 3.1.1.1.3.a.
40602024	As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-03.02, item 3.1.1.1.3.b.
40602025	Caso o ambiente de Nível 3 possua forro ou piso falsos, deverão ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior.	DOC-ICP-03.02, item 3.1.1.1.3.c.
40602026	Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deverá ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.	DOC-ICP-03.02, item 3.1.1.1.3.d.
40602027	Poderão existir no PSBio vários ambientes de nível 3 para abrigar e segregar, quando for o caso: i. equipamentos de produção e cofre de armazenamento; ii. equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).	DOC-ICP-03.02, item 3.1.1.1.3.e.
40602028	O terceiro nível avançado – ou nível 3.1 –, no interior ao ambiente de nível 3, deverá compreender pelo menos um gabinete reforçado trancado, que abrigará o banco com a base de dados biométrico da ICP-Brasil.	DOC-ICP-03.02, item 3.1.1.1.4.
40602029	Para garantir a segurança do material armazenado, os gabinetes deverão obedecer às seguintes especificações mínimas: i. ser feitos em aço ou material de resistência equivalente; ii. possuir tranca com chave.	DOC-ICP-03.02, item 3.1.1.1.4.a.
40602030	Todos os servidores e elementos de infraestrutura e proteção do segmento de rede, tais como roteadores, *hubs*, *switches* e *firewalls* devem: a) operar em ambiente com segurança equivalente, no mínimo, ao nível 3 citado neste documento; b) possuir acesso lógico restrito por meio de sistema de autenticação e autorização de acesso.	DOC-ICP-03.02, item 3.1.1.2.

4.6.3 Manter energia elétrica

40603001	A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.	DOC-ICP-02, item 9.3.3.14.
40603002	Deverão ser providenciados mecanismos para garantir a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote.	DOC-ICP-03.02, item 3.1.1.3.j.
40603003	O PSBio deverá conter dispositivos de controle de iluminação e oscilação na corrente elétrica em todo seu ambiente físico.	DOC-ICP-03.02, item 3.1.1.3.f.

4.6.4 Manter sistema de combate a incêndio

40604001	O PSBio deverá conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico.	DOC-ICP-03.02 item 3.1.1.3.f.

4.7 Manter recursos humanos, composto pelos subprocessos:

4.7.1 Admitir pessoas

40701001	Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.	DOC-ICP-02, item 7.3.1.1.
40701002	Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, incluindo as atividades finalísticas de PSBio.	DOC-ICP-02, item 7.3.1.2 e DOC-ICP-03.02, item 2.8.
40701003	A entrevista de Admissão deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.	DOC-ICP-02, item 7.3.4.1.
40701004	O PSBio deverá ter uma Política de Gestão de Pessoas que disponha sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.	DOC-ICP-03.02, item 2.1.

40701005	Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.	DOC-ICP-02, item 7.3.4.2.
40701006	Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil, verificação de antecedentes e verificação de grau de instrução.	DOC-ICP-02, item 7.3.3.
40701007	O pessoal do PSBio, e contratados, deverão possuir um dossiê contendo os documentos previstos no DOC-ICP-03.02, item 2, alínea “g”.	DOC-ICP-03.02, item 2.7.
40701008	O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.	DOC-ICP-02, item 7.3.1.3.

4.7.2 Manter capacitação de pessoas

40702001	A comprovação da capacidade técnica do pessoal envolvido nos serviços prestados pelo PSBio deverá estar à disposição para eventuais auditorias e fiscalizações.	DOC-ICP-03.02, item 2.2.
40702002	Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.	DOC-ICP-02, item 6.1.3.
40702003	Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.	DOC-ICP-02, item 6.1.4.
40702004	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar os incidentes descritos no DOC-ICP-02.	DOC-ICP-02, item 13.2.3.
40702005	Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.	DOC-ICP-02, item 7.3.7.
40702006	Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.	DOC-ICP-02, item 7.3.5.2.

4.7.3 Manter habilitação de pessoas

40703001	As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.	DOC-ICP-02, item 8.2.1.
40703002	Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.	DOC-ICP-02, item 9.3.4.16.
40703003	Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.	DOC-ICP-02, item 10.2.1.
40703004	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.	DOC-ICP-02, item 10.2.2.
40703005	Todos os empregados do PSBio deverão estar identificados por uma credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo máximo de 1 (um) ano de validade. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário.	DOC-ICP-02, item 7.3.6.

4.7.4 Avaliar desempenho

40704001	Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.	DOC-ICP-02, item 7.3.5.1.
40704002	Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.	DOC-ICP-02, item 7.3.8.1.
40704003	Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.	DOC-ICP-02, item 7.3.8.2.

40704004	Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.	DOC-ICP-02, item 7.3.8.3.
40704005	As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.	DOC-ICP-02, item 7.3.8.4.

4.7.5 Suspender, movimentar e desligar pessoas

40705001	Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.	DOC-ICP-02, item 6.1.5.
40705002	O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público, sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.	DOC-ICP-02, item 7.3.9.
40705003	O empregado ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a entidade, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.	DOC-ICP-02, item 7.3.10.
40705004	Quando da demissão, deverão ser acrescentados ao dossiê do empregado ou servidor as evidências de exclusão dos acessos físico e lógico nos ambientes do PSBio e a declaração assinada de que não possui pendências, conforme previsto no item 7.3.10 do DOC-ICP-02.	DOC-ICP-03.02, item 2.9.
40705005	Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.	DOC-ICP-02, item 7.3.11.

5 Os processos nos PSC – Prestadores de Serviço de Confiança estão assim distribuídos:

5.1 Manter credenciamento de PSC, composto pelos subprocessos:

5.1.1 Manter requisitos de manutenção de credenciamento

50101001	Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 do DOC-ICP-03.	DOC-ICP-03, item 2.1.
50101002	O PSC deve comunicar, desde logo, ao ITI qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores.	DOC-ICP-03, item 3.6.a.i.
50101003	A entidade credenciada para desenvolver as atividades de PSC comunicar ao ITI qualquer alteração na sua Declaração de Práticas de Prestadores de Serviço de Confiança – DPPSC, Plano de Capacidade Operacional – PCO e Política de Segurança – PS.	DOC-ICP-03, item 3.6.a.iii.
50101004	A entidade credenciada para desenvolver as atividades de PSC deverá encaminhar ao ITI relatórios de auditorias em até 30 (trinta) dias após a conclusão das mesmas.	DOC-ICP-03, item 3.6.b.
50101005	A entidade credenciada para desenvolver as atividades de PSC deve manter a conformidade com suas respectivas DPPSC, PCO e PS, demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust.*	DOC-ICP-17, item 8.1.1.
50101006	Caso ocorra uma ou mais das hipóteses previstas no item 4.6.1 do DOC-ICP-03, o PSC deve ser descredenciado.	DOC-ICP-03, item 4.6.1.

5.1.2 Manter condições fisco-tributárias e econômico-financeiras

50102001	O PSC deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.	DOC-ICP-03, Anexo VI, item 2.

50102002	O PSC deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos à sua qualificação econômico-financeira: a)Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente. b)Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.	DOC-ICP-03, item 2.1.c e Anexo VI, item 3.

5.1.3 Manter contrato de seguro

50103001	Manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de armazenamento de chaves privadas para usuários finais, com cobertura suficiente e compatível com o risco dessas atividades.	DOC-ICP-17, item 9.1.1.n.

5.1.4 Manter e cumprir a Política de Segurança - PS do PSC

50104001	Todos os empregados devem possuir conhecimento da PS do PSC que a deve divulgar.	DOC-ICP-02, item 6.1.2.
50104002	Os empregados, as chefias e os prestadores de serviços devem conhecer os deveres e as responsabilidades definidas na PS.	DOC-ICP-02, item 7.4.1 a 7.4.5.
50104003	O PSC tornará disponível para todo o seu pessoal, pelo menos: a) sua DPPSC; b) a PS; c) documentação operacional relativa às suas atividades; e d) contratos, normas e políticas relevantes para suas atividades.	DOC-ICP-17, item 5.3.8.1.

5.1.5 Comunicar mudanças operacionais e violação de normas

50105001	O PSC deve comunicar formalmente e imediatamente as mudanças operacionais ocorridas em seu ambiente de certificação e qualquer violação de normas da ICP-Brasil.	DOC-ICP-03, item 3.6.a.
50105002	O PSC deve comunicar, desde logo, à AC-Raiz a violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil..	DOC-ICP-03, item 3.6.a.ii.

5.1.6 Regularizar não conformidades identificadas

50106001	A entidade auditada deve cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas.	DOC-ICP-08, item 9.1.

5.2 Credenciar e manter entidades operacionalmente vinculadas, composto pelos subprocessos:

5.2.1 Auditar entidades operacionalmente vinculadas

50201001	Deverão ser realizadas auditorias nas entidades integrantes da ICP-Brasil conforme frequência estabelecida na DOC-ICP-08.	DOC-ICP-02, item 11.3.
50201002	O PSC é responsável pela realização de auditorias anuais nas entidades a ele vinculadas, para fins de manutenção de credenciamento,	DOC-ICP-17, item 8.1.6.
50201003	O PSC deve encaminhar ao ITI relatórios de auditorias realizadas nas suas instalações técnicas, até 30 (trinta) dias após a conclusão das mesmas.	DOC-ICP-03, item 3.6.b.
50201004	A equipe de auditoria deve ser totalmente independente da entidade auditada, aplicando-se no que couber, as regras de suspeição e impedimentos estabelecidas nos artigos 134 e 135 do Código de Processo Civil.	DOC-ICP-08, item 7.1.
50201005	Os auditores que realizarão a auditoria devem firmar declaração, sob as penas da lei, de que não se enquadram em quaisquer das causas de impedimento tratadas no DOC-ICP-08.	DOC-ICP-08, item 7.3.
50201006	Os serviços de auditoria devem ser executados diretamente pela entidade de auditoria credenciada junto à ICP-Brasil, vedada a subcontratação total ou parcial de serviços.	DOC-ICP-08, item 6.1.6.
50201007	As fiscalizações e auditorias realizadas nos PSC da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades estão em conformidade com suas respectivas DPPSCs, PCOs e PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust.*	DOC-ICP-17, item 8.1.1.

5.2.2 Observar procedimentos de extinção de entidades operacionalmente vinculadas

50202001	Nos descredenciamentos de PSC ou PSS, os PSCs ao qual se vinculam devem executar os procedimentos previstos no item 4 do DOC-ICP-03.	DOC-ICP-03, item 4.6.2, e item 4.4.
50202002	Os PSC devem executar os procedimentos descrito em suas DPPSC em relação ao disposto no item 4.7, que trata da extinção dos serviços de PSC.	DOC-ICP-17, item 4.7.

5.2.3 Observar procedimentos de credenciamento de entidades operacionalmente vinculadas

50203001	Os PSC devem observar os critérios a serem atendidos pelos candidatos a credenciamento na ICP-Brasil sob sua vinculação.	DOC-ICP-03, itens 2.1, 2.1.6. e 2.1.4.
50203002	As solicitações dos candidatos ao credenciamento como PSS na ICP-Brasil devem ser encaminhadas à PSC ou candidato a PSC a que o candidato a PSS esteja operacionalmente vinculado, por meio do formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS.	DOC-ICP-03, item 2.2.5.1.1.
50203003	O PSC ou candidato a PSC que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz, a qual será protocolada perante o Protocolo Geral da AC Raiz.	DOC-ICP-03, item 2.2.5.1.2 e 2.2.5.1.3.

5.2.4 Manter credenciamento de entidades operacionalmente vinculadas

50204001	Qualquer alteração em atos constitutivos, estatuto, contrato social ou administradores seus ou de seus vinculados; desvinculação de PSS credenciados; ou ainda violação das diretrizes e normas técnicas da ICP-Brasil cometidas pela própria ou pelos PSSs que lhe sejam operacionalmente vinculados devem ser comunicadas ao ITI.	DOC-ICP-03, itens 3.6.a.
50204002	O PSS deve observar a DPC, as PCs e a PS da AC, ou a DPCT, as PCTs e PS da ACT ou a DPPSC e PS do PSC a que estiver vinculado.	DOC-ICP-03, item 3.4.b.
50204003	O PSC responsável responde pelos danos que der causa.	DOC-ICP-17, item 9.2.1.

5.3 Executar Fases do Ciclo do PSC, composto pelos subprocessos:

5.3.1 Gerenciar o armazenamento de chaves privadas

50301001	As chaves privadas dos usuários finais, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em *hardware* criptográficos, devem estar armazenadas dentro dos espaços (*slots*), ou equivalente, da fronteira criptográfica e segurança física de um HSM com certificação INMETRO válida no âmbito da ICP-Brasil, endereçados por conta de usuário.	DOC-ICP-17.01, item 6.1.1.
50301002	As chaves privadas dos usuários deve ser de uso, conhecimento e controle exclusivo do titular, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário do PSC ou dependentes de outras chaves criptográficas.	DOC-ICP-17.01, item 6.1.2.
50301003	O PSC deve prover mecanismos de duplo fator de autenticação ao titular para acesso à chave privada, devendo ser um fator dentro da fronteira criptográfica do HSM e outro dentro do ambiente seguro e primeira interface de comunicação com HSM ou ambos dentro da fronteira criptográfica do HSM. Cada fator deve ser de uma classe diferente (conhecimento, posse ou biometria).	DOC-ICP-17.01, item 6.1.3.
50301004	Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja a transmissão e os dados de autenticação por meio de criptografia.	DOC-ICP-17.01, item 6.1.3.
50301005	Deverá ser feita, em outro ambiente físico de contingência, a cópia das chaves dos usuários finais, observados os mesmos requisitos de armazenamento do ambiente principal. A entrada do ambiente de contingência deve ser em até 48 horas.	DOC-ICP-17.01, item 6.1.4.
50301006	Os espaços para armazenamento das chaves privadas dos usuários finais poderão ser liberados desde que não haja renovação por parte do mesmo ou a revogação da chave, entretanto deve-se manter o registro de armazenamento das chaves conforme Declaração de Prática do Prestador de Serviço de Confiança – DPPSC.	DOC-ICP-17.01, item 6.1.5.
50301007	O PSC deve descrever os procedimentos técnicos e operacionais que serão usados para a liberação de um espaço (*slot*) onde estava armazenada a chave privada de um subscritor.	DOC-ICP-17, item 4.5.

5.3.2 Dar suporte a Protocolos

50302001	Os HSMs certificados na ICP-Brasil devem suportar a interface PKCS#11, atendendo às exigências de especificação da ICP-Brasil e os requisitos apresentados no item 6.2.1.a.	DOC-ICP-17.01, item 6.2.1.
50302002	O módulo criptográfico deve suportar as chamadas de PKCS#11 (Cryptoki) definidas no item 6.2.1.b e as funções definidas no item 6.2.1.c.	DOC-ICP-17.01, item 6.2.1.b e 6.2.1.c.
50302003	Os HSMs certificados na ICP-Brasil devem suportar o protocolo *Key Management Interoperability Protocol* – KMIP, versão 1.3 ou superior, devendo seguir, também, os requisitos que constam no item 6.2.2.	DOC-ICP-17.01, item 6.2.2.

5.3.3 Manter requisitos de segurança e disponibilidade para serviços de confiança

50303001	Poderá ser arquitetado um *pool* de HSM para operação, replicação e gerenciamento das chaves dos usuários finais, devendo seguir os requisitos apontados no item 6.3.1.	DOC-ICP-17.01, item 6.3.1.
50303002	O PSC deve descrever os procedimentos de recuperação previstos para utilização nas hipóteses de sincronismo com a fonte confiável de tempo da ICP-Brasil ou, se for o caso, com o *pool* de HSM para operação.	DOC-ICP-17, item 4.6.3.
50303003	Os PSCs no âmbito da ICP-Brasil devem atender aos critérios mínimos de 99,99% de "nível de tempo de atividade" (*uptime*) a ser verificado por mês.	DOC-ICP-17.01, item 6.3.2.
50303004	Deverá ser utilizado o protocolo TLS, definido pela RFC 5246 ou a versão atualizada, para comunicação com serviços de confiança.	DOC-ICP-17.01, item 6.4.1.1.
50303005	Deverá ser utilizado o *framework* OAuth 2.0 (RFC 6749 e RFC 7636) para implementação da interface aos serviços de confiança dos PSC.	DOC-ICP-17.01, item 6.4.1.2.
50303006	A URI de base – URI-base – definirá o estilo e formato dos endereços HTTPS de serviços de confiança. A URI de base conterá número correspondendo à versão de API definida pela ICP-Brasil.	DOC-ICP-17.01, item 6.4.2.1. e 6.4.2.2.
50303007	O uso de chaves privadas em PSC deverá ser precedido de solicitação bem-sucedida da Requisição de Código de Autorização, da Requisição de *Token* de Acesso e serviço de assinatura utilizando chave de usuários.	DOC-ICP-17.01, item 6.4.3.1.

50303008	As aplicações não deverão coletar fatores de autenticação do usuário. Para este fim, os PSC deverão se comunicar diretamente com equipamento do usuário, previamente identificado e cadastrado junto ao PSC de forma segura.	DOC-ICP-17.01, item 6.4.3.2.
50303009	Para obter acesso aos serviços de confiança, os PSC deverão implementar obrigatoriamente o Serviço de Cadastro de Aplicação com Certificado ICP-Brasil para SSL.	DOC-ICP-17.01, item 6.4.3.3.
50303010	O acordo de nível de serviço para todos os serviços credenciados do PSC deverá ser de no mínimo 99,99%.	DOC-ICP-17.01, item 7.9.

5.3.4 Manter serviços de confiança

50304001	Obrigatoriamente o PSC deverá disponibilizar os seguintes serviços de confiança: i. Código de Autorização, ii. Token de Acesso, iii. Assinatura, iv. Cadastro de Aplicação com Certificado, v. Listagem de Certificados do Titular, vi. Localização de Titular e vii. Recuperação de Certificado. Esses serviços devem ser implementados seguindo o disposto no item 6.4.5.	DOC-ICP-17.01, item 6.4.4.a. e 6.4.5.
50304002	Opcionalmente o PSC poderá disponibilizar os seguintes serviços de confiança: i. Cadastro de Aplicação sem Certificado, ii. Token de Acesso para Aplicação, iii. Manutenção de Aplicação, iv. Autorização com Credenciais do Titular. Esses serviços devem ser implementados seguindo o disposto no item 6.4.6.	DOC-ICP-17.01, item 6.4.4.b. e 6.4.6.
50304003	O serviço Cadastro de Aplicação sem Certificado é obrigatório para todas as aplicações que utilizarem serviços de autorização sem certificados ICP-Brasil.	DOC-ICP-17.01, item 6.4.6.1.
50304004	O serviço Manutenção de Cadastro de Aplicação é obrigatório para todas as aplicações que utilizarem serviços de autorização não identificadas por certificados ICP-Brasil para SSL.	DOC-ICP-17.01, item 6.4.6.2.

5.3.5 Verificar a Lista de Prestador de Serviço de Confiança – LPSC

50305001	A Lista de Prestadores de Serviço de Confiança – LPSC contendo as entidades credenciadas no âmbito da ICP-Brasil, como Prestadores de Serviço de Confiança – PSC, será publicada no repositório da AC Raiz, em versão textual e em XML, e atualizada no prazo máximo de 180 dias.	DOC-ICP-17.01, item 6.5.1 e 6.5.2.

50305002	A autenticidade e a integridade da versão processável por máquina da lista compilada é assegurada por meio de uma assinatura digital XMLDSig suportada por um certificado digital do ITI.	DOC-ICP-17.01, item 6.5.3.
50305003	As versões da LPSC e o certificado que assina a LPSC serão publicados no repositório da AC Raiz.	DOC-ICP-17.01, item 6.5.4.
50305004	A autenticidade e integridade da lista compilada devem ser verificadas pelas partes confiáveis antes de qualquer uso.	DOC-ICP-17.01, item 6.5.5.

5.3.6 Manter serviços de assinatura digital

50306001	Antes de iniciar o procedimento de assinatura o sistema deve verificar a validade do certificado. Ao receber o retorno da assinatura o sistema deve bater a resposta com a chave pública.	DOC-ICP-17.01, item 7.2.3.
50306002	Os dispositivos para criação de assinatura devem conter os certificados de assinatura ou possuírem uma referência inequívoca a eles. Devem, ainda, verificar os dados de autenticação do assinante.	DOC-ICP-17.01, item 7.3.2.
50306003	Os equipamentos para criação de assinaturas devem possuir certificação INMETRO válido no âmbito da ICP-Brasil, conforme definido no conjunto de documentos DOC-ICP-10.	DOC-ICP-17.01, item 7.3.3.
50306004	A interface entre a aplicação de assinatura e o dispositivo ou equipamento de criação devem garantir que somente com a autenticação do titular do certificado, que deve ter controle exclusivo da chave privada, seja possível requerer a criação dos dados de uma assinatura digital.	DOC-ICP-17.01, item 7.4.1.
50306005	O uso do dispositivo de criação deve exigir que o usuário insira dados específicos de autenticação do assinante. Toda informação trocada entre a aplicação e o dispositivo deve trafegar de forma criptografada.	DOC-ICP-17.01, item 7.4.2.
50306006	Mais de um mecanismo de autenticação deve ser usado para fornecer uma garantia de autenticação suficiente e devem ser de uma forma que evite ataques de representação.	DOC-ICP-17.01, item 7.4.3 e 7.4.4.
50306007	Todos os algoritmos e tamanho de chaves envolvidos no cálculo de qualquer elemento da assinatura digital encontram-se definidos no documento DOC-ICP-01.01.	DOC-ICP-17.01, item 7.5.1.
50306008	Os PSC devem implementar assinaturas digitais baseadas nas políticas de assinatura padronizadas e aprovadas na ICP-Brasil. Todos os formatos e	DOC-ICP-17.01, item 7.6.

	perfis de assinatura digital no âmbito da ICP-Brasil estão definidos no conjunto de documentos DOC-ICP-15 e seus complementares.	
50306009	O processo de validação de uma assinatura digital deve ser realizada contra uma política explícita de assinatura digital, que consiste de um conjunto de restrições de validação, denominada Política de Assinatura, e deve gerar um relatório com indicação da situação de validação (Válida, Inválida ou Indeterminada), fornecendo os detalhes da validação técnica de cada uma das restrições aplicáveis, que podem ser relevantes para a aplicação demandante na interpretação dos resultados.	DOC-ICP-17.01, item 7.8.1.
50306010	A validade de uma assinatura digital é avaliada pelo verificador utilizando a mesma política de assinatura usada na criação dessa assinatura digital. Os requisitos para geração e verificação de assinaturas digitais no âmbito da ICP-Brasil estão descritos no documento DOC-ICP-15.01.	DOC-ICP-17.01, item 7.8.2 e 7.8.3.
50306011	No processo de validação de uma assinatura digital, deve-se verificar a validade das Políticas de Assinatura por meio da Lista de Políticas de Assinatura Aprovadas (LPA), publicada no repositório da AC Raiz.	DOC-ICP-17.01, item 7.8.4.

5.4 Manter publicações, composto pelos subprocessos:

5.4.1 Manter DPPSC

50401001	Qualquer alteração na DPPSC deverá ser submetida à aprovação da AC-Raiz.	DOC-ICP-17, item 1.5.
50401002	Toda DPPSC elaborada no âmbito da ICP-Brasil deve observar requisitos e estrutura do DOC-ICP-17.	DOC-ICP-17, item 1.1.4 e 1.1.6.
50401003	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 1.2 o nome da instituição e o OID atribuído para a respectiva DPPSC.	DOC-ICP-17, item 1.2.
50401004	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar as informações das entidades envolvidas e a aplicabilidade dos serviços prestados pelo PSC.	DOC-ICP-17, item 1.3.
50401005	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar a categoria das atividades que prestará: a) armazenamento de chaves privadas dos subscritores; ou b) serviço de assinatura digital, verificação da assinatura digital; ou c) ambos.	DOC-ICP-17, item 1.3.1.2.

50401006	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 1.4 os dados de contato do PSC responsável pela DPPSC.	DOC-ICP-17, item 1.4.
50401007	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 2 as responsabilidades do repositório e publicação.	DOC-ICP-17, item 2.
50401008	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 3 os requisitos de identificação e autorização.	DOC-ICP-17, item 3.
50401009	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar os requisitos operacionais referentes aos serviços que presta.	DOC-ICP-17, item 4.
50401010	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 5 os controles de segurança física, procedimental e pessoal.	DOC-ICP-17, item 5.
50401011	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 6 os Controles Técnicos de Segurança.	DOC-ICP-17, item 6.
50401012	Toda DPPSC elaborada no âmbito da ICP-Brasil deve indicar no item 7 as Políticas de Assinatura Digital que pratica.	DOC-ICP-17, item 7.
50401013	Toda DPPSC elaborada no âmbito da ICP-Brasil deve tratar no item 8 sobre as Auditorias e Avaliações de Conformidade.	DOC-ICP-17, item 8.
50401014	Toda DPPSC elaborada no âmbito da ICP-Brasil deve tratar, no item 9, dos assuntos de caráter comercial, como obrigações e direitos.	DOC-ICP-17, item 9.

5.4.2 Manter publicação de informações do PSC

50402001	O PSC deve publicar em sua página *web* a DPPSC e a Política de Segurança que implementa.	DOC-ICP-17, item 9.1.1.g e 2.1.1.2.b.
50402002	O PSC deve publicar em sua página *web* a capacidade de armazenamento das chaves privadas dos subscritores que opera e os serviços que implementa.	DOC-ICP-17, item 2.1.1.2.a e 2.1.1.2.c.
50402003	O PSC deve publicar em sua página *web* as condições gerais mediante as quais são prestados os serviços de armazenamento de chaves privadas, assinatura digital e verificação da assinatura digital.	DOC-ICP-17, item 2.1.1.2.d.
50402004	O PSC deve publicar em sua página *web* se pretende continuar a prestar o serviço ou se está mediante a qualquer fiscalização dos serviços.	DOC-ICP-17, item 2.1.1.2.e.

5.4.3 Informar frequência de publicação

50403001	A informação de frequência de atualização das publicações deve constar no item 2.1.2 da DPPSC, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.	DOC-ICP-17, item 2.1.2.

5.5 Manter segurança da informação, composto pelos subprocessos:

5.5.1 Manter inventário de ativos

50501001	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
50501002	O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.	DOC-ICP-02, item 8.2.12 e 9.3.5.10.
50501003	O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.	DOC-ICP-02, item 9.2.5.

5.5.2 Manter Plano de Continuidade do Negócio - PCN

50502001	Todo PSC integrante da ICP-Brasil deverá manter e testar anualmente, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente, seu Plano de Continuidade do Negócio (PCN).	DOC-ICP-17, item 9.1.1.m, DOC-ICP-17.01, item 11 e DOC-ICP-02, item 6.4.1.
50502002	Todos os incidentes devem ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.	DOC-ICP-02, item 6.4.4.
50502003	Todos os ativos de processamento das entidades devem estar relacionados no PCN.	DOC-ICP-02, item 7.4.3.c.

50502004	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.	DOC-ICP-02, item 13.2.3.
50502005	Em um processo de gerenciamento de riscos, que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, os seguintes pontos principais devem ser identificados: a) o que deve ser protegido; b) a análise de riscos (contra quem ou contra o que deve ser protegido); c) avaliação de riscos (análise da relação custo/benefício).	DOC-ICP-02, item 12.1.
50502006	A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: a) requisitos de segurança definidos pelo serviço; b) objetivo do serviço, público-alvo; c) classificação da informação; d) forma de acesso; e) frequência de atualização do conteúdo; f) forma de administração do serviço e volume de tráfego.	DOC-ICP-02, item 9.3.3.23.
50502007	O processo de gerenciamento de riscos deve ser revisto anualmente pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.	DOC-ICP-02, item 6.2.

5.5.3 Manter documentos armazenados

50503001	Toda a documentação fornecida ao pessoal deve estar classificada segundo a política de classificação de informação definida pelo PSC e deve ser mantida atualizada.	DOC-ICP-17, item 5.3.8.2 e DOC-ICP-17.01, item 8.
50503002	A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.	DOC-ICP-02, item 9.2.1.
50503003	Todos os registros arquivados devem ser classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a PS da ICP-Brasil.	DOC-ICP-17, item 4.4.2.
50503004	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.	DOC-ICP-02, item 9.3.5.9.
50503005	O PSC deve estabelecer que uma segunda cópia de todo o material arquivado deverá ser armazenada em ambiente diferente às instalações	DOC-ICP-17, item 4.4.3.1.

	principais do PSC responsável, recebendo o mesmo tipo de proteção utilizada por ele no arquivo principal.	
50503006	As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias, devendo a integridade ser verificada, no mínimo, a cada 6 (seis) meses.	DOC-ICP-17, item 4.4.3.2 e 4.4.3.3.
50503007	O PSC deve estabelecer os períodos de retenção para cada registro arquivado, observando que os registros de armazenamento de chaves privadas e/ou certificados digitais, de assinaturas digitais criadas, de verificações das assinaturas digitais e, por ventura, dos documentos armazenados, inclusive arquivos de auditoria, deverão ser retidos por, no mínimo, 7 (sete) anos.	DOC-ICP-17, item 4.4.1.2.
50503008	Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser triturados antes de ir para o lixo.	DOC-ICP-17, item 5.1.7.1.
50503009	Todos os dispositivos eletrônicos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, deverão ser fisicamente destruídos.	DOC-ICP-17, item 5.1.7.2.
50503010	O PSC deverá, em sua Política de Segurança da Informação, definir como será realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado *backup*.	DOC-ICP-17.01, item 9.1.
50503011	A salvaguarda de ativos da informação deverá ter descrita as formas de execução dos seguintes processos: i. Procedimentos de *backup*; ii. Indicações de uso dos métodos de *backup*; iii. Tabela de temporalidade; iv. Local e restrições de armazenamento e salvaguarda em função da fase de uso; v. Tipos de mídia; vi. Controles ambientais do armazenamento; vii. Controles de segurança; viii. Teste de restauração de *backup*.	DOC-ICP-17.01, item 9.2.
50503012	O PSC deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.	DOC-ICP-17.01, item 9.3.

5.6 Manter sistemas aplicativos, composto pelos subprocessos

5.6.1 Manter sistemas de informação

50601001	As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.	DOC-ICP-02 item 9.3.1.1.
50601002	A documentação dos sistemas deve ser mantida atualizada.	DOC-ICP-02 item 9.3.1.1.
50601003	A cópia de segurança deve ser testada e mantida atualizada.	DOC-ICP-02

		item 9.3.1.1.
50601004	Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.	DOC-ICP-02 item 9.3.1.5.
50601005	As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.	DOC-ICP-02 item 9.3.1.5.
50601006	Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).	DOC-ICP-02 item 9.3.5.11.
50601007	Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.	DOC-ICP-02 item 10.2.3.
50601008	O PSC deve descrever, quando aplicáveis, os controles implementados pelo PSC responsável no desenvolvimento de sistemas e no gerenciamento de segurança.	DOC-ICP-17 item 6.2.

5.6.2 Manter bases de dados

50602001	Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.	DOC-ICP-02, item 10.1.4.
50602002	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.	DOC-ICP-02, item 10.3.1.
50602003	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.	DOC-ICP-02, item 9.2.2.
50602004	Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.	DOC-ICP-02, item 9.3.3.17.
50602005	As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.	DOC-ICP-02, item 9.3.5.4.
50602006	Devem ser estabelecidos os formatos e padrões de data e hora contidos em	DOC-ICP-17,

	cada tipo de registro.	item 4.4.4.
50602007	Proteção lógica adicional (criptografia) e senhas devem ser adotados para evitar o acesso não autorizado às informações. O arquivo de senhas deve ser criptografado e ter acesso controlado.	DOC-ICP-02, item 9.3.2.5 e item 9.3.4.5.

5.7 Manter segurança lógica e rede, composto pelos subprocessos:

5.7.1 Manter sistemas básicos

50701001	Os aplicativos e equipamentos utilizados nos processos de certificação digital devem possuir certificado de homologação da ICP-Brasil ou Certificação INMETRO.	DOC-ICP-01.01, item 3.
50701002	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.	DOC-ICP-02, item 9.3.2.3.
50701003	As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.	DOC-ICP-02, item 9.3.2.4.
50701004	A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.	DOC-ICP-02, item 9.3.2.6.
50701005	Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.	DOC-ICP-02, item 9.3.2.7.
50701006	Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.	DOC-ICP-02, item 9.3.3.3.
50701007	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.
50701008	As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas	DOC-ICP-17,

	pelos respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.	item 6.3.1.3.

5.7.2 Manter equipamentos protegidos de ameaças

50702001	O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o "*Efeito Tempest*".	DOC-ICP-02, item 9.3.3.1.
50702002	Mecanismos de segurança baseados em sistemas de proteção (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.	DOC-ICP-02, item 9.3.3.19.
50702003	A ativação da rede deve respeitar a ordem prevista no DOC-ICP-02, item 9.3.3.26. Os sistemas de certificação devem ser dispostos em segmentos de rede que devem ser isolados por meios diversos, como por exemplo: a) utilizando virtual "*lans*" (*vlan*); b) utilizando de *firewall*; c) utilizando artifícios de roteamento.	DOC-ICP-02, itens 9.3.3.26 e 9.3.3.27.
50702004	Ativos de processamento da rede, a exemplo de "*switches*" e roteadores, quando possuírem recursos básicos de segurança como acesso mediante senhas e outros, devem ser configurados para utilizá-los, visando reforçar seus controles de segurança.	DOC-ICP-02, itens 9.3.3.3.
50702005	A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.	DOC-ICP-02, item 9.3.3.4.
50702006	Nos computadores pessoais, devem ser adotadas medidas para combate de vírus, realização de *backups*, controle de acesso e uso de *software* não autorizado.	DOC-ICP-02, item 9.3.5.3.
50702007	Em todos os equipamentos devem ser sistematizados procedimentos para combate a processos destrutivos (virus, "*worms"* e cavalos-de-tróia).	DOC-ICP-02, item 9.3.6 e DOC-ICP-17, item 6.3.5.2.
50702008	As ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando periodicamente os administradores	DOC-ICP-02, item 9.3.3.30.

	das redes sobre as tentativas de intrusão.	
50702009	Os sistemas e os equipamentos do PSC, usados nos processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverão implementar, entre outras, as seguintes características: a) controle de acesso aos serviços e perfis do PSC; b)clara separação das tarefas e atribuições relacionadas a cada perfil qualificado do PSC; c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações; d) geração e armazenamento de registros de auditoria do PSC; e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e f) mecanismos para cópias de segurança (*backup*).	DOC-ICP-17, item 6.1.2.1.
50702010	Qualquer equipamento, ou parte desse, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações do PSC, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, observados os dispostos no ato de descredenciamento, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade do PSC. Todos esses eventos deverão ser registrados para fins de auditoria.	DOC-ICP-17, item 6.1.2.3.
50702011	Qualquer equipamento incorporado ao PSC deverá ser preparado e configurado como previsto na PS implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.	DOC-ICP-17, item 6.1.2.4.
50702012	Definir procedimentos formais para a eliminação segura de mídias desnecessárias.	DOC-ICP-02, item 9.3.5.12.

5.7.3 Manter *logs* e trilhas de auditoria

50703001	Informações de segurança não geradas pelo sistema de certificação devem ser registradas.	DOC-ICP-17, item 4.3.1.2.
50703002	Registrar e analisar periodicamente violações de segurança.	DOC-ICP-02, item 9.2.3.
50703003	Definir, analisar periodicamente e proteger devidamente arquivos de *logs* de sistemas.	DOC-ICP-02, item 9.3.1.3 e DOC-ICP-17, item 4.3.2.

50703004	O PSC deve manter localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses.	DOC-ICP-17, item 4.3.3.
50703005	O PSC deve descrever os mecanismos obrigatórios para proteger os seus registros de auditoria contra leitura não autorizada, modificação e remoção.	DOC-ICP-17, item 4.3.4.1.
50703006	O PSC deve descrever e localizar os recursos utilizados pelo PSC responsável para a coleta de dados de auditoria.	DOC-ICP-17, item 4.3.6.
50703007	Para os sistemas de controle de acesso lógico, os registros de atividades (*logs*) devem ser analisados periodicamente.	DOC-ICP-02, item 9.3.4.15.

5.7.4 Manter cópias de segurança e restauração

50704001	O PSC deve descrever os procedimentos adotados pelo PSC responsável para gerar cópias de segurança (*backup*) de seus registros de auditoria e a sua periodicidade, que não deve ser superior a uma semana.	DOC-ICP-17, item 4.3.5.
50704002	O PSC deve descrever na DPPSC os procedimentos para recuperação de recursos computacionais corrompidos.	DOC-ICP-17, item 4.6.2.
50704003	Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações.	DOC-ICP-02, item 9.3.2.9.
50704004	Uma sala de armazenamento externa à instalação técnica principal do PSC deve ser usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala deverá estar disponível a pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e deverá atender aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.	DOC-ICP-17, item 5.1.8.

5.7.5 Manter controle de acesso a rede

50705001	O tráfego das informações no ambiente de rede deverá ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos.	DOC-ICP-17.01, item 5.1.
50705002	Não poderão ser admitidos acessos externos à rede interna do PSC. As tentativas de acessos externos deverão ser inibidas e monitoradas por meio de aplicativos que criem barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão.	DOC-ICP-17.01, item 5.2.

50705003	Deverão ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada mês. Os testes na rede deverão ser documentados e as vulnerabilidades detectadas corrigidas.	DOC-ICP-17.01, item 5.3.
50705004	A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.	DOC-ICP-02, item 9.3.3.9.
50705005	Devem ser implementados mecanismos de *firewall* em equipamentos de utilização específica, configurados exclusivamente para tal função. Os *firewalls* deverão ser dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno ao PSC.	DOC-ICP-17, item 6.3.2.1.
50705006	O acesso lógico aos elementos de infraestrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.	DOC-ICP-17, item 6.3.1.4.
50705007	As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, semanal e todas as ações tomadas em decorrência desse exame deverão ser documentadas.	DOC-ICP-17, item 6.3.4.
50705008	O acesso via rede aos sistemas do PSC deverá ser permitido somente para os seguintes serviços: a) pela EAT da ICP-Brasil, para o sincronismo e auditoria dos sistemas de assinaturas; b)pelo PSC, para a administração dos sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT; c) pelo subscritor, para a armazenamento e acesso à chave privada e aos serviços de assinatura digital, verificação da assinatura digital.	DOC-ICP-17, item 6.3.1.6.
50705009	Nos ambientes de rede, registrar e analisar periodicamente eventos de segurança.	DOC-ICP-02, item 9.3.3.10.
50705010	O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.	DOC-ICP-02, item 9.3.3.15.
50705011	Componentes críticos da rede local devem ser mantidos em salas	DOC-ICP-02,

	protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.	itens 9.3.3.2.
50705012	Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, deverão estar localizados e operar em ambientes de nível, no mínimo, 3 avançado.	DOC-ICP-17, item 6.3.1.2 e DOC-ICP-17.01 item 3.1.1.3.

5.7.6 Manter controle de acesso lógico

50706001	Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.	DOC-ICP-02, item 9.3.2.2.
50706002	O ambiente operacional dos sistemas deve ser monitorado.	DOC-ICP-02, item 9.3.2.3.
50706003	O PSC deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a PS da ICP-Brasil, com procedimentos de validação dessas senhas.	DOC-ICP-17, item 5.2.3.3.
50706004	Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.	DOC-ICP-02, item 9.3.1.2.
50706005	O responsável pela autorização ou confirmação da autorização de acesso lógico a sistemas e servidores deve ser claramente definido e registrado.	DOC-ICP-02, item 9.3.2.1.
50706006	O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido.	DOC-ICP-02, item 9.3.2.1.
50706007	As autorizações de acesso lógico das máquinas servidoras devem ser revistas, confirmadas e registradas continuamente.	DOC-ICP-02, item 9.3.2.1.
50706008	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.	DOC-ICP-02, item 9.3.3.7.
50706009	O arquivo de senhas deve ser criptografado e ter o acesso controlado.	DOC-ICP-02, item 9.3.4.5.
50706010	O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.	DOC-ICP-02, item 9.3.4.8.
50706011	O sistema de controle de acesso deverá estar baseado em um ambiente de nível 3.	DOC-ICP-17, item 5.1.2.3.

5.8 Manter infraestrutura, composto pelos subprocessos:

5.8.1 Manter equipamentos de computação

50801001	Módulo criptográfico para geração de chaves assimétricas de usuário final e armazenamento da chave privada de titular de certificado deve ser homologado pela ICP-Brasil ou possuir certificação INMETRO.	DOC-ICP-01.01, item 3.
50801002	A DPPSC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada dos subscritores do PSC responsável.	DOC-ICP-17, item 6.4.
50801003	Preferentemente, *nobreaks*, geradores e outros componentes da infraestrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção.	DOC-ICP-17.01, item 3.1.1.1.2.c.

5.8.2 Manter controle de acesso físico

50802001	Acesso aos componentes de infraestrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.	DOC-ICP-02, item 8.2.10.
50802002	A segurança de todos os ambientes do PSC deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana).	DOC-ICP-17, item 5.1.2.2.1.
50802003	O uso de equipamentos nas instalações do PSC só pode ser realizado após a autorização formal e sob supervisão.	DOC-ICP-02, item 8.2.13.
50802004	Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).	DOC-ICP-02, item 8.2.14.
50802005	Acesso de visitantes aos ambientes do PSC devem ser registrados e supervisionados.	DOC-ICP-02, item 8.2.15.
50802006	Devem ser instalados e testados regularmente sistemas de detecção de intrusos de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.	DOC-ICP-02, item 8.2.17.
50802007	Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui	DOC-ICP-02,

	cartões/chaves deverá ser mantida.	item 8.2.4.
50802008	Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.	DOC-ICP-02, item 8.2.5.
50802009	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.	DOC-ICP-02, item 8.2.6.
50802010	Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.	DOC-ICP-02, item 8.2.8.
50802011	A entrada e saída, de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.	DOC-ICP-02, item 8.2.9.
50802012	Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.	DOC-ICP-02, item 9.3.3.11.
50802013	A infraestrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.	DOC-ICP-02, item 9.3.3.13.
50802014	Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries	DOC-ICP-02, item9.3.3.2
50802015	Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).	DOC-ICP-02, item 9.3.5.2.
50802016	O PSC deve registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação como os registros de acessos físicos.	DOC-ICP-17, item 4.3.1.2.
50802017	O PSC deve possuir pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSC.	DOC-ICP-17.01, item 3.1.1.1.
50802018	Para garantir a segurança do material armazenado, o cofre ou o gabinete	DOC-ICP-17.01,

	deverá ser feito em aço ou material de resistência equivalente; e, possuir tranca com chave.	item 3.1.1.1.4.a.
50802019	O primeiro nível – ou nível 1 – deverá situar-se após a primeira barreira de acesso às instalações do PSC. O ambiente de nível 1 do PSC na ICP-Brasil desempenha a função de interface com cliente ou fornecedores que necessita comparecer ao PSC.	DOC-ICP-17.01, item 3.1.1.1.1.
50802020	O segundo nível – ou nível 2 – será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSC. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.	DOC-ICP-17.01, item 3.1.1.1.2.
50802021	O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-17.01, item 3.1.1.1.2.a.
50802022	O acesso ao nível 2 deverá ser permitido apenas a pessoas que trabalhem diretamente com as atividades de serviços de armazenamento dos certificados para usuários finais e serviços de assinatura digital e verificação da assinatura digital ou ao pessoal responsável pela manutenção de sistemas e equipamentos do PSC, como administradores de rede e técnicos de suporte de informática. Demais funcionários do PSC ou do possível ambiente que esta compartilhe não deverão acessar este nível.	DOC-ICP-17.01, item 3.1.1.1.2.b.
50802023	Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações do PSC, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.	DOC-ICP-17.01, item 3.1.1.1.2.d.
50802024	O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação do PSC. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários e serviços de assinatura digital e verificação da assinatura digital deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.	DOC-ICP-17.01, item 3.1.1.1.3.
50802025	No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica	DOC-ICP-17.01, item 3.1.1.1.3.a.

	ou digitação de senha;	
50802026	As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.	DOC-ICP-17.01, item 3.1.1.1.3.b.
50802027	Caso o ambiente de Nível 3 possua forro ou piso falsos, deverão ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior.	DOC-ICP-17.01, item 3.1.1.1.3.c.
50802028	Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deverá ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário;	DOC-ICP-17.01, item 3.1.1.1.3.d.
50802029	O ambiente de nível 3 deverá ser dotado, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 2.	DOC-ICP-17, item 5.1.2.2.3 e 5.1.2.2.4.
50802030	O ambiente de Nível 3 do PSC deve estar instalado em local protegido contra a exposição à água, infiltrações e inundações.	DOC-ICP-17, item 5.1.4.
50802031	O terceiro nível avançado – ou nível 3.1 –, especificamente para os PSC de assinatura digital, no interior ao ambiente de nível 3, deverá compreender pelo menos um gabinete reforçado trancado, que abrigará todo o *hardware* e *software* utilizado pelo PSC de assinatura digital.	DOC-ICP-17.01, item 3.1.1.1.4.
50802032	O quarto nível – ou nível 4 – especificamente para os PSC de armazenamento de chaves privadas, interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação do PSC de armazenamento de chaves privadas. Todos os sistemas e equipamentos necessários a essas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente	DOC-ICP-17.01, item 3.1.1.1.5.

	estiver ocupado.	
50802033	No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.	DOC-ICP-17.01, item 3.1.1.1.6.
50802034	Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.	DOC-ICP-02, item 8.2.11.
50802035	A segurança de todos os ambientes do PSC deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana).	DOC-ICP-17, item 5.1.2.2.1.

5.8.3 Manter ar-condicionado

50803001	O sistema de ar-condicionado deve possuir redundância.	DOC-ICP-17, item 5.1.3.9.
50803002	O sistema de climatização deve atender às condições ambientais estabelecidas na Norma NBR 11515.	DOC-ICP-17, item 5.1.3.7. e 5.1.6.
50803003	A temperatura dos ambientes atendida pelo sistema de climatização deve ser permanentemente monitorada por sistema de notificação e alarme.	DOC-ICP-17, item 5.1.3.8.

5.8.4 Manter energia elétrica

50804001	A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.	DOC-ICP-02, item 9.3.3.14.
50804002	O PSC deverá possuir mecanismos que permitam, em caso de falta de energia: a) iluminação de emergência em todos os ambientes, acionada automaticamente; b) continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.	DOC-ICP-17, item 5.1.2.2.5.
50804003	A energia elétrica para a infraestrutura do PSC deve possuir sistemas e	DOC-ICP-17,

	dispositivos que garantam o fornecimento ininterrupto.	item 5.1.3.1.
50804004	Todos os cabos elétricos devem estar protegidos por tubulações ou dutos apropriados.	DOC-ICP-17, item 5.1.3.2.
50804005	Sistema de aterramento deve ser implantado.	DOC-ICP-17, item 5.1.3.1.
50804006	Tubulações, dutos, calhas, quadros e caixas - de passagem, distribuição e terminações - devem ser construídos de forma a facilitar vistorias e a detecção de tentativas de violações.	DOC-ICP-17, item 5.1.3.3.
50804007	Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados.	DC-ICP-17, item 5.1.3.3.
50804008	Todos os cabos devem ser catalogados e vistoriados no mínimo a cada 6 (seis) meses.	DOC-ICP-17, item 5.1.3.4.
50804009	Deve ser mantida atualizada a topologia de rede de cabos.	DOC-ICP-17, item 5.1.3.5.
50804010	Instalações elétricas provisórias, fiações expostas e conexões inadequadas não devem ser admitidas.	DOC-ICP-17, item 5.1.3.6.

5.8.5 Manter sistema de combate a incêndio

50805001	Nas instalações do PSC não será permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.	DOC-ICP-17 item 5.1.5.1.
50805002	No interior do ambiente nível 3 devem existir no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de *sprinklers* no prédio, o ambiente de nível 3 do PSC não deverá possuir saídas de água, para evitar danos aos equipamentos.	DOC-ICP-17, item 5.1.5.2.
50805003	O ambiente de nível 3 deve possuir sistema de prevenção contra incêndios, que acione alarmes preventivos uma vez detectada fumaça no ambiente.	DOC-ICP-17, item 5.1.5.3.
50805004	Nos demais ambientes do PSC deverão existir extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio.	DOC-ICP-17, item 5.1.5.4.
50805005	Mecanismos específicos deverão ser implantados pelo PSC para garantir a segurança de seu pessoal e de seus equipamentos em situações de	DOC-ICP-17, item 5.1.5.5.

	emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.	

5.9 Manter recursos humanos, composto pelos subprocessos:

5.9.1 Admitir pessoas

50901001	Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.	DOC-ICP-02, item 7.3.1.1.
50901002	Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, incluindo as atividades finalísticas do PSC.	DOC-ICP-02, item 7.3.1.2, DOC-ICP-17.01, item 2.8.
50901003	Todo o pessoal do PSC responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL.	DOC-ICP-17, item 5.3.7.
50901004	O PSC deverá ter uma Política de Gestão de Pessoas que disponha sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.	DOC-ICP-17.01, item 2.1.
50901005	A entrevista de Admissão deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.	DOC-ICP-02, item 7.3.4.1.
50901006	Todo pessoal envolvido nas atividades realizadas pelo PSC, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.	DOC-ICP-17.01, item 2.3.
50901007	Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público.	DOC-ICP-02, item 7.3.4.2.
50901008	Todo o pessoal do PSC responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de	DOC-ICP-17, item 5.3.1.

	armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL. O PSC responsável poderá definir requisitos adicionais para a contratação.	
50901009	Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil.	DOC-ICP-02, item 7.3.3.

5.9.2 Manter capacitação de pessoas

50902001	Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.	DOC-ICP-02, item 6.1.3.
50902002	Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.	DOC-ICP-02, item 6.1.4.
50902003	Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.	DOC-ICP-02, item 7.3.7.
50902004	Todos os empregados do PSC deverão receber treinamento específico antes de obter qualquer tipo de acesso.	DOC-ICP-17, item 5.2.1.3.
50902005	Todo o pessoal do PSC responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverão receber treinamento documentado, suficiente para o domínio dos seguintes temas: a) princípios e tecnologias dos sistemas e *hardwares* de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais em uso no PSC; b) ICP-Brasil; c) princípios e tecnologias de certificação digital e de assinaturas digitais; d)princípios e mecanismos de segurança de redes e segurança do PSC; e) procedimentos de recuperação de desastres e de continuidade do negócio; f) familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança; g) familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema; h)outros assuntos relativos a	DOC-ICP-17, item 5.3.3.

	atividades sob sua responsabilidade.	
50902006	Todo o pessoal do PSC responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do PSC.	DOC-ICP-17, item 5.3.4.
50902007	Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar os incidentes descritos no DOC-ICP-02.	DOC-ICP-02, item 13.2.3.
50902008	Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.	DOC-ICP-02, item 7.3.5.2.
50902009	A comprovação da capacidade técnica do pessoal envolvido nos serviços prestados pelo PSC deverá estar à disposição para eventuais auditorias e fiscalizações.	DOC-ICP-17.01, item 2.2.

5.9.3 Manter habilitação de pessoas

50903001	Todo empregado do PSC terá sua identidade e perfil verificados antes de: a) ser incluído em uma lista de acesso físico às instalações do PSC; b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis do PSC; c) ser incluído em uma lista para acesso lógico aos sistemas do PSC.	DOC-ICP-17, item 5.2.3.1.
50903002	Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.	DOC-ICP-02, item 10.2.1.
50903003	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.	DOC-ICP-02, item 10.2.2.
50903004	O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.	DOC-ICP-02, item 7.3.1.3.
50903005	Todos os empregados do PSC deverão estar identificados por uma	DOC-ICP-02,

	credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo máximo de 1 (um) ano de validade. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário.	item 7.3.6.
50903006	As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.	DOC-ICP-02, item 8.2.1.
50903007	Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.	DOC-ICP-02, item 9.3.4.16.
50903008	O PSC responsável pela DPPSC deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente os serviços do ambiente sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.	DOC-ICP-17, item 5.2.1.1.
50903009	O PSC deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação: administrador do sistema, operador de sistema e auditor de sistema.	DOC-ICP-17, item 5.2.1.2.
50903010	O tipo e o nível de acesso dos empregados do PSC serão determinados, em documento formal, com base nas necessidades de cada perfil.	DOC-ICP-17, item 5.2.1.3.
50903011	Todas as tarefas executadas no cofre ou gabinete onde se localizam os serviços do PSC deverão requerer a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. Para os casos de cópias das chaves dos usuários e portabilidade da mesma serão necessários, no mínimo, 3 (três) empregados com perfis distintos e qualificados. As demais tarefas do PSC poderão ser executadas por um único empregado.	DOC-ICP-17, item 5.2.2.
50903012	Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.	DOC-ICP-02, item 6.3.
50903013	Na DPPSC devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados no PSC responsável, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.	DOC-ICP-17, item 5.2.

5.9.4 Avaliar desempenho

50904001	Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.	DOC-ICP-02, item 7.3.5.1.
50904002	Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.	DOC-ICP-02, item 7.3.8.1.
50904003	Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.	DOC-ICP-02, item 7.3.8.2.
50904004	Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.	DOC-ICP-02, item 7.3.8.3.
50904005	As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.	DOC-ICP-02, item 7.3.8.4.

5.9.5 Suspender, movimentar e desligar pessoas

50905001	Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.	DOC-ICP-02, item 6.1.5.
50905002	O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público, sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.	DOC-ICP-02, item 7.3.9.
50905003	Quando um empregado se desligar do PSC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro do PSC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver ao PSC no ato de seu desligamento.	DOC-ICP-17, item 5.2.1.4.
50905004	O empregado ou servidor firmará, antes do desligamento, declaração de	DOC-ICP-02,

	que não possui nenhum tipo de pendência junto às diversas unidades que compõem a entidade, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.	item 7.3.10.
50905005	Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades.	DOC-ICP-02, item 7.3.11.
50905006	A DPPSC pode definir uma política a ser adotada pelo PSC responsável e pelos PSSs vinculados para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.	DOC-ICP-17, item 5.3.5.
50905007	Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional, o PSC deverá, de imediato, suspender o acesso dessa pessoa aos sistemas, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.	DOC-ICP-17, item 5.3.6.1.
50905008	O PSC deverá ter procedimentos formais de apuração e responsabilização em caso de descumprimento das regras estabelecidas pelas suas políticas ou pelas normas da ICP-Brasil.	DOC-ICP-17.01, item 2.6.
50905009	As punições passíveis de aplicação, em decorrência de processo administrativo, são: a) advertência; b) suspensão por prazo determinado; ou c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.	DOC-ICP-17, item 5.3.6.4.