Diário Oficial
Municípios de Santa Catarina

Quarta-feira, 21 de outubro de 2026 às 17:16, Florianópolis - SC

PUBLICAÇÃO

Nº 8833714: DECRETO Nº 142/2026 - POLÍTICA DA SEGURANÇA DA INFORMAÇÃO SALTO VELOSO LGPD

ENTIDADE

Prefeitura Municipal de Salto Veloso

MUNICÍPIO

Salto Veloso

https://diariomunicipal.sc.gov.br/?q=id:8833714

CIGA - Consórcio de Inovação na Gestão Pública
Rua Gen. Liberato Bittencourt, n.º 1885 - Sala 102, Canto - CEP 88070-800 - Florianópolis / SC
https://diariomunicipal.sc.gov.br

ICP Brasil Assinado Digitalmente por Consórcio de Inovação na Gestão Pública Municipal - CIGA

DECRETO N° 142, DE 21 DE OUTUBRO DE 2026.

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) NO ÂMBITO DA ADMINISTRAÇÃO MUNICIPAL DE SALTO VELOSO E DÁ OUTRAS PROVIDÊNCIAS.

NEREU BORGA, Prefeito Municipal de Salto Veloso, no uso de suas atribuições, em conformidade com a Lei Orgânica de Salto Veloso, e com os artigos 6º, VII e VIII, 46 a 50 da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e a Lei Federal nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet),

DECRETA:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) da Administração Pública Municipal de Salto Veloso/SC, que estabelece princípios, diretrizes, responsabilidades e medidas técnicas e administrativas para a proteção das informações e dos dados pessoais tratados pelo Município.

§ 1º. Esta Política dá cumprimento ao dever de adotar medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, previsto nos arts. 46 a 49 da Lei Federal nº 13.709/2018.

§ 2º. Na aplicação desta Política serão observados, como referência técnica, o Guia Orientativo de Segurança da Informação e o Checklist de Medidas de

Segurança publicados pela Agência Nacional de Proteção de Dados (ANPD), a Resolução CD/ANPD nº 15/2024 e as normas técnicas ABNT NBR ISO/IEC 27001 e 27002.

§ 3º. Esta Política foi aprovada pelo Comitê de Privacidade e Proteção de Dados Pessoais de Salto Veloso em 10/09/2026.

Art. 2º. A PSI tem por objetivos:

I – preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações do Município;

II – proteger os dados pessoais e os direitos dos titulares;

III – prevenir, detectar e responder a incidentes de segurança, reduzindo seus impactos;

IV – assegurar a continuidade dos serviços públicos que dependem de tecnologia da informação; e

V – promover a cultura de segurança da informação entre os agentes públicos.

Art. 3º Esta Política aplica-se:

I – aos órgãos da Administração direta e, no que couber, às entidades da Administração indireta do Município;

II – a todos os ativos de informação do Município, em meio físico ou digital, incluindo dados, documentos, sistemas, aplicativos, equipamentos, redes e instalações; e

III – a todos os agentes políticos, servidores, empregados, ocupantes de cargos em comissão, estagiários, contratados, parceiros, fornecedores e demais pessoas que acessem ou tratem informações do Município.

Art. 4º Para os efeitos deste Decreto, considera-se:

I – agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra

forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Municipal;

II – agentes de tratamento: o controlador e o operador de dados pessoais;

III – ameaça: conjunto de fatores externos ou internos com potencial de causar dano a um sistema ou organização;

IV – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

V – ANPD: Agência Nacional de Proteção de Dados;

VI – aplicativo: programa de computador desenvolvido para processar dados de modo eletrônico, de forma a facilitar e reduzir o tempo do usuário na execução de uma tarefa;

VII – ativos de informação: meios de armazenamento, transmissão e processamento da informação, os equipamentos e sistemas utilizados para tal, os locais onde se encontram esses meios, as pessoas que a eles têm acesso e os dados e informações que tenham valor para o Município;

VIII – autenticação de dois fatores ou multifator (MFA): processo de segurança que exige que o usuário forneça dois ou mais meios de identificação antes de acessar sua conta;

IX – autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física, equipamento, sistema, órgão ou entidade;

X – backup: cópia de segurança dos dados de um sistema computacional, que permite sua guarda, proteção e recuperação, com fidelidade ao original;

XI – banco de dados: conjunto estruturado de dados inter-relacionados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

XII – Comitê: o Comitê de Privacidade e Proteção de Dados Pessoais do Município;

XIII – confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoas, sistemas, órgãos ou entidades

não autorizados;

XIV – controlador: o Município de Salto Veloso, por meio de seus órgãos, e as entidades da Administração indireta quanto aos dados pessoais que tratam;

XV – controle de acesso: conjunto de procedimentos, recursos e meios utilizados para conceder ou bloquear o acesso a recursos físicos ou computacionais, que, via de regra, requer autenticação;

XVI – criptografia: técnica que transforma a informação de modo que somente quem possui a chave adequada consiga lê-la, protegendo-a durante o armazenamento e a transmissão;

XVII – dado pessoal: informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, telefone, e-mail e placa de veículo;

XVIII – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XIX – descarte: eliminação segura de informações, documentos, mídias e acervos digitais;

XX – disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por pessoa, sistema, órgão ou entidade devidamente autorizados;

XXI – dispositivos móveis: equipamentos portáteis com capacidade de processamento ou de armazenamento, tais como notebooks, smartphones, tablets, pendrives, HDs externos e cartões de memória;

XXII – firewall: recurso de hardware ou software que examina o tráfego de entrada e saída de uma rede e bloqueia o acesso que não atenda aos critérios de segurança especificados;

XXIII – gestão de segurança da informação: processo que integra a gestão de riscos, a gestão de continuidade, o tratamento de incidentes, a conformidade e as seguranças física, lógica e organizacional aos processos institucionais, não se limitando à tecnologia da informação;

XXIV – gestor de segurança da informação: agente público responsável pela coordenação técnica das ações de segurança da informação, designado na forma do art. 8º deste Decreto;

XXV – hardening: conjunto de ajustes de configuração que reduzem as vulnerabilidades de sistemas e equipamentos, como a desativação de serviços desnecessários e a troca de senhas padrão;

XXVI – incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais, nos termos da Resolução CD/ANPD nº 15/2024;

XXVII – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXVIII – informação pessoal: informação relacionada à pessoa natural identificada ou identificável, cujo acesso é restrito nos termos do art. 31 da Lei Federal nº 12.527/2011;

XXIX – informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou protegida por sigilo legal, judicial ou profissional, nos termos da Lei Federal nº 12.527/2011;

XXX – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXXI – inteligência artificial generativa: sistema computacional capaz de gerar textos, imagens, áudios ou outros conteúdos a partir de instruções fornecidas pelo usuário;

XXXII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XXXIII – Plano de Resposta a Incidentes: plano instituído por Decreto próprio, que define os recursos, as responsabilidades e as ações necessárias para a gestão de incidentes de segurança envolvendo dados pessoais;

XXXIV – privacidade desde a concepção e por padrão: adoção de medidas de segurança e de proteção de dados desde a fase de concepção de produtos, serviços e sistemas até a sua execução, nos termos do art. 46, § 2º, da Lei Federal nº 13.709/2018;

XXXV – pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente em ambiente controlado e seguro;

XXXVI – risco de segurança da informação: potencial de que uma ameaça explore vulnerabilidades de um ativo de informação, causando dano ao Município ou aos titulares;

XXXVII – segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXVIII – titular: pessoa natural a quem se referem os dados pessoais objeto de tratamento;

XXXIX – tratamento: toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XL – unidades organizacionais: as secretarias, diretorias e setores do Município;

XLI – vazamento de dados: transmissão ou exposição não autorizada de dados para destino externo à organização, por meio eletrônico ou físico, de forma acidental ou intencional;

XLII – vulnerabilidade: fragilidade de um ativo de informação ou de um controle que pode ser explorada por uma ou mais ameaças.

Art. 5º São princípios desta Política:

I – confidencialidade, integridade, disponibilidade e autenticidade da

informação;

II – menor privilégio e necessidade de conhecer: cada usuário terá apenas o acesso indispensável às suas atribuições;

III – necessidade: coleta e retenção apenas dos dados indispensáveis à finalidade pública;

IV – privacidade desde a concepção e por padrão;

V – prevenção e gestão de riscos proporcional à criticidade dos ativos e à natureza dos dados;

VI – responsabilização e prestação de contas, com registro das ações relevantes de segurança; e

VII – transparência, compatibilizando a segurança da informação com o acesso à informação pública.

CAPÍTULO II
DA ESTRUTURA E DAS RESPONSABILIDADES

Art. 6º Compete ao Chefe do Poder Executivo aprovar esta Política, prover os recursos necessários à sua implementação e designar o Gestor de Segurança da Informação.

Art. 7º Compete ao Comitê de Privacidade e Proteção de Dados Pessoais:

I – acompanhar a implementação desta Política e propor sua revisão;

II – aprovar normas e orientações complementares de segurança da informação;

III – avaliar anualmente o relatório de conformidade previsto no art. 50 deste Decreto; e

IV – deliberar sobre exceções a esta Política, mediante justificativa registrada em ata.

Art. 8º O responsável pelo setor de Tecnologia da Informação exercerá a

função de Gestor de Segurança da Informação, salvo designação diversa por ato do Chefe do Poder Executivo, competindo-lhe:

I – coordenar a implementação das medidas técnicas desta Política;

II – manter o inventário dos ativos de informação e o registro de acessos privilegiados;

III – gerenciar backups, atualizações, vulnerabilidades e registros de eventos (logs);

IV – apoiar o Encarregado na resposta a incidentes de segurança; e

V – elaborar o relatório anual de conformidade em segurança da informação.

Art. 9º. Compete ao Encarregado pelo Tratamento de Dados Pessoais orientar os agentes públicos sobre a proteção de dados pessoais, receber comunicações de incidentes e conduzir a comunicação à ANPD e aos titulares, nos termos do Plano de Resposta a Incidentes de Segurança envolvendo Dados Pessoais.

Art. 10. Compete aos Secretários Municipais e às chefias imediatas:

I – solicitar, revisar e comunicar a revogação dos acessos dos agentes públicos sob sua chefia;

II – identificar as informações sensíveis e sigilosas tratadas em sua unidade; e

III – zelar pelo cumprimento desta Política em sua unidade.

Art. 11. Compete a todos os usuários:

I – cumprir esta Política e as normas complementares;

II – utilizar os ativos de informação exclusivamente para fins institucionais;

III – preservar o sigilo de suas credenciais de acesso; e

IV – comunicar imediatamente qualquer incidente, suspeita de incidente ou vulnerabilidade.

CAPÍTULO III
DA GESTÃO DE ATIVOS E DE RISCOS

Art. 12. O setor de Tecnologia da Informação manterá inventário atualizado dos ativos de informação, com a identificação dos equipamentos, sistemas, bases de dados, responsáveis e fornecedores, indicando aqueles que tratam dados pessoais sensíveis.

Art. 13. As informações serão classificadas, quanto ao acesso, em:

I – públicas: de livre acesso, nos termos da Lei Federal nº 12.527/2011;

II – pessoais: de acesso restrito ao titular, aos agentes públicos autorizados e às hipóteses legais; e

III – sigilosas: protegidas por sigilo legal, judicial, profissional ou classificadas na forma da Lei Federal nº 12.527/2011.

Art. 14. Os riscos de segurança da informação serão avaliados periodicamente, priorizando os ativos críticos e os que tratam dados pessoais sensíveis, de forma integrada à matriz de risco e ao plano de ação do programa de adequação à LGPD.

CAPÍTULO IV
DO CONTROLE DE ACESSO

Art. 15. O acesso aos sistemas e às informações seguirá os processos de autenticação, que identifica o usuário, autorização, que define o que ele pode fazer, e auditoria, que registra o que foi feito.

Art. 16. Cada usuário terá conta individual e intransferível, sendo proibido o compartilhamento de contas, logins e senhas entre agentes públicos ou com terceiros.

Art. 17. A criação de contas dependerá de solicitação da chefia imediata, com indicação do perfil de acesso necessário, e será executada pelo setor de Tecnologia da Informação.

§ 1º Os acessos serão revogados ou ajustados imediatamente no desligamento, afastamento ou mudança de função do usuário, cabendo à unidade de lotação e ao setor de Recursos Humanos comunicar o fato ao setor de Tecnologia da Informação.

§ 2º Os acessos serão revisados, no mínimo, semestralmente, com a exclusão de contas inativas ou sem titular identificado.

Art. 18. As contas com privilégios de administrador serão restritas aos agentes que necessitem exercer essa função, não poderão ser utilizadas em atividades rotineiras e terão seu uso registrado.

Art. 19. Os sistemas serão configurados, sempre que possível, para impedir senhas que não atendam a requisitos mínimos de complexidade, observado o seguinte:

I – as senhas terão, no mínimo, 8 (oito) caracteres, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

II – é obrigatória a substituição das senhas padrão fornecidas por fabricantes e fornecedores de software ou hardware;

III – é vedada a reutilização da senha institucional em serviços particulares; e

IV – as senhas não poderão ser anotadas em agendas, bilhetes ou qualquer meio que coloque em risco o acesso.

Art. 20. Será utilizada autenticação multifator (MFA):

I – obrigatoriamente, nos acessos remotos à rede municipal, nas contas com

privilégio de administrador e nos serviços em nuvem que contenham dados pessoais; e

II – sempre que tecnicamente possível, nos sistemas e bases de dados que contenham dados pessoais, em especial os sensíveis, e no e-mail institucional.

Art. 21. O acesso remoto à rede municipal somente ocorrerá por conexão segura (VPN) e mediante autorização expressa do Gestor de Segurança da Informação.

Art. 22. Os sistemas que tratam dados pessoais manterão registros (logs) de acesso e das operações relevantes, protegidos contra alteração, pelo prazo mínimo de 6 (seis) meses, para fins de auditoria e apuração de incidentes.

CAPÍTULO V
DA SEGURANÇA DOS DADOS ARMAZENADOS

Art. 23. A coleta e o armazenamento de dados pessoais limitar-se-ão ao mínimo necessário para a finalidade pública, observados os prazos da Política de Guarda e Eliminação de Documentos do Município.

Art. 24. Os dados pessoais sensíveis serão protegidos, sempre que possível, por criptografia ou pseudonimização, inclusive em cópias de segurança.

Art. 25. É vedada a transferência de dados pessoais das estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos, salvo com autorização da chefia imediata e criptografia.

Parágrafo único. Os dispositivos externos autorizados serão inventariados, cifrados e guardados em local seguro.

Art. 26. Serão realizados backups periódicos dos sistemas e dados, observadas as seguintes regras:

I – manutenção de, ao menos, uma cópia offline ou isolada da rede, para proteção contra ataques de ransomware;

II – armazenamento em local seguro e distinto dos sistemas principais;

III – periodicidade compatível com a criticidade de cada sistema, definida pelo Gestor de Segurança da Informação; e

IV – realização de testes periódicos de restauração, com registro de sua execução.

Art. 27. Antes do descarte, da doação ou da devolução de equipamentos e mídias, os dados serão eliminados por sobrescrita ou formatação segura ou, não sendo possível, a mídia será destruída fisicamente, observada a Política de Guarda e Eliminação de Documentos.

Parágrafo único. Quando o descarte for realizado por terceiro, o contrato exigirá o registro e a comprovação da destruição.

Art. 28. Os dados pessoais desnecessariamente expostos em sítios eletrônicos, portais e redes públicas serão removidos ou anonimizados, preservadas as informações cuja divulgação seja exigida pela Lei Federal nº 12.527/2011.

Art. 29. É vedado o uso da estrutura computacional do Município para acessar conteúdos ou instalar programas sem vinculação com a atividade pública, bem como desativar ou contornar as configurações de segurança das estações de trabalho.

CAPÍTULO VI
DA SEGURANÇA FÍSICA E DO AMBIENTE DE TRABALHO

Art. 30. As salas de servidores e equipamentos de rede terão acesso restrito às pessoas autorizadas e contarão, sempre que possível, com proteção elétrica e de climatização adequadas.

Art. 31. Os agentes públicos observarão as práticas de mesa limpa e tela limpa:

I – documentos físicos com dados pessoais serão guardados em gavetas ou armários fechados, e não deixados sobre as mesas;

II – o computador será bloqueado sempre que o usuário se afastar da estação de trabalho; e

III – documentos com dados pessoais não serão esquecidos em impressoras, copiadoras ou áreas de atendimento.

CAPÍTULO VII
DA SEGURANÇA DAS COMUNICAÇÕES

Art. 32. O Município utilizará conexões cifradas (TLS/HTTPS) em todos os serviços públicos digitais e nas comunicações de e-mail institucional e, quando aplicável, filtro de aplicação web (WAF).

Art. 33. As comunicações oficiais serão feitas por e-mail institucional, que contará com filtros antispam e antivírus integrados, sendo vedado o uso de e-mail particular para o envio de documentos com dados pessoais.

Art. 34. O uso de aplicativos de mensagens para atendimento ou comunicação institucional observará o seguinte:

I – utilização de contas ou números institucionais, com criptografia de ponta a ponta;

II – envio apenas dos dados pessoais estritamente necessários; e

III – vedação do envio de dados pessoais sensíveis, salvo quando

indispensável ao atendimento do titular e com sua ciência.

Art. 35. É obrigatória a instalação e a manutenção de firewall na rede municipal e de antivírus e antimalware atualizados em todas as estações de trabalho e servidores.

CAPÍTULO VIII
DA GESTÃO DE VULNERABILIDADES

Art. 36. O Gestor de Segurança da Informação manterá programa de gestão de vulnerabilidades que contemple:

I – atualização periódica de sistemas operacionais, aplicativos e equipamentos, com aplicação das correções de segurança disponibilizadas pelos fabricantes;

II – substituição ou isolamento de sistemas e equipamentos sem suporte do fabricante;

III – varreduras periódicas de antivírus e de vulnerabilidades, priorizando os ativos expostos à internet;

IV – priorização da correção conforme a criticidade da vulnerabilidade e do ativo afetado; e

V – hardening de servidores, estações de trabalho e equipamentos de rede.

Art. 37. O usuário relatará prontamente qualquer fato ou ameaça à segurança, como fragilidade, mau funcionamento, mensagem suspeita ou presença de vírus, à chefia imediata, ao Gestor de Segurança da Informação ou ao Encarregado, pelo e-mail lgpd@saltoveloso.sc.gov.br.

CAPÍTULO IX
DOS DISPOSITIVOS MÓVEIS E DOS SERVIÇOS EM NUVEM

Art. 38. Os dispositivos móveis institucionais, como notebooks, tablets e smartphones, terão bloqueio por senha ou biometria e, sempre que possível, criptografia e funcionalidade de localização e apagamento remoto dos dados.

Art. 39. O uso de dispositivos particulares no tratamento de dados pessoais de responsabilidade do Município depende de autorização da chefia imediata e da adoção das medidas mínimas de segurança definidas pelo Gestor de Segurança da Informação, devendo os dispositivos de uso institucional e particular ser separados sempre que possível.

Art. 40. A contratação de serviços de computação em nuvem que armazenem ou processem dados pessoais observará:

I – contrato com acordo de nível de serviço que contemple a segurança dos dados armazenados;

II – avaliação prévia de que o serviço atende aos requisitos desta Política;

III – indicação da localização dos dados e, havendo transferência internacional, observância da regulamentação da ANPD;

IV – controle de acesso por usuário e autenticação multifator;

V – rotina de backup e obrigação de comunicação imediata de incidentes ao Município; e

VI – devolução e eliminação segura dos dados ao término do contrato.

CAPÍTULO X
DA AQUISIÇÃO E DO DESENVOLVIMENTO DE SISTEMAS

Art. 41. Os sistemas utilizados para o tratamento de dados pessoais serão estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e aos princípios da Lei Federal nº 13.709/2018, nos termos de seu art. 49, desde a fase de concepção até a execução.

Art. 42. Os termos de referência e os contratos de aquisição, locação ou desenvolvimento de sistemas, sítios eletrônicos e aplicativos preverão requisitos mínimos de segurança e privacidade, como controle de acesso por perfil, registro de logs, criptografia, backup, atualização e suporte, e exportação dos dados ao fim do contrato.

Art. 43. Os ambientes de teste e de treinamento não utilizarão dados pessoais reais, salvo se anonimizados ou mediante justificativa e controles equivalentes aos do ambiente de produção.

Art. 44. É vedada a inserção de dados pessoais, dados pessoais sensíveis ou informações sigilosas em ferramentas de inteligência artificial generativa que não tenham sido contratadas ou formalmente autorizadas pelo Município.

§ 1º. O uso de ferramentas autorizadas observará a finalidade pública, os princípios da Lei Federal nº 13.709/2018 e a revisão humana do conteúdo gerado antes de sua utilização em atos administrativos.

§ 2º. O Comitê de Privacidade e Proteção de Dados Pessoais poderá expedir orientações complementares sobre o uso de inteligência artificial no Município.

CAPÍTULO XI

DOS CONTRATOS, DA CONFIDENCIALIDADE E DA CONSCIENTIZAÇÃO

Art. 45. Os contratos com fornecedores e parceiros que tenham acesso a dados pessoais conterão cláusulas de segurança da informação e proteção de dados que disciplinem, entre outros pontos:

I – a atuação do fornecedor como operador, tratando os dados exclusivamente conforme as instruções do Município, vedado o tratamento para finalidade diversa;

II – as regras de compartilhamento e de subcontratação;

III – as medidas de segurança exigidas e o direito de fiscalização pelo Município;

IV – a comunicação imediata de incidentes de segurança; e

V – a devolução ou eliminação dos dados ao término do contrato.

Art. 46. Os agentes públicos e os prestadores de serviço com acesso a dados pessoais firmarão Termo de Confidencialidade, obrigação que subsiste após o término do vínculo, nos termos do art. 47 da Lei Federal nº 13.709/2018.

Art. 47. O Município promoverá treinamento em segurança da informação e proteção de dados no ingresso do agente público e, periodicamente, para todos os agentes, abordando, no mínimo:

I – o uso correto dos controles de segurança dos sistemas utilizados no trabalho diário;

II – a prevenção de golpes, phishing, engenharia social e contaminação por vírus;

III – as práticas de mesa limpa e tela limpa e a vedação ao compartilhamento de senhas; e

IV – o dever de comunicar incidentes e vulnerabilidades, em ambiente que incentive essa comunicação.

CAPÍTULO XII
DOS INCIDENTES E DA CONTINUIDADE DOS SERVIÇOS

Art. 48. Os incidentes de segurança serão tratados conforme o Plano de

Resposta a Incidentes de Segurança envolvendo Dados Pessoais, instituído por Decreto próprio, e comunicados pelo e-mail lgpd@saltoveloso.sc.gov.br.

Art. 49. O Gestor de Segurança da Informação manterá procedimentos de recuperação dos sistemas críticos, com definição de prioridades de restauração e responsáveis, testados ao menos uma vez por ano.

CAPÍTULO XIII
DO MONITORAMENTO E DAS DISPOSIÇÕES FINAIS

Art. 50. O Gestor de Segurança da Informação apresentará ao Comitê de Privacidade e Proteção de Dados Pessoais, anualmente, relatório de conformidade indicando as medidas implementadas, as pendentes e o respectivo plano de ação.

Art. 51. Esta Política será revisada anualmente ou sempre que houver mudança significativa na legislação, nas orientações da ANPD ou na infraestrutura tecnológica do Município.

Art. 52. A identidade e o contato do Encarregado pelo Tratamento de Dados Pessoais serão publicados no sítio eletrônico oficial do Município, em local de fácil acesso.

Art. 53. O descumprimento desta Política sujeitará o infrator às sanções disciplinares previstas no Estatuto dos Servidores Públicos do Município e, no caso de contratados, às sanções contratuais, sem prejuízo das responsabilidades civil e penal.

Art. 54. Os casos omissos e as dúvidas sobre esta Política serão submetidos ao Comitê de Privacidade e Proteção de Dados Pessoais.

Art. 55. Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Salto Veloso/SC, 21 de outubro de 2026.

NEREU BORGA
Prefeito Municipal