

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

PREFEITURA MUNICIPAL DE NOVO-XINGU-RS

ANO 2025/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO):

Vagner Kuster Goppinger

Matrícula: 2269-1

lgpd@novoxingu.rs.gov.br

COMITÊ GESTOR DE PROTEÇÃO DE DADOS – NOVO XINGU/RS:

Elizabete Holz Tasso Tomazeli (Matrícula: 1097-9) – Sec. Educação e Cultura

Elizandro Sergio Holz Tasso (Matrícula: 2029-0) – Gabinete do Prefeito

Evanio Gaediche Moraes (Matrícula: 1018-9) – Sec. de Obras

Gilmar Zanela Do Nascimento (Matrícula: 2033-8) – Sec. Agricultura

Jucilene Lucia Ramos (Matrícula: 2033-8) – Sec. Assistência Social

Luana Kuster (Matrícula: 2048-6) – Sec. Adm. Plan. e Finanças

Rubia Cristina Samuel Fiori (Matrícula: 2038-9) – Sec. Saúde

PREFEITO MUNICIPAL

Gélcio Martinelli

Como usar:

Esta PSI é normativa e imediatamente aplicável a todos os órgãos, servidores efetivos, comissionados, estagiários, terceirizados, prestadores e fornecedores que tratem informação do Município. Onde houver previsão “mínima”, aplica-se no mínimo aqui definido; órgãos podem adotar controles mais restritivos conforme sua criticidade.

DIRETRIZES GERAIS, ESCOPO E PAPÉIS

1. Finalidade e princípios

- 1.1. Estabelecer diretrizes, responsabilidades e controles para proteger a informação do Município de Novo Xingu (em qualquer forma ou meio) quanto a confidencialidade, integridade, disponibilidade e autenticidade, em conformidade com a LGPD (Lei 13.709/2018) e boas práticas (ISO/IEC 27001/27002).
- 1.2. Princípios: necessidade, finalidade, minimização, transparência, segurança por padrão e por desenho, responsabilização e prestação de contas.

2. Escopo

- 2.1. Abrange todas as Secretarias e Departamentos e todos os sistemas e ativos (servidores físicos e em nuvem).
- 2.2. Abrange também fornecedores/operadores que tratem dados e ativos municipais.

3. Definições essenciais

- Ativo de informação: dado, sistema, serviço, equipamento, meio físico/digital.
- Dados pessoais/sensíveis: conforme LGPD (dados de saúde, crianças/adolescentes, biometria etc.).
- Controlador: Município de Novo Xingu (representado pelo Prefeito).
- Operador: pessoa/empresa que realiza o tratamento em nome do Município.
- Incidente de segurança: evento que compromete CIAA (confidencialidade, integridade, disponibilidade, autenticidade) ou viole a LGPD.

4. Papéis e responsabilidades

- Prefeito (Controlador): aprova esta PSI, assegura recursos, responde pela governança.
- Controle Interno (Órgão Gestor da PSI): mantém, revisa e audita a PSI; coordena plano anual de auditoria; reporta-se ao Prefeito.
- DPO (Encarregado): orienta conformidade LGPD, canal com titulares/ANPD, opina sobre incidentes e avaliações de risco, valida inventário e RIPD.
- Comitê de Segurança e Privacidade (CSP): composto por Controle Interno, DPO, TI (SoftSul), Jurídico, representantes das Secretarias; delibera sobre riscos, exceções, prioridades técnicas e comunicações.
- Gestores de Unidade: garantem implementação local dos controles, inventário de ativos, gestão de acessos e cumprimento de políticas.
- Usuários: cumprem esta PSI e políticas correlatas; reportam incidentes imediatamente.
- Fornecedores/Operadores (SoftSul, Governança Brasil e outros): cumprem esta PSI e contratos com cláusulas LGPD, confidencialidade, segurança, notificação de incidentes e auditoria.

5. Classificação da informação

5.1. Nível de classificação (rotulagem obrigatória em documentos/sistemas):

- Pública: divulgação irrestrita (ex.: Portal da Transparência).
- Uso Interno: acesso restrito a servidores do Município (ex.: memorandos, ofícios não sigilosos).
- Confidencial: acesso limitado por necessidade de conhecer (ex.: folha de pagamento nominal, dados tributários, processos licitatórios em curso).
- Sigilosa (Dados Pessoais/Sensíveis): acesso estritamente controlado (ex.: saúde – prontuários e-SUS; educação – dados de crianças; assistência social; dados bancários; investigações internas).

5.2. Regras:

- Mínimo necessário; proibida circulação de Confidencial/Sigilosa por e-mail pessoal ou nuvens não autorizadas.
- Criptografia obrigatória para Confidencial/Sigilosa em repouso e em trânsito (ver Seção 11).
- Etiquetagem digital/física visível; responsabilidade do criador/gestor do processo.

6. Gestão de ativos

6.1. Inventário: cada Secretaria mantém inventário de ativos (hardware, software, dados, responsáveis, classificação). Controle Interno consolida inventário municipal.

6.2. Propriedade e custodiante: todo ativo tem dono (gestor de negócio) e custodiante técnico (TI/fornecedor).

6.3. Ciclo de vida: aquisição homologada, registro, etiquetagem, configuração segura, manutenção, descarte seguro (eliminação/anonimização; mídia com wipe criptográfico).

7. Gestão de identidades e acessos (IAM)

7.1. Princípios:

Identidade única, menor privilégio, segregação de funções, revalidação trimestral de acessos.

7.2. Autenticação:

Senhas: mínimo 8 caracteres (usuários) e 12 (administradores), complexidade, expiração 180 dias (ou troca forçada por comprometimento), bloqueio após 5 tentativas, MFA obrigatória para contas privilegiadas, e-mail, VPN, portais críticos.

**** PROIBIDO O COMPARTILHAMENTO DE CREDENCIAIS ****

7.3. Onboarding/Offboarding:

Criação/alteração/remoção formal via chamado; desligamento remove acessos no dia.

7.4. Acesso privilegiado:

Uso de contas nominativas + elevação temporária; sessões administrativas auditadas e logadas.

8. Uso aceitável de recursos

8.1. Correio eletrônico e Internet:

Uso institucional; proibido conteúdo ilícito, pirataria, armazenamento de dados sigilosos em e-mails sem criptografia; anexos sigilosos apenas por repositórios internos autorizados.

8.2. Armazenamento em nuvem:

Permitido somente em ambientes contratados pelo Município (ex.: AWS do Portal, Google for workspace, Governança Brasil). Vedado uso de nuvens pessoais (Google Drive pessoal, Dropbox, iCloud etc.).

8.3. Dispositivos removíveis:

Bloqueados por padrão; exceções pontuais e cifradas autorizadas pelo CSP; é proibido transportar dados Sigilosos sem criptografia e autorização.

8.4. Dispositivos móveis/BYOD:

Acesso remoto somente por VPN e dispositivos gerenciados/aderentes (antivírus, patch, bloqueio de tela, criptografia); BYOD permitido apenas a e-mail e agenda, sem armazenamento local de dados Sigilosos.

8.5. Impressão e descarte:

Impressão de Confidencial/Sigilosa sob supervisão; descarte em coleta segura (tritador classe P-4+ ou empresa certificada).

8.6. Redes sociais e mensageria:

Evitar compartilhamento de dados pessoais; vedado enviar Confidencial/Sigilosa por WhatsApp; se houver chatbot oficial, utilizar fluxos e termos aprovados.

SEGURANÇA FÍSICA, OPERACIONAL, DE REDES E CRIPTOGRAFIA

9. Segurança física e ambiental

9.1. Áreas críticas (CPD, salas de servidores):

Acesso controlado (chave/cartão), registro de entradas, CFTV onde aplicável, climatização, proteção elétrica e nobreak/gerador conforme viabilidade.

9.2. Estações de trabalho:

Bloqueio automático 10 min; proibição de senhas anotadas; portas USB controladas.

9.3. Visitantes e terceiros:

Credenciamento, acompanhamento e registro; proibida captura de imagens de racks/monitores com dados.

10. Segurança operacional

10.1. Backups

- Frequência diária para banco de dados
- De hora em hora durante horário comercial mais duas vezes fora do horário comercial para arquivos em servidor de arquivos
- Retenção mínima:
 - 30 dias para backups diários
 - 12 semanas para backups semanais
 - 12 meses para backups mensais
- Teste de restauração:
Trimestral com relatório ao CSP

1. Escopo:

Servidores de dados/aplicações, servidores de arquivos e instâncias em nuvem.

10.2. Antimalware/EDR:

Obrigatório em servidores e estações com varredura ativa e atualização automática. Gestão centralizada em painel de controle com tratamento de riscos de forma remota.

10.3. Gestão de mudanças:

Mudanças em produção aprovadas (CSP/gestor), janela definida, plano de rollback, registro.

10.4. Gestão de vulnerabilidades e patches:

Patches de segurança: até 30 dias (alta), 7 dias, se crítico/explorado; inventário de versões; varredura mensal; mitigação documentada.

10.5. Logs e trilhas de auditoria:

Servidores, firewalls, VPN, e-mail, aplicativos críticos:

- logs centralizados
- Retenção mínima: 180 dias (preferencialmente, até 3 anos)
- Acesso a logs restritos
- Relógios sincronizados (serviço NTP)

11. Segurança de redes e comunicações

11.1. Topologia e segmentação

Rede municipal interligada por fibra óptica deve ser segmentada por VLAN por Secretaria, com ACLs restritivas (bloqueio de lateralidade). Todo o tráfego deve sair exclusivamente pelo firewall no servidor de borda gerido atualmente pela empresa SoftSul.

11.2. Wifi:

Redes separadas: **Corporativa**, com criptografia mínima WPA2-Enterprise e **Visitantes**, isolada, sem acesso a ativos internos, com portal cativo e registro de termos.

11.3. Tráfego externo:

Filtragem de conteúdo, IDS/IPS (quando disponível), bloqueio de portas não essenciais, política de egress/ingress mínima

11.4. Criptografia e protocolos:

11.4.1. Em trânsito

- TLS 1.2 / 1.3 para emails
- TLS 1.2 / 1.3 em algoritmo RSA ou ECDSA: para portal institucional e portal da transparência
- TLS 1.2 / 1.3 em algoritmo RSA ou ECDSA: para serviços online
 - Em trânsito

11.4.2. Em repouso

Cifragem de bases e arquivos sigilosos/confidenciais

11.4.3. Gestão de chaves

Guarda segura, rotação anual (ou após incidente), acesso mínimo

DESENVOLVIMENTO/CONTRATAÇÕES, FORNECEDORES E PRIVACIDADE

12. Aquisição, desenvolvimento e manutenção de sistemas

12.1. Princípios de privacidade by design/by default:

Coleta mínima, anonimização quando possível, logs de acesso, perfis por papel.

12.2. Requisitos de segurança nos termos de referência/contratos:

Criptografia, autenticação forte, segregação de ambientes (dev/homolog/prod), testes (funcionais e de segurança) e manual de continuidade.

12.3. Homologação:

Antes de produção, validação de segurança e privacidade pelo CSP/DPO.

12.4. Integrações/API:

por TLS, com autenticação (token/MTLS) e escopo mínimo; proibir chaves embutidas em código.

13. Gestão de fornecedores (operadores)

13.1. Contratos devem conter:

Finalidade, papéis LGPD (controlador/operador), confidencialidade, segurança mínima, subcontratação condicionada, notificação de incidente imediata, auditoria, portabilidade/remoção segura ao término.

13.2. Avaliação periódica:

Desempenho de segurança (SLA, testes de restauração, qualidade de logs), conformidade LGPD, relatório anual ao CSP.

14. Proteção de dados pessoais (LGPD)

14.1. Bases legais por processo;

Atualização do Inventário de Dados Pessoais (IDP) por cada Secretaria; validação semestral pelo DPO.

14.2. Direitos do titular:

Canal ativo em <https://novoxingu.rs.gov.br/transparencia/geral/lgpd>
prazos e respostas padronizados; registro das requisições e evidências.

14.3. Dados sensíveis e de crianças/adolescentes:

Controles reforçados (acesso nominal, logs, segregação); para Saúde (e-SUS) e Educação, aplicar princípio do mínimo necessário e relatórios restritos.

14.4. Compartilhamento externo:

Não praticado como regra; quando obrigatório (ex.: TCE-RS, órgãos federais), fazer por meios oficiais, com registro e trilha de auditoria.

14.5. Cookies/portais:

Não utilizados; manter declaração pública atualizada.

INCIDENTES, CONTINUIDADE, CONFORMIDADE E TREINAMENTO

15. Resposta a incidentes

15.1. Time de Resposta a Incidentes (TRI):

Controle Interno (líder), DPO, TI (SoftSul), Jurídico, área afetada e comunicação.

15.2. Fluxo mínimo:

detecção → contenção → erradicação → recuperação → lições aprendidas.

15.3. Prazos internos (SLO):

- Detecção e registro em até 2 horas úteis após identificação.
- Análise inicial/classificação em 8 horas úteis.
- Comunicação ao DPO/Controle Interno imediata nos casos com risco relevante.
- Comunicação a titulares/ANPD: tempestiva conforme avaliação do DPO/Jurídico (objetivo interno ≤ 48 horas após confirmação, quando houver risco/dano relevante).

15.4. Registro:

Todos os incidentes documentados (causa raiz, impacto, dados afetados, ações e prevenção).

15.5. Testes:

Simulado anual de incidente de dados pessoais.

16. Continuidade de negócios e recuperação de desastres (BCP/DRP)

16.1. RTO/RPO (parâmetros iniciais, revisáveis pelo CSP):

- e-SUS (Saúde): RTO 8h / RPO 24h.
- Portal/Transparência: RTO 24h / RPO 24h.
- Sistemas Tributários/Contábil/Folha (Governança Brasil): RTO 24h / RPO 24h.
- Arquivos departamentais críticos: RTO 48h / RPO 24h.

16.2. Local alternativo/Plano de continuidade:

Execução mínima em contingência (prioridade Saúde, Finanças, Administração); lista de contatos e fornecedores; checklists; responsabilidades.

16.3. Testes de DR:

Anual; relatório ao Prefeito, CSP e DPO.

17. Conformidade e auditoria

17.1. Auditorias semestrais:

(ou conforme plano anual) pelo Controle Interno; escopo: acessos, logs, patches, backups, classificação, contratos.

17.2. Relatórios:

Relatório Semestral de Conformidade; Relatório Anual de Segurança e Privacidade.

17.3. Sanções disciplinares:

Descumprimento desta PSI sujeita o infrator às penalidades previstas no estatuto/CLT/contratos, sem prejuízo de responsabilização civil e penal.

18. Conscientização e capacitação

18.1. Treinamento inicial obrigatório para todos os servidores; reciclagem anual; trilhas específicas para Saúde, Educação, Finanças, RH, TI.

18.2. Campanhas trimestrais (phishing simulado, cartilhas, ofícios circulares).

18.3. Registro de participação para fins de governança e prestação de contas.

EXCEÇÕES, CICLO DE VIDA, ANEXOS E MODELOS

19. Exceções e mudanças

19.1. Exceções a esta PSI devem ser temporárias, justificadas e aprovadas pelo CSP e DPO (com prazos e mitigadores).

19.2. Gestão de mudanças de política:

Propostas pelo Controle Interno; revisão anual (ou a qualquer tempo por necessidade legal/técnica).

20. Publicidade e vigência

20.1. Esta PSI entra em vigor na data de sua publicação por decreto/portaria e deve ser divulgada no Portal da Transparência e intranet/setores.

20.2. Documentos correlatos (listados a seguir) são parte integrante desta PSI.

ANEXOS NORMATIVOS (INTEGRANTES DA PSI)

Anexo A - Política de Senhas (resumo normativo)

Tamanho mínimo: 08 (usuário), 12 (admin).

Complexidade: mistura de maiúsculas, minúsculas, dígitos e caracteres especiais.

Validade: 180 dias (ou maior, conforme risco); troca imediata por suspeita.

Bloqueio após 5 tentativas; histórico 10; MFA para contas privilegiadas, e-mail, VPN e sistemas críticos.

Anexo B — Política de Backup e Restauração

Frequências e retenções conforme item 10.1.

Backups testados trimestralmente; restaurações documentadas; acesso aos repositórios de backup restrito e logado.

Backups contendo dados sensíveis cifrados.

Anexo C — Política de Classificação e Rotulagem

Níveis (Pública, Uso Interno, Confidencial, Sigilosa) e exemplos por Secretaria (Saúde: prontuário – Sigilosa; Finanças: folha nominal – Confidencial; Educação: dados de alunos – Sigilosa; Protocolo em curso – Confidencial; Lei publicada – Pública).

Rótulos visíveis; revisão semestral de classificações por gestores.

Anexo D — Política de Dispositivos Removíveis e BYOD

Removíveis bloqueados por padrão; uso só cifrado e com autorização formal.

BYOD restrito a e-mail e agenda via MDM/controles; proibido armazenar dados Sigilosos no dispositivo pessoal.

Anexo E — Política de E-mail e Internet

Proibido encaminhar dados Confidenciais/Sigilosos a contas externas.

Anexos sensíveis apenas por canais/autorização segura (repositório interno, link autenticado, criptografia).

Bloqueio de categorias de sites maliciosos; logs conforme item 10.5/11.3.

Anexo F — Política de VPN e Acesso Remoto

VPN obrigatória para acesso externo; MFA; perfis por função; proibição de split-tunneling em acessos a dados Sigilosos.

Dispositivo remoto deve atender baseline (antimalware, patches, criptografia, bloqueio de tela).

Anexo G — Procedimento de Resposta a Incidentes (PRI)

Formulário de registro; matriz de severidade (Crítico/Alto/Médio/Baixo); papéis do TRI; comunicação interna; interação com DPO/ANPD; prazos SLO (item 15.3); lições aprendidas.

Anexo H — Matriz de Segmentação de Rede (Plano de Correção)

Segmentação VLAN: mapear por Secretaria/serviço; ACLs mínimas; bloquear lateralidade; Wi-Fi visitante isolado; inventário de regras; revisão trimestral.

Prazo-alvo: desenho em 30 dias; implementação em 90 dias; relatório ao Prefeito.

Anexo I — Tabela de RTO/RPO por Sistema

e-SUS: RTO 8h / RPO 24h;

Portal/Transparência (AWS): RTO 24h / RPO 24h;

Tributário/Contábil/Folha (Governança Brasil): RTO 24h / RPO 24h;

Arquivos críticos por Secretaria: RTO 48h / RPO 24h.

Obs.: CSP pode ajustar conforme testes de DR e capacidade contratada.

Anexo J — Conformidade e Evidências

Lista mínima de evidências: inventário de ativos; matriz de acessos; relatórios de backup e testes; relatórios de patches; atas do CSP; relatórios semestrais do Controle Interno; registros de treinamentos; registros de solicitações de titulares; logs.

DISPOSIÇÕES FINAIS

Qualquer omissão nesta PSI será dirimida pelo Controle Interno, ouvido o DPO e o CSP.

Esta PSI substitui versões anteriores e deve ser revista anualmente ou a qualquer tempo diante de mudanças relevantes (legais, tecnológicas, organizacionais).

Novo Xingu/RS, 19 de dezembro de 2025

DPO - Prefeitura Municipal de Novo Xingu/RS