www.serpro.gov.br

Requisitos Operacionais Mínimos
do
Prestador de Serviço de Confiança
SERPRO

(RO PSC SERPRO)

Versão 1.0 de Novembro 2017

Serviço Federal de Processamento de Dados SERPRO

SUMÁRIO

Lista de Acrônimos

SIGLA - DESCRIÇÃO
AC - Autoridade Certificadora
AC RAIZ - Autoridade Certificadora Raiz da ICP-Brasil
ACT - Autoridade de Carimbo de Tempo
AR - Autoridade de Registro
AUDIBRA - Instituto dos Auditores Internos do Brasil
CD - Compact Disc
CG - Comitê Gestor da ICP-Brasil
CFC - Conselho Federal de Contabilidade
CGU - Controladoria Geral da União
CGAF - Coordenação Geral de Auditoria e Fiscalização
CMMI - Capability Maturity Model Integration
CNPJ - Cadastro Nacional de Pessoas Jurídicas
COBIT - Control Objectives for Information and related Technology
COSO - Committee of Sponsoring Organizations
CVM - Comissão de Valores Mobiliários
DAFN - Diretoria de Auditoria, Fiscalização e Normalização
DOU - Diário Oficial da União
DVD - Digital Versatile Disc
EAT - Entidade de Auditoria do Tempo – ICP-Brasil
IBRACON - Instituto dos Auditores Independentes do Brasil
ICP-BRASIL - Infraestrutura de Chaves Públicas Brasileira
IIA - Information Systems Audit and Control Association
ISACA - Information Systems Audit and Control Association
IEC - International Electrotechnical Commission
ISO - International Organization for Standardization
ITIL - Information Technology Infrastructure Library
MPS-BR - Melhoria de Processo do Software Brasileiro
PDF - Portable Document Format
PLAAO - Plano Anual de Auditoria Operacional
PSC - Prestador de Serviço de Confiança
PSCert - Prestadores de Serviço de Certificação
PSS - Prestadores de Serviço de Suporte
SHA - Secure Hash

1. DISPOSIÇÕES GERAIS

a) Este documento tem por finalidade estabelecer os requisitos mínimos de segurança e os procedimentos operacionais a serem adotados pelo Prestador de Serviço de Confiança SERPRO (PSC SERPRO).

b) Suplementa, para o PSC SERPRO, os regulamentos contidos no documento DOC-ICP-03, DOCICP- 04, DOC-ICP-08 e DOC-ICP-09, tomando como base também a Política de Segurança da ICPBrasil – DOC-ICP-02.

c) Os requisitos contidos neste documento foram apresentados quando do credenciamento do PSC SERPRO para armazenamento de certificados digitais dos usuários finais e são mantidos atualizados durante seu funcionamento enquanto estiver credenciado na ICP-Brasil.

d) O PSC SERPRO possui uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que são seguidos em suas dependências e atividades, em consonância com o DOC-ICP-02.

e) Há um exemplar da Política de Segurança da Informação, no formato impresso, disponível para consulta no Nível 1 (vide regulamento no item 3) de segurança do PSC SERPRO.

f) A Política de Segurança da Informação do PSC SERPRO é seguida por todo pessoal envolvido nas atividades realizadas pelo PSC, do seu próprio quadro ou contratado.

g) Este documento define normas de segurança que são aplicadas nas áreas internas ao PSC SERPRO, assim como no trânsito de informações, armazenamento de certificados e materiais com entidades externas.

h) A seguir são informados os requisitos que observados quanto à segurança de pessoal, segurança física, segurança lógica, segurança de rede, requisitos mínimos para armazenamento de chaves privadas, 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 PSC SERPRO possui uma Política de Gestão de Pessoas que dispõe 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 PSC está à disposição para eventuais auditorias e fiscalizações.

c) Todo pessoal envolvido nas atividades realizadas pelo PSC, do próprio quadro ou contratado, assina um termo, com garantias jurídicas, que garante o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.

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

e) Aplicar-se 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 PSC SERPRO.

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

g) O quadro de pessoal do PSC SERPRO 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 são admitidos estagiários no exercício fim das atividades do PSC SERPRO.

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

i. Evidências de exclusão dos acessos físico e lógico nos ambientes do PSC SERPRO;

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 PSC SERPRO.

3.1.1.1.1. O primeiro nível – ou nível 1 – 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.

3.1.1.1.2. O segundo nível – ou nível 2 – é interno ao primeiro e requer a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSC SERPRO. A passagem do primeiro para o segundo nível exigi identificação por meio eletrônico e o uso de crachá.

a) O ambiente de nível 2 é separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso;

b) O acesso a este nível é permitido apenas a pessoas que trabalhem diretamente com as atividades de serviços de armazenamento dos certificados para usuários finais 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 SERPRO ou do possível ambiente que esta compartilhe não acessa este nível;

c) Evita-se acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção de nobreaks, geradores e outros componentes de infraestrutura;

d) Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do PSC SERPRO, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e sob supervisão.

3.1.1.1.3. O terceiro nível – ou nível 3 – situar-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação do PSC SERPRO. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários é realizada nesse nível. Somente pessoas autorizadas podem permanecer nesse nível.

a) No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são 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 são de alvenaria ou material de resistência equivalente ou superior. Não há 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;

3.1.1.1.4. Não se aplica.

3.1.1.1.5. O quarto nível – ou nível 4 –, interior ao terceiro, é onde ocorrem as atividades especialmente sensíveis da operação do PSC SERPRO de armazenamento de chaves privadas. Todos os sistemas e equipamentos necessários a essas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exigi, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

3.1.1.1.6 No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são 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 permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

3.1.1.1.7. As salas-cofre são construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas são sanadas por normas internacionais pertinentes.

3.1.1.2. Podem existir, no PSC SERPRO, vários ambientes de quarto nível, para abrigar e segregar, quando for o caso:

a)Equipamentos de produção on-line; e

b)Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

3.1.1.3. Todos os servidores e elementos de infraestrutura e proteção do segmento de rede, tais como roteadores, hubs, switches e firewalls:

a) operam em ambiente com segurança equivalente, no mínimo, ao nível 4 citado neste documento;

b) possuem acesso lógico restrito por meio de sistema de autenticação e autorização de acesso;

3.1.1.4. O PSC SERPRO atende aos seguintes requisitos:

a) O ambiente físico do PSC SERPRO contém dispositivos que autenticam e registram o acesso de pessoas informando data e hora desses acessos;

b) O PSC SERPRO possui as imagens que garantem a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente;

c) É realizado 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 PSC SERPRO portam crachás de identificação, inclusive os visitantes;

e) Só é permitido o trânsito de material de terceiros pelos ambientes físicos do PSC SERPRO 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 PSC SERPRO possui 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 tem tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção tem seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do PSC SERPRO;

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

i) Em caso de inoperância dos sistemas automáticos, o controle de acesso físico é realizado provisoriamente por meio de um livro de registro onde consta quem acessou, a data, hora e o motivo do acesso;

j) Há mecanismos que garantem 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;

l) No caso de armazenamento de chaves privadas para usuários finais, há dois ambientes, sendo obrigatoriamente um para operação e outro para contingência;

m) No caso do PSC ser uma AC da ICP-Brasil, pode ser utilizado o nível 4 para abrigo do hardware criptográfico que armazenará as chaves privadas dos usuários finais, assim como os serviços de autenticação, desde que em gabinete cadeado, cujo a chave do cadeado deve estar em posse de funcionário distinto dos perfis lógicos do PSC, segregados dos que operam o ambiente de uma AC;

n) Todos os equipamentos e ambiente computacional que serão utilizados no PSC SERPRO deverão ter sua data e horário sincronizados com a EAT.

4. SEGURANÇA LÓGICA

a) O acesso lógico ao ambiente computacional do PSC SERPRO se da, no mínimo, mediante usuário individual e senha, que é trocada periodicamente;

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

c) Os equipamentos têm mecanismos de bloqueio de sessão inativa;

d) O PSC SERPRO explícita a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários estão 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, do hardware criptográfico, do banco de dados e de aplicações em geral têm suas senhas segregadas de forma que o acesso lógico a esses ambientes se dê por, pelo menos, duas pessoas autorizadas;

f) Todo equipamento do PSC SERPRO possui log ativo e seu horário sincronizado com uma fonte confiável de tempo da ICP-Brasil;

g) As informações como log, trilhas de auditoria (do armazenamento de certificados digitais ao serviço de assinatura), registros de acesso (físico e lógico) e imagens possuem cópia de segurança cujo armazenamento será de, no mínimo, 6 anos;

h) Os softwares dos sistemas operacionais, os antivírus e aplicativos de segurança são mantidos atualizados;

i) É vedado qualquer tipo de acesso remoto ao ambiente de nível 3.

5. SEGURANÇA DE REDE

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

b) Não são admitidos acessos externos a rede interna do PSC SERPRO. As tentativas de acessos externos são inibidas e monitoradas por meio de aplicativos que criam barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão;

c) São 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 são documentados e as vulnerabilidades detectadas corrigidas.

6. REQUISITOS PARA ARMAZENAMENTO DE CHAVES PRIVADAS

6.1 Armazenamento dos certificados digitais

a) As chaves dos usuários finais, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, estão armazenados dentro dos espaços (slots), ou equivalente, da fronteira criptográfica e segura física de um HSM homologado na ICP-Brasil, endereçados por conta de usuário;

b) Esse acesso ou comando de exportação às chaves provadas dos usuários é de uso e conhecimento e controle exclusivo do titular, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário do PSC SERPRO ou dependentes de outras chaves criptográficas;

c) O PSC SERPRO provê mecanismos de duplo fator de autenticação ao titular para acesso à chave privada, 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 é de uma classe diferente (conhecimento, posse ou biometria). Os mecanismos de autenticação empregam método ou protocolo de validação que protege a transmissão e os dados de autenticação por meio de criptografia. Esta funcionalidade é apensada aos requisitos técnicos na renovação de homologação dos HSM e são:

i) Senhas (PIN/PUK): segundo regras da ICP-Brasil;

ii) OTP: segundo regras da RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);

iii) Biometria: segundo regras da ICP-Brasil;

iv) Certificado de atributo: segundo regras da ICP-Brasil;

v) Push Notification: segundo regras do XMPP extension protocol ou semelhante;

vi) Outras autenticações semânticas em acordo com esse documento e previamente aprovadas pela AC Raíz.

d) É realizada , 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.

e) Esses espaços para armazenamento das chaves privadas dos usuários finais podem ser liberados desde que não haja renovação por parte do mesmo ou a revogação da chave, entretanto mantém-se o registro de armazenamento das chaves conforme Declaração de Prática do Prestador de Serviço de Confiança SERPRO – DPPSC SERPRO.

6.2 Protocolo

6.2.1 Os HSMs certificados na ICP-Brasil devem suportar a interface PKCS#11, atendendo as exigências de especificação da ICP-Brasil, além dos relatados nesse documento, os seguintes requisitos:

a) Gerar chaves simétricas especificando os componentes de chaves simétricas em texto claro;

• Gerar par de chaves especificando os componentes de chaves assimétricas em texto claro. Por exemplo os componentes Módulo, Expoente público, tamanho em bits, etc;

• Cifrar e decifrar chaves especificando os componentes de chaves simétricas ou assimétrica em texto claro;

• Exportar e importar chaves (PKCS#12) especificando os componentes de chaves assimétricas privadas criptografados;

• Assinar conteúdo especificando os componentes de chaves assimétricas públicas em texto claro;

• Verificar assinatura especificando os componentes de chaves assimétricas públicas em texto claro.

b) O módulo criptográfico deve suportar as seguintes chamadas de PKCS#11 (Cryptoki):

• C_Initalize

• C_Finalize

• C_OpenSession

• C_CloseSession

- C_Init_Token
- C_Init_PIN
- C_Login
- C_Logout
- C_CreateObject
- C_DestroyObject
- C_GetAttributeValue
- C_SetAttributeValue
- C_EncryptInit
- C_Encrypt
- C_DecryptInit
- C_Decrypt
- C_DigestInit
- C_Digest
- C_DigestKey
- C_SignInit
- C_Sign
- C_VerifyInit
- C_Verify
- C_GenerateKey
- C_GenerateKeyPair
- C_DeriveKey

• C_GenerateRandom

•C_WrapKey

•C_UnwrapKey

c) Sendo obrigatória a implementação das seguintes funções:

• C_GenerateKey especificando templates de chaves simétricas;

• C_GenerateKeyPair especificando templates de chaves assimétricas;

• C_Sign para realizar assinatura de um conteúdo;

• C_Verify para verificar a assinatura de um conteúdo;

• C_Encrypt para cifrar um dado com uma chave já construída;

• C_Decrypt para decifrar um dado com uma chave já construída;

• C_CreateObject especificando templates de chaves assimétricas (no mínimo chave pública);

• C_DestroyObject especificando o handle do objeto.

6.2.2 Não se aplica.

6.2.2.1 Não se aplica.

6.2.2.2 Não se aplica.

6.2.2.3 Não se aplica.

6.2.2.4 Não se aplica.

6.2.2.5 Não se aplica.

6.2.2.6 Não se aplica.

NOTA 1: Não se aplica.

6.2.2.7 Não se aplica.

6.2.2.8 Não se aplica.

6.2.2.9 Não se aplica.

6.2.2.10 Não se aplica.

NOTA 1: Não se aplica.

6.2.2.11 Não se aplica.

6.3 Rede

6.3.1 Pode ser arquitetado um pool de HSM para operação, replicação e gerenciamento das chaves dos usuários finais, seguindo, alé m dos relatados nesse documento, os seguintes requisitos:

a) Especificação e estabelecimento de uma comunicação segura (sessão SSL/TLS) ou equivalente entre os HSM;

b) Os HSM poderão estar em ambientes distintos desde que os mecanismos de acesso e segurança se mantenham os descritos neste documento.

6.3.2 O PSC SERPRO atende aos critérios mínimos de 99,9% de “nível de tempo de atividade” (uptime) a ser verificado por mês.

7. SERVIÇO DE ASSINATURA DIGITAL, VERIFICAÇÃO DE ASSINATURA DIGITAL E ARMAZENAMENTO DE DOCUMENTOS ASSINADOS.

7.1. Introdução

7.1.1. Não se aplica.

7.2. Criação de Assinaturas

7.2.1. Não se aplica.

7.2.2. Não se aplica.

7.2.3. Não se aplica.

NOTA: Não se aplica.

7.3. Dispositivos para criação de assinaturas

7.3.1. Não se aplica.

7.3.2. Não se aplica.

7.3.3. Não se aplica.

7.4. Interface da aplicação com o dispositivo de criação de assinaturas

7.4.1. Não se aplica.

7.4.2. Não se aplica.

7.4.3. Não se aplica.

7.4.4. Não se aplica.

NOTA 1: Não se aplica.

NOTA 2: Não se aplica.

7.5. Suítes de Assinatura

7.5.1. Não se aplica.

7.6. Formatos de Assinaturas

7.6.1. Não se aplica.

7.6.2. Não se aplica.

7.7. Assinatura com Carimbo do Tempo

7.7.1. Não se aplica.

7.7.2. Não se aplica.

7.7.3. Não se aplica.

7.8. Validação de Assinaturas

7.8.1. Não se aplica.

7.8.2. Não se aplica.

7.8.3. Não se aplica.

7.9. Acordo de Nível de Serviço

7.9.1. Não se aplica.

8. CLASSIFICAÇÃO DA INFORMAÇÃO

8.1. Toda informação gerada e custodiada pelo PSC SERPRO é classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação.

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

8.3. Não se aplica.

8.3.1. Não se aplica.

8.3.2. Não se aplica.

8.3.3. Não se aplica.

8.3.4. Não se aplica.

NOTA: o PSC SERPRO é uma entidade da Administração Pública Federal – APF, ou seja, são aplicadas as disposições do Decreto nº 7.845/2012 e demais normas aplicáveis à APF, no que couber.

9. SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

9.1. O PSC SERPRO, em sua Política de Segurança da Informação, define como é realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado backup.

9.2. A salvaguarda de ativos da informação descreve 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 PSC SERPRO possui política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

10. GERENCIAMENTO DE RISCOS

O PSC SERPRO possui 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.

11. PLANO DE CONTINUIDADE DE NEGÓCIOS

É implementado e testado no PSC SERPRO um Plano de Continuidade do Negócio – PCN, 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.

12. ANÁLISES DE REGISTRO DE EVENTOS

Todos os registros de eventos (logs, trilhas de auditorias e imagens) são analisados, no mínimo, mensalmente e um relatório deverá é gerado com assinatura do responsável pelo PSC SERPRO. Todos os registros da transação biométrica por parte do PSC SERPRO são guardados por um período de 6 anos.

13. PLANO DE CAPACIDADE OPERACIONAL

O PSC SERPRO elaborou e mantém atualizado anualmente um Planejamento de

Capacidade Operacional – PCO para determinar a capacidade de produção atual e futura com níveis de desempenho satisfatórios para responder a novas demandas, fornecendo níveis satisfatórios de serviços aos usuários, visando dimensionar os sistemas para suportar o crescimento orgânico, picos de utilização e sazonalidades.

O PCO possui, no mínimo:

- Determinação dos níveis de serviços requeridos pelos usuários;

- Analise da capacidade de processamento de dados instalada; e

- Dimensionamento da capacidade necessária de infraestrutura, hardware, comunicação de dados e link de internet para atender os níveis de serviços atuais e futuros;