Política de Segurança do PSBIO VALID na ICP-Brasil

PS do PSBIO VALID
Versão 2.0 de 01/07/2020.

ÍNDICE

CONTROLE DE ALTERAÇÕES:

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.0	01/09/2019	-	-	Criação da PS do PSBIO
2.0	03/07/2020	-	-	Atualização da Política de Segurança do PSBIO VALID.

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

1. INTRODUÇÃO

1.1. Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos a serem adotados pelo PRESTADOR DE SERVIÇOS BIOMÉTRICOS - PSBIO VALID da ICP-Brasil.

1.2. Os requisitos informados nesta política deverão ser apresentados quando do credenciamento do PSBIO VALID e mantidos atualizados durante seu funcionamento enquanto entidade estiver credenciado na ICP-Brasil.

1.3. Deverá existir um exemplar da Política de Segurança da Informação no formato impresso disponível para consulta no Nível 1 de segurança do PSBIO VALID.

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

2. OBJETIVOS

A Política de Segurança do PSBIO VALID tem os seguintes objetivos:

a) Definir o escopo da segurança das entidades;

b) Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades reduzindo os riscos e garantindo a integridade, o sigilo e a disponibilidade das informações dos sistemas de informação e recursos;

c) Servir de referência para auditoria, apuração e avaliação de responsabilidades;

d) Definir normas de segurança que deverão ser aplicadas nas áreas internas ao PSBIO VALID assim como no trânsito de informações e materiais com entidades externas.

3. ABRANGÊNCIA

A Política de Segurança abrange os seguintes aspectos:

a) Requisitos de segurança humana;

b) Requisitos de segurança física;

c) Requisitos de segurança lógica;

d) Requisitos biométricos.

4. TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

5. CONCEITOS E DEFINIÇÕES

Serão destacadas, a seguir, algumas definições de termos considerados relevantes para o entendimento desta Política de Segurança:

a) Ativo de Informação – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos do PSBIO VALID;

b) Ativo de Processamento – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades relacionadas à PSBIO VALID, tanto os produzidos internamente quanto os adquiridos;

c) Controle de Acesso – são restrições ao acesso às informações de um sistema exercidas pela gerência de segurança da informação do PSBIO VALID;

d) Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

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

f) Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança do PSBIO VALID;

g) Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo do PSBIO VALID;

h) Política de Segurança – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação do PSBIO VALID;

i) Proteção dos Ativos – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

j) Responsabilidade – são as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

k) Senha Fraca ou Óbvia – é aquela na qual utilizam-se caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequencias numéricas simples, palavras com significado em qualquer língua, dentre outras.

6. REGRAS GERAIS

6.1. GESTÃO DE SEGURANÇA

6.1.1. A Política de Segurança do PSBIO VALID aplica-se a todos os recursos humanos, administrativos e tecnológicos a ela relacionados de modo permanente ou temporário.

6.1.2. Esta política é comunicada e divulgada para todo o pessoal envolvido, garantindo que todos tenham consciência da Política e a pratiquem na organização.

6.1.3. Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado na política de segurança.

6.1.4. Um programa de conscientização sobre segurança da informação é implementado através de treinamentos específicos, assegurando que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações do PSBIO VALID

6.1.5. Os procedimentos são documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

6.1.6. O PSBIO VALID deve possuir mecanismo e repositório centralizado para manutenção de trilhas, logs e demais notificações de incidentes. O Gerente de Segurança é informado, uma vez que qualquer tentativa de violação seja detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra ataques empreendidos contra esses mecanismos.

6.1.7. Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, estão em conformidade com esta Política de Segurança.

6.1.8. É considerada proibida qualquer ação que não esteja explicitamente permitida na Política de Segurança do PSBIO VALID ou que não tenha sido previamente autorizada pelo Gerente de Segurança da PSBIO VALID

6.1.9. Toda informação gerada e custodiada pelo PSBIO VALID deverá ser classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação;

6.1.10. A classificação da informação no PSBIO VALID deverá ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada;

6.1.11. 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 VALID. Todos os registros da transação biométrica por parte do PSBIO VALID deverão ser guardados por um período de 7 anos.

6.2. GERENCIAMENTO DE RISCOS

O PSBIO VALID implementa análises de risco periodicamente através de sua própria estrutura e de terceiros.

O processo de gerenciamento de riscos é revisto anualmente para prevenção contra riscos, inclusive aqueles advindos de novas

tecnologias, visando a elaboração de planos de ação apropriados para proteção dos componentes ameaçados.

6.3. SALVAGUARDA DE ATIVOS DE INFORMAÇÃO

6.3.1. Todos os ativos do PSBIO VALID são inventariados, classificados, permanentemente atualizados, e possuem gestor responsável formalmente designado, conforme descrição a seguir:

6.3.2. Os ativos de TI são inventariados pela área de Infraestrutura (ambientes do PSBIO VALID e corporativo). Os inventários de Segurança Física também são mantidos pela área de Infraestrutura.

6.3.3. Todas as informações críticas para o funcionamento do PSBIO VALID devem possuir seus dados salvaguardados em formato eletrônico (backup).

6.3.4. Os seguintes procedimentos estão devidamente descritos e formalizados:

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.

6.3.5. O PSBIO VALID deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

6.4. PLANO DE CONTINUIDADE DO NEGÓCIO

6.4.1. O Plano de Continuidade do Negócio do PSBIO VALID é testado pelo menos uma vez por ano, garantindo a continuidade dos serviços críticos ao negócio.

7. REQUISITOS DE SEGURANÇA DE PESSOAL

7.1. DEFINIÇÃO

Conjunto de medidas e procedimentos de segurança a serem observados por todos funcionários e prestadores de serviço, necessários à proteção dos ativos do PSBIO VALID;

7.2. OBJETIVOS

7.2.1. Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos do PSBIO VALID;

7.2.2. Prevenir e neutralizar as ações de pessoas que possam comprometer a segurança do PSBIO VALID.

7.2.3. Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados à PSBIO VALID, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham.

7.2.4. Orientar o processo de avaliação de todo o pessoal que trabalhe no PSBIO VALID, mesmo em caso de funções desempenhadas por prestadores de serviço.

7.3. DIRETRIZES

7.3.1. O Processo de Admissão

7.3.1.1. São adotados critérios rígidos para o processo seletivo de candidatos em funções ligadas a operação do PSBIO VALID, com o propósito de selecionar pessoas reconhecidamente idôneas e sem antecedentes que possam vir a comprometer a segurança ou credibilidade do PSBIO VALID

7.3.1.2. O PSBIO VALID não admitirá estagiários no exercício de atividades diretamente relacionadas com seus processos operacionais;

7.3.1.3. Todo pessoal envolvido nos projetos coordenados pelo PSBIO VALID, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garantam o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato;

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

7.3.1.5. 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 VALID

7.3.1.6. Os funcionários do PSBIO VALID, 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;
viii. Termo de sigilo.

7.3.2. As Atribuições da Função

As atribuições de cada função são relacionadas de acordo com a característica das atividades desenvolvidas, considerando-se os seguintes itens:

a) A descrição sumária das tarefas inerentes à função;
b) As necessidades de acesso a informações sensíveis;

Nesse tópico são descritas as razões pelas quais é justificado o acesso do funcionário às informações sensíveis ao PSBIO VALID São priorizadas as tarefas e as diferentes funções que o respectivo cargo desempenhará.

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

Esse tópico diz respeito ao setor ou nível físico ao qual o funcionário tem acesso e está intimamente ligado ao item b.

d) As necessidades de contato de serviço interno e/ou externo;

Esse tópico, também relacionado ao cargo do funcionário, diz respeito à necessidade do mesmo em manter contatos de serviço interno e/ou externo à PSBIO VALID;

Os funcionários com contatos externos seguem procedimentos que incluem a assinatura de acordo de confidencialidade antes do acesso da entidade externa a qualquer informação classificada.

e) As características de responsabilidade, decisão e iniciativas inerentes à função; Todas as exceções que tenham impacto na segurança devem sempre ser submetidas, para aprovação prévia, à área de Segurança.
f) A qualificação técnica necessária ao desempenho da função;

Nesse tópico serão levantadas as qualificações técnicas necessárias ao desempenho da função. As informações contidas nesse tópico têm origem no Departamento de Recursos Humanos.

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

7.3.3. O Levantamento de Dados Pessoais

O levantamento de dados pessoais é elaborado através de pesquisa, feita por empresa especializada, do histórico da vida pública do candidato, com o propósito de verificação de seu perfil.

7.3.4. A Entrevista de Admissão

7.3.4.1. É realizada, por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados durante o levantamento de dados pessoais do candidato;

7.3.4.2. São avaliadas, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato são apenas aquelas de caráter público;

7.3.5. O Desempenho da Função

7.3.5.1. Periodicamente, o desempenho dos funcionários é acompanhado e avaliado com o propósito de detectar a necessidade de atualização técnica e de segurança;

7.3.5.2. É dado aos funcionários ou prestadores de serviços do PSBIO VALID acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

7.3.6. A Credencial de Segurança

7.3.6.1. O funcionário é identificado por meio de uma credencial (crachá apropriado) que habilita seu acesso físico, de acordo com o grau de sigilo compatível ao cargo e/ou à função a ser desempenhada;

7.3.6.2. A Credencial de Segurança somente é concedida pela área de Segurança ou por área designada pelo Gerencia e é fundamentada na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função;

7.3.6.3. É de um ano o prazo de validade máximo de concessão a um indivíduo de uma credencial de segurança. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário, por ato da Gerencia de Segurança, enquanto exigir a necessidade do serviço.

7.3.7. Treinamento em Segurança da Informação

7.3.7.1. A Política de Segurança e suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos são apresentada aos funcionários e prestadores de serviço, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento.

7.3.7.2. Todo funcionário é treinado na ocasião de sua admissão na companhia e passa por uma reciclagem ao menos uma vez por ano.

7.3.8. Acompanhamento no Desempenho da Função

7.3.8.1. São realizados processos de avaliação de desempenho da função que documentam a observação do comportamento pessoal e funcional dos funcionários. A avaliação é realizada pela chefia imediata dos mesmos;

7.3.8.2. São registrados os atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do funcionário;

7.3.8.3. Os comportamentos incompatíveis ou que possam gerar comprometimentos à segurança são averiguados e comunicados à chefia imediata;

7.3.8.4. As chefias imediatas asseguram que todos os funcionários ou prestadores de serviços tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

7.3.9. O Processo de Desligamento, Férias e Licença.

7.3.9.1. O acesso de ex-funcionários às instalações do PSBIO VALID é restrito às áreas de acesso público.

7.3.9.2. Sua credencial, sua identificação, seu crachá, o uso de equipamentos, mecanismos e acessos físicos e lógicos são revogados.

7.3.9.3. Quando da demissão, o referido dossiê deverá possuir os seguintes documentos:

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

7.3.10. O Processo de Liberação

O funcionário ou prestador de serviço assina, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto ao PSBIO VALID

7.3.11. A Entrevista de Desligamento

É realizada entrevista de desligamento para orientar o funcionário ou prestador de serviço sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência no PSBIO VALID

7.4. DEVERES E RESPONSABILIDADES

7.4.1. Deveres dos funcionários ou prestadores de serviços

São deveres dos empregados ou prestadores de serviço:

a) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
b) Cumprir a política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
c) Utilizar os sistemas de informações do PSBIO VALID e os recursos a ela relacionados somente para os fins previstos pela gerência de segurança;
d) Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
e) Manter o caráter sigiloso da senha de acesso aos recursos e sistemas do PSBIO VALID;
f) Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
g) Responder, por todo e qualquer acesso, aos recursos do PSBIO VALID bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo para esse fim utilizado;
h) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;

i) Comunicar, imediatamente, ao seu superior imediato e/ou ao Gerente de Segurança o conhecimento de qualquer irregularidade ou desvio.

7.4.2. Responsabilidades dos cargos de chefias

A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

a) Gerenciar o cumprimento da Política de Segurança do PSBIO VALID por parte de seus funcionários e prestadores de serviços;
b) Identificar os desvios praticados e adotar as medidas corretivas apropriadas;
c) Impedir o acesso de funcionários demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do funcionário;
d) Proteger, no nível físico e lógico, os ativos de informação e de processamento do PSBIO VALID relacionados com a sua área de atuação;
e) Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações do PSBIO VALID;
f) Comunicar formalmente à área de Segurança quais os funcionários e prestadores de serviço, sob sua supervisão, que podem acessar as informações do PSBIO VALID, seguindo as normas de classificação de informações e os perfis de cada cargo;
g) Comunicar formalmente ao Departamento Pessoal quais os funcionários e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários;
h) Comunicar formalmente ao Departamento Pessoal aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

7.4.3. Responsabilidades Gerais

São responsabilidades gerais:

a) Cada área que detém os ativos de processamento e de informação é responsável por eles, provendo a sua proteção de acordo com a política de classificação da informação da VALID;
b) Todos os ativos de informações têm claramente definidos os responsáveis pelo seu uso;
c) Todos os ativos de processamento estão relacionados no Plano de Continuidade do Negócio - PCN;

7.4.4. Responsabilidades da Gerência de Segurança

São responsabilidades da Gerência de Segurança:

a) Estabelecer as regras de proteção dos ativos do PSBIO VALID;
b) Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
c) Revisar, anualmente, as regras de proteção estabelecidas;
d) Restringir e controlar o acesso e os privilégios de usuários remotos e externos;
e) Elaborar e manter atualizado o Plano de Continuidade do Negócio - PCN;

f) Executar as regras de proteção estabelecidas pela Política de Segurança;
g) Detectar, identificar, registrar e comunicar à AC Raiz as violações ou tentativas relevantes e significativas de acesso não autorizadas;
h) Definir e aplicar, para cada usuário de TI, restrições de acesso à rede, como horários autorizados, dias autorizados, entre outras;
i) Manter registros de atividades de usuários de TI (*log*s) por um período de no mínimo 7 (sete) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc);
j) Limitar o prazo de Validade das contas de prestadores de serviço ao período da contratação.
k) Verificar a exclusão das contas inativas.
l) Autorizar o fornecimento de senhas de contas privilegiadas somente aos funcionários que necessitem efetivamente dos privilégios segundo sua descrição de cargos, mantendo-se o devido registro e controle.

7.4.5 Responsabilidades dos prestadores de serviço:

São previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos.

7.5 SANÇÕES

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

8. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

8.1. Definição

Ambiente físico é aquele composto por todo o ativo permanente das entidades integrantes da ICP-Brasil.

8.2. Diretrizes Gerais

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

8.2.2. A localização das instalações e o sistema de certificação do PSBIO VALID não são publicamente identificados.

8.2.3. Existem sistemas de segurança para acesso físico, permitindo controlar e auditar o acesso aos sistemas de certificação.

8.2.4. São estabelecidos controles duplicados sobre o inventário e cartões/chaves de acesso. Uma lista atualizada do pessoal que possui cartões/chaves é mantida pela área de Segurança.

8.2.5. Chaves criptográficas são mantidas sob custódia da área de Criptografia e fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

8.2.6. Perdas de cartões/chaves de acesso são imediatamente comunicadas ao responsável pela Gerência de Segurança da PSBIO VALID. Ele toma as medidas apropriadas para prevenir acessos não autorizados.

8.2.7. Os sistemas da AC estão localizados em área protegida (ambientes de nível 4) e afastada de fontes potentes de magnetismo ou interferência de rádio frequência.

8.2.8. Recursos e instalações críticas ou sensíveis devem ser fisicamente protegidos de acesso não autorizado, dano, ou interferência, com barreiras de segurança e controle de acesso. A proteção deve ser proporcional aos riscos identificados. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

8.2.9. A entrada e saída, nestas áreas ou partes dedicadas, são automaticamente registradas com data e hora definidas e são revisadas periodicamente pelo responsável pela Gerência de Segurança e mantidas em local adequado e sob sigilo.

8.2.10. O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal das áreas de Segurança e Infraestrutura.

8.2.11. São utilizados sistemas de detecção de intrusão para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.

8.2.12. O inventário de todo o conjunto de ativos de processamento é registrado e mantido atualizado, mensalmente.

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

8.2.14. Nas instalações da PSBIO VALID todos utilizam crachá de identificação e devem informar à Gerência de Segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não-acompanhado.

8.2.15. Visitantes as instalações da PSBIO VALID são supervisionadas. Suas horas de entrada e saída e o local de destino são registrados. Essas pessoas têm acesso apenas às áreas específicas, com propósitos autorizados, e esses

acessos seguem instruções baseadas nos requisitos de segurança da área visitada.

8.2.16. Os ambientes onde ocorrem os processos críticos da PSBIO VALID são monitorados, em tempo real, com as imagens registradas por meio de sistemas de CFTV.

8.2.17. Sistemas de detecção de intrusos foram instalados e são testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis nos ambientes onde ocorrem processos críticos. As áreas não ocupadas possuem um sistema de alarme que permanece sempre ativado, desligando-se quando o sistema de controle de acesso identifica a entrada de alguém autorizado.

9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

9.1. DEFINIÇÃO

Ambiente lógico é composto por todo o ativo de informações da PSBIO VALID.

9.2. DIRETRIZES GERAIS

9.2.1. O acesso lógico ao ambiente computacional do PSBIO VALID se dará no mínimo mediante usuário individual e senha, que deverá ser trocada periodicamente;

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

9.2.3. Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa;

9.2.4. O PSBIO VALID 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;

9.2.5. Todo equipamento do PSBIO VALID deverá ter log ativo e seu horário sincronizado com uma fonte confiável de tempo;

9.2.6. As informações como log, trilhas de auditoria, registros de acesso (físico e lógico) e imagens deverão ter cópia de segurança cujo armazenamento será de 7 anos.

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

9.2.8. As violações de segurança são registradas e esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria;

Cada tipo de registro é analisado com forma e periodicidade própria de acordo com sua natureza, procedimento este realizado tanto pela área de Segurança como de Infraestrutura. Os registros são protegidos e armazenados de acordo com a sua classificação e mantidos sob custódia da área responsável;

Os tipos de registros mantidos pelo PSBIO VALID englobam:

- Registros de Sistemas Operacionais – login, logout, acesso a arquivos do sistema, dentre outros. Tais registros devem ser avaliados semanalmente.
- Registros de Aplicativos – registros de transações realizadas por servidores Web, Bancos de Dados. Tais registros devem ser avaliados semanalmente.
- Registros de Firewall e Roteadores– pacotes e conexões aceitas e rejeitadas. Tais registros devem ser avaliados semanalmente.
- Registros do Sistema de Detecção de Invasão – tentativas de invasão da rede externa para a rede interna e vice-versa. Tais registros devem ser avaliados on-line permanentemente.

9.3. DIRETRIZES ESPECÍFICAS

9.3.1. Sistemas

9.3.1.1. A documentação dos sistemas é mantida atualizada. Cópias de segurança dos sistemas são testadas e mantidas atualizadas

9.3.1.2. Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados.

As autorizações devem ser realizadas segundo sua criticidade:

- Usuários só poderão ter acesso a sistemas uma vez que tenham autorização do Departamento Pessoal;
- Exceções só poderão ser autorizadas pelo Gerente de Segurança ou por seu substituto em caso de impedimento.

9.3.1.3. Os arquivos de logs são criteriosamente definidos para permitir recuperação nas situações de falhas, auditorias nas situações de violações de segurança e contabilização do uso de recursos.

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

É gerado periodicamente um hash dos seguintes componentes do sistema:

- Arquivos críticos do sistema operacional;
- Arquivos críticos das aplicações;
- Arquivos que contenham informações classificadas estáticas.

9.3.1.5. 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;

9.3.2. Máquinas servidoras

9.3.2.1. O acesso lógico ao ambiente ou serviços disponíveis em servidores é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. Todas as exceções devem ser aprovadas pelo Gerente de Segurança.

9.3.2.2. São adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do sistema operacional. Existem medidas preventivas, como procedimentos detectivos que permitam a identificação de qualquer anomalia.

Os eventos são armazenados em relatórios de segurança (logs) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros. Todos os registros são mantidos pela área de Segurança em local seguro e centralizado;

9.3.2.3. As máquinas são sincronizadas para permitir o rastreamento de eventos;

9.3.2.4. São utilizados somente softwares autorizados pela PSBIO VALID nos seus equipamentos. É realizado o controle da distribuição e instalação dos mesmos;

9.3.2.5. O acesso remoto a máquinas servidoras é realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

9.3.2.6. Os procedimentos de cópia de segurança (backup) e de recuperação estão documentados, atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações.

9.3.3. Redes do PSBIO VALID

9.3.3.1. O tráfego das informações no ambiente de rede é protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

9.3.3.2. Não poderão ser admitidos acessos do mundo externo a rede interna do PSBIO VALID 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;

9.3.3.3. 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.

9.3.3.4. A configuração de todos os ativos de processamento é averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nestes ativos em sua primeira ativação;

9.3.3.5. Serviços vulneráveis são eliminados ou trocados por similares mais seguros;

9.3.3.6. O acesso lógico aos recursos da rede local é realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela administração da

rede, baseado nas responsabilidades e tarefas de cada usuário.

9.3.3.7. A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só ocorrem a partir de autorização formal e mediante supervisão;

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

9.3.3.9. São definidos relatórios de segurança (logs) periódicos de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Tais relatórios são disponibilizados e armazenados de maneira segura. As anormalidades identificadas nestes relatórios são tratadas segundo a sua severidade. Entre elas, inclui-se:

- Ataques Externos e Internos;
- Utilização indevida de Recursos;
- Falhas de subsistemas.

9.3.3.10. O tráfego de informações é monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança;

9.3.3.11. São observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

9.3.3.12. Informações sigilosas, corporativas ou que possam causar prejuízo a terceiros estão protegidas e não são enviadas para outras redes sem proteção adequada;

9.3.3.13. Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) são utilizados para proteger as transações entre redes externas e a rede interna do PSBIO VALID;

9.3.3.14. Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, fazem uso de tal controle;

9.3.3.15. Ambientes de rede considerados críticos são isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;

9.3.3.16. Conexões entre as redes do PSBIO VALID e redes externas estão restritas somente àquelas que visem efetivar os processos necessários à operação do PSBIO VALID;

9.3.3.17. As ferramentas de detecção de intrusos são implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão.

9.3.4. Controle de acesso lógico (baseado em senhas)

9.3.4.1. Usuários e aplicações que necessitem ter acesso a recursos do PSBIO VALID são identificados e autenticados;

9.3.4.2. Não é permitido a nenhum usuário obter direitos de acesso de outro usuário;

9.3.4.3. O arquivo de senhas é criptografado e o seu acesso controlado;

9.3.4.4. As autorizações são definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);

9.3.4.5. As senhas são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada;

9.3.4.6. O sistema de controle de acesso possui mecanismos que impedem a geração de senhas fracas ou óbvias; a execução de tarefas).

9.3.4.7. As seguintes características das senhas são definidas:

- O conjunto de caracteres permitidos deve incluir letras (maiúsculas e minúsculas), números e caracteres especiais;
- Tamanho mínimo é de 8 caracteres;
- Não existe tamanho máximo;
- O prazo de Validade máximo é de 90 dias;
- As trocas são realizadas através dos mecanismos nativos dos sistemas operacionais;
- Restrições específicas para cada ambiente, aplicação ou plataforma poderão ser adotadas, se necessárias.

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

9.3.4.9. O sistema de controle de acesso permite ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só é executada após a identificação positiva do usuário. A senha digitada não é exibida;

9.3.4.10. Os usuários são bloqueados após 45 dias sem acesso e/ou 3 tentativas sucessivas de acesso mal sucedidas.

9.3.4.11. O sistema de controle de acesso solicita nova autenticação após 20 minutos de inatividade da sessão (*time-out*).

9.3.4.12. O registro das atividades (*log*s) do sistema de controle de acesso é definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *log*s devem ser periodicamente analisados.

9.3.4.13. Os usuários e administradores do sistema de controle de acesso são formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

9.3.5. Computação pessoal

9.3.5.1. As estações de trabalho, incluindo equipamentos portáteis ou *stand alone* e informações, são protegidos contra danos ou perdas, bem como uso ou exposições indevidos;

9.3.5.2. São adotadas medidas de segurança lógica referentes ao combate a vírus, backup, controle de acesso e uso de software não-autorizado;

9.3.5.3. As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de backup;

9.3.5.4. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo as entidades da ICP-Brasil, só são utilizadas em equipamentos da PSBIO VALID onde foram geradas ou naqueles equipamentos por ela autorizados, com controles adequados.

9.3.5.5. Os usuários de TI utilizam apenas softwares licenciados pelo fabricante nos equipamentos da PSBIO VALID, observadas as normas da ICP-Brasil e legislação de software;

9.3.5.6. A impressão de documentos sigilosos é feita sob supervisão e devem seguir os requisitos definidos na Política de Classificação da Informação;

9.3.5.7. O inventário dos recursos é mantido atualizado;

9.3.5.8. Os sistemas em uso solicitam nova autenticação após 20 minutos de inatividade da sessão (time-out);

9.3.5.9. As mídias são eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias são definidos, para minimizar os riscos.

9.3.6. Combate a Vírus de Computador

Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia *e worms*) são sistematizados e englobam máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

10. REQUISITOS DE SEGURANÇA DOS RECURSOS BIOMÉTRICOS

10.1. Requisitos Gerais

10.1.1. Os CERTIBIOs 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 deste requerente, em um ou mais bancos/sistemas de dados biométrico da ICP-Brasil, como estabelecido no ADE 03.I (ADE BIOMETRIA), bem como os descritos neste documento.

AC VALID RFB.

11. AUDITORIA

11.1. As atividades do PSBIO VALID estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade do PSBIO VALID em atender aos requisitos da ICP-Brasil;

11.2. O resultado das auditorias pré-operacionais é um item fundamental a ser considerado no processo de credenciamento do PSBIO VALID, da mesma forma que o resultado das auditorias operacionais e fiscalizações é item fundamental para a manutenção da condição de credenciada;

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

11.4. Além de auditadas, o PSBIO VALID pode ser fiscalizada pela AC Raiz a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

12. GERENCIAMENTO DE RISCOS

12.1. Definição

Processo que visa à proteção dos serviços do PSBIO VALID, por meio da eliminação, redução ou transferência dos riscos. Os seguintes pontos principais são identificados:

a) O que deve ser protegido;

b) Análise de riscos (contra quem ou contra o que deve ser protegido);

c) Avaliação de riscos (análise da relação custo/benefício).

12.2. Fases Principais

O gerenciamento de riscos consiste das seguintes fases principais:

a) Identificação dos recursos a serem protegidos – *hardware*s, rede, *software*, dados, informações pessoais, documentação, suprimentos;

b) Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);

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

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

e) Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

f) Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

g) Reavaliação periódica dos riscos em intervalos de tempo não superiores a 1 (um) ano;

12.3. RISCOS RELACIONADOS À PSBIO VALID

Os riscos avaliados para o PSBIO VALID compreendem, dentre outros, os seguintes:

SEGMENTO	***RISCOS***
Dados e Informação	Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição.
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, perda de conhecimento.
Rede	*Hacker*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço.
Hardware	Indisponibilidade, interceptação (furto ou roubo) ou falha.
Software e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento ou falha.

12.4. CONSIDERAÇÕES GERAIS

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

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

12.4.3. É necessária a participação e o envolvimento da alta administração do PSBIO VALID

12.5. IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS

O gerenciamento de riscos no PSBIO VALID é conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

13. PLANO DE CONTINUIDADE DO NEGÓCIO

13.1. DEFINIÇÃO

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos do PSBIO VALID, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

13.2. DIRETRIZES GERAIS

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

13.2.2. Um Plano de Continuidade do Negócio – PCN deverá ser implementado e testado no PSBIO VALID, 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.

13.2.3. O PSBIO VALID possui seu Plano de Continuidade do Negócio que estabelece o tratamento adequado dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.

13.2.4. Todo pessoal envolvido com o Plano de Continuidade do Negócio deve receber um treinamento específico para poder enfrentar eventuais incidentes;

14. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

REF.	NOME DO DOCUMENTOS	CÓDIGO
[1]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09