ESTADO DO RIO GRANDE DO SUL
MINISTÉRIO PÚBLICO
GABINETE DO PROCURADOR-GERAL DE JUSTIÇA
ASSESSORIA LEGISLATIVA

PROVIMENTO N. 36/2024-PGJ

Institui a Política de Segurança Cibernética e da Informação - PSCI do Ministério Público do Estado do Rio Grande do Sul, cria o Comitê de Segurança Cibernética e da Informação – CSCI e dá outras providências.

O PROCURADOR-GERAL DE JUSTIÇA ALEXANDRE SIKINOWSKI SALTZ, no uso das atribuições que lhe conferem o artigo 109, inciso I, da Constituição do Estado e o artigo 4.º, § 5.º, da Lei Estadual n. 7.669, de 17 de junho de 1982,

CONSIDERANDO a relevância da segurança institucional para o exercício livre e independente das funções atribuídas constitucionalmente ao Ministério Público;

CONSIDERANDO a necessidade de desenvolver uma cultura de segurança no âmbito do Ministério Público do Estado do Rio Grande do Sul que englobe a proteção e a salvaguarda das pessoas, do material, das áreas e instalações e dos ativos de informação;

CONSIDERANDO a necessidade de instituir uma política uniforme de segurança institucional no âmbito do Ministério Público no Estado do Rio Grande do Sul, com o estabelecimento de diretrizes gerais e mecanismos capazes de garantir, em todo Estado, e a despeito das especificidades locais, as condições necessárias para o pleno exercício das atividades da Instituição e de seus integrantes;

CONSIDERANDO o disposto nas normas ABNT NBR 16167:2013 (Segurança da Informação - Diretriz para classificação, rotulação e tratamento da informação), ABNT NBR ISO/IEC 27001/2022 (Segurança da Informação/Segurança Cibernética e Proteção à Privacidade), ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para controles de segurança da informação) e ABNT NBR ISO/IEC 27002:2022 (Segurança da Informação, Segurança Cibernética e Proteção da Privacidade – Controles de Segurança da Informação);

CONSIDERANDO o disposto na Lei n.º 11.419/2006 (Dispõe sobre a informatização do processo judicial), Lei n° 12.527/2011 (Lei de Acesso à Informação), a Lei n° 12.965/2014 (Lei do Marco Civil da Internet) e a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);

CONSIDERANDO o disposto na Resolução n.º 156/2016 do CNMP (Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público), a Resolução n.º 171/2017 do CNMP (Política Nacional de Tecnologia da Informação),

Resolução nº 260/2023 do CNMP (Doutrina de Inteligência do Ministério Público), bem como as boas práticas de governança de dados e segurança da informação;

CONSIDERANDO o disposto no Provimento n.º 54/2018 - PGJ do Ministério Público do Estado do Rio Grande do Sul (Política de Segurança Institucional do Ministério Público do Estado do Rio Grande do Sul) e o Provimento n.º 17/2022 -PGJ do Ministério Público do Estado do Rio Grande do Sul (Disciplina a aplicação da Lei Geral de Proteção de Dados Pessoais – Lei Federal n. 13.709/2018, no âmbito do Ministério Público do Estado do Rio Grande do Sul e cria o Núcleo de Proteção de Dados Pessoais);

CONSIDERANDO o disposto no Guia do Framework de Privacidade e Segurança da Informação, o Guia de Gerenciamento de Vulnerabilidades, o Guia de Avaliação de Riscos de Segurança e Privacidade, o Guia de Requisitos e de Obrigações quanto à Segurança da Informação e Privacidade e o Guia de Resposta a Incidentes de Segurança, todos da plataforma GOV.br;

CONSIDERANDO o atual processo de transformação digital identificado na sociedade contemporânea e o uso da internet por parte do Ministério Público no acesso e tratamento de dados, o que enseja atenção e implementação de política voltada à Segurança Cibernética e da Informação.

RESOLVE, tendo em vista o que consta **no PGEA nº 02434.000.073/2022,** editar o seguinte **PROVIMENTO**:

Capítulo I
Disposições Preliminares

Art. 1.º Este Provimento institui a Política de Segurança Cibernética e da Informação - PSCI no âmbito do Ministério Público do Estado do Rio Grande do Sul - MPRS.

Parágrafo Único. A PSCI é a ação estratégica institucional essencial que protege os sistemas informatizados e os dados sob responsabilidade do Ministério Público do Estado do Rio Grande do Sul, garantindo o exercício contínuo e seguro das atividades funcionais e de gestão.

Art. 2.º A PSCI estabelece princípios, diretrizes e orientações para todos os integrantes do Ministério Público do Rio Grande do Sul.

Art. 3.º A PSCI compreende um conjunto de medidas e instrumentos que visam a prevenir, detectar, tratar e responder às ameaças digitais, por meio de processos e de usuários, com a finalidade de proporcionar a confidencialidade, a integridade, a

disponibilidade, a autenticidade, o não-repúdio e a privacidade dos dados e sistemas do Ministério Público do Estado do Rio Grande do Sul.

Capítulo II
Dos Princípios

Art. 4.º São princípios que regem a Política de Segurança Cibernética e da Informação:

I – proteção aos direitos e garantias fundamentais dos usuários;

II – integração e cooperação interinstitucional para a mitigação e combate às ameaças e às vulnerabilidades cibernéticas;

III – prevenção a incidentes e eventos de segurança cibernética, mediante atuação preventiva, proativa e reativa;

IV - confidencialidade dos dados e informações sigilosas;

V – desenvolvimento de soluções tecnológicas, sistemas e aplicações com foco na segurança, a fim de proteger os dados e informações da instituição;

VI – estabelecimento de padrões para a manutenção constante da Segurança da Informação;

VII – conscientização e capacitação para fomento da cultura da segurança cibernética e da informação;

VIII - acesso mínimo necessário para o exercício das funções;

IX – atualidade dos recursos tecnológicos e das técnicas e processos da segurança cibernética e da informação;

X - orientação à gestão de segurança cibernética e de riscos;

XI - articulação e integração entre as ações de cibersegurança, proteção de dados e ativos de informação;

XII - o elemento humano como peça fundamental e objeto de especial atenção.

Capítulo III
Dos Objetivos

Art. 5.º A PSCI do Ministério Público do Estado do Rio Grande do Sul tem como objetivos:

I – proteger as comunicações internas e externas da Instituição visando à manutenção da disponibilidade, integridade, confidencialidade, autenticidade e privacidade dos ativos de informação do Ministério Público do Estado do Rio Grande do Sul;

II - proteger Dados Sensíveis e Críticos contra acessos não autorizados;

III - prevenir a divulgação, modificação, remoção ou destruição indevida dos dados sob responsabilidade da instituição;

IV – manter a disponibilidade dos sistemas e redes de modo a garantir a continuidade das atividades funcionais da Instituição, mesmo em caso de incidentes de segurança;

V – eleger soluções que propiciem a segurança dos membros, servidores, demais colaboradores e seus familiares;

VI – evitar e prevenir eventos e incidentes de segurança, mediante a mitigação dos riscos e resposta aos incidentes de segurança;

VII – desenvolver e disseminar uma cultura de uso seguro e eficaz dos recursos tecnológicos da instituição;

VIII - ofertar subsídios e definir padrões mínimos para orientar a tomada de decisões e a elaboração de normas, processos, práticas, procedimentos e técnicas de cibersegurança;

IX – estimular a criação de redes de cooperação entre os atores relacionados à segurança cibernética e da informação para a troca de experiências e difusão de boas práticas;

X – buscar a conscientização através de capacitações e treinamentos, a fim de tornar os membros, servidores e demais colaboradores do Ministério Público do Estado do Rio Grande do Sul agentes ativos na prevenção e repressão a ameaças cibernéticas;

XI – ser agente de sustentação do Planejamento Estratégico do Ministério Público do Estado do Rio Grande do Sul.

Capítulo IV
Dos Instrumentos

Art. 6.º São instrumentos prioritários da Política de Segurança Cibernética e da Informação:

I - o Planejamento Estratégico Nacional do Ministério Público e o Planejamento Estratégico do Ministério Público do Estado do Rio Grande do Sul;

II - a Política de Segurança Institucional do Ministério Público do Estado do Rio Grande do Sul;

III - os protocolos, atos normativos e manuais expedidos pelo Ministério Público do Estado do Rio Grande do Sul.

Capítulo V
Do Sistema de Cibersegurança

Art. 7.º O Sistema de Cibersegurança do Ministério Público do Estado do Rio Grande do Sul é formado pelo Comitê de Segurança Cibernética e da Informação - CSCI e pelo Gabinete de Gerenciamento de Crise Cibernética.

Art. 8.º O Comitê de Segurança Cibernética e da Informação, órgão central da administração da PSCI, é composto:

I - pelo Subprocurador-Geral de Justiça de Gestão Estratégica, seu presidente;

II - pelo Coordenador do Núcleo de Inteligência do Ministério Público - NIMP;

III - pelo Coordenador da Divisão de Tecnologia da Informação e Comunicação;

IV – pelo Coordenador da Unidade de Segurança da Informação;

V – por um Promotor-Corregedor indicado pelo Corregedor-Geral do Ministério Público;

VI – por três membros do Ministério Público indicados pela Subprocuradoria-Geral de Justiça de Gestão Estratégica;

VII – por três servidores, indicados pela Subprocuradoria-Geral de Justiça de Gestão Estratégica.

§ 1.º O Comitê reunir-se-á conforme a necessidade e por provocação de seu presidente.

§ 2.º Nos casos de afastamento e/ou impedimento de integrante do CSCI, será indicado substituto pelo Subprocurador-Geral de Justiça de Gestão Estratégica.

Art. 9.º São atribuições do Comitê de Segurança Cibernética e da Informação:

I – estabelecer, alterar e revisar a estratégia de segurança cibernética e da informação;

II – sugerir a adoção de regras e procedimentos relativos à utilização segura dos recursos tecnológicos disponibilizados no âmbito da Instituição;

III – fomentar, planejar, promover a coordenação, a cooperação e a articulação das ações para o cumprimento e acompanhamento da implementação desta Política;

IV - articular-se com as unidades responsáveis pelas áreas afetadas, com o fim de promover e coordenar a mútua cooperação, auxiliando, quando solicitado, na gestão de incidentes de cibersegurança;

V – estabelecer critérios, indicadores e avaliar o nível de maturidade em cibersegurança que permitam monitorar a execução desta PSCI e dos seus instrumentos;

VI - acompanhar a adoção de boas-práticas, bem como o cumprimento dos indicadores definidos para a gestão da cibersegurança, inclusive mediante participação em redes de cooperação do Poder Público;

VII - elaborar instruções, manuais e outros instrumentos de atuação ou orientação na esfera de suas atribuições;

VIII - estabelecer os prazos e os procedimentos de guarda dos históricos de operações realizadas pelos usuários nas redes, sistemas e equipamentos da instituição, bem como o histórico de navegação, downloads e uploads na internet em regulamento próprio;

IX – zelar pelo cumprimento e conformidade da PSCI com os padrões e regulamentações estabelecidos;

X – exercer outras atribuições correlatas que lhe forem conferidas.

Art. 10. Nos casos de situação de alta e crítica violação à segurança cibernética, poderá ser convocado o Gabinete de Gerenciamento de Crise Cibernética, por ato do Procurador-Geral de Justiça.

Parágrafo único. O Gabinete de Gerenciamento de Crise Cibernética será composto obrigatoriamente:

I - pelo Subprocurador-Geral de Justiça de Gestão Estratégica, seu presidente; (Redação conferida pelo Provimento n. 44/2026-PGJ)

II - pelo Coordenador do Gabinete de Inteligência, Segurança e Investigação – GISI, seu coordenador executivo; (Redação conferida pelo Provimento n. 44/2026-PGJ)

III - pelo Coordenador do Núcleo de Inteligência do Ministério Público - NIMP;" (Redação conferida pelo Provimento n. 44/2026-PGJ)

IV - pelo Coordenador da Divisão de Tecnologia da Informação e Comunicação; (Inciso acrescentado pelo Provimento n. 44/2026-PGJ)

V - pelo Coordenador da Unidade de Segurança da Informação; (Inciso acrescentado pelo Provimento n. 44/2026-PGJ)

VI - por um Promotor-Corregedor indicado pelo Corregedor-Geral do Ministério Público; (Inciso acrescentado pelo Provimento n. 44/2026-PGJ)

VII - por três membros do Ministério Público indicados pela Subprocuradoria Geral de Justiça de Gestão Estratégica; (Inciso acrescentado pelo Provimento n. 44/2026-PGJ)

VIII - por três servidores, indicados pela Subprocuradoria-Geral de Justiça de Gestão Estratégica. (Inciso acrescentado pelo Provimento n. 44/2026-PGJ)

Art. 11. Caberá ao Gabinete de Gerenciamento de Crise Cibernética decidir extraordinariamente acerca de medidas urgentes mitigadoras e de resposta aos incidentes de segurança nos casos de:

I – violação de segurança cibernética crítica ou alta que inviabilize ou comprometa o regular funcionamento do Ministério Público do Estado Rio Grande do Sul;

II – vazamento de dados pessoais sob responsabilidade do Ministério Público do Estado do Rio Grande do Sul;

III – violação à confidencialidade, integridade, disponibilidade, autenticidade ou privacidade dos dados e informações sob responsabilidade do Ministério Público do Estado do Rio Grande do Sul;

IV – demais situações que possam comprometer a segurança cibernética e da informação da Instituição.

Art. 12. Poderá ser admitida, por ato fundamentado do Gabinete de Gerenciamento de Crise Cibernética, a colaboração eventual de entidades públicas ou privadas, nas hipóteses em que seja notória a especialização da entidade na área de cibersegurança, com vistas ao atendimento de demandas específicas e delimitadas pelo ato respectivo, tais como:

I – realização de auditorias externas em matéria de cibersegurança;

II – capacitações e treinamentos em cibersegurança para enfrentamento da situação;

III – auxílio técnico no atendimento a incidentes cibernéticos relevantes que extrapolem a capacidade de enfrentamento pelo Ministério Público do Estado do Rio Grande do Sul.

Parágrafo único. Servidores e membros do Ministério Público poderão ser designados, convidados ou convocados para auxílio, orientação e consulta em relação às medidas mitigatórias e de resposta.

Capítulo VI
Diretrizes Gerais

Art. 13. A regulamentação, os processos e a estratégia da utilização das redes, sistemas e equipamentos deverão priorizar mecanismos capazes de garantir a proteção dos sistemas e dos dados sob responsabilidade do Ministério Público do Estado do Rio Grande do Sul, mediante o uso consciente de cada um dos usuários.

Art. 14. Os instrumentos utilizados para garantir a proteção dos sistemas e dos dados têm por objetivo prevenir contra todas as ameaças conhecidas e emergentes.

Art. 15. A utilização dos recursos tecnológicos do Ministério Público do Estado do Rio Grande do Sul deverá ser restrita e necessária à execução do objeto do serviço.

Art. 16. Nas contratações de bens e serviços, convênios e instrumentos congêneres, firmados pelo Ministério Público do Estado do Rio Grande do Sul que exijam

conexão com as redes e sistemas, ou que envolvam tratamento de dados por quaisquer meios, é obrigatória a prévia avaliação da Divisão de Tecnologia da Informação e Comunicação acerca dos riscos à segurança cibernética e da informação e quanto à necessidade de cláusula de confidencialidade.

Seção I
Diretrizes Gerais para o Tratamento da Informação

Art. 17. O trânsito e o manuseio das informações, dentro e fora das redes, e nos sistemas do Ministério Público do Estado do Rio Grande do Sul obedecerão às cautelas necessárias para a proteção dos dados e informações.

Parágrafo único. Na elaboração das rotinas e dos fluxos de trabalho desenvolvidos internamente pelo Ministério Público do Estado do Rio Grande do Sul deverão ser observadas as medidas de segurança da informação aplicáveis à espécie.

Seção II
Da Segurança Física e do Ambiente

Art. 18. A segurança física da infraestrutura da tecnologia da informação tem como objetivo evitar danos à estrutura que sustenta os sistemas e evitar manipulações, inserções, subtrações e acesso aos ativos de informação, bem como assegurar a ampla disponibilidade dos serviços, inclusive com implementação de redundância dos recursos.

Art. 19. Sempre que se mostrar mais vantajoso, deverão ser priorizadas soluções e desenhos de arquitetura que utilizem infraestrutura e serviços em nuvem, consideradas as questões orçamentarias, de segurança e estratégicas.

Art. 20. A escolha e a manutenção dos locais onde se encontram os equipamentos de infraestrutura deverão mitigar e prevenir ameaças ambientais, técnicas e humanas.

Parágrafo único. Deverá ser implementado sistema de controle de acessos a áreas sensíveis dentro da Instituição.

Seção III
Da Gestão de Riscos

Art. 21. O Ministério Público do Estado do Rio Grande do Sul promoverá testes de intrusão, para o fim de avaliar a resiliência das suas redes e sistemas e o tempo de resposta à ação.

§ 1.º Os testes deverão recair prioritariamente sobre os riscos e as ameaças com maior criticidade.

§ 2.º Para fins de execução do disposto no *caput*, poderão ser realizados termos de cooperação com entidades externas ou a contratação de prestadores de serviços especializados na área.

§ 3.º A Divisão de Tecnologia da Informação e Comunicação e a Unidade de Segurança da Informação prestarão, quando solicitado, apoio a testes de intrusão realizados na área de inteligência e contrainteligência.

Art. 22. Os resultados dos testes e análises serão documentados e encaminhados à Subprocuradoria-Geral de Justiça de Gestão Estratégica para análise e providências

Parágrafo único. O documento será armazenado pelo prazo mínimo de 5 (cinco) anos, servindo como objeto de estudo e análise da estratégia de segurança cibernética.

Art. 23. Os testes deverão observar as cautelas necessárias para que eventuais impactos na disponibilidade dos serviços sejam minimizados.

Seção IV
Da Gestão de Incidentes em Segurança Cibernética

Art. 24. Caberá a Unidade de Segurança da Informação documentar os eventos e os incidentes de segurança ocorridos nas redes, sistemas e equipamentos do Ministério Público do Estado do Rio Grande do Sul.

Seção V
Da Gestão de Ativos, do Uso dos Recursos Operacionais e Controles de Acessos

Art. 25. Os usuários das redes e sistemas do Ministério Público do Estado do Rio Grande do Sul terão acesso à internet para a realização de suas funções.

Parágrafo único. A regulamentação quanto aos níveis de acesso e a sua concessão será disciplinada em instrumento próprio e deverá observar a natureza das funções desempenhadas no Ministério Público do Estado do Rio Grande do Sul, respeitando o princípio do acesso mínimo necessário para o exercício da função.

Art. 26. Cabe à Divisão de Tecnologia da Informação e Comunicação prestar manutenção e suporte técnico somente aos equipamentos e softwares de propriedade do Ministério Público do Estado do Rio Grande do Sul.

Seção VI
Da Gestão de Incidentes

Art. 27. Os incidentes de segurança cibernética e da informação classificam-se em:

I - Crítico: todo o incidente de segurança que envolva os Dados Sensíveis e Críticos ou que interrompa a continuidade dos serviços do Ministério Público do Estado do Rio Grande do Sul.

II - Alto: Todo o incidente de segurança que comprometa parcialmente a disponibilidade de serviços, redes, equipamentos e sistemas essenciais ou que diga respeito a acesso, destruição, manipulação ou vazamento de dados sob responsabilidade do Ministério Público do Estado do Rio Grande do Sul.

III - Médio: Todo o incidente de segurança relacionado a tentativas de acessos não autorizados e qualquer incidente que comprometa parcialmente a disponibilidade de serviços, redes, equipamentos e sistemas não essenciais do Ministério Público do Estado do Rio Grande do Sul.

IV - Baixo: Incidentes relacionados ao descumprimento de normas da PSCI que não tenha o potencial de causar relevantes danos a redes, sistemas, equipamentos e dados de responsabilidade do Ministério Público do Estado do Rio Grande do Sul.

Art. 28. Os incidentes críticos e altos serão imediatamente comunicados à Subprocuradoria-Geral de Justiça de Gestão Estratégica para ciência e providências.

Parágrafo único. No caso de incidentes que envolvam dados pessoais ou dados pessoais sensíveis, será comunicado ao Encarregado pelo Tratamento de Dados Pessoais, nos termos da Lei n.º 13.709/2018 - LGPD.

Seção VII
Da Gestão de Continuidade

Art. 29. A Divisão de Tecnologia da Informação e Comunicação elaborará o Plano de Continuidade nos casos de incidentes de segurança e submeterá à análise do CSCI.

Parágrafo único. O plano referido no *caput* conterá os protocolos de resposta e mitigação do incidente, seus planos de teste, os responsáveis pelas ações, o tempo específico para as medidas saneadoras e os seus resultados bem como estratégias para o restabelecimento completo ou parcial das redes e sistemas do Ministério Público do Estado do Rio Grande do Sul.

Seção VIII
Da Auditoria

Art. 30. Serão armazenados, para fins de auditoria, o histórico de operações realizadas pelos usuários nas redes, sistemas e equipamentos da instituição, bem como o histórico de navegação, downloads e uploads na internet.

§ 1º Os dados referidos no *caput* identificarão o usuário pelo *login*, data e local de execução das ações.

§ 2º A responsabilidade do usuário sobre cada operação contida no histórico de utilização será atribuída ao titular da conta de usuário (*login*) que a executou.

Seção IX
Da Responsabilidade do Usuário

Art. 31. Todo o usuário da rede e sistemas do Ministério Público do Estado do Rio Grande do Sul é agente responsável pela segurança cibernética e da informação.

Art. 32. São deveres do usuário:

a) zelar pela segurança física e lógica dos equipamentos e acessórios de informática colocados à sua disposição pelo Ministério Público do Estado do Rio Grande do Sul;

b) manter atualizados e seguros os equipamentos particulares quando utilizados em serviço, a fim de proteger os dados e as informações institucionais;

c) utilizar senhas fortes e exclusivas nos sistemas do Ministério Público do Estado do Rio Grande do Sul;

d) realizar a troca periódica da senha sempre que necessário;

e) utilizar a VPN apenas enquanto estiver realizando atividades de trabalho;

f) solicitar liberação de acesso à VPN de modo antecipado ao CSCI, quando ausente do país;

g) não compartilhar credenciais de sistemas corporativos, ou mesmo se utilizar de credenciais alheias;

h) manter habilitadas e atualizadas as soluções ou políticas de segurança dos equipamentos ou dispositivos institucionais;

i) não desabilitar sistemas de proteção dos equipamentos ou dispositivos institucionais;

j) não conectar equipamento ou dispositivo pessoal que ofereça risco à rede e sistemas institucionais;

k) abster-se de utilizar credenciais de sistemas corporativos, internos e/ou externos, para fins estranhos ao objeto do serviço;

i) informar, ao e-mail apoio@mprs.mp.br, imediatamente, qualquer situação suspeita que possa ensejar incidente de segurança cibernética e da informação, tais como phishing ou spams;

m) informar, ao e-mail apoio@mprs.mp.br, situação de perda, roubo ou extravio de equipamentos, corporativos ou particulares, que contenham dados sensíveis ou críticos vinculados à atividade profissional;

n) descartar documentos e dispositivos eletrônicos que contenham Dados Sensíveis e Críticos de modo definitivo e cujo conteúdo não possa ser recuperado por terceiro;

o) zelar pelo cumprimento desta PSCI e entender suas responsabilidades como ator na proteção dos ativos de informação.

Art. 33. A equipe da Divisão de Tecnologia da Informação e Comunicação poderá, em casos de riscos à segurança da rede, dos sistemas, dos dados e informações, e equipamentos, adotar medidas cautelares e restringir preventivamente o acesso à conta do usuário, equipamentos e recursos.

Parágrafo único. A utilização dos recursos de sistemas de informação, boas práticas e recomendações de uso serão regradas em instrumento próprio.

Art. 34. O uso de equipamentos, plataformas, aplicações, ferramentas e similares que não sejam disponibilizados ou homologados pela Instituição e possam ensejar situação de risco deverão ser previamente submetidos à avaliação da Divisão de Tecnologia da Informação e Comunicação.

Parágrafo único. Os casos excepcionais e de maior complexidade poderão ser submetidos à análise do CSCI.

Art. 35. Eventuais descumprimentos ao disposto nesta seção serão documentados pela Unidade de Segurança da Informação, mediante o envio de relatório à Subprocuradoria-Geral de Justiça de Gestão Estratégica, para a análise e providências.

Art. 36. As violações às disposições desta política e das regulamentações sujeitam o usuário à responsabilidade civil, criminal e administrativo-disciplinar previstas em lei.

Capítulo VII
Das Definições

Art. 37. São considerados Dados Sensíveis e Críticos - DSC:

a) os dados pessoais e dados pessoais sensíveis, conforme definido na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais;

b) os dados produzidos e armazenados pelos setores de inteligência, grupos específicos de combate ao crime organizado, de segurança institucional e de atribuição originária do Procurador-Geral de Justiça;

c) os dados classificados como secretos e ultrassecretos nos termos da Ordem de Serviço 06/2015-PGJ;

d) os dados referentes a procedimentos-administrativo disciplinares de membros e servidores do Ministério Público do Estado do Rio Grande do Sul;

e) os dados cadastrais que possam identificar endereços de membros e servidores do Ministério Público do Estado do Rio Grande do Sul, bem como de seus familiares;

f) qualquer outro quando assim classificado pelo Procurador-Geral de Justiça.

Art. 38. O Glossário de Segurança da Informação do Gabinete de Segurança Institucional, estabelecido pela Portaria GSI/PR n. 93, de 26 de setembro de 2019, será considerado para fins de referência normativa desta Política.

Capítulo IX
Disposições Finais e Transitórias

Art. 39. A presente PSCI deverá ser implementada no prazo de 5 (cinco) anos, consideradas as circunstâncias técnicas, humanas, orçamentárias e estratégicas.

§ 1.º A PSCI será revista a cada 2 (dois) anos ou conforme necessidade verificada antes deste prazo.

§ 2.º O plano de implementação da Política será elaborado a partir de propostas multidisciplinares das unidades da Subprocuradoria-Geral de Justiça de Gestão Estratégica.

Art. 40. Revogam-se as disposições em contrário.

Art. 41. Este Provimento entra em vigor na data de sua publicação.

PROCURADORIA-GERAL DE JUSTIÇA, em Porto Alegre, 7 de junho de 2024.

ALEXANDRE SIKINOWSKI SALTZ,
Procurador-Geral de Justiça.

Registre-se e publique-se.

Gilmar Possa Maroneze,
Procurador de Justiça,
Secretário-Geral.