DECRETO Nº 1.937, DE 30 DE MARÇO DE 2026

INSTITUI A POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL DE JABORANDI/SP, APROVA O TERMO DE RESPONSABILIDADE/COMPROMISSO E O PLANO DE CONTINUIDADE DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, E DÁ OUTRAS PROVIDÊNCIAS.

SILVIO VAZ DE ALMEIDA, Prefeito do Município de Jaborandi, Estado de São Paulo, no uso de suas atribuições legais,

DECRETA:

Art. 1º Fica instituída a Política Municipal de Segurança da Informação e Comunicações, doravante denominada PMSIC, aplicável à Administração Pública Municipal direta e, no que couber, às entidades e fundos sob controle do Município.

Art. 2º Ficam aprovados, como partes integrantes deste Decreto:

I - Anexo I: Política Municipal de Segurança da Informação e Comunicações;

II - Anexo II: Termo de Responsabilidade/Compromisso para uso de recursos de TIC e assinatura eletrônica;

III - Anexo III: Plano de Continuidade dos Serviços de TIC.

Art. 3º A PMSIC tem por objetivos:

I - Proteger os ativos de informação do Município;

II - Assegurar a continuidade dos serviços públicos digitais e de suporte tecnológico;

III - reduzir riscos de incidentes, vazamentos, indisponibilidades, fraudes e perdas de dados;

IV - Estabelecer responsabilidades claras para usuários, gestores e terceiros;

V - Assegurar conformidade com a legislação aplicável e com as melhores práticas de segurança e gestão de riscos.

Art. 4º A PMSIC fundamenta-se, especialmente, na Constituição Federal, na Lei nº 12.527/2011, na Lei nº 13.709/2018, na Lei nº 14.063/2020, na Lei nº 14.129/2021, na MP nº 2.200-2/2001, nas normas da família ISO/IEC 27000, na ISO 31000, nos atos municipais de LGPD e governo digital já publicizados pelo Município, bem como no Regulamento de Comunicação de Incidente de Segurança da ANPD (Palácio do Planalto).

Art. 5º A coordenação central da PMSIC caberá à Secretaria de Comunicação e Governo Digital, com apoio do Comitê de Tecnologia da Informação, do Encarregado pelo Tratamento de Dados Pessoais, da Assessoria Jurídica, do Controle Interno e dos demais gestores setoriais. (transparencia.jaborandi.sp.gov.br)

Art. 6º Este Decreto entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

PREFEITURA MUNICIPAL DE JABORANDI
Em 30 de março de 2026.

SILVIO VAZ DE ALMEIDA
Prefeito Municipal

Registrado na Secretaria da Prefeitura Municipal, Publicado no lugar de costume, na data supra.

ROBSON F. DE ALMEIDA
Redator

ANEXO I

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1. Objeto e abrangência

1.1. Esta Política estabelece princípios, diretrizes, controles mínimos, competências e procedimentos para proteção dos ativos de informação, físicos e digitais, do Município de Jaborandi/SP.

1.2. Aplica-se a:
a) servidores efetivos;
b) empregados públicos;
c) agentes políticos;
d) ocupantes de cargos em comissão e funções gratificadas;
e) estagiários, bolsistas, aprendizes e voluntários;
f) prestadores de serviço, terceirizados, fornecedores e contratados;
g) qualquer pessoa física ou jurídica que utilize, administre, desenvolva, hospede, mantenha ou acesse recursos tecnológicos ou informações do Município.

2. Princípios

2.1. A PMSIC observará os princípios de legalidade, impessoalidade, moralidade, publicidade, eficiência, transparência, responsabilização, rastreabilidade, prevenção, proporcionalidade, continuidade, segregação de funções, necessidade, minimização de dados, melhoria contínua e segurança desde a concepção.

2.2. A segurança da informação deverá equilibrar proteção, utilidade pública, transparência administrativa e continuidade do serviço.

3. Diretrizes gerais

3.1. Todo ativo de informação deverá possuir responsável definido.

3.2. Todo acesso deverá observar necessidade de negócio, privilégio mínimo e segregação de funções.

3.3. Toda informação municipal deverá ser classificada e tratada segundo seu risco, valor público, sensibilidade e obrigação legal.

3.4. Toda contratação de TIC deverá conter cláusulas mínimas de segurança, confidencialidade, proteção de dados, resposta a incidentes, auditoria, devolução ou eliminação de dados ao término do contrato e plano de saída.

3.5. Todo usuário com acesso a recursos municipais deverá assinar o **Termo de**

Responsabilidade/Compromisso antes da liberação de credenciais ou equipamentos.

3.6. A segurança da informação será implantada de modo compatível com a capacidade operacional do Município, sem tolerar controles fictícios.

4. Governança e responsabilidades

4.1. Compete ao Prefeito Municipal:
I. aprovar a política e assegurar patrocínio institucional;
II. garantir apoio orçamentário e decisório;
III. deliberar, quando necessário, sobre riscos residuais de alto impacto.

4.2. Compete à Secretaria de Comunicação e Governo Digital:
I. coordenar a implementação da PMSIC;
II. propor normas complementares;
III. manter inventário de ativos críticos;
IV. supervisionar controles de acesso, backup, registro de eventos, monitoramento e resposta a incidentes;
V. coordenar planos de continuidade, testes e revisão anual.

4.3. Compete ao Comitê de TI:
I. acompanhar a execução da política;
II. deliberar sobre prioridades, tratamento de riscos e exceções relevantes;
III. aprovar revisões periódicas e relatórios de maturidade.

4.4. Compete ao Encarregado pelo Tratamento de Dados Pessoais:
I. orientar a administração quanto à LGPD;
II. atuar em conjunto com TI e Jurídico em incidentes que envolvam dados pessoais;
III. apoiar medidas de prevenção, treinamento e responsabilização.

4.5. Compete aos secretários, diretores e chefias:
I. indicar responsáveis setoriais por informações e sistemas;
II. garantir que suas equipes cumpram a política;
III. comunicar admissões, desligamentos, mudanças de lotação e necessidade de acessos.

4.6. Compete aos usuários:
I. utilizar os recursos de TIC estritamente para fins institucionais ou autorizados;
II. proteger senhas, certificados e dispositivos;
III. comunicar imediatamente qualquer suspeita de incidente, extravio, vazamento, fraude, falha ou uso indevido;
IV. cumprir o Termo de Responsabilidade/Compromisso.

5. Classificação e tratamento da informação

5.1. As informações municipais serão classificadas, no mínimo, em:
I. **Pública**: divulgação permitida, observada a integridade e autenticidade;
II. **Uso Interno**: circulação restrita às unidades e agentes autorizados;
III. **Restrita**: acesso condicionado a necessidade funcional, controle reforçado e registro;
IV. **Sigilosa ou protegida por lei**: acesso restrito nos termos da legislação aplicável;
V. **Dados pessoais** e **dados pessoais sensíveis**: tratamento submetido, cumulativamente, à LGPD e aos controles desta Política.

5.2. A classificação deverá ser revista sempre que houver alteração de contexto, risco, base legal ou finalidade.

5.3. A publicidade administrativa não elimina a necessidade de proteção da autenticidade, integridade e disponibilidade da informação. (Palácio do Planalto)

6. Controle de acesso e identidade

6.1. O acesso a sistemas, redes, e-mail, arquivos, bancos de dados, nuvens, aplicações web e dispositivos obedecerá aos seguintes critérios:

I. identificação individual e intransferível;
II. autenticação compatível com o risco;
III. revisão periódica de perfis;
IV. bloqueio tempestivo de acessos de desligados, afastados ou remanejados;
V. vedação ao uso de contas genéricas, salvo exceção formalmente justificada e controlada;
VI. adoção progressiva de múltiplo fator de autenticação para contas privilegiadas, acessos remotos e sistemas críticos.

6.2. O compartilhamento de senhas, tokens, certificados, sessões, crachás ou credenciais é proibido.

6.3. Perfis administrativos deverão ser segregados dos perfis de uso cotidiano.

7. Uso aceitável de recursos de TIC

7.1. Equipamentos, redes, sistemas, correio eletrônico, armazenamento, internet, aplicativos, domínios, plataformas e bases de dados do Município destinam-se prioritariamente ao serviço público.

7.2. É vedado:
I. instalar software, extensão, aplicativo ou equipamento não autorizado;
II. desabilitar antivírus, firewall, criptografia ou qualquer controle de segurança;
III. copiar dados municipais para meios particulares sem autorização;

IV. utilizar recursos institucionais para finalidade ilícita, eleitoral vedada, comercial privada, assédio, fraude ou divulgação indevida;
V. conectar dispositivos pessoais à rede institucional sem regra expressa;
VI. armazenar senhas em papel exposto, arquivos desprotegidos ou mensagens não seguras.

7.3. O Município poderá monitorar, registrar e auditar o uso de seus recursos institucionais, nos limites da legalidade, proporcionalidade e finalidade administrativa.

8. Dispositivos, infraestrutura e proteção técnica

8.1. Os ativos de TIC deverão, sempre que aplicável, possuir:
I. inventário atualizado;
II. identificação patrimonial ou lógica;
III. configuração padronizada;
IV. atualização de segurança;
V. proteção antimalware;
VI. cópias de segurança;
VII. registro de eventos;
VIII. restrição de portas, serviços e privilégios desnecessários;
IX. descarte seguro e sanitização antes de reutilização ou baixa.

8.2. A infraestrutura crítica deverá contar, progressivamente, com segmentação de rede, proteção perimetral, controle de acesso físico, redundância mínima e procedimentos de recuperação.

9. Assinatura eletrônica

9.1. O Município adotará a classificação legal de assinatura eletrônica prevista na Lei nº 14.063/2020, observando os níveis **simples**, **avançado** e **qualificado**. (Palácio do Planalto)

9.2. Para fins operacionais internos, o Município também distinguirá:
I. **assinatura eletrônica gratuita**: aquela disponibilizada sem custo direto ao usuário ou ao ato específico, por plataforma pública ou solução institucional autorizada;
II. **assinatura eletrônica onerosa**: aquela baseada em certificado digital ICP-Brasil, plataforma contratada, assinatura em nuvem paga ou outro mecanismo com custo institucional ou individual autorizado. (Palácio do Planalto)

9.3. Regras de uso:
I. a assinatura eletrônica gratuita poderá ser utilizada em atos de baixo ou médio risco, comunicações internas, despachos ordinários, ciência, protocolos, pareceres, manifestações, expedientes administrativos e documentos para os quais não haja exigência legal de nível superior, desde que a solução adotada assegure autenticidade e rastreabilidade adequadas;

II. a assinatura eletrônica onerosa, preferencialmente **qualificada ICP-Brasil**, será obrigatória quando houver exigência legal, contratual ou normativa, bem como para atos de alto impacto jurídico, financeiro, patrimonial, tributário, previdenciário, sancionatório, licitatório, contratual, admissional, exoneração, autorização de pagamento, movimentação bancária, documentos com dados pessoais sensíveis ou risco elevado de fraude;
III. a definição do nível mínimo de assinatura para cada classe documental será detalhada em norma complementar ou matriz de assinatura eletrônica;
IV. é proibido compartilhar certificado digital, token, senha, dispositivo criptográfico ou conta usada para assinatura;
V. todo usuário assinante responderá pessoalmente pelo uso indevido de sua credencial.

9.4. Na dúvida entre conveniência e segurança, prevalecerá a segurança do ato.

10. Gestão de riscos de TIC

10.1. A identificação, análise, avaliação, tratamento, aceitação, monitoramento e comunicação de riscos de TIC seguirão metodologia formal baseada nas seguintes referências:
I. **ISO/IEC 27000**;
II. **ISO/IEC 27001**;
III. **ISO/IEC 27002**;
IV. **ISO/IEC 27003**;
V. **ISO/IEC 27004**;
VI. **ISO/IEC 27005**;
VII. **ISO 31000**. (ISO)

10.2. O processo de gestão de riscos deverá incluir, no mínimo:
I. definição do contexto;
II. inventário de ativos críticos;
III. identificação de ameaças, vulnerabilidades e impactos;
IV. probabilidade e impacto;
V. definição do nível de risco;
VI. tratamento por evitar, reduzir, transferir, compartilhar ou aceitar;
VII. designação do responsável pelo risco;
VIII. registro em **Mapa ou Registro de Riscos de TIC**;
IX. revisão anual e sempre que houver mudança relevante, incidente grave, contratação crítica, implantação de novo sistema ou auditoria.

10.3. Os riscos críticos ou altos somente poderão ser aceitos mediante decisão formal da autoridade competente, com justificativa e prazo para reavaliação.

11. Registro de eventos, backup e recuperação

11.1. Os sistemas e ativos críticos deverão gerar registros mínimos de autenticação, falhas, alterações administrativas, exportação de dados, tentativas indevidas de acesso e eventos relevantes de segurança.

11.2. Os logs deverão ser protegidos contra alteração indevida e mantidos pelo prazo definido em norma complementar, observadas as exigências legais.

11.3. As cópias de segurança deverão observar, no mínimo:
I. periodicidade compatível com o serviço;
II. segregação entre produção e backup;
III. ao menos uma cópia externa ou logicamente isolada;
IV. testes periódicos de restauração;
V. proteção contra sobrescrita, exclusão indevida e ransomware.

12. Incidentes de segurança

12.1. Considera-se incidente de segurança qualquer evento confirmado ou suspeito que comprometa, ou possa comprometer, confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade de informação ou serviço de TIC.

12.2. Todo incidente deverá ser registrado, classificado e tratado segundo criticidade.

12.3. Deverão existir, no mínimo, as seguintes fases:
I. detecção e registro;
II. contenção;
III. análise e erradicação;
IV. recuperação;
V. comunicação interna e externa;
VI. lições aprendidas.

12.4. Incidentes envolvendo dados pessoais deverão ser avaliados conjuntamente por TI, Encarregado e Jurídico, para fins de eventual comunicação à ANPD e aos titulares, na forma aplicável. (Serviços e Informações do Brasil)

13. Continuidade dos serviços de TIC

13.1. O Município manterá **Plano de Continuidade dos Serviços de TIC**, atualizado e testado, contemplando indisponibilidade de energia, internet, sistemas, equipamentos, credenciais, data center, nuvem, integridade de dados e incidentes cibernéticos.

13.2. O plano deverá definir serviços críticos, tempos de recuperação, responsabilidades, fluxos de comunicação, contingências manuais, restauração de backups e critérios de retorno à normalidade.

13.3. O **Anexo III** integra esta Política para todos os efeitos.

14. Contratações e terceiros

14.1. Toda contratação que envolva TIC, nuvem, hospedagem, suporte, desenvolvimento, monitoramento, vigilância, software, manutenção ou tratamento de dados deverá prever:

I. cláusula de confidencialidade;
II. obrigação de cumprimento da LGPD e desta Política;
III. dever de notificar incidente em prazo compatível com a criticidade;
IV. controles de acesso e trilhas de auditoria;
V. política de backup e recuperação;
VI. segregação de ambientes;
VII. devolução, migração ou eliminação segura dos dados ao término contratual;
VIII. vedação de subcontratação sensível sem autorização;
IX. possibilidade de auditoria e evidências de conformidade.

15. Capacitação e cultura

15.1. O Município promoverá programa contínuo de conscientização em segurança da informação, privacidade, engenharia social, uso de e-mail, senhas, assinaturas eletrônicas, tratamento de dados pessoais e resposta a incidentes.

15.2. Novos usuários deverão receber orientação inicial antes ou imediatamente após a concessão de acesso.

15.3. Gestores, administradores de sistemas e operadores de dados terão capacitação reforçada.

16. Auditoria, monitoramento e responsabilização

16.1. O cumprimento desta Política poderá ser verificado por auditorias, relatórios de conformidade, revisões de acesso, testes de restauração, análises de logs, simulações e verificações documentais.

16.2. O descumprimento desta Política sujeitará o infrator às medidas administrativas, civis e penais cabíveis, sem prejuízo do ressarcimento ao erário e da responsabilização contratual.

17. Revisão e melhoria contínua

17.1. Esta Política será revisada, no mínimo, anualmente, e extraordinariamente quando houver:

I. alteração legal relevante;
II. incidente grave;
III. auditoria com achados críticos;

IV. mudança tecnológica significativa;
V. revisão do PDTIC.

17.2. As revisões serão submetidas ao Comitê de TI e à autoridade competente.

ANEXO II
TERMO DE RESPONSABILIDADE/COMPROMISSO PARA USO DE RECURSOS DE TIC E ASSINATURA ELETRÔNICA
Identificação do usuário:
Nome: _____
CPF: _____
Cargo/Função: _____
Secretaria/Unidade: _____

Declaro que:

1. recebi acesso a recursos de TIC, informações, sistemas, equipamentos, contas, e-mail e/ou certificados vinculados ao Município de Jaborandi/SP, exclusivamente para fins institucionais;
2. li, compreendi e me comprometo a cumprir a Política Municipal de Segurança da Informação e Comunicações;
3. utilizarei minhas credenciais de modo pessoal, sigiloso e intransferível, sendo proibido compartilhar senhas, tokens, certificados, contas, sessões ou dispositivos de autenticação;
4. não instalarei softwares, aplicativos, extensões, equipamentos ou serviços sem autorização;
5. respeitarei a classificação da informação, o sigilo legal, a LGPD e as regras de acesso;
6. comunicarei imediatamente qualquer suspeita ou ocorrência de perda, furto, acesso indevido, vazamento, malware, fraude, indisponibilidade ou uso indevido;
7. reconheço que o uso dos recursos institucionais poderá ser monitorado e auditado, nos limites da lei e para fins de segurança, integridade, continuidade e responsabilização;
8. devolverei equipamentos, mídias, documentos, crachás, chaves, tokens e demais ativos quando solicitado ou por desligamento, mudança de função ou término de vínculo;
9. quanto à **assinatura eletrônica**, observarei as seguintes regras:
   a) utilizarei somente soluções autorizadas pelo Município;
   b) a **assinatura eletrônica gratuita** somente será usada quando juridicamente admitida e compatível com o risco do ato;
   c) a **assinatura eletrônica onerosa**, especialmente a baseada em certificado digital ICP-Brasil, será utilizada nos casos exigidos por lei, norma interna ou pela criticidade do documento;

d) não compartilharei certificado digital, token, dispositivo criptográfico, senha ou conta utilizada para assinar;
e) responderei pelo uso indevido da minha assinatura eletrônica;

10. reconheço que assinaturas eletrônicas regularmente autorizadas produzem efeitos jurídicos nos termos da legislação aplicável;
11. tenho ciência de que o descumprimento deste Termo poderá ensejar responsabilização administrativa, civil e penal;
12. comprometo-me a manter conduta diligente, íntegra e compatível com a proteção do interesse público.

Local e data: _____
Assinatura do usuário: _____
Assinatura da chefia imediata: _____
Assinatura da unidade de TIC: _____

ANEXO III
PLANO DE CONTINUIDADE DOS SERVIÇOS DE TIC

1. Finalidade

Assegurar a continuidade ou a recuperação tempestiva dos serviços de TIC essenciais ao funcionamento da Prefeitura de Jaborandi/SP, reduzindo impactos ao atendimento da população, à arrecadação, à saúde, à transparência e à gestão administrativa.

2. Premissas

2.1. O PDTIC local prioriza estruturação da TI, melhoria da infraestrutura e segurança, backup, sincronia em nuvem, comunicação digital e novos canais de atendimento.

2.2. O ambiente municipal já expõe digitalmente serviços e sistemas como **E-SUS, SCPI e SIS**, o que torna continuidade e recuperação temas concretos, não decorativos. (Jaborandi)

3. Hipóteses de acionamento

O Plano poderá ser acionado, isolada ou cumulativamente, em situações como:

I. indisponibilidade total ou parcial de internet, link ou rede interna;
II. falha grave de servidor, nuvem, autenticação, banco de dados ou armazenamento;
III. ransomware, malware, invasão, sequestro de conta ou comprometimento de credenciais;
IV. falha elétrica, incêndio, alagamento, queda estrutural ou evento climático;
V. perda, corrupção ou exclusão indevida de dados críticos;
VI. indisponibilidade de fornecedor essencial;
VII. incidente envolvendo dados pessoais com risco relevante;
VIII. qualquer cenário que interrompa serviço crítico por período superior ao RTO definido.

4. Governança de crise

4.1. Comitê mínimo de continuidade
a) Coordenador de Continuidade: responsável de TIC;
b) Decisor estratégico: Secretário de Comunicação e Governo Digital;
c) Apoio jurídico e LGPD: Assessoria Jurídica e Encarregado;
d) Apoio institucional: Gabinete/Comunicação;
e) Apoio operacional setorial: chefias das áreas afetadas;
f) Controle e registro: Controle Interno, quando cabível.

4.2. Competências
I. avaliar gravidade e declarar nível do incidente;
II. priorizar serviços;
III. acionar contingência manual ou tecnológica;
IV. comunicar internamente e, quando cabível, externamente;
V. autorizar restauração, failover, substituição ou retomada controlada;
VI. registrar lições aprendidas.

5. Níveis de severidade

Nível 1: impacto baixo, sem interrupção relevante, recuperação pela rotina.
Nível 2: impacto moderado, afeta unidade ou serviço importante, exige coordenação.
Nível 3: impacto alto, interrompe serviço crítico ou afeta dados sensíveis.
Nível 4: crise severa, múltiplos serviços críticos, repercussão pública ou risco jurídico relevante.

6. Serviços críticos, metas de recuperação e contingência mínima

6.1. Conectividade, firewall, autenticação e acesso remoto
RTO: até 4 horas
RPO: até 1 hora
Contingência: link secundário ou conexão móvel emergencial; troca rápida de equipamento perimetral; bloqueio de acessos suspeitos; uso de acesso local restrito para funções críticas.

6.2. Saúde e sistemas assistenciais essenciais
Abrangência mínima: E-SUS e sistemas de apoio ao atendimento
RTO: até 4 horas
RPO: até 1 hora
Contingência: operação manual controlada, formulários padronizados, posterior sincronização, priorização absoluta de credenciais e conectividade nas unidades assistenciais.

6.3. Financeiro, contabilidade, arrecadação e sistemas correlatos
Abrangência mínima: SCPI e integrações de arrecadação
RTO: até 8 horas em dias úteis; prioridade máxima em fechamento, folha e arrecadação
RPO: até 4 horas
Contingência: processamento em estação segura de contingência, uso de backup validado, suspensão temporária de rotinas não essenciais, autorização formal para reprocessamento.

6.4. Portal institucional, transparência, e-mail e canais digitais
RTO: até 8 horas
RPO: até 24 horas
Contingência: página estática de contingência, publicação de comunicado

institucional, redirecionamento temporário para canal alternativo, preservação de logs e evidências.

6.5. Protocolo, tramitação e gestão documental digital
RTO: até 24 horas
RPO: até 8 horas
Contingência: protocolo manual numerado, controle físico de entrada e saída, posterior regularização no sistema.

6.6. Arquivos institucionais e compartilhamento de documentos
RTO: até 8 horas
RPO: até 24 horas
Contingência: restauração seletiva por prioridade, espelho em nuvem ou mídia isolada, limitação temporária de edição.

7. Estratégia de backup

7.1. O Município adotará política de cópias de segurança compatível com criticidade dos serviços, observando, no mínimo:

I. backup diário dos dados críticos;
II. cópia semanal completa;
III. cópia mensal preservada em ambiente logicamente isolado ou imutável;
IV. retenção definida por tabela própria;
V. teste mensal de restauração de arquivos críticos e teste trimestral de restauração de sistema crítico.

7.2. Nenhum backup será considerado confiável sem teste de restauração.

8. Procedimento de acionamento

1. detectar a falha ou incidente;
2. registrar ocorrência e horário inicial;
3. classificar severidade;
4. acionar coordenador de continuidade;
5. isolar causa quando necessário;
6. ativar contingência do serviço afetado;
7. comunicar autoridades e áreas impactadas;
8. restaurar por ordem de prioridade;
9. validar integridade e segurança antes do retorno;
10. encerrar formalmente o evento com relatório pós-incidente.

9. Comunicação

9.1. Toda crise deverá observar comunicação objetiva, tempestiva e proporcional.

9.2. A comunicação externa será centralizada pela autoridade competente.

9.3. Em incidente com dados pessoais, a avaliação de comunicação à ANPD e aos titulares seguirá a legislação e o regulamento aplicável. (Serviços e Informações do Brasil)

10. Recursos mínimos de contingência

I. lista atualizada de contatos críticos;
II. inventário dos ativos prioritários;
III. credenciais de contingência sob custódia segura;
IV. estação de administração segregada;
V. mídia ou repositório seguro para restauração;
VI. formulários manuais para saúde, protocolo e atendimento essencial;
VII. modelos de comunicado interno e externo.

11. Testes e revisão

11.1. O Plano será testado:
I. semestralmente, por simulação de mesa;
II. anualmente, por teste operacional de pelo menos um serviço crítico;
III. extraordinariamente, após incidente grave ou mudança relevante.

11.2. Cada teste produzirá relatório com falhas, prazos, evidências e plano de correção.

12. Critério de retorno à normalidade

O retorno ao ambiente normal somente ocorrerá quando:
I. a causa raiz tiver sido removida ou controlada;
II. os dados restaurados tiverem sido validados;
III. os controles de segurança mínimos estiverem restabelecidos;
IV. houver autorização formal do coordenador do incidente ou da autoridade competente.