INSTRUÇÃO DE SERVIÇO INTERNO SCGE Nº 04/2023

A **SECRETÁRIA DA CONTROLADORIA-GERAL DO ESTADO DE PERNAMBUCO**, no uso das atribuições que lhe são conferidas pela Lei nº 18.139, de 18 de janeiro de 2023,

Considerando a necessidade de promover a adequação de infraestrutura de tecnologia da informação da SCGE-PE à Política Estadual de Segurança da Informação – PESI, instituída no Decreto nº 49.914, de 10 de Dezembro de 2020,

Considerando a necessidade de estabelecer diretrizes para a implementação de processos de gestão de riscos de segurança da informação da SCGE-PE, em observância à Política de Segurança da Informação, definida no Anexo Único da Portaria SCGE nº 14, de 22 de abril de 2022,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º. Instituir a Política de Gestão de Riscos de Segurança da Informação e Privacidade (PGRSIP), como parte integrante da Política de Segurança da Informação da SCGE-PE, com objetivo de:

I - Apoiar a implementação da Política e Segurança da Informação da SCGE-PE;

II - Subsidiar e propiciar a Avaliação de Riscos de Segurança da Informação e Privacidade (SI&P) prevista na Portaria SCGE nº 41/2023, por meio da definição do Método de Avaliação de Riscos de Segurança da Informação (SI&P).

Art. 2º. Para efeitos desta Instrução de Serviço Interna, os conceitos a seguir devem ser considerados por todos os componentes responsáveis pela gestão de riscos de SI&P:

I - Segurança da Informação: medidas de salvaguarda da confidencialidade, integridade, disponibilidade à autenticidade das informações, estejam elas armazenadas ou em trânsito e em sua forma eletrônica, escrita ou falada, abrangendo, inclusive, a segurança dos recursos humanos, das áreas e instalações das comunicações, processamento e armazenamento, assim como as medidas destinadas a prevenir, detectar, deter e documentar eventuais ameaças e incidentes;

II - Privacidade: direito fundamental que tem como virtude o controle que cada pessoa tem sobre as informações que lhe dizem respeito e que circunscrevem sua esfera pessoal, incluindo aspectos relacionados à intimidade e a atos que, embora possam ser externados, ainda

permanecem sob a esfera de controle do próprio indivíduo;

III - Risco: possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos;

IV - Risco Residual: risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos;

V - Gestão de Risco: conjunto de ações e instrumentos que uma entidade coloca em prática para identificar e mitigar riscos relativos ao seu negócio, compreendendo, além das atividades de avaliação de riscos e de monitoramento, os instrumentos de governança e de gestão que suportam a concepção, a implementação, o monitoramento e a melhoria contínua da gestão de riscos;

VI - Política de Gestão de Risco: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;

VII - Apetite a Riscos: quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir;

VIII - Gestor do Processo: colaborador responsável pelo gerenciamento das etapas do processo, pela implementação de melhorias e pelo monitoramento dos indicadores de desempenho, com vistas a assegurar a correta execução das atividades relacionadas e ao alcance dos resultados propostos.

CAPÍTULO II
DA AVALIAÇÃO DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Art. 3º. Define-se como Avaliação de Riscos de Segurança da Informação e Privacidade (SI&P), o processo conduzido pelas estruturas de governança da Administração ou por outros profissionais da entidade, de identificação dos principais riscos enfrentados, de análise dos controles internos estabelecidos e de aferição dos níveis de risco residual, expressos em termos da combinação das consequências e de suas probabilidades.

Art. 4º. A Avaliação de Riscos de SI&P deverá ser implementada de forma gradual em todos os processos que tratam dados pessoais, por meio de ciclos de avaliação executados em intervalos regulares ou sempre que houver mudanças significativas no ambiente de risco, no escopo do sistema de gestão ou nas atribuições da SCGE-PE.

Art. 5º. O Encarregado de dados pessoais, no momento do estabelecimento do escopo das avaliações de risco, deverá observar a ordem de relevância dos processos de negócio estabelecida na elaboração do diagnóstico preliminar prevista na Portaria SCGE nº 41/2023.

Art. 6º. O dirigente máximo do órgão ou da entidade poderá adicionar ou excluir processos e atividades do escopo das avaliações de riscos de SI&P motivando a respectiva ação.

CAPÍTULO III
DO MÉTODO DE AVALIAÇÃO DE RISCOS DE SI&P

Art. 7º. Define-se como Método de Avaliação de Riscos de SI&P, o conjunto ordenado de procedimentos estabelecidos pela SCGE-PE para uniformizar o processo de avaliação dos riscos relacionados à segurança da informação e privacidade de uma organização.

Art. 8º. O Método de Avaliação de Riscos de SI&P proposto nesta PGRSI tem por referência o

Guia de Avaliação de Riscos de Segurança e Privacidade do Governo Federal desenvolvido pela União, cujo modelo foi adaptado à realidade estadual e às regras dispostas na Política de Gestão de Riscos da SCGE-PE.

Art. 9º. O Método de Avaliação de Riscos de SI&P da PGRSI consistirá nas etapas de:

I - Análise do cenário atual, mediante a identificação e avaliação dos riscos relacionados ao sistema de tratamento de dados pessoais;

II - Proposição de novos controles internos que ocasionem melhorias nos processos de negócio, considerando a probabilidade de ocorrência e os impactos decorrentes da materialização dos eventos de risco de inadequação à LGPD e à segurança da informação.

Parágrafo único. Os controles internos previstos no inciso II deverão ser consolidados em um Plano de Implementação de Controles Internos de SI&P que compreenda a definição de atividades, planos, métodos, indicadores e procedimentos interligados para tratar a causa e/ou a consequência do evento de risco.

Art. 10. O Plano de Implementação de Controles Internos de SI&P será monitorado observando o modelo disponibilizado para a planilha de monitoramento prevista no art. 7º do anexo único da Portaria SCGE nº 45/2022, que estabelece a Política de Gestão de Riscos da Secretaria da Controladoria-Geral do Estado.

Art. 11. O Método de Avaliação de Riscos de SI&P proposto por esta Política deverá ater-se aos riscos de privacidade dos dados pessoais sob responsabilidade da SCGE e deverá identificar controles capazes de aperfeiçoar a segurança da informação em relação aos atributos de confidencialidade, integridade e disponibilidade, de maneira que os eventos encontrados sejam reduzidos a níveis aceitáveis, considerando o apetite a risco da Secretaria.

Art. 12. A SCGE deverá detalhar o Método de Avaliação de Riscos de SI&P por meio da elaboração Manual Técnico que contenha, no mínimo:

I - Descrição da metodologia de cálculo da probabilidade, impacto e do nível de risco de SI&P;

II - Listagem e descrição dos Eventos de Risco de SI&P;

III - Listagem e descrição dos Controles Internos de SI&P;

IV - Adequação da metodologia ao Método de Gerenciamento de Riscos Corporativo da SCGE-PE.

CAPÍTULO IV
DOS PAPÉIS E DAS RESPONSABILIDADES

Art. 13. O processo de gestão de riscos de segurança da informação e privacidade é composto pelos seguintes responsáveis:

I - Secretário da Controladoria-Geral do Estado;

II - Encarregado de Dados Pessoais;

III - Diretoria de Tecnologia da Informação do Controle Interno – DTCI;

IV - Assessoria Especial de Controle Interno – AECI;

V - Gestor do Processo;

VI - Conselho Deliberativo de Gestão – CDG.

Art. 14. Compete ao Secretário da Controladoria-Geral do Estado, enquanto representante legal da SCGE-PE, no tocante a presente política:

I - Tomar conhecimento do andamento e dos resultados dos Ciclos de Avaliação de Riscos de SI&P;

II - Tomar conhecimento e aprovar os Planos de Implementação de Controles de SI&P Internos elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão.

Art. 15. Compete ao Encarregado de Dados Pessoais:

I - Instituir e coordenar os Ciclos de Avaliação de Riscos de SI&P;

II - Instituir, coordenar e monitorar os Planos de Implementação de Controles Internos, elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão, e suas revisões;

III - Tomar conhecimento do Método de Avaliação de Riscos de SI&P elaborado pela DTCI.

Art. 16. Compete à Diretoria de Tecnologia da Informação do Controle Interno - DTCI:

I - Apoiar tecnicamente os Gestores do Processo na realização das Avaliações de Riscos de SI&P dos processos priorizados;

II - Apoiar os Gestores do Processo na elaboração dos Planos de Implementação de Controles Internos, elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão, e suas revisões;

III - Definir o Método de Avaliação de Riscos de SI&P e suas revisões;

IV - Elaborar o Manual de Técnico de Avaliação de Riscos de SI&P, e suas revisões.

Art. 17. Compete à Assessoria Especial de Controle Interno - AECI:

I - Apoiar tecnicamente os Gestores do Processo na realização das Avaliações de Riscos de SI&P dos processos priorizados;

II - Apoiar os Gestores do Processo na elaboração dos Planos de Implementação de Controles Internos, elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão, e suas revisões.

Art. 18. Compete aos Gestores de Processos:

I - Realizar, em conjunto com a DTCI, as Avaliações de Riscos de SI&P dos processos priorizados;

II - Elaborar os Planos de Implementação de Controles Internos de SI&P;

III - Implementar as medidas de controle propostas;

IV - Revisar os Planos de Implementação de Controles Internos, quando cabível.

Art. 19. Compete ao Comitê Deliberativo de Gestão - CDG:

I - Tomar conhecimento do andamento e dos resultados dos Ciclos de Avaliação de Riscos de SI&P;

II - Aprovar os Planos de Implementação de Controles Internos elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 20. A SCGE-PE deverá avaliar os controles estratégicos e operacionais implementados de forma contínua, de modo a manter-se adaptada às futuras evoluções e mudanças de atribuições da SCGE-PE.

Art. 21. Quando novos processos forem criados, a avaliação de controles será realizada previamente e poderá resultar na atualização do Plano de Implantação de Controles existente, ou em um novo Plano.

Art. 22. O Processo de Gestão de Riscos de SI&P previsto nesta instrução é parte integrante do Processo de Gestão de Risco da SCGE-PE.

Art. 23. As situações não previstas nesta Instrução de Serviço Interno devem ser apreciadas à luz da Portaria SCGE nº 45, de 18 de novembro de 2022, que aprova a Política de Gestão de Riscos da SCGE-PE

Art. 24. Esta Instrução de Serviço Interno entra em vigor na data de sua publicação no site da Secretaria da Controladoria-Geral do Estado.

Erika Gomes **Lacet**

Secretária da Controladoria-Geral do Estado

Documento assinado eletronicamente por **Erika Gomes Lacet**, em 19/10/2023, às 11:03, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **42363024** e o código CRC **3B40DC81**.

SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

Rua Santo Elias, 535, - Bairro Espinheiro, Recife/PE - CEP 52020-095, Telefone: 3183-0800