

Política de Segurança da Informação

Anexo Único
2ª Edição
Agosto/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BRUNO CAMPOS PEREIRA

Controlador-Geral do Estado

DANIELA QUEIROZ ROCHA

Chefe de Gabinete

THIAGO COUTO LAGE

Subcontrolador-Geral do Estado

DÉBORA TAVARES DURSO

Auditora-Geral do Estado

ALLAN COSTA DOS REIS

Corregedor-Geral do Estado

EUGENIO MANUEL DA SILVA MACHADO

Ouvidor-Geral do Estado

Elaborado por:

Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI (Resolução CGE nº 376, de 19 de setembro de 2025).

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

COMITÊ INTEGRADO DE GOVERNANÇA DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

Gabinete da Controladoria Geral do Estado

Thiago Augusto de Azevedo Cavalcante

Suplente: Luiz Flavio Mathias de Mello Moraes

Subcontroladoria Geral do Estado

Letícia Spínola Flávio

Suplente: Suelen Aparecida Rodrigues de Oliveira

Corregedoria Geral do Estado

Camila Alves Ribeiro

Suplente: Beatriz Lage Brum

Auditoria Geral do Estado

Marcus Vinícius dos Santos

Suplente: Daniella Kircher

Ouvidoria e Transparência Geral do Estado

Tiago Nunes Figueiredo

Suplente: Myrla Raianne Ferreira dos Santos

Diretoria Geral de Administração e Finanças

Luiz Augusto Guimarães Silva

Suplente: Patrícia Viçoso Figueiredo

Assessoria de Planejamento e Orçamento

Jorge Pereira da Silva

Suplente: Maria Victória Silveira de Andrade Cordeiro

Assessoria de Tecnologia da Informação

Claudio José Ascenção de Andrade

Suplente: Roberta da Silva Macedo Mello

Gestor de Segurança da Informação

Daiene dos Santos Costa

Suplente: Renato Mattos Miragaia

Encarregado Setorial pelo Tratamento de Dados Pessoais

Rafael Antônio da Silva Vianna

Suplente: Myrla Raianne Ferreira dos Santos.

DOCUMENTO PÚBLICO

Este documento é classificado como público e pode ser acessado e compartilhado livremente, observadas as normas e legislações vigentes. As informações nele contidas destinam-se à divulgação das práticas e diretrizes de gestão de riscos adotadas pelo órgão. Sua reprodução é permitida, desde que preservada a integridade do conteúdo e mencionada a fonte institucional. Alterações que comprometam o significado ou a finalidade das informações são de responsabilidade de seus autores.

CONTROLE DE VERSÃO

Data	Versão	Autor	Alteração	Responsável
23/10/2025	1.0	Controladoria Geral do Estado do Rio de Janeiro	Elaboração da Política de Segurança da Informação	Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI
14/08/2026	2.0	Controladoria Geral do Estado do Rio de Janeiro	Revisão Geral da Política de Segurança da Informação	Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI

SUMÁRIO

CAPÍTULO I - ESCOPO	6
Seção I – Finalidade	6
Seção II – Princípios	7
Seção III - Estrutura Normativa	8
Seção IV – Abrangência	8
CAPÍTULO II – REFERÊNCIAS LEGAIS E NORMATIVAS	8
CAPÍTULO III – TERMOS E DEFINIÇÕES	11
CAPÍTULO IV – PAPÉIS E RESPONSABILIDADES	15
CAPÍTULO V - Diretrizes	25
Seção I - Gestão de acesso	25
Seção II - Uso aceitável dos ativos de informação	26
Seção III - Trabalho remoto e uso de dispositivos móveis	28
Seção IV - Ambiente físico	29
Seção V - Classificação da informação	29
Seção VI - Transferência da informação	30
Seção VII – Privacidade	31
Seção VIII - Códigos maliciosos	32
Seção IX – Fornecedores	32
Seção X - Serviços em nuvem	32
Seção XI - Incidentes de segurança e de privacidade	33
Seção XII - Vulnerabilidades técnicas	33
Seção XIII - Inteligência de ameaças	34
Seção XIV - Controles criptográficos e gerenciamento de chaves	34
Seção XV - Registro de auditoria	34
Seção XVI - Desenvolvimento de software	35
Seção XVII - Cópia de segurança	35
Seção XVIII - Continuidade do negócio	35
Seção XIX - Uso de dispositivo pessoal no trabalho	35
CAPÍTULO VI – Documentos Complementares	36
CAPÍTULO VII - Processo Disciplinar	37

CAPÍTULO VIII - Vigência.....	37
REFERÊNCIAS	38

CAPÍTULO I - ESCOPO

Seção I – Finalidade

Art. 1º Esta Política de Segurança da Informação tem como finalidade estabelecer as responsabilidades, deveres e penalidades relacionados à proteção da informação, promovendo uma cultura organizacional voltada à preservação da confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações sob a custódia da Controladoria Geral do Estado do Rio de Janeiro (CGE/RJ), abrangendo dados e ativos de Informação do governo, do cidadão, de outros órgãos e entidades públicas, de fornecedores e de quaisquer partes envolvidas em acordos institucionais com a CGE/RJ.

Seção II – Princípios

Art. 2º As diretrizes desta Política aplicam-se a todo o ciclo de vida da informação — incluindo criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte — e são fundamentadas nos seguintes princípios:

- I. **confidencialidade:** garantia de que a informação seja acessível apenas a pessoas, entidades ou processos devidamente autorizados;
- II. **integridade:** garantia de que a informação esteja correta, completa e protegida contra alterações indevidas
- III. **disponibilidade:** garantia de que a informação esteja acessível e utilizável sempre que necessária, por pessoas, entidades ou processos autorizados;
- IV. **autenticidade:** garantia da identidade e origem legítima da informação e de seus responsáveis;

- V. **legalidade:** garantia de que o tratamento da informação observe as legislações vigentes e aplicáveis, especialmente as relacionadas à proteção de dados pessoais e à transparência pública.

Seção III - Estrutura Normativa

Art. 3º A estrutura normativa da Segurança da Informação na CGE/RJ é composta por esta Política e poderá ser complementada por normas específicas, procedimentos operacionais e instruções de trabalho, conforme a necessidade e a evolução dos processos institucionais.

Art. 4º Os procedimentos operacionais serão elaborados conforme previsto nesta Política ou quando identificada a necessidade de detalhamento técnico, visando orientar a aplicação de métodos, tecnologias e controles no âmbito da segurança da informação é da privacidade.

Art. 5º As normas complementares e os procedimentos operacionais deverão ser desenvolvidos de forma progressiva, após a aprovação e publicação desta Política. Todos os documentos relacionados à estrutura normativa devem ser revisados, no mínimo, anualmente ou sempre que houver atualizações legais, normativas ou tecnológicas relevantes.

Art. 6º Esta Política constitui instrumento normativo que define regras e responsabilidades a serem observadas por todos os envolvidos nas atividades institucionais, fornecendo direcionamento claro para aplicação das medidas de segurança da informação.

Art. 7º A estrutura desta Política abrange diretrizes, normas, procedimentos e instruções de trabalho, alinhada às melhores práticas em segurança da informação.

Seção IV – Abrangência

Art. 8º Esta Política aplica-se a todos os públicos que mantenham vínculo direto ou indireto com a CGE/RJ, incluindo servidores, consultores, dirigentes, estagiários, fornecedores, trabalhadores terceirizados, visitantes e demais partes envolvidas em acordos institucionais.

CAPÍTULO II – REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 9º Esta política foi estabelecida a partir das seguintes referências normativas e legais:

- I. **A Constituição da República Federativa do Brasil, de 05 de outubro de 1988**, com destaque ao art. 37, caput, o qual dispõe que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência;
- II. **A Lei federal nº 9.507, de 12 de novembro de 1997** (Lei do Habeas Data);
- III. **Lei nº 12.527, de 18 de novembro de 2011** (Lei de Acesso à Informação);
- IV. **Lei nº 12.965, de 23 de abril de 2014** (Marco Civil da Internet);
- V. **Lei nº 13.709, de 14 de agosto de 2018** (Lei Geral de Proteção de Dados Pessoais);
- VI. **A Medida Provisória nº 1.317, de 17 de setembro de 2025** que Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências;
- VII. **A Lei Estadual nº 7.989, de 14 de junho de 2018** que dispõe sobre o sistema de controle interno do Poder Executivo do estado do Rio de Janeiro, cria a Controladoria Geral do Estado do Rio de Janeiro e o Fundo de Aprimoramento de Controle Interno, organiza as carreiras de controle interno, e dá outras providências;

- VIII. **Decreto-Lei nº 220, de 18 de julho de 1975** - Regime Jurídico dos Funcionários Públicos Cíveis do Poder Executivo do Estado do Rio de Janeiro;
- IX. **Decreto estadual nº 2.479, de 08 de março de 1979** - Regulamento do Estatuto dos Funcionários Públicos Cíveis do Poder Executivo do Estado do Rio de Janeiro;
- X. **Decreto nº 43.583, de 11 de maio de 2012** (Código de Ética Profissional do Servidor Público Civil do Poder Executivo do Estado do Rio de Janeiro);
- XI. **Decreto estadual nº 46.475, de 25 de outubro de 2018** que regulamenta, no âmbito do Poder Executivo estadual, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, em conformidade ao disposto na Lei nº 12.527, de 18 de novembro de 2011;
- XII. **Decreto estadual nº 48.209, de 19 de setembro de 2022** que regulamenta a Lei Estadual nº 5.427, de 01 de abril de 2009, no que dispõe sobre a produção e tramitação eletrônica de documentos e processos administrativos na Administração Pública Estadual, e dá outras providências;
- XIII. **Decreto estadual nº 48.891, de 10 de janeiro de 2024** que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, em conformidade com a lei federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- XIV. **Resolução CGE nº 265, de 29 de fevereiro de 2024** que atualiza o programa especial de gestão de trabalho remoto - PEGTR, no âmbito da controladoria geral do estado, e dá outras providências;

- XV. **Resolução CGE nº 376, de 28 de julho de 2025** que cria o Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado – **CGTI**;

- XVI. **Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021** que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro - EGTIC/RJ, notadamente o art. 1º, IV, que prevê a instituição de Instruções Normativas para a efetivação da Governança de Tecnologia da Informação e Comunicação no Estado do Rio de Janeiro, bem como o art. 11, do Anexo B, que trata de ações de governança voltadas à segurança da informação e à proteção de dados;

- XVII. **Instrução Normativa PRODERJ/PRE nº 5, de 20 de março de 2024** que regulamenta os procedimentos para contratação e celebração de acordos envolvendo soluções de tecnologia da informação e comunicação - TIC, assim como para o desenvolvimento de softwares e aplicativos a serem observados pelos órgãos e entidades integrantes da administração direta e indireta do poder executivo do estado do rio de janeiro;

- XVIII. **Instrução Normativa PRODERJ/PRE nº 07, de 29 de maio de 2025** que regulamenta os procedimentos de segurança da informação em soluções de tecnologia da informação e comunicação - TIC a serem adotados pelos órgãos e entidades integrantes da administração direta e indireta do Poder Executivo do Estado do Rio de Janeiro;

- XIX. **A NORMA ABNT NBRISO/ IEC27701:2019** –Técnicas de segurança para gestão da privacidade da informação;

- XX. **ANORMA ABNT NBRISO/IEC27001:2022**–Segurança da informação, segurança cibernética e proteção à privacidade – Sistema de Gestão de Segurança da Informação;

- XXI. **ANORMA ABNT NBRISO/IEC27002:2022**–Segurança da informação, segurança cibernética e proteção à privacidade – Controles de Segurança da Informação.

CAPÍTULO III – TERMOS E DEFINIÇÕES

Art. 10. Para os fins desta Política, aplicam-se as seguintes definições:

- I. **acesso básico:** acesso concedido aos ativos de informação de uso comum a todos os servidores, estagiários, fornecedores e trabalhadores terceirizados, cuja gestão de acesso é de responsabilidade da CGE/RJ;
- II. **ameaça:** fator interno e externo, intencional ou não, com potencial para causar dano a um ativo de informação por meio da exploração de uma vulnerabilidade;
- III. **ameaça cibernética:** ameaça deliberada, em ambiente digital, caracterizada por ações ou mecanismos maliciosos conduzidos por agentes externos, como *hackers*;
- IV. **ativo de informação:** qualquer meio (tecnológico ou não) utilizado para criação, transmissão, processamento, utilização, armazenamento, recuperação ou descarte de informações que possuam valor institucional para a CGE/RJ;
- V. **ativo tecnológico:** componente, físico ou lógico, integrante da infraestrutura tecnológica da CGE/RJ ou devidamente autorizado para uso institucional, ainda que de propriedade pessoal;
- VI. **cliente:** pessoa natural que utiliza os serviços públicos prestados pela CGE/RJ;
- VII. **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

- VIII. **dado pessoal:** informação relacionada à pessoa natural identificada ou identificável, nos termos da legislação vigente;
- IX. **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- X. **evento de privacidade da informação:** evento relacionado à segurança da informação que envolva dados pessoais, sem, contudo, configurar incidente;
- XI. **evento de segurança da informação:** qualquer ocorrência, intencional ou acidental, que possa representar violação real ou potencial às diretrizes desta Política ou de seus documentos complementares;
- XII. **fornecedor:** pessoa, física ou jurídica, de direito público ou privado, que forneça produto ou serviço para a CGE/RJ;
- XIII. **incidente de privacidade da informação:** incidente de segurança da informação que envolva dados pessoais e possa acarretar risco ou dano relevante aos titulares;
- XIV. **incidente de segurança da informação:** evento que comprometa, de forma comprovada, os princípios de segurança da informação — confidencialidade, integridade, disponibilidade, autenticidade ou legalidade;
- XV. **informação sensível:** informação classificada com algum grau de sigilo, que requer proteção contra acessos, usos ou divulgações não autorizadas;
- XVI. **inteligência de ameaças:** processo de coleta, correlação e análise de informações provenientes de diversas fontes sobre ameaças cibernéticas,

visando identificar padrões e tendências que permitam antecipar e mitigar riscos;

- XVII. *login*:** identificação de usuário utilizada para autenticação em sistemas computacionais com mecanismos de controle de acesso, geralmente associada a uma senha ou credencial segura;
- XVIII. oportunidade de privacidade da informação:** situação favorável relacionada à proteção de dados pessoais, cuja exploração pode aprimorar os controles de privacidade;
- XIX. oportunidade de segurança da informação:** situação favorável relacionada à segurança da informação, cuja exploração contribua positivamente para os objetivos institucionais de proteção da informação;
- XX. processo:** conjunto estruturado de atividades inter-relacionadas que transformam insumos em produtos ou serviços com valor agregado;
- XXI. registro de auditoria:** registro cronológico e detalhado das ações executadas em sistemas ou recursos tecnológicos, possibilitando rastreabilidade e verificação de autoria, tempo e local da atividade — também denominado como trilha de auditoria, *log* ou registro de evento;
- XXII. risco de privacidade da informação:** possibilidade de ocorrência de evento que comprometa dados pessoais, afetando os direitos dos titulares e os princípios legais aplicáveis;
- XXIII. risco de segurança da informação:** possibilidade de ocorrência de evento que comprometa os objetivos de segurança da informação, decorrente da exploração de vulnerabilidades por ameaças externas;

- XXIV. **servidor:** agente público vinculado à CGE/RJ, independentemente do regime jurídico de trabalho ou forma de contratação (efetivo, comissionado, temporário ou estatutário);
- XXV. **tarefa administrativa:** atividade executada por usuário com privilégios elevados (credencial de administrador), destinada à gestão e ao controle de redes, sistemas operacionais, bancos de dados, softwares ou plataformas tecnológicas. Inclui, entre outras, as ações de instalação, desinstalação, configuração, ajuste de parâmetros, gerenciamento de permissões, monitoramento e demais intervenções críticas para a operação, a segurança e a disponibilidade dos ativos tecnológicos;
- XXVI. **trabalhador terceirizado:** Pessoa vinculada à empresa contratada, que presta serviços à CGE/RJ sob responsabilidade do fornecedor;
- XXVII. **usuário:** agente (humano ou automatizado) que interage com ativos tecnológicos sob responsabilidade da CGE/RJ;
- XXVIII. **vulnerabilidade técnica:** fraqueza identificada em um ativo tecnológico que possa ser explorada por uma ameaça, resultando em comprometimento da segurança da informação.

CAPÍTULO IV – PAPÉIS E RESPONSABILIDADES

Art. 11. Compete à alta administração da CGE/RJ prover orientação e apoio às ações de segurança da informação, em consonância com os objetivos institucionais e a legislação vigente.

Art. 12. Compete a cada servidor, consultor, dirigente, estagiário, trabalhador, terceirizado, visitantes e demais partes:

- I. responder por eventuais prejuízos ou danos decorrentes do descumprimento desta Política e de seus documentos complementares;
- II. zelar pelo uso exclusivo e seguro de suas credenciais de acesso, as quais são pessoais, intransferíveis e de sua inteira responsabilidade;
- III. participar dos treinamentos e ações de conscientização em segurança da informação fornecidos pela CGE/RJ;
- IV. comunicar imediatamente qualquer evento ou incidente relacionado à segurança da informação, conforme os canais definidos;
- V. compete aos usuários a responsabilidade integral pelas informações armazenadas localmente na área de trabalho de seus dispositivos, não cabendo à CGE-RJ qualquer responsabilidade pela perda de dados decorrente desse armazenamento.

Art. 13. Compete ao gestor de cada área (assessor, coordenador, superintendente) ou agente formalmente delegado.

- I. monitorar o cumprimento desta Política, bem como de seus documentos complementares, pelos servidores, estagiários e trabalhadores terceirizados sob sua responsabilidade;
- II. solicitar, junto à Assessoria de Gestão de Pessoas, a publicação no Diário Oficial do Estado relativa à entrada ou saída de servidores e estagiários sob sua gestão, acompanhada da abertura do respectivo chamado no Sistema de Controle de Chamados ou de e-mail enviado para **helpdesk@cge.rj.gov.br**, visando viabilizar a entrega ou devolução dos dispositivos tecnológicos utilizados;

- III. definir e gerenciar os perfis, direitos e níveis de acesso dos sistemas cuja gestão de acesso lhe compete;
- IV. encaminhar, obrigatoriamente, à área de Tecnologia da Informação, por meio do Sistema de Controle de Chamados ou de e-mail **helpdesk@cge.rj.gov.br**, as solicitações referentes a:
 - a) Liberação das pastas de rede dos usuários sob sua responsabilidade;
 - b) Atualização das informações de chefia no **Sistema de Logística**.
- V. realizar revisões periódicas dos acessos aos sistemas, dados e recursos sob sua responsabilidade, assegurando que os acessos estejam compatíveis com as funções desempenhadas;
- VI. promover a segregação de funções nos processos sob sua gestão, de forma a prevenir conflitos de interesse e reduzir riscos operacionais e de segurança;
- VII. identificar, avaliar e comunicar riscos relacionados à segurança e à privacidade da informação, no âmbito dos ativos sob sua responsabilidade;
- VIII. disponibilizar esta Política, o termo de responsabilidade e os materiais de conscientização aos servidores, estagiários, fornecedores e trabalhadores terceirizados sob sua gestão, no início da prestação de serviços;
- IX. solicitar os dispositivos tecnológicos e os acessos lógicos necessários aos trabalhadores terceirizados;
- X. solicitar os acessos físicos pertinentes aos trabalhadores terceirizados;
- XI. elaborar e manter atualizado o mapeamento dos dados pessoais (ROPA – Registro das Operações de Tratamento de Dados Pessoais) relacionados às atividades, processos, sistemas e serviços sob sua gestão, em conformidade

com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e com as orientações do Encarregado pelo Tratamento de Dados Pessoais da CGE-RJ.

Art. 14. Compete à Assessoria de Gestão de Pessoas (RH):

- I. informar, tempestivamente, às áreas responsáveis pela gestão de credenciais de acesso quaisquer alterações no vínculo dos colaboradores, tais como ingresso, desligamento, afastamento ou mudança de função;
- II. realizar o processo de seleção e contratação de cargos terceirizados, estagiários e prestadores de serviços considerando, quando aplicável, a verificação de antecedentes, observando os princípios da legalidade, ética e proporcionalidade, bem como a adequação aos riscos de segurança e privacidade inerentes às funções a serem desempenhadas;
- III. disponibilizar, aos servidores, terceirizados e estagiários, no momento da contratação, esta Política, os materiais de conscientização sobre segurança e privacidade da informação, bem como o Termo de Responsabilidade, para ciência e assinatura formal;
- IV. informar à área de tecnologia a necessidade de revogação de acessos de colaboradores desligados;
- V. cumprir e promover o cumprimento desta Política e de suas normas complementares.

Art. 15. Compete a Diretoria Geral de Administração e Finanças (DGAF):

- I. o DGAF deve garantir que os acessos físicos ao perímetro de segurança estejam protegidos por mecanismos de controle de entrada;

- II. conceder acesso físico ao perímetro de segurança a todos os servidores, estagiários, fornecedores e trabalhadores terceirizados, de acordo com a necessidade relacionada ao exercício das suas funções;
- III. realizar análise crítica anualmente das credenciais de acesso sob sua custódia, adotando revisão de acesso sempre que identificado a necessidade de alteração.

Art. 16. Compete a Assessoria de Comunicação (ASSCOM):

- I. apoiar a divulgação desta Política e de seus documentos complementares, garantindo que as diretrizes, bem como as responsabilidades associadas à segurança e à privacidade da informação estejam acessíveis e comunicadas sempre que houver necessidade;
- II. promover a cultura de segurança da informação no âmbito de atuação da CGE/RJ.

Art. 17. Compete à Assessoria de Tecnologia da Informação (ASSTINF):

- I. operar ferramentas de prevenção, detecção, resposta e mitigação de incidentes de segurança da informação e privacidade;
- II. responder tecnicamente aos incidentes de segurança detectados, adotando as medidas necessárias para sua contenção, erradicação e recuperação;
- III. reportar, de forma tempestiva, sobre os incidentes identificados e as devidas tratativas ao Gestor de Incidentes;

- IV.** corrigir vulnerabilidades técnicas identificadas nos ativos tecnológicos sob sua responsabilidade;
- V.** manter os ativos tecnológicos atualizados com as correções de segurança, patches e atualizações recomendadas pelos fabricantes ou fornecedores;
- VI.** garantir que os serviços, sistemas e equipamentos relacionados à segurança da informação, sejam monitorados gerando relatórios semanais de status, desempenho e conformidade;
- VII.** implementar, monitorar e manter mecanismos de proteção perimetral, contemplando firewall, filtragem de tráfego, Sistema de Detecção e Intrusão (IDS), Sistema de Prevenção de Intrusão (IPS) e demais soluções de defesa;
- VIII.** implementar e manter controles de segurança lógica, quando aplicável, nas plataformas sob sua responsabilidade, abrangendo bancos de dados, sistemas operacionais, redes, ambientes em nuvem e demais ativos tecnológicos;
- IX.** restringir, ao mínimo necessário, os privilégios administrativos, limitando também a quantidade de administradores com permissão para exclusão de registros de auditoria, em conformidade com o princípio do menor privilégio e da rastreabilidade;
- X.** definir e gerenciar os perfis, direitos e níveis de acesso dos sistemas e softwares cuja gestão de acesso lhe compete;
- XI.** realizar, no mínimo semestralmente, a revisão dos acessos aos sistemas e softwares sob sua responsabilidade, garantindo sua aderência às funções e perfis dos usuários;

- XII.** apoiar na definição dos requisitos técnicos de segurança e privacidade da informação a serem incorporados nos processos de contratação de fornecedores de serviços e soluções tecnológicas;
- XIII.** garantir a homologação dos dispositivos tecnológicos e softwares utilizados na CGE/RJ, assegurando que estejam aderentes às diretrizes de segurança e privacidade estabelecidas nesta Política;
- XIV.** garantir que as configurações de segurança necessárias nos dispositivos tecnológicos e softwares homologados, sejam aplicáveis em conformidade com esta Política e com seus documentos complementares;
- XV.** monitorar, proativamente, o ambiente tecnológico, utilizando ferramentas que permitam verificar a disponibilidade, o desempenho e a capacidade dos ativos críticos à operação institucional;
- XVI.** garantir a segurança no desenvolvimento de códigos e sistemas, adotando boas práticas, padrões de codificação segura e atualizações periódicas dos frameworks e bibliotecas utilizados, com foco na mitigação de vulnerabilidades conhecidas;
- XVII.** adotar metodologia formal de desenvolvimento seguro, aplicando os princípios de segurança e de privacidade desde a concepção dos sistemas e durante todo seu ciclo de desenvolvimento;
- XVIII.** apoiar, no âmbito de sua competência, as iniciativas de melhoria contínua da segurança e da privacidade da informação no ambiente institucional;

Art. 18. Compete ao Encarregado pelo Tratamento de Dados Pessoais:

- I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II. receber comunicações da Agência Nacional de Proteção de Dados - ANPD e adotar providências;
- III. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- IV. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;
- V. apoiar na elaboração dos Relatórios de Operações de Dados Pessoais (ROPA) junto aos donos do processo, garantindo a conformidade a LGPD;
- VI. atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados - ANPD, na forma da Lei nº 13.709/2018;
- VII. responder sobre os incidentes que envolvam dados pessoais garantindo a comunicação efetiva a ANPD, em atendimento a LGPD.

Art. 19. Compete ao Gestor de Segurança da Informação:

- I. elaborar e atualizar periodicamente os procedimentos de segurança da CGE-RJ;
- II. implementar e analisar os mecanismos e procedimentos relacionados à segurança da informação, com o intuito de preservar a integridade, a confidencialidade e a privacidade dos dados sob a guarda e responsabilidade dos órgãos e entidades;

- III. definir estratégia de conscientização e cultura de segurança da informação no âmbito de atuação da CGE-RJ;
- IV. propor recursos necessários às ações de segurança da informação, no âmbito de atuação da CGE-RJ;
- V. indicar os responsáveis pelo tratamento de resposta a incidentes no âmbito de atuação da CGE-RJ;

Art. 20. Compete ao Gestor de Incidentes:

- I. definir metodologia de Resposta a Incidentes Cibernéticos no âmbito da CGE-RJ;
- II. aprovar as decisões sobre os eventos de segurança, observando toda a tratativa necessária durante o tratamento;
- III. compartilhar com os demais órgãos e entidades da Administração Pública Estadual, os eventos de segurança, após ocorrência, para fins de prevenção, bem como as eventuais soluções, para fins de replicação de conhecimentos e experiências;
- IV. elaborar procedimentos de tratamento de incidentes que apoiem a equipe técnica em futuras tratativas;
- V. comunicar tempestivamente, as tratativas dos incidentes críticos ao Gestor de Segurança da Informação.

Art. 21. Compete ao Comitê Integrado de Governança de Tecnologia e Segurança da Informação - CGTI:

- I. aprovar políticas, diretrizes e planos estratégicos de TI e segurança da informação;
- II. homologar o Plano Estratégico e Diretor de Tecnologia da Informação – PEDTIC;
- III. monitorar indicadores de desempenho de TI e segurança da informação;
- IV. avaliar e aprovar demandas de novas soluções tecnológicas, observando os princípios da Lei Federal nº 14.133/2021 e do Decreto Estadual nº 45.600/2016;
- V. aprovar e apoiar a implementação da Política de Segurança da Informação e o Programa de Governança em Privacidade e Proteção de Dados Pessoais;
- VI. promover capacitação e conscientização sobre segurança da informação, em alinhamento com a Instrução Normativa PRODERJ/PRE nº 7/2025;
- VII. monitorar e avaliar periodicamente a eficácia das medidas de segurança adotadas, recomendando ajustes e melhorias conforme necessário;
- VIII. assegurar a proteção e confidencialidade das informações sensíveis e críticas da CGE-RJ, prevenindo vazamentos, acessos não autorizados e outros incidentes de segurança.

Art. 22. Comitê Integrado de Governança de Tecnologia e Segurança da Informação (CGTI) será composto pelos gestores ou representantes, sendo um efetivo e um suplente, das seguintes unidades:

- a) Gabinete da Controladoria Geral;
- b) Subcontroladoria Geral do Estado;
- c) Corregedoria Geral do Estado;
- d) Auditoria Geral do Estado;
- e) Ouvidoria e Transparência Geral do Estado;

- f) Diretoria Geral de Administração e Finanças;
- g) Assessoria de Tecnologia da Informação;
- h) Gestor de Segurança da Informação;
- i) Encarregado Setorial pelo Tratamento de Dados Pessoais.

Art. 23. Compete à Corregedoria da CGE/RJ apurar infrações cometidas por servidores contra esta Política ou contra cláusulas de segurança e privacidade, mediante sindicância, ou outro procedimento administrativo investigatório.

CAPÍTULO V - Diretrizes

Seção I - Gestão de acesso

Art. 24. A CGE/RJ deve vincular o controle de acesso a uma credencial única, pessoal e intransferível, vedando o uso de credenciais compartilhadas.

Art. 25. O acesso a ativos de informação somente será concedido mediante a assinatura do Termo de Responsabilidade de Segurança da Informação.

Art. 26. O acesso à informação e às funcionalidades dos sistemas deve ser restrito por meio de perfis de acesso previamente definidos.

Parágrafo único. Os perfis de acesso devem observar os princípios da necessidade de conhecer, necessidade de uso e privilégio mínimo, restringindo-se a permissões estritamente necessárias para o desempenho das funções atribuídas.

Art. 27. A criação de identidades e a atribuição de direitos de acesso devem ser precedidas solicitação e autorização formal.

Art. 28. A revogação de identidades e direitos de acesso deve ocorrer mediante solicitação formal, especialmente em casos de desligamento, mudança de função ou encerramento de contrato.

Art. 29. Os direitos de acesso devem ser revogados imediatamente quando se tornarem desnecessários para o desempenho das atividades institucionais.

Art. 30. Os sistemas devem exigir o uso de senhas complexas, observando os seguintes critérios mínimos:

- I. mínimo de 14 (quatorze) caracteres;
- II. inclusão de, no mínimo:
 - a. Uma letra minúscula;
 - b. Uma letra maiúscula;
 - c. Um caractere numérico;
 - d. Um caractere especial.

Parágrafo único. Caso o sistema não imponha tais critérios de forma automática, o usuário é responsável por configurar sua senha de acordo com o padrão estabelecido.

Art. 31. Em dispositivos que exigem senhas exclusivamente numéricas, é vedado o uso de sequências óbvias ou de fácil associação, como datas de aniversário, números sequenciais ou números de telefone.

Art. 32. É vedado ao usuário expor, compartilhar ou revelar sua senha a terceiros, independentemente da natureza do vínculo ou do contexto.

Seção II - Uso aceitável dos ativos de informação

Art. 33. Os ativos de informação da CGE/RJ devem ser utilizados exclusivamente para fins institucionais.

Art. 34. É dever do usuário zelar pela integridade dos dispositivos tecnológicos, sendo vedada qualquer alteração, remoção ou inclusão de componentes de hardware.

Art. 35. É proibida a instalação de softwares não homologados pela CGE/RJ em seus equipamentos.

Art. 36. É vedado realizar downloads de softwares ou arquivos executáveis da internet nos dispositivos institucionais.

Art. 37. Uso de Mídias Removíveis.

- I. O uso de mídias removíveis, como dispositivos USB, CDs, DVDs e similares, é por padrão, bloqueado e controlado em todos os dispositivos da CGE/RJ, visando a proteção dos dados e a prevenção contra riscos de segurança.

Parágrafo único. O não cumprimento das condições previstas neste artigo acarretará a revogação da autorização de uso da mídia removível, além de possíveis medidas disciplinares, conforme o regulamento interno da CGE/RJ.

Art. 38. É proibido o acesso, por meio de equipamentos institucionais, a sites com conteúdo:

- I. de propaganda político-partidária;
- II. ilegais ou que promovam atividade ilícita;
- III. de teor sexual.

Art. 39. É vedado o armazenamento de conteúdos ilegais ou antiéticos em ativos de informação da CGE/RJ.

Art. 40. É proibido o armazenamento de conteúdos pessoais em ativos de propriedade institucional.

Art. 41. É vedado o armazenamento local de informações em dispositivos institucionais sem cópia de segurança na nuvem ou rede da CGE/RJ.

Parágrafo único. As informações devem ser armazenadas exclusivamente nos repositórios designados pela CGE/RJ.

Art. 42. É proibido consumir alimentos ou bebidas nas proximidades de ativos de informação.

Art. 43. É vedada qualquer alteração nas configurações de segurança dos ativos tecnológicos da CGE/RJ.

Art. 44. É proibida a conexão de dispositivos não homologados à rede institucional.

Art. 45. Os computadores devem ser desligados ao final do expediente, salvo em casos de orientação contrária da área de Tecnologia da Informação.

Art. 46. Documentos com informações devem ser retirados imediatamente da impressora após a solicitação de impressão.

Art. 47. As mesas de trabalho devem ser mantidas organizadas, especialmente quanto à exposição de papéis e mídias contendo informações.

Art. 48. Informações exibidas em telas devem ser protegidas contra visualização não autorizada, especialmente em locais públicos ou durante apresentações, filmagens ou capturas de tela.

Art. 49. O dispositivo deve ser bloqueado ou desconectado sempre que o usuário se ausentar de sua estação de trabalho.

Seção III - Trabalho remoto e uso de dispositivos móveis

Art. 50. Em caso de furto ou roubo de dispositivo móvel de propriedade da CGE/RJ ou de dispositivo pessoal homologado para uso institucional, o servidor, estagiário ou trabalhador terceirizado deve notificar imediatamente a CGE/RJ e, assim que possível, registrar boletim de ocorrência.

Art. 51. É vedada a conexão de dispositivos móveis institucionais a redes públicas de Wi-Fi.

Seção IV - Ambiente físico

Art. 52. A CGE/RJ deve garantir que o perímetro e os acessos físicos ao seu ambiente de trabalho estejam protegidos por mecanismos de controle de entrada.

Art. 53. A CGE/RJ deve implementar proteções físicas contra riscos como incêndio, inundação, descarga elétrica, explosões e manifestações civis.

Art. 54. É vedada a remoção, instalação ou movimentação de dispositivos tecnológicos institucionais sem autorização, exceto no caso de dispositivos móveis devidamente registrados.

Art. 55. Antes da reutilização ou descarte, os dispositivos de armazenamento devem ser submetidos à sobrescrição segura ou destruídos fisicamente.

Art. 56. A CGE/RJ deve implementar redundâncias testadas para proteger os dispositivos tecnológicos contra indisponibilidades decorrentes de falhas no fornecimento de energia elétrica, telecomunicações ou climatização.

Art. 57. O cabeamento de energia e de telecomunicações deve ser protegido contra danos e interferências.

Seção V - Classificação da informação

Art. 58. A CGE/RJ deve classificar e rotular as informações quanto ao grau e prazo de sigilo, conforme estabelecido na Lei nº 12.527/2011 (Lei de Acesso à Informação), regulamentada pelo Decreto Estadual nº 46.475/2018, nos níveis: ultrassecreta, secreta e reservada.

§1º Informações de natureza pessoal terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem e poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem, nos termos do Decreto Estadual nº 46.475/2018.

§ 2º É vedado incluir no Sistema Eletrônico de Informações (SEI-RJ) documentos com informações classificadas como ultrassecretas, secretas ou reservadas.

§ 3º As informações classificadas deverão ser inseridas e geridas em sistema próprio, administrado pela CGE/RJ, com controles adequados de segurança e rastreabilidade.

§ 4º O acesso às informações classificadas será restrito às pessoas formalmente autorizadas pela autoridade classificadora ou pela área técnica responsável pela classificação da informação, observado o princípio da necessidade de conhecimento.

Art. 59. No âmbito do SEI-RJ, as informações devem ser registradas quanto ao nível de acesso como públicas, restritas ou sigilosas.

§ 1º Devem ser registrados com nível de acesso restrito ou sigiloso os documentos que contenham informações pessoais ou matérias protegidas por sigilo legal.

§ 2º Documentos e processos que não se enquadrem em hipótese de sigilo deverão ser registrados com nível de acesso público.

Seção VI - Transferência da informação

Art. 60. O e-mail institucional deve ser utilizado exclusivamente para assuntos relacionados às atividades da CGE/RJ.

Parágrafo único. É vedada a utilização de e-mail pessoal para fins institucionais.

Art. 61. É proibido, por meio de mensagens eletrônicas institucional:

- I. enviar mensagens de propaganda, correntes, conteúdo ilegal, antiético ou discriminatório;
- II. enviar arquivos contendo códigos maliciosos;
- III. compartilhar conteúdos que violem direitos de propriedade intelectual;
- IV. cadastrar o e-mail institucional em sites ou aplicativos externos sem autorização formal da CGE/RJ.

Parágrafo único. E-mails institucionais cadastrados em plataformas externas devem ser controlados pela área competente da CGE/RJ.

Art. 62. Informações institucionais devem ser transferidas apenas por aplicações previamente homologadas pela CGE/RJ.

Art. 63. Mensagens eletrônicas sigilosas devem ser classificadas, conforme disposto no Art.58.

Art. 64. Deve-se realizar dupla verificação dos destinatários antes do envio de informações por qualquer meio de comunicação.

Seção VII – Privacidade

Art. 65. A CGE/RJ deve assegurar que o tratamento de dados pessoais observe os preceitos da Lei nº 13.709/2018 (LGPD).

Art. 66. Deve ser implementada uma Política de Privacidade, com informações claras sobre o tratamento de dados e os respectivos prazos de retenção.

Art. 67. As finalidades de tratamento devem ser mapeadas, evitando finalidades ilícitas ou incompatíveis com os direitos dos titulares.

Art. 68. Processos e sistemas devem ser planejados ou ajustados para garantir o tratamento mínimo necessário de dados pessoais.

Seção VIII - Códigos maliciosos

Art. 69. É vedado desabilitar os sistemas de proteção contra códigos maliciosos instalados nos dispositivos institucionais.

Art. 70. É proibido clicar em links ou abrir anexos suspeitos que possam conter conteúdo malicioso.

Seção IX – Fornecedores

Art. 71. O DGAF deve formalizar, em contrato, os requisitos de segurança e privacidade da informação aplicáveis aos fornecedores, atribuindo claramente as responsabilidades de cada parte.

Parágrafo único – Os requisitos contratuais devem ser estendidos à cadeia de suprimentos do fornecedor, por meio de cláusulas específicas.

Seção X - Serviços em nuvem

Art. 72. A contratação de serviços em nuvem deve contemplar cláusulas específicas que abordem:

- I. papéis e responsabilidades, inclusive em incidentes de segurança ou privacidade;
- II. controles de segurança e privacidade aplicáveis, incluindo cópias de segurança, antivírus e gestão de acessos;
- III. recursos de segurança disponibilizados pelo provedor e sua forma de utilização;
- IV. procedimentos para retorno das informações à CGE/RJ em caso de término contratual;
- V. localização dos dados e jurisdição aplicável.

Seção XI - Incidentes de segurança e de privacidade

Art. 73. A CGE/RJ deve manter processo estruturado para gestão de incidentes de segurança e privacidade da informação, contemplando as etapas de detecção,

priorização, escalonamento, análise, resposta, resolução, comunicação e tratamento de lições aprendidas.

Art. 74. Incidentes classificados como de alta criticidade devem ser reportados aos órgãos competentes.

Art. 75. As ações de contenção, erradicação e recuperação devem seguir fluxos padronizados, com base em procedimentos documentados.

Art. 76. As evidências dos incidentes devem ser preservadas para fins de auditoria ou investigação.

Seção XII - Vulnerabilidades técnicas.

Art. 77. A CGE/RJ deve manter processo contínuo de identificação, análise, tratamento e verificação da eficácia das ações corretivas relativas às vulnerabilidades técnicas.

Seção XIII - Inteligência de ameaças

Art. 78. A CGE/RJ deve produzir inteligência de ameaças com base na coleta e análise sistemática de dados relacionados a riscos cibernéticos, visando antecipar ações de resposta e prevenção.

Seção XIV - Controles criptográficos e gerenciamento de chaves

Art. 79. A CGE/RJ deve utilizar criptografia de forma eficaz para assegurar a confidencialidade, autenticidade e integridade das informações, conforme aplicável.

Seção XV - Registro de auditoria

Art. 80. Os registros de auditoria dos ativos tecnológicos da CGE/RJ devem ser obrigatoriamente habilitados, protegidos contra alterações não autorizadas, armazenados por período mínimo definido em norma complementar e monitorados periodicamente por ferramenta automatizada, sempre que tecnicamente viável.

Art. 81. Devem ser registrados, no mínimo, dados sobre: identidade do usuário, data e hora da ação, tipo de operação executada e origem do acesso.

Art. 82. Os eventos críticos de segurança devem gerar alertas automáticos para análise imediata pela equipe técnica.

Art. 83. Os registros devem estar disponíveis para auditoria interna, externa e para apuração de incidentes, quando necessário.

Art. 84. Os registros de auditoria devem estar sincronizados com uma fonte confiável de tempo, garantindo consistência nas informações de data e hora.

Seção XVI - Desenvolvimento de software

Art. 85. No desenvolvimento ou reuso de software, devem ser adotadas metodologias de desenvolvimento seguro, princípios de codificação segura e boas práticas de privacidade.

Seção XVII - Cópia de segurança

Art. 86. A CGE/RJ deve manter cópias de segurança atualizadas das informações institucionais, incluindo arquivos, bancos de dados, e-mails e aplicações.

Seção XVIII - Continuidade do negócio

Art. 87. A CGE/RJ deve manter um Plano de Continuidade do Negócio para situações de crise ou desastre, contemplando medidas que assegurem a segurança e a privacidade da informação.

Art. 88. Os ativos tecnológicos devem dispor de mecanismos de redundância adequados para garantir a disponibilidade das informações.

Seção XIX - Uso de dispositivo pessoal no trabalho

Art. 89. A utilização de dispositivo pessoal para fins de trabalho por acesso remoto depende de autorização formal da área de Tecnologia da Informação, que estabelecerá critérios de segurança específicos.

Art. 90. A utilização de computador pessoal para fins de trabalho exige:

- I. segregação clara entre o uso pessoal e o uso institucional, devendo o usuário assegurar que dados, aplicações e acessos corporativos sejam mantidos separados de conteúdos pessoais, conforme as orientações da área de Tecnologia da Informação;
- II. autorização prévia da área de Tecnologia da Informação.

Parágrafo único. As diretrizes desta Política devem ser integralmente seguidas nos dispositivos pessoais autorizados, excetuando-se apenas as orientações específicas para dispositivos institucionais.

CAPÍTULO VI – Documentos Complementares

Art. 91. Para viabilizar a aplicação desta Política, devem ser instituídos procedimentos específicos que detalhem controles e responsabilidades, incluindo, mas não se limitando a:

- I. Gestão de Acesso Físico e Lógico;
- II. Gestão de Ativos;
- III. Gestão de Mudanças;
- IV. Metodologia de Gestão de Riscos de Segurança da Informação;
- V. Gestão de Vulnerabilidades;
- VI. Gestão de Inteligência de Ameaça;
- VII. Estrutura de Gestão de Incidentes;
- VIII. Gestão de Backup;
- IX. Gestão de Segurança em Redes;
- X. Gestão de Software;
- XI. Gestão de Desenvolvimento Seguro
- XII. Gestão de Fornecedores;
- XIII. Política de Privacidade de Dados Pessoais;
- XIV. Política de Continuidade de Negócios;
- XV. Gestão de Seleção e Contratação de Pessoas;
- XVI. Análise de Impacto nos Negócios (BIA);
- XVII. Plano de Conscientização.

CAPÍTULO VII - Processo Disciplinar

Art. 92. A violação das disposições desta Política ou de seus documentos complementares poderá ensejar sanções administrativas, civis ou judiciais, inclusive desligamento, conforme o caso.

Art. 93. Toda violação ou desvio será investigado com o objetivo de identificar a causa, corrigir falhas e, quando necessário, reestruturar processos e controles.

Art. 94. Constituem, entre outras, condutas passíveis de sanção:

- I. uso ilegal de softwares;
- II. introdução intencional ou acidental de códigos maliciosos;

- III. tentativa ou realização de acesso não autorizado a sistemas ou dado;
- IV. compartilhamento de informações ou documentos classificados como reservados, secretos, ultrassecretos ou pessoais.

Art. 95. Em caso de dúvidas quanto aos princípios ou responsabilidades previstas nesta Política, o colaborador deverá entrar em contato com o Gestor de Segurança da Informação.

Art. 96. A omissão na comunicação de incidentes de segurança da informação será considerada falta grave.

CAPÍTULO VIII - Vigência

Art. 97. Esta Política entra em vigor na data de sua publicação oficial, devendo ser revisada anualmente ou sempre que houver mudanças que impactem significativamente a segurança ou a privacidade da informação no âmbito da CGE/RJ.

Art. 98. Esta Política deverá manter histórico de versões, com identificação das alterações realizadas, data de aprovação e responsáveis pela revisão.

Art. 99. A revisão da Política será coordenada pela CGTI, podendo contar com contribuições de outras áreas envolvidas e, quando aplicável, com consulta à alta administração.

Art. 100. O histórico de versões deve estar disponível para consulta nos canais oficiais da CGE/RJ.

Parágrafo único. As alterações devem ser devidamente registradas no campo apropriado de “Controle de Documento”.

REFERÊNCIAS

- Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados (LGPD) — que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural;
- Portaria PRODERJ/PRE Nº 968, de 05 de agosto de 2022, que institui o manual de procedimentos regulatórios de segurança da informação a ser adotado por todas as repartições, técnicas e administrativas, no âmbito do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ);
- ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa norma também inclui requisitos para a avaliação e o tratamento de riscos de segurança da informação voltados para as necessidades da organização;
- ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;
- ABNT NBR ISO/IEC 27701:2019, que funciona como extensão à ISO 27001 para gerenciamento da privacidade da informação (SGPI);
- ABNT NBR ISO/IEC 22301:2020, Sistemas de Gestão de Continuidade de Negócios (SGCN), que fornece uma estrutura para que as organizações planejem, estabeleçam, implementem, operem, monitorem, revisem, mantenham e

aprimorem continuamente um sistema de gestão documentado para se protegerem contra incidentes disruptivos, reduzirem a probabilidade de sua ocorrência e garantirem a recuperação em caso de desastres;

- ABNT ISO/TS 22317:2023, especificação técnica que fornece diretrizes para a Análise de Impacto nos Negócios (BIA) no contexto de um Sistema de Gestão de Continuidade de Negócios.

**CONTROLADORIA
GERAL**



**GOV
RJ**