ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO (SCGE)

Art. 1º A Política de Segurança da Informação (PSI) da Secretaria da Controladoria-Geral do Estado (SCGE) representa o comprometimento da gestão com a segurança e proteção das informações produzidas ou recebidas por esta Secretaria, estabelecendo instrumentos normativos e organizacionais que assegurem técnica e administrativamente a confidencialidade, a integridade, e disponibilidade dos dados e das informações tratadas no âmbito deste órgão.

Parágrafo único. A SCGE declara o apoio e o comprometimento para alcançar a conformidade com as regulamentações e legislações aplicáveis, assim como com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores etc.).

Art. 2º Para efeitos da PSI da SCGE considera-se:

I - Ativos de TIC: Equipamentos de informática e comunicação, servidores físicos ou virtuais, sistemas e/ou serviços de TIC, softwares, e-mail corporativo, rede local ou internet corporativa, além da própria informação produzida ou armazenada em formato físico ou digital.

II - Acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

III - Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

IV - Classificação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

V - Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

VI - Controles: políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, de natureza administrativa, técnica, de gestão ou legal, com vista a mitigar os riscos identificados;

VII - Credencial de segurança: certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo;

VIII - Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos de TIC correspondentes sempre que necessário;

IX - Grau de sigilo: gradação de segurança atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

X - Incidente de segurança: indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;

XI - Integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;

XII - Risco: a combinação da probabilidade de um evento ocorrer quando uma ameaça explora uma vulnerabilidade e o impacto de tal evento na organização;

XIII - Senha ou palavra-chave: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XIV - Sigilo: segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada;

XV - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Art. 3º São objetivos da Política de Segurança da Informação - PSI da SCGE:

I - Tornar a segurança da informação um insumo no planejamento das atividades da SCGE;

II - Fortalecer a integridade institucional, a partir do diagnóstico de vulnerabilidades na segurança da informação;

III - Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas na SCGE;

IV - Estabelecer as competências e as atribuições dos atores envolvidos nesta política;

V - Definir o método de gestão de riscos de segurança da informação na SCGE;

VI - Elencar os controles necessários para atingir um padrão aceitável de segurança da informação, conforme as legislações existentes e os padrões que o mercado estabelece; e

VII - Difundir no órgão os aspectos relacionados à segurança da informação.

Art. 4º A PSI da SCGE considera a segurança e proteção das informações produzidas ou recebidas por esta Secretaria.

Parágrafo único. As informações produzidas por esta Secretaria, em sua forma eletrônica, escrita ou falada, são consideradas parte do órgão, tendo este a propriedade legal sobre a informação.

Art. 5º A PSI e suas eventuais políticas específicas serão aplicadas a todas as unidades administrativas do órgão, abrangendo os servidores (efetivos do quadro próprio, comissionados, e efetivos de outros órgãos ou poderes da administração pública - cedidos ou em exercício), prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de informações produzidas ou recebidas por esta Secretaria, estendendo-se àqueles que realize tratamento em nome desta Secretaria ou quem quer que tenha acesso a dados ou informações no ambiente (físico ou virtual) da SCGE.

Art. 6º As eventuais políticas específicas ou procedimentos de segurança da informação da Secretaria devem ser estruturadas com base nas boas práticas usuais do mercado, em especial, pelas normas produzidas pela *International Organization for Standardization* (ISO).

Art. 7º A PSI da SCGE considerará os controles internos de gestão e será apoiada por políticas específicas ou procedimentos dos temas que exigem a implementação de controles de segurança da informação adequados aos riscos identificados, tais como:

a) Avaliação de Conformidade de Segurança da Informação;

b) Backup;

c) Classificação da Informação;

d) Controle de Acesso;

e) Desenvolvimento e Manutenção de Sistemas de Informações Seguros;

f) Dispositivos Móveis e Trabalho Remoto Seguro;

g) Gestão de Continuidade e Mudanças;

h) Gestão de Riscos de Segurança da Informação;

i) Proteção contra Malware e Uso e Instalação de Software;

j) Resposta a Incidentes de Segurança da Informação;

k) Segurança Interna e dos Arquivos Físicos;

l) Uso do Correio Eletrônico.

Art. 8º As políticas específicas deverão estar alinhadas à PSI, além de atualizadas, e serão divulgadas na rede interna da SCGE.

Art. 9º A Política de Proteção de Dados Pessoais Local da SCGE, instituída pela Portaria SCGE nº 026/2021, deve ser considerada, para todos os efeitos, como a Política de Privacidade da SCGE.

Art. 10. Atribui-se as responsabilidades para o gerenciamento da segurança da informação na SCGE aos seguintes atores:

a) Comitê Gestor de Segurança da Informação;

b) Gestor de Processo;

c) Equipe Técnica de SI;

d) Usuários.

Art. 11. O Comitê Deliberativo de Gestão (CDG), instituído pelo Decreto nº 49.993, de 18 de dezembro de 2020, desempenhará as funções de Comitê Gestor de Segurança da Informação (CGSI), competindo-lhe:

I - Promover a disseminação e conscientização da segurança da informação na SCGE;

II - Deliberar sobre os recursos necessários para que ações de segurança da informação sejam executadas;

III - Propor a atualização da Política de Segurança da Informação (PSI), propondo revisão e novas políticas específicas, bem como procedimentos que assegurem o controle das ações de política de segurança da informação.

IV - Acompanhar as atividades do plano de incidentes de segurança da informação tecnológica que comprometam dados e/ou a imagem da SCGE;

V - Deliberar sobre as estratégias para mitigar as possíveis causas das vulnerabilidades exploradas.

Art. 12. O Gestor de Processo corresponde ao responsável pela unidade de execução de um determinado processo de trabalho, cabendo a ele:

I - Gerenciar as informações sob sua competência;

II - Autorizar aos usuários o acesso às informações sob sua competência;

III - Realizar, em conjunto com a Equipe Técnica de SI, a avaliação de riscos de segurança da informação;

IV - Elaborar e informar mudanças de perfis de acessos de sua respectiva área ou setor;

V - Classificar a informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas;

VI - Promover medidas de mitigação de riscos de segurança da informação;

VII - Divulgar práticas e políticas específicas definidas pela SCGE aos usuários sob sua responsabilidade;

VIII - Notificar os incidentes de segurança dos ativos sob sua responsabilidade;

IX - Gerenciar as medidas de mitigação de riscos de segurança da informação e avaliar os seus resultados dos processos sob sua responsabilidade.

Art. 13. A Equipe Técnica de SI será composta pelos colaboradores da área de tecnologia da informação, competindo-lhes:

I - Implementar medidas técnicas de segurança solicitadas com base no valor associado às informações e ao impacto oriundo da perda dessas informações;

II - Promover orientação técnica relacionada à segurança da informação;

III - Realizar, em conjunto com o Gestor de Processo, a avaliação de riscos de segurança da informação;

IV - Acompanhar e analisar as transações e alterações relacionadas à segurança da informação, para fins de rastreamento e auditoria;

V - Realizar, periodicamente, monitoramento de segurança no ambiente tecnológico;

VI - Priorizar medidas preventivas, em detrimento de controles reativos;

VII - Apoiar as ações de capacitação na área de Segurança da Informação;

VIII - Viabilizar monitoração e controles com soluções técnicas que não dependam de processos manuais ou não estejam sujeitas a erros humanos.

IX - Apoiar a definição das medidas técnicas de segurança da informação nas aquisições de bens e na contratação de serviços que envolvam ativos de TIC.

Art. 14. São considerados usuários todos os servidores (efetivos do quadro próprio, comissionados, e efetivos de outros órgãos ou poderes da administração pública - cedidos ou em exercício), prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de informações produzidas ou recebidas por esta Secretaria, estendendo-se àqueles que realizem tratamento em nome deste órgão ou quem quer que tenha acesso a dados ou informações no ambiente da SCGE.

Art. 15. Compete aos usuários:

I - Ter boa utilização dos ativos de informação, prezando sempre pela segurança da informação;

II - Manter-se atualizado sobre as boas práticas e políticas específicas de segurança;

III - Ser responsável por sua senha pessoal;

IV - Evitar expor ou compartilhar informações sigilosas ou restritas;

V - Ter ciência da existência de consequências provenientes do uso inadequado dos sistemas computacionais e de informações.

VI - Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política;

VII - Informar, imediatamente, à Equipe Técnica de TI qualquer falha em dispositivo, serviço ou processo relacionado à segurança da informação para que uma ação seja tomada urgentemente;

VIII - Utilizar as informações como ativo da SCGE e mantê-las disponíveis, conforme orientações da Política de Classificação.

Art. 16. A PSI deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do órgão ou da entidade.

Art. 17. A PSI terá revisões periódicas a cada 3(três) anos, ou quando a Equipe Técnica de SI e/ou o Comitê Gestor de Segurança da Informação (CGSI) achar necessário, para permanecer atualizada com os avanços tecnológicos e fatos que necessitem revisão de controles, ameaças, riscos e diretrizes.

Art. 18. O descumprimento do estabelecido na PSI por parte dos usuários poderá acarretar sanções administrativas disciplinares e/ou contratuais, sem prejuízo das responsabilizações nas esferas civil e criminal.