Infraestrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS DE SEGURANÇA PSBIO NA ICP-BRASIL

DOC-ICP-03.02

versão 1.3

29 de maio de 2020

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	Item Alterado	Descrição da Alteração
Instrução Normativa n° 07, de 29.05.2020 (Versão 1.3)	4.g e 11	Altera o tempo de armazenamento dos logs, trilhas de auditorias e imagens.
Instrução Normativa n° 01, de 31.03.2016 (Versão 1.2)	3.1.1.2, 3.1.1.3 (novo) e 6	Atualização dos requisitos dos PSBio.
Instrução Normativa n° 08, de 10.12.2015 (Versão 1.1)	Item 4, "g"	Inclui a previsão de backup para informações como log, trilhas de auditoria.
Resolução nº 114, de 30.09.2015 (Versão 1.0)		Aprova a versão 1.0 do Documento Requisitos mínimos de segurança PSBIO.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC-RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
ADE	Adendo
APF	Administração Pública Federal
DOC-ICP	Documentos Principais da ICP-BRASIL
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
PSBio	Prestador de Serviço Biométrico credenciado na ICP-BRASIL

1. DISPOSIÇÕES GERAIS

a) Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos a serem adotados pelos PRESTADOR DE SERVIÇOS BIOMÉTRICOS - PSBio da ICP-Brasil.

b) Suplementa, para essas entidades, os regulamentos contidos no documento DOC-ICP-05.02, tomando como base também a Política de Segurança da ICP-Brasil – DOC-ICP-02.

c) Os requisitos abaixo informados deverão ser apresentados quando do credenciamento do PSBio e mantidos atualizados durante seu funcionamento enquanto entidade estiver credenciado na ICP-Brasil.

d) O PSBio deverá ter uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que devem ser seguidos em suas dependências e atividades, em consonância com o DOC-ICP-02.

e) Deverá existir um exemplar da Política de Segurança da Informação no formato impresso disponível para consulta no Nível 1 de segurança do PSBio.

f) A Política de Segurança da Informação deverá ser seguida por todo pessoal envolvido nos projetos coordenados pelo PSBio, do seu próprio quadro ou contratado.

g) Este documento define normas de segurança que deverão ser aplicadas nas áreas internas ao PSBio assim como no trânsito de informações e materiais com entidades externas.

h) A seguir são informados os requisitos que devem ser observados quanto a segurança de pessoal, segurança física, segurança lógica, segurança de rede, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios e análise de registros de eventos.

2. SEGURANÇA PESSOAL

a) 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.

b) A comprovação da capacidade técnica do pessoal envolvido nos serviços prestados pelo PSBio deverá estar à disposição para eventuais auditorias e fiscalizações.

c) 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.

d) O termo de sigilo da informação deverá conter cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos da ICP-Brasil.

e) 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.

f) O PSBio deverá ter procedimentos formais de apuração e responsabilização em caso de descumprimento das regras estabelecidas pelas suas políticas ou pelas normas da ICP-Brasil.

g) O pessoal do PSBio, e contratados, deverão possuir um dossiê contendo os seguintes documentos:

i. Contrato de trabalho ou cópia das páginas da carteira de trabalho onde conste o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;
ii. Comprovante da verificação de antecedentes criminais;
iii. Comprovante da verificação de situação de crédito;
iv. Comprovante da verificação de histórico de empregos anteriores;
v. Comprovação de residência;
vi. Comprovação de capacidade técnica;
vii. Resultado da entrevista inicial, com a assinatura do entrevistador;
viii. Declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir as regras aplicáveis da ICP-Brasil;
ix. Termo de sigilo.

h) Não serão admitidos estagiários no exercício fim das atividades do PSBio.

i) Quando da demissão, o referido dossiê deverá possuir os seguintes documentos:

i. Evidências de exclusão dos acessos físico e lógico nos ambientes do PSBio;
ii. Declaração assinada pelo empregado ou servidor de que não possui pendências, conforme previsto no item 7.3.10 do DOC-ICP-02.

3. SEGURANÇA FÍSICA

3.1. Disposições Gerais de Segurança Física

3.1.1. Níveis de acesso

3.1.1.1. São definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSBio.

3.1.1.1.1. 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 necessita comparecer ao PSBio.

3.1.1.1.2. 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.

a) 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;

b) O acesso a este nível 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;

c) 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;

d) 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.

3.1.1.1.3. 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.

a) 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 ou digitação de senha;

b) 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;

c) 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;

d) 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;

e) 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).

NOTA 1: Caso a PSBio se situe dentro de um data center, com requisitos de segurança julgados adequados pela AC-Raiz, poderá ser dispensada a existência de um ambiente de Nível 3 específico para a PSBio.

3.1.1.1.4. 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:

a) 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.

3.1.1.2. 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;

3.1.1.3. Os PSBio devem ainda atender aos seguintes requisitos:

a) O ambiente físico do PSBio deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos;

b) O PSBio deverá conter imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente;

c) 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;

d) Todos que transitam no ambiente físico do PSBio deverão portar crachás de identificação, inclusive os visitantes;

e) 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;

f) O PSBio deverá conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico;

g) 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;

h) Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, deverão estar inventariados com informações que permitam a identificação inequívoca;

i) 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;

j) 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.

4. SEGURANÇA LÓGICA

a) O acesso lógico ao ambiente computacional do PSBio se dará no mínimo mediante usuário individual e senha, que deverá ser trocada periodicamente;

b) Todos os equipamentos do parque computacional deverão ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas;

c) Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa;

d) 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;

e) 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;

f) Todo equipamento do PSBio deverá ter log ativo e seu horário sincronizado com uma fonte confiável de tempo;

g) 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;

h) Os softwares dos sistemas operacionais, os antivírus e aplicativos de segurança devem ser mantidos atualizados.

5. SEGURANÇA DE REDE

a) O tráfego das informações no ambiente de rede deverá ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

b) 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;

c) Deverão ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada 3 meses. Os testes na rede deverão ser documentados e as vulnerabilidades detectadas corrigidas.

6. REQUISITOS BIOMÉTRICOS

Os PSBios deverão ser entidades com capacidade técnica para realizar a identificação (1:N) biométrica, tornando um registro/requerente único em um ou mais bancos/sistemas de dados biométrico para toda ICP-Brasil, e a verificação (1:1) biométrica do requerente de um certificado digital a comparação de uma biometria, que possua característica perene e unívoca, de acordo com os padrões internacionais de uso, como, por exemplo, impressão digital, face, íris, voz, coletada no processo de emissão do certificado digital com outra que está armazenada, com o mesmo registro/indexador (IDN) deste requerente, em um ou mais bancos/sistemas de dados biométrico da ICP-Brasil, como estabelecido no DOC-ICP-05.03, bem como os descritos neste documento.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

a) 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;

b) A classificação da informação no PSBio deverá ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada;

c) A informação poderá ser classificada em:

i. Público: Qualquer ativo de informação, de propriedade do PSBio ou não, que poderá vir ao público sem maiores consequências danosas ao funcionamento normal do PSBio. Poderá ser acessado por qualquer pessoa, seja interna ou externa ao PSBio. Integridade da informação não é vital;

ii. Pessoal: Qualquer ativo de informação relacionado à informação pessoal. Por exemplo: mensagem pessoal de correio eletrônico, arquivo pessoal, dados pessoais, etc;

iii. Interna: Qualquer ativo de informação, de propriedade do PSBio ou não, que não seja considerada pública. Ativo de informação relacionado às atividades do PSBio que é direcionada estritamente para uso interno. A divulgação não autorizada do ativo de informação poderia causar impacto à imagem do PSBio. Por exemplo: código fonte de programa, cronograma de atividades, atas de reuniões, etc;

iv. Confidencial: Qualquer ativo de informação que seja crítico para as atividades do PSBio em relação ao sigilo e integridade. Qualquer material e informação recebida para ensaio, assim como qualquer resultado do ensaio (como relatório) deverá ser considerado confidencial.

NOTA 2: Caso o PSBio seja entidade da Administração Pública Federal - APF, aplicar-se-á as disposições do Decreto nº 7.845/2012 e demais normas aplicáveis à APF, no que couber.

8. SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

a) 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.

b) 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.

c) O PSBio deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

9. GERENCIAMENTO DE RISCOS

O PSBio deverá ter um processo de gerenciamento de riscos, atualizado, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados atualizado, no mínimo, anualmente.

10. PLANO DE CONTINUIDADE DE NEGÓCIOS

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.

11. ANÁLISES DE REGISTRO DE EVENTOS

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.