

Tema: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - SEAP		
Indicação: CG/LGPD - DTIC/DOS	Versão: 2.0	Início: 15/07/2024

1. ABRANGÊNCIA

1.1 Esta política se aplica:

- I. Servidores Públicos, Funcionários Públicos, Comissionados, Residentes Técnicos, Estagiários, Terceirizados e Fornecedores que atuem junto a Secretaria da Administração e da Previdência do Estado do Paraná - SEAP;
- II. Às informações/dados armazenados em meios físicos ou em “nuvem” de propriedade da SEAP, desde que sob legislação que forneça nível de proteção equivalente a LGPD;
- III. A todos os ambientes computacionais e informações/dados neles armazenadas.

2. OBJETIVOS

2.1 São objetivos dessa política:

- I. Tratar a informação como um patrimônio, protegendo-a de acordo com sua sensibilidade e seu grau de exposição do risco;
- II. Garantir a integridade, disponibilidade, confidencialidade e autenticidade das informações;
- III. Estabelecer e padronizar práticas de segurança da informação na SEAP;
- IV. Assegurar a adequação dos processos e práticas da SEAP aos requisitos legais pertinentes a segurança da informação.

3. PRINCÍPIOS

3.1 Para atingir seus objetivos esta política de segurança, é baseada nos seguintes princípios:

- I. **Privacidade:** proteção dos dados pessoais para a garantia do direito fundamental à inviolabilidade da privacidade e intimidade, observando o disposto na Lei Geral de Proteção de Dados (Lei n.º 13.704/2018) e no Decreto Estadual nº. 6.474, de 2020;
- II. **Proteção:** zelo pela proteção das informações, independente do meio em que estão armazenadas ou do ambiente em que estejam sendo processadas ou transitando;
- III. **Adaptação:** adoção de medidas de segurança adaptáveis para atender às necessidades dos serviços e suportar a evolução tecnológica;
- IV. **Proporcionalidade:** adequação dos custos das ações de segurança da informação ao valor dos ativos e informações, considerando os riscos a que estão expostos, seguindo critérios de proporcionalidade;
- V. **Prevenção:** Trabalhar prioritariamente de forma preventiva para obtenção dos objetivos de segurança da informação.

4. DIRETRIZES

4.1. São diretrizes de segurança da informação da SEAP, a serem implementadas e executadas de acordo com a natureza da atividade:

- I. **Disponibilidade:** qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
- II. **Integridade:** qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
- III. **Confidencialidade:** garantia de que somente pessoas/órgãos ou sistemas autorizados tenham acesso às informações transmitidas, ou mantidas em redes, ou sistemas de comunicação;
- IV. **Autenticidade:** qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema
- V. **Primariedade:** qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

5. RESPONSABILIDADES

- 5.1. Cabe a todos os abrangidos por essa política:
 - I. Proteger as informações contra uso, acesso, divulgação, modificação ou destruição não autorizadas conforme as diretrizes dessa política.
 - II. Ocorrências de descumprimento da política, de suas normas, ou demais assuntos relacionados a segurança da informação deverão ser informados ao Núcleo de Integridade e *Compliance* Setorial – NICS.
 - III. Proteger suas contas pessoais contra o uso indevido.
 - IV. Cabe aos gestores de pessoas ou processos cumprir, ou fazer cumprir no âmbito de sua atuação esta política, as normas e os procedimentos de segurança da informação.

6. PENALIDADES

- 6.1. As violações dessa política, mesmo que por omissão ou tentativa não consumada, bem como das demais normas e procedimentos de segurança vigentes, serão passíveis de penalidades:
 - I. Aos servidores públicos caberão as punições prevista em lei;
 - II. Para residentes técnicos e estagiários serão cabíveis os procedimentos previstos em contratos;
 - III. Para terceirizados e fornecedores serão cabíveis os procedimentos previstos em contrato;

7. NORMAS E TERMO DE COMPROMISSO

- 7.1. Para o cumprimento das diretrizes desta política serão editadas normas de segurança da informação, no contexto de cada atividade ou objetivo específico.

- Uso do e-mail corporativo;
- Uso dos computadores e equipamentos corporativo;
- Uso da internet;
- Uso de Certificados Digitais emitidos pela SEAP;
- Uso da VPN;
- Acesso e Desligamento lógico.

7.2. Servidores Públicos, Funcionários Públicos, Comissionados, Residentes Técnicos, Estagiários, Terceirizados e Fornecedores deverão assinar termo de compromisso para uso dos recursos tecnológicos da SEAP.

7.3. As normas e termos de compromisso podem ser atualizadas a qualquer momento conforme legislação vigente e adequação do ativo de tecnologia de dados da SEAP. A cada atualização, será informado os agentes públicos listados no item anterior e solicitado nova confirmação de conhecimento de termo de compromisso.

8. DISPOSIÇÕES FINAIS

8.1. Esta política vigorará a partir de sua publicação e até que seja modificada.

8.2. As dúvidas de interpretação e os casos não previstos nesta Política serão objeto de análise em documento protocolado junto ao Procuradoria Geral do Estado - PGE, Controladoria Geral do Estado - CGE, Conselho Estadual de Tecnologia da Informação e Comunicação do Paraná- CETIC, NICS e Agente de Tratamento de Dados Pessoais da SEAP, junto a gestão superior, quando for o caso.