SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

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 a 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, base de dados, 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, compartilhamento 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 e inesperado que tenha probabilidade de comprometer sistemas

de informação, de redes de computadores ou base de dados;

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: palavra ou ação secreta previamente convencionada entre duas partes como forma de reconhecimento, amplamente utilizada 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 – Garantir a proteção dos ativos de informação da organização;

II – Estabelecer as competências e as atribuições dos atores envolvidos nesta política;

III – Garantir a conformidade com leis e regulamentações de segurança da informação e proteção de dados, nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e da norma ISO 27001;

IV – Buscar minimizar riscos relacionados a incidentes de segurança, como ataques cibernéticos, falhas humanas ou desastres naturais;

V – Promover a cultura de segurança dentro da organização, conscientizando os usuários sobre boas práticas.

Art. 4º Os objetivos da Política de Segurança da Informação se fundamentam nos seguintes pilares:

I – Confidencialidade: garantir que apenas pessoas autorizadas acessem as informações;

II – Integridade: assegurar que os dados não sejam alterados indevidamente;

III – Disponibilidade: garantir que as informações e sistemas estejam acessíveis quando necessário;

IV – Gestão de Riscos: identificar, avaliar e tratar riscos que possam afetar a segurança da informação;

V – Responsabilidade e Rastreabilidade: definir quem faz o quê e manter registros das ações realizadas nos sistemas;

VI – Continuidade do Negócio: garantir que os serviços essenciais continuem funcionando mesmo em situações de crise ou falha.

Art. 5º 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, independentemente do meio ou suporte utilizado, inclusive eletrônico, físico ou verbal, são consideradas parte do órgão, tendo este a propriedade legal sobre a informação.

Art. 6º 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 realizem tratamento em nome desta Secretaria ou quem quer que tenha acesso a dados ou informações no ambiente (físico ou virtual) da SCGE.

Art. 7º As eventuais políticas específicas ou procedimentos de segurança da informação da Secretaria devem ser estruturados com base nas boas práticas usuais do mercado, em especial pelas normas produzidas pela International Organization for Standardization (ISO).

Art. 8º A PSI da SCGE orientará a elaboração de políticas específicas, bem como a implementação de controles de segurança da informação, tais como:

I – Controle de acesso físico e lógico aos sistemas e ambientes de informação;

II – Gestão de riscos relacionados à segurança da informação;

III – Gestão de incidentes de segurança da informação;

IV – Uso seguro de recursos tecnológicos, incluindo redes, dispositivos móveis e mídias removíveis;

V – Auditoria e monitoramento contínuo dos sistemas de informação.

Art. 9º As políticas específicas deverão estar alinhadas à PSI, além de atualizadas, e serão divulgadas na rede interna da SCGE.

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

I – Comitê Gestor de Segurança da Informação (CGSI);

II – Gestor de Processo;

III – Equipe de Segurança da Informação;

IV – Usuários.

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

I – Deliberar sobre os recursos necessários para que ações de segurança da informação sejam executadas;

II – Deliberar, sempre que necessário, sobre questões específicas relacionadas aos controles de segurança da informação;

III – Validar as proposições de 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 a execução do plano de resposta a incidentes de segurança da informação, conforme estabelecido na Instrução de Serviço Interno da SCGE.

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 de Segurança da Informação, 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 confidencialidade, integridade e disponibilidade dessas informações;

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

VII – Garantir o cumprimento das políticas de segurança da informação da SCGE nos processos de suas responsabilidades;

VIII – Assegurar que os processos sob sua responsabilidade estejam em conformidade com as políticas de segurança da informação da Instituição;

IX – Notificar prontamente a Equipe de Segurança da Informação sobre quaisquer incidentes de segurança relacionados aos ativos sob sua responsabilidade;

X – Gerenciar as medidas de mitigação de riscos de segurança da informação e avaliar a eficácia desses processos sob sua responsabilidade.

Art. 13. A Equipe de Segurança da Informação será composta por profissionais qualificados para lidar com a segurança da informação e proteção de dados pessoais, competindo-lhes:

I – Implementar medidas técnicas de prevenção e mitigação de riscos, identificando, analisando e implementando soluções para mitigar riscos de segurança relacionados aos dados pessoais, em conjunto com o Gestor de Processo;

II – Priorizar medidas preventivas, em detrimento de controles reativos;

III – Realizar monitoramento contínuo de segurança no ambiente tecnológico, periodicamente, para:

a) detectar possíveis incidentes de segurança;

b) acompanhar e analisar as transações e alterações relacionadas à segurança da informação, para fins de rastreamento e auditoria;

IV – Criar e implementar políticas de segurança da informação, com foco na proteção dos dados pessoais, garantindo que todos os envolvidos na organização sigam essas diretrizes;

V – Em caso de vazamento ou violação de dados, agir rapidamente para corrigir e comunicar adequadamente a situação aos órgãos reguladores e aos titulares dos dados;

VI – Promover treinamentos regulares para os colaboradores da organização sobre boas práticas de segurança da informação e a importância da proteção dos dados pessoais;

VII – 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, para fins desta Política, todas as pessoas que, no exercício de suas funções ou atribuições, tenham acesso ou realizem qualquer forma de tratamento de informações produzidas ou recebidas pela Secretaria. Incluem-se nesse grupo: servidores efetivos do quadro próprio, servidores comissionados, servidores cedidos ou em exercício provenientes de outros órgãos ou poderes da administração pública, prestadores de serviço, estagiários, colaboradores, consultores externos e quaisquer terceiros que atuem em nome da Secretaria ou que, de alguma forma, tenham acesso aos dados e informações sob sua responsabilidade.

Art. 15. Compete aos usuários, no âmbito de suas atribuições e responsabilidades:

I – Utilizar os sistemas, recursos e informações da Secretaria de forma ética, responsável e conforme as normas vigentes;

II – Proteger os dados e informações sob sua guarda ou aos quais tenham acesso, observando os princípios da confidencialidade, integridade e disponibilidade;

III – Cumprir as diretrizes e normas internas, em conformidade com o estabelecido nesta política e demais instrumentos relacionados ao tratamento de dados e uso de ativos da informação;

IV – Reportar imediatamente à Equipe de Segurança da Informação qualquer incidente de segurança, suspeita de uso indevido de informações ou violação de dados;

V – Zelar pelo sigilo de credenciais de acesso (logins, senhas, chaves ou qualquer outro mecanismo de autenticação), sendo vedado o compartilhamento com terceiros;

VI – Abster-se de acessar, modificar, divulgar ou destruir informações sem a devida autorização ou finalidade compatível com suas atividades institucionais;

VII – Participar de treinamentos, capacitações ou ações de sensibilização promovidas pela Secretaria relacionadas à segurança da informação e proteção de dados;

VIII – Ter ciência das consequências do uso inadequado dos sistemas computacionais, ativos de informação e bases de dados da Secretaria.

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 de Segurança da Informação e/ou o Comitê Gestor de Segurança da Informação (CGSI) julgar 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.

RENATO CIRNE

Secretário da Controladoria-Geral do Estado