SUMÁRIO

1. INTRODUÇÃO

A Secretaria de Estado da Educação do Paraná (SEED-PR), diante do crescimento das ameaças cibernéticas e da complexidade dos seus processos educacionais e administrativos, reconhece a necessidade de consolidar uma **estratégia de Segurança da Informação e TI**. Este plano estratégico visa **proteger ativos críticos**, assegurar a **confidencialidade, integridade e disponibilidade** das informações e garantir a **continuidade dos serviços educacionais**.

2. OBJETIVOS ESTRATÉGICOS

- **OE1** – Estabelecer uma **governança de segurança da informação** integrada aos processos da SEED-PR.
- **OE2** – **Proteger dados pessoais e sensíveis** em conformidade com a LGPD e demais legislações aplicáveis.
- **OE3** – **Gerenciar riscos cibernéticos** de forma contínua, priorizando ativos críticos.
- **OE4** – **Fortalecer a resiliência operacional**, com planos de continuidade de negócios (BCP) e recuperação de desastres (DRP).
- **OE5** – **Promover a cultura de segurança da informação** entre servidores, professores, alunos e parceiros.
- **OE6** – Garantir **melhoria contínua** por meio de auditorias, métricas e revisões periódicas.

3. EIXOS ESTRATÉGICOS E LINHAS DE AÇÃO

3.1. Governança e Compliance

- ✓ Criar um **Comitê de Segurança da Informação** vinculado à DTI e à alta gestão da SEED-PR.
- ✓ Definir e aprovar a **Política de Segurança da Informação (PSI)** e políticas específicas (gestão de acessos, backup, incidentes, descarte de TI etc.).
- ✓ Garantir **alinhamento normativo**: LGPD, Decreto 8.771/2016, ISO/IEC 27001 e 27701.

3.2. Gestão de Riscos e Maturidade

- ✓ Mapear riscos e vulnerabilidades em **nível central, NREs e escolas**.

- ✓ Avaliar a maturidade de segurança (questionários e entrevistas), identificando **pontos fortes e fragilidades**.
- ✓ Utilizar **matriz de probabilidade e impacto** para classificar riscos e definir prioridades de tratamento.

3.3. Proteção de Ativos Críticos

- ✓ Inventariar e classificar ativos de informação (dados de alunos, professores, sistemas administrativos).
- ✓ Implementar **controles de acesso lógico** (IAM), segregação de funções e revisão periódica de privilégios.
- ✓ Definir políticas de **uso de dispositivos móveis, nuvem e ambientes híbridos**.

3.4. Resposta a Incidentes e Continuidade

- ✓ Criar um **Plano de Resposta a Incidentes (PRI)** com papéis, fluxos e canais de comunicação (incluindo órgãos externos como ANPD).
- ✓ Definir e implementar um **Plano de Continuidade de Negócios (BCP)** e **Plano de Recuperação de Desastres (PRD)**.
- ✓ Realizar **testes periódicos** (simulações e exercícios) de incidentes e falhas de TI.

3.5. Capacitação e Conscientização

- ✓ Desenvolver **programas de treinamento contínuos** para servidores e terceirizados.
- ✓ Criar **campanhas de sensibilização** sobre phishing, engenharia social, proteção de dados e boas práticas digitais.
- ✓ Implementar um **programa de reciclagem anual** em segurança da informação.

3.6. Monitoramento e Melhoria Contínua

- ✓ Implantar **Soluções de Monitoramento Contínuo (SIEM/SOC)** para detectar e responder a ameaças em tempo real.
- ✓ Definir **KPIs e KRIs de segurança da informação** (tempo médio de resposta a incidentes, número de vulnerabilidades críticas tratadas, percentual de usuários treinados).
- ✓ Realizar **auditorias periódicas** e relatórios para a alta gestão e órgãos de controle.

4. CRONOGRAMA ESTRATÉGICO

Para melhor entendimento desse plano estratégico, segue o cronograma com os sete produtos a serem entregues, conforme Termo de Referência nº 10677:

Parcela / Produto	Descrição da Entrega	Prazo	Mês Previsto
Produto 1	Documento técnico contendo a **metodologia para avaliação de maturidade de segurança, riscos e vulnerabilidades** no âmbito da SEED, NREs e escolas.	30 dias	Dezembro/2024
Produto 2	Documento técnico com o **levantamento de necessidades** baseado em entrevistas e informações sobre o ambiente atual de TI (sistemas, redes, hardware, software e políticas existentes).	90 dias	Fevereiro/2025
Produto 3	Documento técnico com a **avaliação de maturidade em SI**, pontos fortes e vulnerabilidades, **identificação dos ativos críticos de informação** e suas respectivas vulnerabilidades, além da **descrição das ameaças potenciais**.	150 dias	Abril/2025
Produto 4	Documento técnico com a **análise de impacto** de incidentes, classificação de riscos por probabilidade e impacto e **priorização de tratamento**.	210 dias	Junho/2025
Produto 5	Documento técnico contendo as **Políticas de Segurança da Informação**, alinhadas à LGPD e normas internacionais, abrangendo: gestão de incidentes, controle de acesso, dispositivos móveis, backup, DR, conscientização e treinamento, recomendações de controles de segurança, plano de resposta a incidentes e comunicação.	270 dias	Agosto/2025
Produto 6	Documento técnico com **relatório final das formações realizadas** junto às equipes técnicas da SEED-PR, incluindo registros, formulários de feedback e recomendações de continuidade.	300 dias	Setembro/2025
Produto 7	**Plano de Segurança da Informação consolidado**, prevendo continuidade das atividades em caso de interrupções, plano de recuperação de desastres (DRP), restauração de sistemas críticos, plano de treinamento, campanhas de conscientização, e toda a documentação consolidada (políticas, procedimentos, recomendações).	330 dias	Outubro/2025

5. INDICADORES DE SUCESSO

- Redução do número de **incidentes críticos** registrados.
- Percentual de **ativos críticos com controles implementados**.
- Grau de **maturidade em segurança** (meta: elevar dois níveis até 2026).
- Percentual de **colaboradores treinados em SI** (>80%).
- Conformidade com a **LGPD** e auditorias internas/externas.

6. CONSIDERAÇÕES FINAIS

O **Planejamento Estratégico de Segurança de TI da SEED-PR** é um **instrumento de governança** que integra tecnologia, processos e pessoas. Sua efetividade depende do apoio da **alta gestão**, da **participação dos NREs e escolas** e de um ciclo contínuo de monitoramento, revisão e melhoria.

7. HISTÓRICO DE ALTERAÇÕES DO DOCUMENTO

Data	Descrição (Alteração do Documento)	Autor
15/07/2025	Criação do Documento	NSI SEED-PR
21/08/2025	Atualização e Revisão	NSI SEED-PR