RESOLUÇÃO SEFA Nº 278, DE 6 DE ABRIL DE 2026

Dispõe sobre a Política de Segurança da Informação da Secretaria de Estado da Fazenda (SEFA) e da Receita Estadual do Paraná (REPR).

O **SECRETÁRIO DE ESTADO DA FAZENDA**, no exercício de suas atribuições legais que lhe são conferidas pelo art. 90 da Constituição do Estado do Paraná e pelo art. 4º da Lei Estadual nº 21.352, de 1º de janeiro de 2023;

CONSIDERANDO os deveres de probidade administrativa, nos termos da Lei Federal nº 8.429, de 2 de junho de 1992 - Lei de Improbidade Administrativa;

CONSIDERANDO a responsabilidade institucional quanto à proteção da informação, da privacidade e do sigilo fiscal, nos termos do art. 198 da Lei Federal nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional;

CONSIDERANDO os deveres do agente público, nos termos da Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);

CONSIDERANDO o contido na Lei Estadual nº 17.079, de 23 de janeiro de 2012, que dispõe sobre a informatização dos processos administrativos no âmbito da Secretaria de Estado da Fazenda – SEFA e os meios de identificação eletrônica;

CONSIDERANDO os trabalhos realizados pelo Comitê Gestor de Tecnologia da Informação (CGTI) da Secretaria de Estado da Fazenda (SEFA), nos termos do art. 4º da Resolução 1.566, de 18 de dezembro de 2024;

CONSIDERANDO os trabalhos realizados pelo Comitê de Gestão de Riscos (CGR) da Secretaria de Estado da Fazenda, nos termos da Resolução SEFA n° 184, de 9 de março de 2023, que institui a Política de Gestão de Riscos, e da Resolução SEFA nº 432, de 15 de maio de 2023, que aprova o Regimento Interno do Comitê de Gestão de Riscos (CGR) da Secretaria de Estado da Fazenda (SEFA);

CONSIDERANDO a Política de Privacidade de Dados Pessoais no âmbito da Secretaria de Estado da Fazenda, nos termos da Resolução SEFA nº 647, de 5 de julho de 2023;

CONSIDERANDO os trabalhos realizados pelo Comitê Gestor de Proteção de Dados Pessoais (CGPDP) da Secretaria de Estado da Fazenda, instituído pela Resolução SEFA nº 1.088, de 15 de outubro de 2024;

CONSIDERANDO o contido na Lei Estadual nº 22.324, de 2 de abril de 2025, que institui o Plano de Diretrizes de Inteligência Artificial na Administração Pública Estadual (PDIA/PR), e na Resolução SEFA n° 670, de 6 de agosto de 2025, que institui a Política de Uso de Inteligência Artificial no âmbito da Secretaria de Estado da Fazenda (SEFA) e da Receita Estadual do Paraná (REPR);

CONSIDERANDO a necessidade de alinhar a Segurança da Informação à Estratégia de Tecnologia da Informação da Secretaria de Estado da Fazenda (SEFA) e da Receita Estadual do Paraná (REPR);

CONSIDERANDO a necessidade de estabelecer princípios, diretrizes e responsabilidades para a gestão da segurança da informação no âmbito da SEFA e da REPR; e

CONSIDERANDO o contido no Protocolo nº 25.673.894-5,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º. Fica instituída a Política de Segurança da Informação, no âmbito da SEFA e da REPR, a qual estabelece princípios, diretrizes, responsabilidades e competências aplicáveis à gestão da segurança da informação, alcançando também quaisquer indivíduos ou organizações que mantenham relacionamento direto ou indireto com esses órgãos.

Art. 2º. Esta Política constitui o marco inicial da estruturação da gestão de Segurança da Informação na SEFA e poderá ser complementada por normas específicas, procedimentos e instrumentos aprovados.

Art. 3º. Os procedimentos específicos serão detalhados em normas complementares aprovadas pelo CGTI, mediante proposta do Centro de Tecnologia da Informação e da Comunicação (CTIC) da SEFA, e disponibilizadas nos canais apropriados.

Art. 4º. Para os fins desta Política, consideram-se:

I – Ativos de Informação: o conjunto de dados, documentos, sistemas, redes, infraestrutura tecnológica e suportes físicos que processam ou armazenam informações de interesse da SEFA e da REPR;

II – Tríade da Segurança (CID): garantia de Confidencialidade (acesso apenas por pessoas autorizadas), Integridade (proteção contra alterações indevidas) e Disponibilidade (garantia de que o serviço esteja acessível quando necessário);

III – Sigilo Fiscal: dever de proteção de dados relativos à situação econômica ou financeira do sujeito passivo ou de terceiros e à natureza e estado de seus negócios, conforme o Código Tributário Nacional;

IV – Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança dos sistemas de informação ou à proteção de dados pessoais e fiscais;

V – Usuário: qualquer pessoa física (servidor, estagiário, residente técnico, prestador de serviço ou terceiro) que tenha acesso autorizado aos recursos tecnológicos da SEFA e da REPR;

VI – Desenvolvimento Seguro de Software: conjunto de práticas que incorporam requisitos e controles de segurança ao longo do ciclo de vida de desenvolvimento de sistemas, visando prevenir vulnerabilidades e proteger as informações processadas pelas aplicações;

VII – Risco de Segurança da Informação: possibilidade de ocorrência de evento que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade das informações e dos ativos de informação da SEFA e da REPR, podendo afetar o cumprimento de seus objetivos institucionais, a continuidade dos serviços públicos, o sigilo fiscal ou a proteção de dados pessoais, conforme diretrizes da Política de Gestão de Riscos vigente.

CAPÍTULO II
DO OBJETIVO

Art. 5º. A Política de Segurança da Informação prevista no art. 1º desta Resolução objetiva estabelecer princípios e diretrizes para a proteção das informações e dos ativos de informação da SEFA e da REPR, promovendo sua integração à gestão institucional de riscos, à governança de tecnologia da informação e às diretrizes de proteção de dados pessoais, de modo a assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, a conformidade legal, a proteção do sigilo fiscal e a continuidade dos serviços públicos, preservando a confiança da sociedade na administração fiscal e tributária estadual.

CAPÍTULO III
DA ABRANGÊNCIA

Art. 6º. A Política de Segurança da Informação de que trata esta Resolução se aplica a todos os colaboradores da SEFA e da REPR, incluindo servidores efetivos e comissionados, funcionários cedidos, voluntários, estagiários, residentes técnicos, prestadores de serviços e terceiros.

Parágrafo único. O previsto no caput deste artigo se aplica ao uso em dispositivos da SEFA e/ou dispositivos pessoais quando utilizados para fins de trabalho ou conectados na rede da SEFA, desde que observados os requisitos mínimos de segurança e as diretrizes institucionais aplicáveis, conforme as normas específicas de uso e os limites legais de monitoramento.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 7º. A gestão, a implementação e a operação dos ativos de informação observarão os seguintes princípios que sustentam a política de segurança e resiliência no ambiente público:

I – Conformidade Legal e Normativa: proteção e tratamento de dados em estrita conformidade com leis, decretos, portarias e normas aplicáveis, incluindo a Lei Geral de Proteção de Dados – LGPD, a Lei de Acesso à Informação – LAI e regulamentações específicas fazendárias;

II – Proteção da Tríade de Segurança: garantia contínua da confidencialidade, integridade e disponibilidade das informações e sistemas críticos contra acessos não autorizados, modificações indevidas ou indisponibilidade de serviços;

III – Gestão Baseada em Risco: estabelecimento de controles de segurança proporcionais à criticidade dos dados e à probabilidade de ameaças, assegurando uma governança adaptável e eficiente, em acordo com a Resolução 184, de 9 de março de 2023;

IV – Ética e Responsabilidade Funcional: compromisso de todo servidor e colaborador com o uso íntegro dos recursos tecnológicos, conforme legislação vigente para os agentes públicos;

V – Rastreabilidade e Responsabilização: garantia de que todas as ações realizadas nos sistemas institucionais e no tratamento das informações sejam identificáveis, auditáveis e vinculadas a um responsável, assegurando a transparência e a propriedade intelectual;

VI – Continuidade e Eficiência: promoção da resiliência operacional para garantir que a segurança da informação contribua para a continuidade dos serviços públicos e o ganho de produtividade sem interrupções críticas.

CAPÍTULO V
DAS DIRETRIZES

Art. 8º. A Segurança da Informação na SEFA e na REPR fundamenta-se nas seguintes diretrizes operacionais:

I – Gestão de Riscos de Segurança da Informação: a segurança da informação deve ser orientada pela gestão de riscos institucionais, considerando ameaças, vulnerabilidades e impactos potenciais aos serviços públicos, ao sigilo fiscal e à proteção de dados pessoais;

II – Conformidade com Políticas e Normas Institucionais: os usuários devem observar as políticas, normas e procedimentos institucionais relacionados à segurança da informação e ao uso dos recursos tecnológicos;

III – Classificação e Proteção da Informação: todas as informações devem ser classificadas e protegidas de acordo com sua criticidade e sensibilidade, observando-se o sigilo fiscal e legislação de proteção de dados pessoais (LGPD);

IV – Controle de Acesso e Rastreabilidade: o acesso aos ativos de informação é restrito a usuários autorizados, mediante identificação pessoal e intransferível, com controles baseados no princípio do menor privilégio, podendo ser adotados mecanismos adicionais de autenticação conforme normas complementares. Devem ser adotados mecanismos que permitam o registro e a auditoria das ações realizadas nos sistemas institucionais, assegurando a identificação de responsabilidades;

V – Desenvolvimento Seguro de Software: o desenvolvimento, aquisição ou manutenção de sistemas e aplicações deve observar boas práticas de desenvolvimento seguro, incorporando requisitos de segurança da informação e proteção de dados pessoais desde as fases de concepção, implementação, testes e implantação;

VI – Segurança no Relacionamento com Terceiros: contratações, parcerias e prestação de serviços que envolvam acesso a informações ou sistemas institucionais devem observar requisitos de segurança da informação e proteção de dados pessoais definidos em normas e instrumentos contratuais;

VII – Uso Institucional dos Recursos Tecnológicos: os recursos tecnológicos, sistemas e e-mails corporativos são destinados exclusivamente ao exercício de funções institucionais, sendo vedado o uso para fins privados, comerciais ou ilícitos;

VIII – Uso de Tecnologias Emergentes: o uso de tecnologias emergentes, incluindo soluções baseadas em inteligência artificial, deverá observar as diretrizes institucionais específicas, bem como os princípios de classificação da informação, proteção de dados pessoais e sigilo fiscal, sendo suas condições de uso disciplinadas em normas complementares;

IX – Cultura de Segurança da Informação: a segurança da informação deve ser incorporada às práticas institucionais e ao comportamento dos usuários, promovendo hábitos e atitudes responsáveis no tratamento das informações e no uso de recursos tecnológicos.

Art. 9º. Esta Política observa, no que couber, as diretrizes nacionais relativas à proteção e ao tratamento de informações classificadas, em conformidade com a legislação vigente e sem prejuízo da autonomia normativa do Estado do Paraná.

CAPÍTULO VI
DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 10. A estrutura de Gestão de Segurança da Informação é composta por:

I – Alta Administração;

II – Comitê Gestor da Tecnologia da Informação (CGTI);

III – Comitê de Gestão de Riscos (CGR);

IV – Comitê Gestor de Proteção de Dados Pessoais (CGPDP);

V – Centro de Tecnologia da Informação e da Comunicação (CTIC);

VI – Área Técnica de Segurança da Informação (ASI);

VII – Usuários de Informação.

Art. 11. Compete à Alta Administração:

I – Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da SEFA e da REPR, bem como com tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

II – Formalizar e aprovar a Política de Segurança da Informação da SEFA, bem como suas alterações e atualizações.

Art. 12. Compete ao Comitê Gestor da Tecnologia da Informação (CGTI):

I – Atuar como instância deliberativa para assuntos estratégicos de Segurança da Informação;

II – Acompanhar e orientar a implementação das ações de segurança da informação;

III – Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV – Deliberar sobre normas de segurança da informação;

V – Deliberar sobre exceções relevantes.

Art. 13. Compete ao Comitê de Gestão de Riscos (CGR) da SEFA integrar ao processo institucional a gestão de riscos de Segurança da Informação, conforme Resolução 184, de 9 de março de 2023 ou que venha a substituí-la.

Art. 14. Compete ao Comitê Gestor de Proteção de Dados Pessoais (CGPDP) da SEFA e REPR, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD) e demais normativos e orientações emitidas pela Agência Nacional de Proteção de Dados (ANPD):

I – Orientar e acompanhar a implementação das diretrizes de proteção de dados pessoais no âmbito da SEFA e da REPR;

II – Apoiar a identificação e o tratamento de riscos relacionados ao tratamento de dados pessoais;

III – Atuar de forma integrada com o CGTI e com o CGR nos temas que envolvam simultaneamente segurança da informação, gestão de riscos e proteção de dados pessoais;

IV – Propor diretrizes e instrumentos institucionais relacionados à governança de proteção de dados pessoais.

Art. 15. Compete ao Centro de Tecnologia da Informação e da Comunicação (CTIC), por meio da Área Técnica de Segurança da Informação (ASI), as atividades definidas sobre Segurança da Informação, conforme Regimento Interno do CTIC:

I – Coordenar tecnicamente as ações de Segurança da Informação;

II – Propor normas complementares ao CGTI;

III – Apoiar tecnicamente a gestão de riscos de Segurança da Informação;

IV – Apoiar tecnicamente as ações de proteção de dados pessoais;

V – Comunicar às autoridades competentes eventuais infrações previstas no art. 17 desta Resolução;

VI – Tratar incidentes de Segurança da Informação;

VII – Promover campanhas periódicas de conscientização sobre o uso seguro dos recursos tecnológicos, boas práticas de segurança da informação, prevenção a incidentes cibernéticos e tratamento ético dos dados.

Art. 16. Compete ao Usuário:

I – Observar e cumprir as disposições desta Política e das normas complementares dela decorrentes;

II – Zelar pela confidencialidade, integridade e disponibilidade das informações e dos ativos de informação aos quais tenham acesso;

III – Comunicar tempestivamente ao CTIC qualquer incidente ou suspeita de incidente de Segurança da Informação pelo e-mail seguranca@sefa.pr.gov.br;

IV – Utilizar os sistemas informacionais institucionais exclusivamente para fins relacionados às atividades da SEFA e da REPR;

V – Agir com responsabilidade no tratamento de informações institucionais especialmente aquelas protegidas por sigilo fiscal ou pela legislação de proteção de dados pessoais.

CAPÍTULO VII
DAS VEDAÇÕES

Art. 17. É vedado aos usuários:

I – Acessar, utilizar ou divulgar informações sem autorização;

II – Praticar atos que comprometam ou possam comprometer a segurança dos sistemas ou dos ativos de informação;

III – Compartilhar credenciais, senhas, ou permitir o uso de contas institucionais a terceiros;

IV – Armazenar, transferir ou tratar informações institucionais em ambientes que não atendam às diretrizes institucionais de segurança da informação ou que não estejam em conformidade com normas complementares;

V – Utilizar recursos institucionais em desacordo com sua finalidade pública ou em desconformidade com as normas internas vigentes relativas ao uso dos recursos tecnológicos.

CAPÍTULO VIII
DAS EXCEÇÕES

Art. 18. O descumprimento das diretrizes estabelecidas na Política de Segurança da Informação somente poderá ocorrer mediante autorização formal, caracterizada como exceção devidamente fundamentada.

Art. 19. A solicitação de exceção deverá conter, no mínimo:

I – Descrição clara da diretriz da qual se pretende excepcionar;

II – Justificativa técnica ou administrativa;

III – Análise preliminar dos riscos envolvidos;

IV – Medidas compensatórias propostas, quando aplicável;

V – Prazo determinado para vigência da exceção.

Art. 20. O CTIC, por meio da ASI, realizará a avaliação técnica da solicitação.

Art. 21. Exceções que envolvam riscos relevantes à continuidade dos serviços, dados pessoais ou sigilo fiscal deverão ser submetidas à deliberação do CGTI, CGR e CGPDP.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 22. As irregularidades e incidentes relacionados à segurança da informação deverão ser comunicados à área técnica responsável pela segurança da informação ou pela governança de TIC, para análise preliminar e adoção das medidas cabíveis.

Parágrafo único. Quando caracterizada infração disciplinar, indícios de ilícito ou necessidade de apuração formal, o caso deverá ser encaminhado à Corregedoria-Geral, nos termos da legislação vigente.

Art. 23. O descumprimento desta Resolução poderá acarretar sanções administrativas, civis e criminais, conforme o devido processo legal.

Parágrafo único. O processo administrativo disciplinar decorrente de infração a esta Resolução será conduzido pela Corregedoria-Geral da SEFA, observados o contraditório e a ampla defesa.

Art. 24. Os casos omissos e as situações excepcionais serão dirimidos pelo CGTI, mediante apoio técnico do CTIC/ASI, observada a legislação vigente, os princípios desta Política e as boas práticas de governança em segurança da informação.

Art. 25. Esta Política de Segurança da Informação poderá ser alterada ou atualizada mediante nova Resolução, sempre que necessário, conforme exigências legais ou diretrizes.

Art. 26. Esta Resolução entra em vigor na data de sua publicação.

Curitiba, 6 de abril de 2026.

NORBERTO ANACLETO ORTIGARA
Secretário de Estado da Fazenda

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 11a
Mov. 3

Documento: **27825.673.8945DispoePoliticadeSegurancadaInformacaoSEFA.pdf**.

Assinatura Qualificada realizada por: **Norberto Anacleto Ortigara** em 06/04/2026 13:35.

Inserido ao protocolo **25.673.894-5** por: **Nicholas Andrey Monteiro Watzko** em: 06/04/2026 13:19.

Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento** com o código: