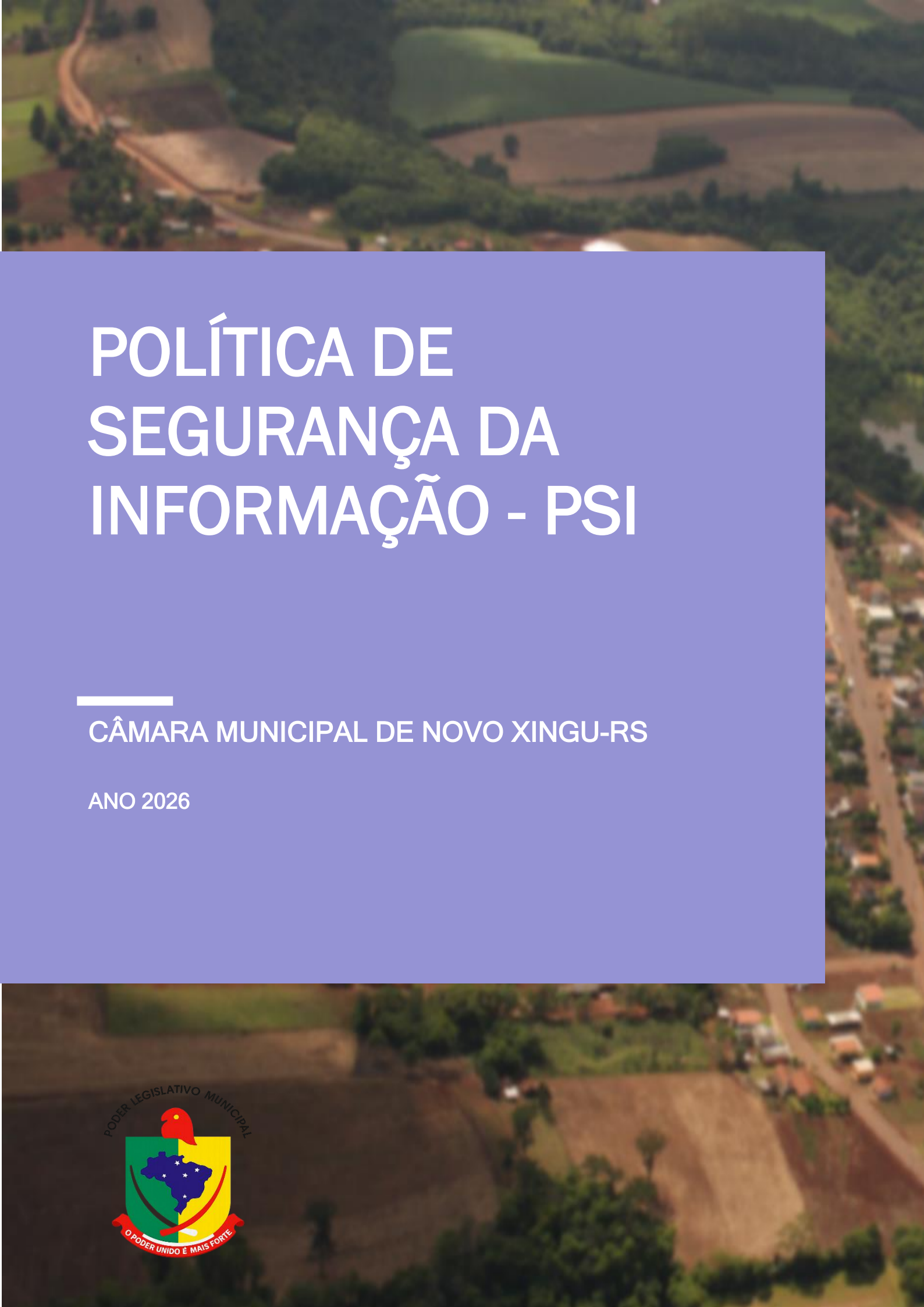

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

CÂMARA MUNICIPAL DE NOVO XINGU-RS

ANO 2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

CÂMARA MUNICIPAL DE VEREADORES DE NOVO XINGU-RS

ANO 2026

ENCARREGADA PELO TRATAMENTO DE DADOS PESSOAIS (DPO):
Lisiane Girotto Cazarotto (Matrícula: 1076-6)

COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS (PORTARIA Nº 004/2026):

I. Eliziane Maria Muller Mahler (Matrícula: 1088-0) - Presidente do Comitê
II. Lisiane Girotto Cazarotto (Matrícula: 1076-6) - Membro
III. Gabriela Caroline Gheler Lauer (Matrícula: 2151-2) - Assessora Jurídica/Membro

MESA DIRETORA:
Luciomar Wahlbrinch-Presidente

DIRETRIZES GERAIS, ESCOPO E PAPÉIS

1. Finalidade e Princípios

1.1 **Finalidade**: Estabelecer diretrizes, responsabilidades e controles para proteger a informação da Câmara Municipal de Novo Xingu (em qualquer forma ou meio) quanto à confidencialidade, integridade, disponibilidade e autenticidade, em conformidade com a LGPD (Lei nº 13.709/2018) e boas práticas internacionais (ISO/IEC 27001/27002).

1.2 **Princípios**: necessidade, finalidade, minimização, transparência, segurança por padrão (security by default), segurança por desenho (security by design), responsabilização e prestação de contas.

2. Escopo

2.1 Abrange todos os gabinetes, setores administrativos, comissões legislativas e todos os sistemas e ativos (servidores físicos, computadores e sistemas em nuvem) do Poder Legislativo.

2.2 Abrange também fornecedores, assessorias contratadas e operadores externos que tratem dados e ativos da Câmara.

3. Definições Essenciais

3.1 **Ativo de informação**: qualquer dado, documento, processo, sistema, serviço, equipamento ou meio físico/digital que possua valor para a Câmara.

3.2 **Dados pessoais/sensíveis**: informações de pessoas naturais identificadas ou identificáveis, bem como dados de origem racial, convicção religiosa, dados de saúde, biometria e dados de crianças/adolescentes, nos termos da LGPD.

3.3 **Controlador**: A Câmara Municipal de Vereadores de Novo Xingu - RS.

3.4 **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (softwares de gestão, assessorias, etc.).

3.5 **Incidente de segurança**: qualquer evento confirmado ou suspeito que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade de ativos de informação ou que viole a LGPD.

4. Papéis e Responsabilidades

4.1 **Mesa Diretora / Presidente** (Controlador): aprova e homologa esta PSI, assegura recursos e responde pela governança institucional.

4.2 **Comitê de Proteção de Dados Pessoais** (Órgão Gestor da PSI): mantém, revisa, fiscaliza e audita a aplicação desta política, reportando-se à Presidência.

4.3 **DPO / Encarregada**: orienta a conformidade com a LGPD, atua como canal com os titulares e com a ANPD, opina sobre incidentes e avaliações de risco.

4.4 **Usuários** (Vereadores, Servidores, Assessores e Estagiários): cumprem esta PSI e políticas correlatas, adotando postura preventiva e reportando incidentes imediatamente.

4.5 **Fornecedores/Operadores** (Sistemas de Gestão, Processo Legislativo e Nuvem): cumprem esta PSI e os contratos contendo cláusulas rígidas de confidencialidade, segurança e notificação de incidentes.

5. Classificação da Informação

5.1 **Nível de classificação** (rotulagem obrigatória em documentos e sistemas novos):

a. **Pública**: divulgação irrestrita por imposição legal (ex.: Leis aprovadas, Sessões gravadas, Portal da Transparência).

b. **Uso Interno**: acesso restrito a servidores e agentes políticos da Câmara para trâmite administrativo de rotina (ex.: memorandos internos, ofícios em elaboração).

c. **Confidencial**: acesso limitado estritamente a quem tem necessidade de conhecer (ex.: folha de pagamento nominal, dados tributários, processos de licitação em andamento).

d. **Sigilosa (Dados Pessoais/Sensíveis)**: acesso sob rigoroso controle (ex.: prontuários médicos e atestados entregues ao RH, dados de filiação sindical de servidores, investigações e sindicâncias internas).

5.2 **Regras**: O tráfego de dados deve guiar-se pelo mínimo necessário, sendo vedada a circulação de documentos Confidenciais ou Sigilosos por e-mail pessoal ou nuvens não institucionais. É obrigatória a criptografia para dados Confidenciais/Sigilosos em trânsito e em repouso.

6. Gestão de Ativos

6.1 **Inventário**: O Comitê manterá atualizado o inventário de ativos da Câmara (contendo listagem de hardwares, softwares, bancos de dados, responsáveis e seu nível de classificação).

6.2 **Ciclo de vida**: Os ativos tecnológicos devem seguir fluxo seguro: aquisição homologada, registro patrimonial, configuração padrão de segurança, manutenção contínua e descarte seguro (mídias digitais devem sofrer wipe/destruição criptográfica completa e papéis devem ser fragmentados).

7. Gestão de Identidades e Acessos (IAM)

7.1 **Princípios**: Identidade única (contas nominais), menor privilégio (acesso apenas ao necessário para o cargo), segregação de funções e revalidação semestral de acessos.

7.2 **Autenticação e Senhas**:

a. **Tamanho mínimo**: 8 caracteres para usuários gerais e 12 caracteres para contas com privilégios de administração de sistemas.

b. **Complexidade**: exigência de letras maiúsculas, minúsculas, números e caracteres especiais.

c. **Expiração**: validade máxima de 180 dias para as senhas, com bloqueio automático da conta após 5 tentativas incorretas consecutivas.

7.3 **É EXPRESSAMENTE PROIBIDO O COMPARTILHAMENTO DE CREDENCIAIS E SENHAS**. As senhas não podem ser anotadas em papéis, post-its ou mantidas sob visualização de terceiros.

7.4 **Offboarding**: O desligamento, exoneração ou fim de contrato de qualquer usuário implica na remoção imediata de todos os seus acessos sistêmicos e físicos no mesmo dia do desligamento.

8. Uso Aceitável de Recursos

8.1 **E-mail e Internet**: O e-mail institucional é ferramenta de trabalho. É proibida a utilização para fins político-partidários, particulares, cadastros em sites de compras ou armazenamento de dados sigilosos sem criptografia.

8.2 **Armazenamento em Nuvem**: Permitido exclusivamente em ambientes contratados formalmente pela Câmara (ex.: Google Workspace institucional, painéis oficiais). Fica proibido o uso de nuvens pessoais (Google Drive pessoal, Dropbox, OneDrive pessoal, iCloud) para guardar arquivos da Câmara.

8.3 **Dispositivos Removíveis**: Uso de pen drives e hards disks externos é bloqueado por padrão nas estações de trabalho. Exceções pontuais devem ser justificadas e os dados gravados devem ser cifrados.

8.4 **Dispositivos Móveis / BYOD**: O acesso remoto aos e-mails e agenda corporativa por dispositivos pessoais é permitido, desde que o aparelho possua senha de bloqueio de tela ativa e antivírus instalado. É proibido baixar e armazenar relatórios com dados Sigilosos diretamente na memória local de celulares particulares.

8.5 **Impressão e Descarte**: Documentos com dados Confidenciais ou Sigilosos impressos devem ser recolhidos imediatamente das impressoras. O descarte de papéis com dados pessoais deve ser realizado obrigatoriamente por meio de fragmentadora de papel, proibido o descarte intacto em lixo comum.

8.6 **Redes Sociais e Mensageria**: Fica proibido o envio de documentos oficiais sigilosos, documentos de identificação ou dados sensíveis de servidores/cidadãos por meio de WhatsApp pessoal.

SEGURANÇA FÍSICA, OPERACIONAL, DE REDES E CRIPTOGRAFIA

9. Segurança Física e Ambiental

9.1 **Áreas Críticas**: O local que abriga os servidores físicos e o distribuidor de rede (rack) da Câmara deve permanecer trancado, com acesso restrito a pessoas autorizadas, mantendo ambiente climatizado e proteção por nobreak.

9.2 **Estações de Trabalho**: Ativação obrigatória de bloqueio automático de tela após 10 minutos de inatividade (atalho Tecla Windows + L). Adota-se a política de "Mesa Limpa" ao final do expediente.

9.3 **Visitantes**: Devem ser identificados na recepção e acompanhados nas dependências da Câmara, sendo proibida a captação de imagens de telas ou locais restritos de tecnologia.

10. Segurança Operacional

10.1 **Backups**:

a. **Frequência**: Diária para os bancos de dados dos sistemas administrativos e legislativos. Para os arquivos compartilhados de rede, backups estruturados de forma incremental em dias úteis.

b. **Retenção mínima**: 30 dias para os backups diários; 12 semanas para os semanais; e 12 meses para os mensais.

c. **Teste de restauração**: Realização semestral de testes de integridade e restauração do backup com registro documental enviado ao Comitê.

d. **Criptografia**: Todos os volumes de backup que contenham dados Confidenciais ou Sigilosos devem ser armazenados de forma cifrada.

10.2 **Antimalware**: Instalação obrigatória de solução antivírus corporativa em todas as estações e servidores, com proteção em tempo real e atualização automática de vacinas.

10.3 **Gestão de Patches e Vulnerabilidades**: As atualizações críticas de segurança dos sistemas operacionais (Windows/Linux) devem ser homologadas e aplicadas em até 30 dias após liberação pelo fabricante (ou em até 7 dias caso haja alerta de vulnerabilidade crítica explorada).

10.4 **Logs e Auditoria**: Os sistemas e servidores devem gerar registros de logs centralizados (quem acessou, modificou ou excluiu o dado), com retenção mínima de 180 dias, acesso restrito e relógios sincronizados pelo protocolo NTP.

11. Segurança de Redes e Comunicações

11.1 **Segmentação**: A rede lógica da Câmara deve ser devidamente protegida, utilizando firewalls na borda da internet para controle de tráfego de entrada e saída (egress/ingress) e bloqueio de portas não essenciais.

11.2 **Wi-Fi**: Fica estabelecida a separação física ou lógica das redes sem fio:

a. Rede Interna/Corporativa: restrita aos computadores institucionais, com autenticação segura.

b. **Rede Visitantes**: isolada da rede administrativa, para uso do público e vereadores em sessões, sem qualquer comunicação com os sistemas internos da Câmara.

11.3 **Criptografia em Trânsito e Repouso**:

a. **Em Trânsito**: Uso obrigatório de protocolo seguro TLS 1.2 ou 1.3 (HTTPS) para o acesso ao Portal da Câmara, Portal da Transparência e painéis legislativos online.

b. **Em Repouso**: Os bancos de dados e pastas que armazenem dados Sigilosos (RH e Finanças) devem utilizar criptografia em nível de arquivo ou disco.

CONTRATAÇÕES, FORNECEDORES E PRIVACIDADE

12. Aquisição e Contratação de Sistemas

12.1 Todo novo sistema de software contratado pela Câmara deve adotar as premissas de Privacy by Design (Privacidade por Design), garantindo coleta mínima de dados, capacidade de gerar logs de auditoria e controle de acessos por nível de usuário.

12.2 Os Termos de Referência e Editais de Licitação na área de tecnologia devem exigir expressamente a conformidade das empresas concorrentes com a LGPD, fornecendo manuais de segurança e plano de continuidade de negócios.

13. Gestão de Fornecedores (Operadores)

13.1 **Cláusulas Contratuais Obrigatórias**: Todos os contratos vigentes com empresas que tratam dados em nome da Câmara devem possuir aditivos de LGPD definindo: finalidades específicas do tratamento, dever de sigilo, proibição de subcontratação sem anuência, obrigação de notificação imediata de incidentes e devolução ou eliminação segura dos dados ao fim do contrato.

14. Proteção de Dados e Direitos do Titular

14.1 **Canal de Atendimento**: A Câmara manterá em seu portal oficial um link ou aba de transparência ativa destinada à LGPD, indicando de forma clara a identidade da Encarregada (DPO) e disponibilizando formulário eletrônico seguro para que os cidadãos exerçam seus direitos (confirmação, acesso e correção de dados).

14.2 **Dados de Crianças e Adolescentes**: Eventuais tratamentos dessas categorias (como dados de dependentes de servidores para fins de auxílios ou eixos de projetos institucionais) devem receber camadas extras de proteção de acesso, exigindo justificativa clara e base legal explícita.

INCIDENTES, CONTINUIDADE E CONFORMIDADE

15. Resposta a Incidentes de Segurança

15.1 **Grupo de Resposta**: Em caso de anomalia, vazamento ou ataque (Ransomware/Invasão), fica ativado o Grupo de Resposta composto pelo Comitê de Proteção de Dados, Assessoria Jurídica e o suporte de TI contratado.

15.2 **Prazos Internos de Resposta (SLO)**:

a. **Detecção e Registro**: Até 2 horas úteis após a identificação da anomalia.
b. **Análise Inicial e Classificação de Risco**: Em até 8 horas úteis.
c. **Comunicação aos Titulares e à ANPD**: Caso o incidente envolva risco ou dano relevante aos titulares, o DPO e a Assessoria Jurídica deverão emitir a comunicação oficial em até 48 horas após a confirmação da severidade do fato.

15.3 Todos os incidentes reais ou suspeitos deverão ser registrados em relatório interno contendo a causa raiz, os dados afetados e as medidas corretivas aplicadas.

16. Continuidade de Negócios e Recuperação de Desastres (BCP/DRP)

16.1 **Parâmetros de Recuperação (RTO / RPO Target):**

a. **Portal Institucional / Transparência**: RTO (Tempo máximo de recuperação) de 24 horas / RPO (Perda máxima tolerável de dados) de 24 horas.
b. Sistemas Administrativos (RH, Contabilidade e Folha): RTO de 24 horas / RPO de 24 horas.
c. **Sistema de Processo Legislativo e Votação**: RTO de 12 horas / RPO de 24 horas.
d. **Arquivos Digitais Departamentais**: RTO de 48 horas / RPO de 24 hours.

16.2 Em caso de indisponibilidade física do prédio da Câmara por sinistro, as atividades administrativas críticas serão desempenhadas em regime de teletrabalho de contingência via acessos seguros em nuvem.

17. Conformidade, Sanções e Treinamentos

17.1 **Auditorias**: O Comitê de Proteção de Dados realizará anualmente auditoria de conformidade para checar as matrizes de acesso aos sistemas, rotinas de backup e conformidade de contratos de fornecedores.

17.2 **Sanções**: O descumprimento deliberado das normas práticas contidas nesta PSI sujeitará os servidores e colaboradores às penalidades disciplinares e administrativas previstas no Estatuto dos Servidores Públicos do Município, e acarretará sanções pecuniárias e rescisão contratual para empresas prestadoras de serviço, sem prejuízo de responsabilização civil e criminal.

17.3 **Capacitação**: A Câmara promoverá ações de conscientização (cartilhas digitais ou reuniões de orientação) para servidores e vereadores sobre proteção de dados, uso de senhas e prevenção a golpes virtuais.

Novo Xingu - RS, 26 de maio de 2026.