DIÁRIO OFICIAL
Estado do Rio Grande do Sul

ATOS DO GOVERNADOR

DECRETOS

Atos do Governador

DECRETO

DECRETO Nº 56.804, DE 29 DE DEZEMBRO DE 2022.

Institui a Política de Segurança da Informação do Estado.

O **GOVERNADOR DO ESTADO DO RIO GRANDE SO SUL**, no uso das atribuições que lhe confere o art. 82, incisos V e VII, da Constituição do Estado,

DECRETA:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação, constituída por um conjunto de princípios, objetivos, papéis e diretrizes para a implementação de ações de segurança da informação e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas, no âmbito da administração pública estadual direta, autárquica e fundacional.

§ 1º Os requisitos e diretrizes estabelecidos nesta política são considerados mínimos e obrigatórios, sendo permitida, de acordo com as necessidades de negócio ou das exigências legais, a adoção de medidas mais rígidas.

§ 2º A Política de Segurança da Informação observará o Decreto nº 56.106, de 24 de setembro de 2021, que instituiu a Política de TIC.

Art. 2º Para os efeitos deste Decreto, considera-se:

I - ativos: qualquer coisa que tenha valor para a organização, tais como pessoas, processos, tecnologias e ambientes;

II - autenticação: o processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou que fazem parte de uma transação eletrônica;

III - auditoria: o processo de coleta de evidências de uso dos recursos, para identificar as partes envolvidas em um processo de acesso ou troca de informações;

IV - autorização: o processo de concessão de permissão para acesso às informações, ativos, funcionalidades das aplicações, após a correta identificação e autenticação dos usuários ou dos dispositivos;

V - autenticidade: garantia de que as partes envolvidas (usuários, dispositivos, informações), identificadas em um processo de comunicação como remetentes ou autores, sejam exatamente quem dizem ser;

VI - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

VII - conformidade: processo de garantia de cumprimento de obrigações contratuais com servidores, fornecedores, credores, entre outros, com os aspectos legais e regulatórios relacionados à administração pública estadual;

VIII - conteúdo inadequado: conteúdo obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, de incitação ao ódio e à violência, de teor político-partidário, jogos, correntes e pirâmides, investimentos em bolsa de valores, moedas eletrônicas ou qualquer outro conteúdo contrário ao uso racional e coerente dos ativos de Tecnologia da Informação do Estado e aos princípios da administração pública estadual;

IX - conteúdo ilegal: conteúdo relativo à prática de crimes de racismo, xenofobia, pornografia infantil, violação de direitos humanos, violação de direitos autorais ou qualquer outro que viole as disposições da legislação brasileira vigente;

X - conteúdo nocivo: conteúdo que apresente risco potencial à segurança da informação, como roubo de informações, disseminação de softwares maliciosos, fraudes digitais, entre outros;

XI - criticidade: gravidade do impacto ao negócio, causada pela ausência de um ativo, interrupção de um serviço ou acesso não autorizado a informações;

XII - disponibilidade: todos os ativos de tecnologia da informação, incluindo informações criadas ou adquiridas por um indivíduo ou instituição, deverão estar sempre disponíveis quando requisitado;

XIII - dispositivos móveis: todo e qualquer dispositivo computacional portátil capaz de processar e armazenar informações;

XIV - federação: relação de confiança entre domínios;

XV- ferramentas de Proteção de Rede e de Perímetro: são aquelas compostas por soluções de prevenção à intrusão - IPS-, proteção a ataques de negação de serviço - DDoS -, e de "Firewall";

XVI - irretratabilidade: também conhecida como não repúdio, garante que uma informação existente e autêntica seja irrevogável, bem como que o seu emissor não possa negar a sua autoria;

XVII - incidente de segurança da informação: qualquer acontecimento adverso, confirmado ou sob suspeita, que impacte na segurança da informação dos ativos da organização;

XVIII - integridade: a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la de alterações indevidas por pessoas não autorizadas;

XIX - risco: efeito da incerteza nos objetivos;

XX - severidade: gravidade do dano que determinado ativo pode sofrer devido à exploração de uma vulnerabilidade;

XXI - usuário: pessoa autorizada a utilizar ativos de TIC; e

XXII - vulnerabilidades: são fragilidades presentes ou associadas a ativos que manipulam ou processam informações que, ao serem exploradas por um atacante, permitem a ocorrência de um incidente de segurança.

Art. 3º São objetivos da Política Estadual de Segurança da Informação:

I - promover as ações necessárias à manutenção e à evolução da segurança da informação de maneira uniforme e igualitária entre todos os órgãos e entidades supervisionadas;

II - instituir diretrizes que orientem a correta aplicação dos recursos e processos tecnológicos;

III - definir os papéis e as responsabilidades de forma a promover as atitudes necessárias à construção de uma cultura organizacional voltada à proteção dos ativos tecnológicos;

IV - promover a transversalidade das tecnologias e serviços de Segurança da Informação;

V - promover a preservação dos ativos de informação; e

VI - implementar o Sistema de Gestão de Segurança da Informação no Estado.

Art. 4º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

II - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

III - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

IV - legalidade: qualidade da informação que garante que a informação foi produzida e disponibilizada em conformidade com a legislação vigente;

V - confidencialidade: qualidade da informação que garante que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

VI - clareza: as regras de segurança dos ativos de segurança da informação e comunicações são precisas, concisas e de fácil entendimento;

VII - equanimidade: as normas e regras de segurança da informação são obedecidas por todos, sem distinção de cargo ou função;

VIII - menor privilégio: restringir o acesso às informações ao estritamente necessário ao exercício das funções;

IX - responsabilidade: os agentes públicos têm o dever de conhecer e respeitar todas as normas de segurança da informação e comunicações da Administração Pública Estadual; e

X - auditabilidade: todos os eventos significantes dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento.

Art. 5º A Política Estadual de Segurança da Informação deverá observar:

I - a aderência à Política de TIC deverá ser respeitada e registrada nas Políticas de Segurança da Informação dos órgãos subordinados a esta;

II - a aderência à Política de Segurança da Informação, instituída neste Decreto, deverá ser respeitada e registrada nas Políticas de Segurança da Informação dos órgãos subordinados à Política de TIC;

III - o alinhamento ao Planejamento Estratégico de Governo, ao Planejamento Estratégico de Tecnologia da Informação e Comunicação e ao Plano Diretor de Tecnologia da Informação e Comunicação; e

IV - os custos associados à segurança da informação deverão ser compatíveis com os custos dos ativos a que se deseja proteger, assim como os custos provenientes de prejuízos causados por eventuais incidentes cibernéticos por exploração de vulnerabilidade destes ativos.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 6º São responsabilidades dos usuários:

I - estar ciente e conhecer a política instituída neste Decreto, suas normativas complementares e legislações de referência;

II - zelar pela guarda das informações e permissões que lhe forem concedidas;

III - zelar pelos ativos que lhe forem disponibilizados;

IV - reportar qualquer incidente ou evento que apresente risco de segurança ao seu superior imediato;

V - participar dos cursos de capacitação em segurança da informação disponibilizados pelo Sistema de Governança e Gestão de TIC do Estado; e

VI - evitar o registro ou a reprodução de informações consideradas críticas em meio físico.

Art. 7º São atribuições dos gestores:

I - solicitar acesso, para seus subordinados, aos sistemas em uso no exercício da sua função, respeitando os princípios e as diretrizes desta política;

II - zelar pela correta aplicação das diretrizes instituídas neste Decreto;

III - zelar pela correta aplicação das regras e procedimentos estabelecidos em normativas complementares à Política de Segurança da Informação do Estado;

IV - incentivar a participação, por parte da sua equipe, nos cursos de capacitação em Segurança da Informação, disponibilizados pelo Sistema de Governança e Gestão de TIC do Estado; e

V - agir, sempre que for identificada falha de segurança nos ativos e usuários sob sua responsabilidade, acionando a área de TIC do seu órgão, ou ainda o Comitê de Segurança da Informação do Estado, se necessário.

Art. 8º Além das responsabilidades de usuário elencadas no art. 6º deste Decreto, cabe aos administradores de TIC:

I - implementar níveis de permissão, respeitando o princípio do menor privilégio;

II - minimizar o uso de contas genéricas e não vinculadas a usuários e a administradores;

III - implementar e gerenciar os elementos técnicos necessários à adequada execução desta política e suas normativas complementares; e

IV - atuar como disseminador dos princípios e das diretrizes constantes neste Decreto.

Art. 9º São responsabilidades do Centro de Tecnologia da Informação e Comunicação do Estado do Rio Grande do Sul S.A. - PROCERGS:

I - qualificar a segurança da informação, no âmbito da instituição, com o objetivo de resguardar os ativos do Estado, físicos e virtuais, sob sua responsabilidade;

II - comunicar ao Comitê de Segurança da Informação sobre qualquer incidente de segurança da informação envolvendo os ativos do Estado, físicos e virtuais, sob sua responsabilidade;

III - apoiar os órgãos em suas iniciativas de qualificar a segurança da informação;

IV - apoiar os órgãos quando da identificação de incidentes de segurança da informação e vulnerabilidades técnicas; e

V - apoiar os órgãos na disseminação desta Política e dos conceitos de segurança da informação.

Art. 10. São responsabilidades do Sistema de Governança e Gestão de TIC:

I - manter atualizadas as normativas e os padrões que regem a Política de Segurança da Informação do Estado;

II - fomentar trilhas de capacitação em segurança da informação para os diversos níveis de responsabilidade; e

III - realizar a governança dos ativos transversais de segurança da informação.

CAPÍTULO III

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 11. O Comitê de Segurança da Informação - CSI é órgão colegiado de caráter permanente.

Art. 12. O CSI será composto por especialistas técnicos indicados pelos seguintes órgãos:

I - Secretaria de Planejamento, Governança e Gestão;

II - Secretaria da Casa Civil;

III - Procuradoria-Geral do Estado;

IV - Secretaria da Fazenda;

V - Secretaria da Inovação, Ciência e Tecnologia; e

VI - Secretaria da Segurança Pública.

Parágrafo único. A presidência do Comitê de Segurança da Informação será definida a partir de deliberação do colegiado, em reunião ordinária, por maioria simples.

Art. 13. Compete ao Comitê de Segurança da Informação:

I - propor as estratégias, as diretrizes e as orientações quanto à segurança da informação;

II - propor padrões de TIC dentro da sua área de atuação;

III - monitorar a Política de Segurança da Informação;

IV - assessorar o Sistema de Governança e Gestão de TIC na implementação das ações de segurança da informação;

V - fornecer subsídios aos gestores e aos demais Comitês nas decisões relativas à segurança da informação;

VI - revisar periodicamente e propor alterações na Política de Segurança da Informação e nos demais documentos normativos relacionados à Política;

VII - propor a criação de grupos de trabalho para estudar e propor soluções específicas sobre segurança da informação;

VIII - propor investimentos relacionados à segurança da informação, com o objetivo de reduzir os riscos e melhorar a resolução de incidentes de segurança;

IX - avaliar as Políticas de Segurança da Informação dos órgãos e das entidades supervisionadas quanto à aderência a esta Política e a Política de TIC;

X - promover ações de capacitação em segurança da informação;

XI - monitorar os incidentes, riscos e vulnerabilidades;

XII - promover ações para mitigação de riscos de segurança da informação;

XIII - promover ações para eliminar vulnerabilidades; e

XIV - atender ao Sistema de Governança e Gestão de TIC sempre que acionado.

CAPÍTULO IV

DAS DIRETRIZES DA POLÍTICA ESTADUAL DE SEGURANÇA DA INFORMAÇÃO

Art. 14. O acesso aos ativos de informação do órgão ou da entidade deve ser precedido de adesão formal aos termos desta normativa, mediante assinatura de termo de responsabilidade pelo servidor.

Art. 15. São diretrizes para resposta a incidentes de TIC:

I - o Sistema de Governança e Gestão de TIC, por intermédio do Comitê de Segurança da Informação, publicará

normativa padronizando o processo de resposta a incidentes de Segurança da Informação;

II - a Política de Segurança da Informação do órgão deverá prever a criação e a manutenção do registro de eventos de segurança da informação;

III - os registros de evento de segurança da informação deverão ser classificados como informação de uso interno, restrito ou confidencial; e

IV - as informações dos registros de evento de segurança da informação devem ser protegidas contra o acesso não autorizado e contra possível adulteração.

Art. 16. São diretrizes para a gestão de incidentes de segurança da informação:

I - a gestão de incidentes de segurança da informação compreenderá os seguintes processos:

a) solução de incidentes;

b) mitigação das consequências de incidentes;

c) criação de protocolos e padrões próprios; e

d) monitoria das ações e protocolos implementados.

II - o Sistema de Governança e Gestão de TIC, por intermédio do CSI, deverá estabelecer metodologia que possibilite a identificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos incidentes de segurança da informação, observando:

a) os registros de evento de segurança da informação deverão ser classificados como informação de uso interno, restrito ou confidencial;

b) o acesso externo será permitido apenas na forma da Lei Federal nº 12.527, de 18 de novembro de 2011, que é regulamentada no âmbito do Governo do Estado pelo Decreto nº 49.111, de 16 de maio de 2012; e

c) as informações deverão ser disponibilizadas ao CSI sempre que solicitado.

III - os órgãos e as entidades subordinados a política de TIC, com apoio do Sistema de Governança e Gestão de TIC, deverão implementar e executar as atividades de gestão de incidentes de segurança da informação associadas aos ativos de informação sob sua responsabilidade; e

IV - a gestão incidentes de segurança da informação deverá estar alinhada e integrada à gestão de riscos e à gestão de vulnerabilidades técnicas.

Art. 17. São diretrizes para classificação das informações:

I - a classificação da informação deverá estar aderente à legislação vigente incluindo, mas não limitado a:

a) Lei Federal nº 12.527/2011, regulamentada no âmbito da administração pública estadual pelo Decreto nº 49.111/2012, e pelo Decreto nº 53.164, de 10 de agosto de 2016; e

b) Decreto nº 53.164, de 10 de agosto de 2016, que regulamenta, no âmbito da administração pública estadual, os procedimentos para a classificação de informações.

Art. 18. São diretrizes para uso da internet:

I - o acesso à internet deverá ser monitorado e gerenciado;

II - deverão ser aplicados, sempre que possível, ferramentas de proteção de rede e de perímetro;

III - os níveis de permissão de acesso deverão estar de acordo com as atribuições dos usuários; e

IV - deverão ser bloqueados os acessos aos conteúdos considerados inadequados, ilegais, ou que ofereçam riscos à segurança da informação.

Art. 19. São diretrizes para uso do correio eletrônico:

I - a ferramenta de correio eletrônico oficial do Estado deverá ser utilizada apenas para fins institucionais, sendo vedado o uso de correios privados para este fim;

II - é vedado o uso do correio eletrônico corporativo para fins particulares, tais como redes sociais, estabelecimentos comerciais, ou qualquer outro serviço não diretamente vinculado ao exercício de suas funções;

III - o serviço de correio eletrônico deverá contar com cópia de segurança conforme diretrizes do art. 26 deste Decreto;

IV - o acesso às mensagens é restrito ao remetente e ao destinatário, sendo estas invioláveis, salvo por determinação administrativa autorizada pela autoridade máxima da pasta (ou autoridade equivalente) ou por motivo de segurança institucional;

V - a Política de Segurança da Informação do órgão deverá contemplar os métodos e protocolos seguros para acesso ao serviço de correio eletrônico;

VI - é proibido o envio e recebimento de mensagens de conteúdo impróprio relativo à pornografia, racismo, xenofobia, violência, incitação ao ódio, invasão de computadores, propaganda político-partidária, jogos de azar, correntes e pirâmides, investimentos privados, por meio da estrutura de correio eletrônico do Estado; e

VII - é vedado o redirecionamento automático, de e-mail, para caixas particulares.

Art. 20. São diretrizes para uso de ferramentas de colaboração e produtividade:

I - a ferramenta de colaboração e produtividade oficial do Estado deverá ser utilizada apenas para fins institucionais;

II - deverá ser priorizado o uso da ferramenta de colaboração e produtividade oficial do Estado, conforme resolução do Sistema de Governança e Gestão de TIC;

III - é permitido o uso de ferramentas parceiras, não homologadas para tráfego e/ou registro de informações classificadas como públicas, respeitando o que estabelece o art. 19 desta política, observando-se que são consideradas homologadas as ferramentas de fornecedores com contrato celebrado com o Estado;

IV - é permitida a federação entre ferramentas de colaboração, com outros entes públicos ou privados, desde que com prévia anuência do CSI;

V - o compartilhamento de informações classificadas como públicas, com usuários fora do domínio do Estado, por meio de "links" ou pastas, deve atender às diretrizes deste Decreto.

VI - será permitida a troca de informações sigilosas entre entes públicos, para efeito de suas atribuições institucionais, e desde que previsto em instrumento legal;

VII - é pré-requisito para inclusão de usuários do tipo convidado, não servidores do poder executivo estadual, a formalização da indicação dos mesmos; e

VIII - o nível de formalização dependerá da criticidade das informações contidas nos grupos e equipes que o convidado fará parte.

Art. 21. São diretrizes para uso de dispositivos móveis:

I - a Política de Segurança da Informação do órgão, quando tratar de dispositivos móveis corporativos, deverá considerar os seguintes aspectos:

a) a administração e configuração dos recursos de segurança do equipamento deverão ser centralizadas na Tecnologia da Informação -TI - do órgão;

b) o equipamento deverá estar apto ao monitoramento e ao atendimento remoto; e

c) sempre que possível, deve-se utilizar recursos de rastreamento.

II - a Política de Segurança da Informação do órgão, quando tratar de dispositivos móveis próprios do servidor, deverá considerar os seguintes aspectos:

a) requisitos mínimos de segurança conforme os incisos V e VI do art. 25 deste Decreto; e

b) requisitos de segurança, para a realização de atividades que envolvam informações classificadas como críticas ou pessoais.

Art. 22. São diretrizes para a gestão de ativos de tecnologia da informação:

I - os ativos de tecnologia da informação pertencem ao órgão, podendo ser realocados a qualquer tempo, no âmbito da organização, por necessidade de serviço;

II - os ativos do Estado deverão ser utilizados para realização de atividades relacionadas às competências da organização;

III - para os casos em que o órgão mantém infraestrutura de servidores de aplicação e arquivos, deverá ser assegurada a segurança física de acesso aos recursos;

IV - o órgão deverá manter atualizado o inventário de ativos de TI;

V - a gestão de ativos é responsabilidade da área de tecnologia da informação do órgão;

VI - as informações produzidas e mantidas, resultantes da atividade da organização, são consideradas ativos de propriedade do Estado, sendo seu conteúdo de responsabilidade da área gestora, devendo sua classificação observar as diretrizes elencadas no art. 20 deste Decreto;

VII - o processo de descarte de ativos deverá garantir a inutilização de dispositivos de armazenamento ou a eliminação segura dos dados neles contidos; e

VIII - deverão ser utilizados recursos de criptografia, sempre que possível, para a proteção do armazenamento e tráfego de dados.

Art. 23. São diretrizes para controle de acesso:

I - permissões de acesso devem respeitar o princípio do menor privilégio, garantindo apenas o acesso aos recursos necessários para realização de uma dada tarefa, pelo tempo necessário ao desempenho desta tarefa;

II - deverá ser minimizado o uso de contas genéricas e não vinculadas a usuários e a administradores;

III - a Política de Segurança da Informação do órgão deverá prever as condições necessárias para acesso aos recursos de TIC incluindo, mas não limitado a:

a) termo de responsabilidade, contendo a ciência aos termos desta Política; e

b) curso de capacitação em segurança da informação condizente com as atribuições do cargo e dos recursos disponibilizados.

IV - a Política de Segurança da Informação do órgão deverá estabelecer as regras para permissão de acesso incluindo, mas não limitado a:

a) requisitos para a autorização formal de pedidos de acesso;

b) procedimentos para remoção de direitos de acesso;

c) regras bem definidas para o acesso privilegiado;

d) regras para renovação de permissões sempre que ocorrer a movimentação/remoção do servidor; e

e) obrigatoriedade ou não do uso de múltiplo fator de autenticação, salvo disposição específica do CSI.

V- a Política de Segurança da Informação do órgão deverá estabelecer as regras para gestão de senhas incluindo, mas não limitado a:

a) nível mínimo de complexidade;

b) prazo para renovação; e

c) tamanho da senha.

VI - todos os acessos devem ser rastreáveis para que o usuário seja identificado individualmente; e

VII - os processos de concessão ou remoção de acesso deverão, preferencialmente, ser iniciados na área de Recursos Humanos da organização.

Art. 24. São diretrizes para cópia de segurança:

I - o tempo de guarda e frequência das rotinas de cópia de segurança deverão ser proporcionais e compatíveis com a criticidade das informações a serem protegidas;

II - o tempo de guarda, sempre que possível, deverá atender as normativas específica incluindo, mas não limitado a:

a) Instrução Normativa nº 01/2017 do Sistema de Arquivos do Estado do Rio Grande do Sul - SIARQ/RS, que dispõe sobre o Plano de Classificação de Documentos - PCD e a Tabela de Temporalidade de Documentos - TTD, para os órgãos da administração pública direta do Estado; e

b) Lei Federal nº 13.709, de 14 de agosto de 2018, regulamentada, no âmbito do Estado, pelo Decreto nº 55.986/2021 e pelo Decreto nº 55.987/2021.

III - a Política de Segurança da Informação do órgão deverá estabelecer a frequência, o tempo de guarda e a periodicidade de testes das cópias de segurança armazenadas;

IV - as cópias de segurança deverão receber segurança física e lógica compatível com a criticidade das informações armazenadas; e

V - recomenda-se a guarda de cópia de segurança em meio físico externo, ou por meio de adoção de mecanismos de proteção contra sequestro de dados; e

VI - deve-se observar distância geográfica suficiente para escapar dos danos de um desastre ocorrido no local principal.

Art. 25. São diretrizes para trabalho remoto:

I - os ativos tecnológicos do Estado, em uso no trabalho remoto, deverão ser utilizados para realização de atividades relacionadas às competências da organização;

II - é vedado o uso dos ativos tecnológicos do Estado por terceiros;

III - os ativos de tecnologia da informação, disponibilizados para uso em trabalho remoto, pertencem ao órgão, podendo ser solicitada a devolução a qualquer tempo;

IV - as atividades realizadas durante o trabalho remoto serão acompanhadas para fins de auditoria;

V - sempre que possível, o acesso remoto aos ativos do Estado deverá considerar a utilização de múltiplo fator de autenticação;

VI - equipamentos próprios, que serão utilizados no trabalho remoto, deverão ser providos com os seguintes requisitos mínimos de segurança, mas não limitado a:

a) sistema operacional regularizado e atualizado;

b) proteção de antivírus atualizada; e

c) "Firewall" ativo.

Art. 26. São diretrizes para contratação de serviços de TIC:

I - todos os contratos de prestação de serviços conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política de Segurança da Informação;

II - todos os contratos de prestação de serviços conterão cláusula específica sobre aderência à Lei Federal nº 13.709/2018 e as suas legislações complementares;

III - as tecnologias a serem contratadas deverão ser compatíveis com a arquitetura digital do Estado;

IV - sistemas operados em ambientes externos à infraestrutura de rede do Estado à segurança da informação,

preferencialmente, pela PROCERGS; e

V - contratos de desenvolvimento deverão, preferencialmente, utilizar métodos de desenvolvimento de "softwares" seguros.

Parágrafo único . As diretrizes estabelecidas neste artigo também se aplicam a prestação de serviços em nuvem.

Art. 27. São diretrizes para a comunicação da segurança da informação:

I - a Política de Segurança da Informação do órgão ou da entidade deverá estar disponível para consulta dos usuários a qualquer tempo;

II - a Política de Segurança da Informação do Estado, suas referências e normativas assessórias, deverão ser disponibilizadas para consulta dos usuários a qualquer tempo;

III - sempre que possível, deverão estar disponíveis, aos usuários, materiais de capacitação em segurança da informação abrangendo, mas não limitado a:

a) capacitação básica em segurança da informação para todos os usuários;

b) segurança da informação para lideranças;

c) pré-requisitos e boas práticas de segurança da informação para o teletrabalho; e

d) princípios básicos da classificação da informação.

CAPÍTULO V

DA GESTÃO DE VULNERABILIDADES E DE RISCOS

Art. 28. A gestão de vulnerabilidades técnicas compreende os seguintes processos:

I - identificação de vulnerabilidades;

II - proposição de ações de melhoria;

III - criação de protocolos e padrões próprios; e

IV - monitoria das ações e protocolos implementados.

§ 1º O Sistema de Governança e Gestão de TIC, por intermédio do CSI, deverá estabelecer metodologia que possibilite a identificação, a priorização, o tratamento, a comunicação e a monitoração periódica das vulnerabilidades técnicas.

§ 2º Os órgãos e as entidades subordinados à política de TIC, com apoio do Comitê de Segurança da Informação, deverão implementar e executar as atividades de gestão de vulnerabilidades técnicas associadas aos ativos de informação sob sua responsabilidade.

§ 3º A gestão de vulnerabilidades técnicas deverá estar alinhada e integrada à gestão de riscos e à gestão de incidentes de segurança da informação.

Art. 29. A gestão de riscos compreende os seguintes processos:

I - identificação de ameaças;

II - realização de análises de impacto;

III - priorização ações de mitigação dos riscos;

IV - criação protocolos e padrões próprios; e

V - monitoria das ações e protocolos implementados.

§ 1º O Sistema de Governança e Gestão de TIC, por intermédio do CSI, deverá estabelecer metodologia que possibilite a identificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

§ 2º Os órgãos e as entidades subordinados à política de TIC, com apoio do CSI, deverão implementar e executar as atividades de gestão dos riscos de segurança da informação e de comunicações associados aos ativos de informação sob sua responsabilidade.

§ 3º A gestão de riscos deverá estar alinhada e integrada à gestão de vulnerabilidades técnicas e à gestão de incidentes de segurança da informação.

§ 4º A gestão de risco deverá estar alinhada com o planejamento estratégico de TIC do Estado.

§ 5º As ações de gestão de risco devem ser implementadas nos níveis de tecnologia, de processos e de pessoas.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 30. As ações que violem esta Política de Segurança da Informação poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 31. Este Decreto entra em vigor na data de sua publicação.

PALÁCIO PIRATINI , em Porto Alegre, 29 de dezembro de 2022.

RANOLFO VIEIRA JÚNIOR ,

Governador do Estado.

Registre-se e publique-se.

PAULO ROBERTO DIAS PEREIRA,

Secretário-Chefe da Casa Civil, Adjunto.

RANOLFO VIEIRA JÚNIOR
Praça Marechal Deodoro, s/nº, Palácio Piratini
Porto Alegre

RANOLFO VIEIRA JÚNIOR
Governador do Estado
Praça Marechal Deodoro, s/nº
Porto Alegre
Fone: 5132104100

Publicado no Caderno do Governo (DOE) do Rio Grande do Sul
Em 30 de Dezembro de 2022

Protocolo: **2022000808172**

Publicado a partir da página: **10**