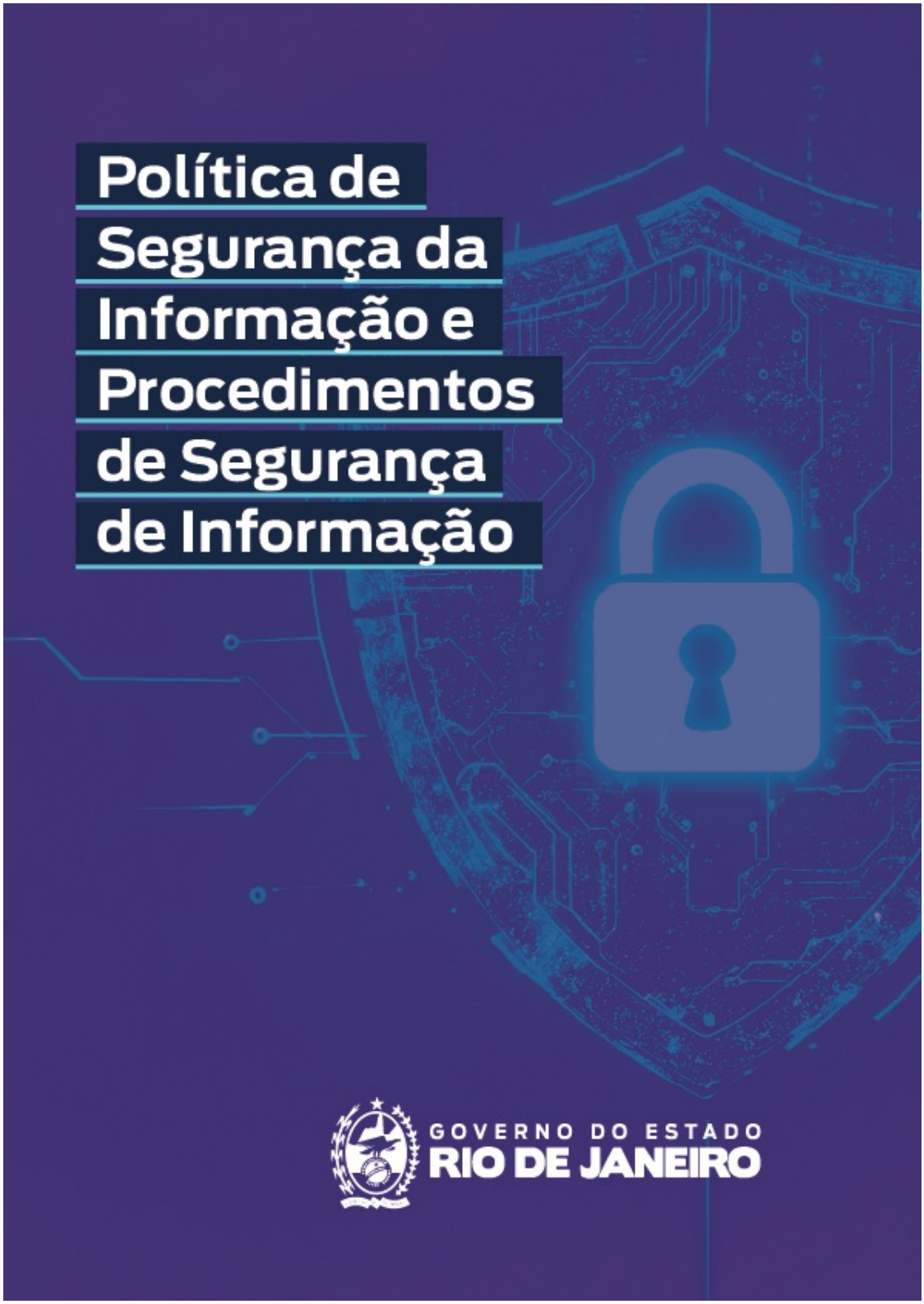
Governo do Estado do Rio de Janeiro

Secretaria de Estado de Transformação Digital

Gabinete do Secretário

ANEXO I



SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL – SETD
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E
PROCEDIMENTOS DE SEGURANÇA
DA INFORMAÇÃO

SETEMBRO 2025 – 4ª EDIÇÃO

SUMÁRIO

1. TERMOS E ABREVIAÇÕES

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
Backup	Cópia de dados de um dispositivo de armazenamento a outro para poderem ser restaurados em caso da perda dos dados originais
CSIC	Comissão de Segurança da Informação e Comunicação da SETD
IN	Instrução Normativa
Login	Conjunto de credenciais e procedimentos usados para identificar um determinado usuário
NBR	Norma Técnica Brasileira
NSTIC	Nível Setorial de Tecnologia da Informação e Comunicação
NUVEM (*Cloud Computing*)	Fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, *software* e serviços de computação sob demanda por meio da *internet*
PEI	Planejamento Estratégico Institucional
PCN	Plano de Continuidade de Negócio
PRODERJ	Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
SEI-RJ	Sistema Eletrônico de Informações do Rio de Janeiro
Senha	Conjunto de caracteres que fornece acesso a algo
SETD	Secretaria de Estado de Transformação Digital
SETIC/RJ	Sistema Estadual de Tecnologia da Informação e Comunicação
SOFTWARE	Sequência de instruções escritas para serem interpretadas por um computador para executar tarefas específicas
TIC	Tecnologia da Informação e Comunicação
USB	*Universal Serial Bus*

2. DA ELABORAÇÃO

2.1. Status do Documento

ELABORAÇÃO	2024
REVISÃO ANUAL	Sim
REVISÃO EXTRAORDINÁRIA	-

2.2. Controle de Versões

Data	Versão	Alteração	Motivação/Justificativa	Responsável
DEZ/2023	1.0	Inclusão da Normativa	Publicação da Política de Segurança da Informação e Comunicação, conforme a IN 02.	Assessoria Especial

DEZ/2023	1.1	Inclusão de Capítulo	Inclusão das Disposições Finais.	Assessoria Especial
JAN/2024	1.2	Revisão	Revisão Geral.	Assessoria Especial
FEV/2024	1.3	Revisão	Revisão Geral.	Chefia de Gabinete
MAI/2024	1.4	Inclusão de Termo	Inclusão de Termo de Responsabilidade de Dispositivos Removíveis.	Assessoria Especial
OUT/2024	1.5	Revisão do documento	Revisão Geral das Diretrizes de Segurança da Informação da SETD.	Every Cybersecurity and GRC Solutions
OUT/2024	2.0	Aprovação do documento	Revisão Geral das Diretrizes de Segurança da Informação da SETD.	Assessoria Especial
AGO/2025	3.0	Revisão	Revisão Geral das Diretrizes de Segurança da Informação da SETD.	Assessoria Especial
SET/2025	4.0	Inclusão de Capítulo e atualização de Normativa	Inclusão do Capítulo "3. DA REVISÃO", e substituição da IN 02, não mais vigente, pela atual IN 07.	Assessoria Especial

3. DA REVISÃO

A Política de Segurança da Informação e os Procedimentos de Segurança da Informação da SETD deverão ser revisados anualmente, facultando-se a realização de ajustes adicionais sempre que se mostrarem necessárias adequações ou correções quanto às ações previstas, metas, prazos e responsáveis.

4. ESCOPO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.1. Para os fins do disposto nesta Política, a segurança da informação abrange:

1. Segurança e defesa cibernética;
2. Segurança física;
3. Proteção de dados organizacionais;
4. Proteção de dados pessoais; e
5. Ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

4.2. As diretrizes estabelecidas nesta Política devem estar alinhadas ao Planejamento Estratégico Institucional (PEI) e em consonância com os valores institucionais.

4.3. Esta Política aplica-se a todos os servidores, funcionários, estagiários, fornecedores, trabalhadores terceirizados e às partes envolvidas em acordos (independente dos instrumentos administrativos utilizados) com a SETD.

4.4. Integram esta Política todos os documentos complementares destinados à proteção e à privacidade da informação.

4.5. Os contratos, convênios, acordos e outros instrumentos congêneres devem atender aos requisitos especificados neste documento.

4.6. Esta Política abrange diretrizes gerais relativas ao uso e compartilhamento de ativos de informação ao longo de todo o seu ciclo de vida, incluindo criação, manuseio, divulgação, armazenamento, transporte e descarte. Seu

propósito é garantir a continuidade dos processos vitais da SETD, consoante com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como em consonância com os valores éticos e as melhores práticas de Segurança da Informação e da Comunicação.

5. CONCEITOS E DEFINIÇÕES

5.1. Para efeitos dessa Política, entende-se por:

I - ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - ADWARE: sigla de *advertising software*;

III - AMBIENTE CIBERNÉTICO: inclui usuários, redes, dispositivos, *software*, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;

IV - AMEAÇA: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

V - ANÁLISE DE INCIDENTES: consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito dessa análise é identificar o escopo do incidente, sua extensão, sua natureza e os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

VI - ANÁLISE DE RISCOS: uso sistemático de informações para identificar fontes e estimar o risco;

VII - ANÁLISE DE VULNERABILIDADES: verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas;

VIII - ATIVIDADE MALICIOSA: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema;

IX - AUDITORIA: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

X - AUTENTICAÇÃO: processo que busca verificar a identidade digital de uma entidade de um sistema, quando ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

XI - AUTENTICAÇÃO DE DOIS FATORES (2 FACTOR AUTHENTICATION): processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas;

XII - AUTENTICIDADE: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

XIII - AVALIAÇÃO DE RISCOS: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

XIV - BANCO DE DADOS: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

XV - BACKUP: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

XVI - BIOMETRIA: verificação da identidade de um indivíduo por meio de uma característica física;

XVII - BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso;

XVIII - COMISSÃO DE SEGURANÇA DA INFORMAÇÃO: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública estadual;

XIX - COMPUTAÇÃO EM NUVEM: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

XX - CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

XXI - CONSCIENTIZAÇÃO: atividade que tem por finalidade orientar sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

XXII - CONTINUIDADE DE NEGÓCIOS: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;

XXIII - CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Geralmente, requer procedimentos de autenticação;

XXIV - CRIPTOGRAFIA: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XXV - CUSTODIANTE: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante, ou dos ativos de informação que compõem o sistema de informação, que não lhe pertence, mas que está sob sua custódia;

XXVI - DADO PESSOAL: informação relacionada à pessoa natural identificada ou identificável;

XXVII -DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XXVIII - DISPOSITIVOS MÓVEIS: equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: *e-books*, *notebooks*, *netbooks*, *smartphones*, tablets, *pendrives*, *USB drives*, HD externo, e cartões de memória;

XXIX - DOCUMENTO: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XXX - E-MAIL: sigla de correio eletrônico (*electronic mail*);

XXXI - ENCARREGADO: pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XXXII -EVENTO: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XXXIII - EVENTO DE SEGURANÇA: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XXXIV - FIREWALL: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de *hardware* ou *software*, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXXV - GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor

agregado;

XXXVI
- GESTÃO DE INCIDENTES CIBERNÉTICOS: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;

XXXVII
- GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XXXVIII
- GESTOR DE SEGURANÇA DA INFORMAÇÃO: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública estadual;

XXXIX
- INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XL - INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XLI - INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XLII - INTERNET: rede global, composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

XLIII - LGPD: sigla de Lei Geral de Proteção de Dados Pessoais;

XLIV - LOG (REGISTRO DE AUDITORIA): registro de eventos relevantes em um dispositivo ou sistema computacional;

XLV - MALWARE: *software* malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de *software* costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de *malware* estão os vírus, *worms*, *trojans* (ou cavalos de Troia), *spyware, adware e rootkits;*

XLVI - MEDIDAS DE SEGURANÇA: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XLVII -MÍDIA: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, c*ompact disk* (CD), fitas, papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

XLVIII
- NECESSIDADE DE CONHECER: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo “necessidade de conhecer”, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XLIX - NÍVEIS DE ACESSO: especificam quanto de cada recurso ou sistema o usuário pode utilizar;

L - OBSOLESCÊNCIA TECNOLÓGICA: ciclo de vida do *software* ou de equipamento, definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias;

LI - PERFIL DE ACESSO: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

LII - PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública estadual mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente;

LIII - PLANO DE GESTÃO DE INCIDENTES: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

LIV - PLANO DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: documentação que compõe o processo de gestão de riscos de segurança da informação, que deve conter, pelo menos, a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de

informação que serão objeto de tratamento; a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; os tipos de riscos; o nível de severidade dos riscos; um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração;

LV - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública estadual, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

LVI - PRESTADOR DE SERVIÇO: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

LVII - RANSOMWARE: tipo de *malware*, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados;

LVIII - REDE DE COMPUTADORES: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

LIX - RISCO: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

LX - RISCO DE SEGURANÇA DA INFORMAÇÃO: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

LXI - ROOTKIT: conjunto de programas e de técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (*root* ou administrator), mas, sim, para manter o acesso privilegiado em um computador previamente comprometido;

LXII - SEGURANÇA CIBERNÉTICA: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

LXIII - SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

LXIV - SI: sigla de segurança da informação;

LXV - SISTEMA DE ACESSO: conjunto de ferramentas que se destina a controlar e a dar a uma pessoa permissão de acesso a um recurso;

LXVI - SISTEMA DE INFORMAÇÃO: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

LXVII -SPYWARE: tipo de *malware*. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger, screenlogger* e *adware* são alguns tipos específicos de *spyware*;

LXVIII - TECNOLOGIA DA INFORMAÇÃO: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

LXIX - TERMO DE RESPONSABILIDADE: termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

LXX - TRATAMENTO DE INCIDENTES CIBERNÉTICOS: consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

LXXI - USUÁRIO DE INFORMAÇÃO: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública estadual, formalizada por meio da assinatura de Termo de Responsabilidade;

LXXII -VÍRUS: seção oculta e autorreplicante de um *software* de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (inserindo uma cópia sua e tornando-se parte) de outro programa. Não é autoexecutável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo;

LXXIII
- VULNERABILIDADE: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha; e

LXXIV
- WORM: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores.

6. PRINCÍPIOS

6.1. As ações relacionadas à Segurança da Informação e Comunicação são norteadas pelos princípios constitucionais elencados no rol do art. 37 da Constituição da República Federativa do Brasil, bem como o princípio da dignidade da pessoa humana, prevista no Art. 1º, inciso III, da Constituição da República, e o Art. 5º da Constituição do Estado do Rio de Janeiro, além dos princípios da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro, instituída pela Portaria PRODERJ/PRE n.^{0} 825, de 26 de fevereiro de 2021, pela Instrução Normativa PRODERJ/PRE N.º 07, de 29 de maio de 2025, pela:

I - Confidencialidade;

II - Integridade;

III - Disponibilidade;

IV - Autenticidade;

V - Publicidade;

VI - Responsabilidade;

VII - Não repúdio; e

VIII - Prevenção.

7. COMISSÃO DE SEGURANÇA DA INFORMAÇÃO

7.1. Fica estabelecida a Comissão de Segurança da Informação (CSI), incumbida de propor, debater, aprimorar e difundir a cultura e aplicação das normas relacionadas à Segurança da Informação e Comunicação no âmbito da SETD.

7.2. A composição da Comissão de Segurança da Informação e Comunicação será a seguinte:

I - **Gestor de Segurança da Informação:** Responsável pelo NSTIC/RJ na SETD e presidente desta Comissão;

II - **Responsável pelo Tratamento e Respostas a Incidentes:** Será o Suplente Responsável do NSTIC/RJ;

III - **Encarregado pelo Tratamento de Dados Pessoais:** Responsável pela Ouvidoria na SETD; e

IV - **Diretor Geral de Administração e Finanças:** Responsável pelos Recursos Humanos**.**

7.3. Fica estabelecido que qualquer área da SETD poderá participar das reuniões da CSIC, desde que convidada e mediante comunicação prévia, caso necessário.

8. PAPÉIS E RESPONSABILIDADES

8.1. Além das responsabilidades inseridas no Art. 17 do Capítulo IV, Seção I, da IN 07 do PRODERJ, fica estabelecido os papéis e responsabilidades abaixo.

8.2. Caberá a CSI:

8.2.1. Reunir-se, periodicamente ou mediante um risco, evento ou incidente (seja de segurança, seja de privacidade da informação) que requeira atuação imediata desse comitê;

8.2.2. Atuar como responsável e exercer liderança quanto à melhoria dos processos relacionados ao tema de

Segurança da Informação na SETD;

8.2.3. Avaliar propostas e sugerir alterações na Política de Segurança da Informação e normativos complementares, submetendo-os à apreciação da autoridade competente;

8.2.4. Propor em conjunto com a Assessoria de Comunicação (ASSCOM), um plano de conscientização e educação anual em segurança e privacidade da informação, de forma contínua para servidores, estagiários e consultores.

8.2.5. Promover, por meio de parcerias e acordos de cooperação, conhecimentos específicos às equipes técnicas.

8.2.6. Propor, por meio da metodologia de riscos adotada pela SETD, soluções para tratar riscos, oportunidades, eventos e incidentes (seja de segurança ou privacidade da informação) identificados na secretaria; e

8.2.7. Analisar as infrações contra essa Política, examinando se a infração causou um incidente de segurança ou privacidade da informação – em caso positivo, classificar o incidente, e recomendar formalmente ao:

8.2.7.1. Gestor de Contrato: a aplicação de sanção, conforme definido no contrato (ou instrumento administrativo equivalente), ao fornecedor, consultor, ou a outras partes envolvidas que tenham cometido a infração.

8.2.7.2. Corregedor Interno: a abertura de uma sindicância para processo disciplinar ao servidor ou funcionário infrator à Corregedoria Interna (CORREG).

8.2.7.3. Encarregado pelo Tratamendo de Dados Pessoais: tomar as medidas necessárias de acordo com o Plano de Continuidade de Negócios (PCN).

8.3. Caberá à Área de Segurança e Tecnologia da Informação, integrante da Assessoria Especial (ASSESP):

8.3.1. Criar, avaliar e monitorar os normativos relacionados à Segurança da Informação, garantindo adequação à legislação federal e estadual;

8.3.2. Assessorar as demais áreas da organização na definição dos critérios de segurança da informação, incluindo contratos com fornecedores e serviços;

8.3.3. Gerenciar os requisitos de segurança, estabelecidos para a operação, administração e comunicação dos recursos tecnológicos, bem como para o suporte ao usuário (incluindo dispositivos móveis);

8.3.4. Identificar e monitorar ameaças cibernéticas mediante inteligência de ameaças;

8.3.5. Identificar e tratar vulnerabilidades técnicas;

8.3.6. Restringir os privilégios dos administradores e a quantidade de administradores que podem excluir registros de auditoria (*logs*) ao mínimo necessário;

8.3.7. Homologar os dispositivos tecnológicos e os *softwares* para utilização na SETD;

8.3.8. Prover, continuamente, os controles necessários para cumprir as diretrizes de segurança e privacidade desta Política nos dispositivos tecnológicos e *softwares* homologados na organização; e

8.3.9. Monitorar o ambiente tecnológico por meio de soluções de monitoramento da disponibilidade, do desempenho e da capacidade dos ativos tecnológicos críticos do negócio.

8.4. Caberá aos Responsáveis de Área:

8.4.1. Atuar como um agente conscientizador do tema “Segurança da Informação” para os usuários sob sua supervisão, alertando-os sobre as regras definidas na presente Política;

8.4.2. Incorporar práticas de segurança da informação nos processos de trabalho sob sua responsabilidade;

8.4.3. Manter, criar, alterar ou excluir as contas de usuários sob sua supervisão, considerando o mínimo acesso necessário para execução das atividades;

8.4.4. Monitorar e tratar os registros de auditoria (*logs*) e, informar ao CSIC e ao superior imediato, quaisquer anomalias ou alterações nos *logs*;

8.4.5. Comunicar esta Política e, caso necessário, normas complementares a funcionários, consultores e fornecedores contratados;

8.4.6. Incluir, nas especificações técnicas dos bens ou serviços contratados ou a serem adquiridos, regras que protejam a segurança e privacidade da informação – quando dados pessoais ou dados sensíveis estiverem envolvidos, requer-se observância das políticas, procedimentos e diretrizes específicas sobre o tema.; e

8.4.7. Relatar à área de Segurança e Tecnologia da Informação, bem como ao superior imediato, via processo estabelecido, eventuais incidentes de segurança da informação e suspeitas ou violações desta Política e de suas normas complementares.

8.5. Caberá à Coordenadoria Administrativa e ao Recursos Humanos (COOADM) da SETD:

8.5.1. Garantir que os **Apêndices** desta Política sejam assinados por todos os colaboradores que estejam atuando em prol da SETD, mesmo que temporariamente;

8.5.2. Relatar à área de Segurança e Tecnologia da Informação e ao superior imediato, via processo estabelecido, eventuais incidentes de segurança da informação, bem como suspeitas ou violações desta Política e de suas normas complementares;

8.5.3. Incluir práticas de segurança e privacidade da informação em seus processos; e

8.5.4. Notificar, conforme o procedimento estabelecido, as áreas responsáveis pela segurança da informação sobre qualquer alteração ou desligamento de um funcionário ou consultor, incluindo mudanças de cargo, função, lotação, bem como afastamentos por períodos superiores a 30 (trinta) dias.

8.6. Caberá à Corregedoria Interna (CORREG):

8.6.1. Apurar, quando recomendado pela CSIC, mediante sindicância, as infrações cometidas pelos servidores contra esta Política e contra as cláusulas de segurança e privacidade da informação existentes nos contratos de trabalho.

Parágrafo único: A aplicação da penalidade é responsabilidade da CORREG.

8.7. Caberá aos Usuários de Informação:

8.7.1. Conhecer e cumprir essa Política, bem como suas normas complementares;

8.7.2. Conhecer e assinar os apêndices dessa Política;

8.7.3. Não divulgar informações não públicas, para pessoas não autorizadas, a fim de mitigar possíveis situações que coloquem em risco a segurança e imagem da SETD;

8.7.4. Utilizar as informações e os recursos tecnológicos em sua posse, exclusivamente, para os objetivos da SETD;

8.7.5. Quaisquer acessos realizados com o seu *login,* uma vez que essa credencial é única, pessoal e intrasferível;

8.7.6. Relatar à área de Segurança e Tecnologia da Informação e ao superior imediato, via processo estabelecido, eventuais incidentes de segurança da informação, bem como suspeitas ou violações desta Política e de suas normas complementares; e

8.7.7. Realizar os treinamentos em segurança e privacidade da informação fornecidos pela SETD.

9. DIRETRIZES GERAIS

9.1. As informações criadas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas, referentes à SETD, são patrimônio da Secretaria, e devem ser classificadas e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o seu ciclo de vida.

Parágrafo Primeiro: o uso das informações deverá ser feito apenas para o desempenho das atividades profissionais ou para a geração de políticas públicas.

Parágrafo Segundo: toda informação deve ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade. Para tanto, devem ser observados os parâmetros definidos na Lei Federal nº 13.709/2018, no Decreto Estadual 48.891/2024, no Decreto Estadual nº 46.730/2019 e no Decreto Estadual nº 46.475/2018. Nesse sentido, os gestores da informação devem assegurar que as classificações atribuídas sejam revisadas periodicamente.

Parágrafo Terceiro: não poderão ser incluídos no SEI-RJ, os documentos com informações classificáveis nos níveis de sigilo estabelecidos nos art. 23 e 24 da Lei Federal nº 12.527/2011, bem como no art. 26 do Decreto Estadual nº 46.475/2018, a saber: ultrassecreto, secreto e reservado.

9.2. Todos os contratos ou acordos de cooperação técnica celebrados pela SETD com prestadores de serviços ou outros entes devem incluir cláusulas que assegurem a observância da Política de Segurança da Informação e Comunicação e, caso necessário, seus normativos complementares, além da manutenção do sigilo das informações durante e após a vigência do contrato.

9.3. Todos os servidores, consultores, estagiários e fornecedores (em qualquer vínculo, função ou nível hierárquico na organização) são responsáveis pela segurança, zelo e bom uso dos ativos aos quais possuem acesso.

9.4. Toda informação custodiada em ativos de Tecnologia da Informação e Comunicação, na SETD, deve possuir cópia de segurança (*backup*) e ser guardada em local protegido.

9.5. Todas as informações relacionadas à SETD, independentemente de estarem armazenadas em ativos da organização ou em ativos de terceiros, devem ser protegidas para evitar alterações, acessos ou eliminações indevidas.

9.6. A SETD deverá implementar instrumentos de declaração de responsabilidade e compromisso de sigilo e

confidencialidade sobre todas as informações obtidas em decorrência da relação institucional com a SETD.

Parágrafo Primeiro: esses instrumentos devem ser assinados por todos os usuários mencionados nesse documento (item 2.3) nas fases de admissão, nomeação e contratação, incluindo representantes de empresas terceirizadas, em conformidade com o Decreto Estadual 48.891/2024.

Parágrafo Segundo: os instrumentos devem ser considerados como imprescritíveis, irrevogáveis e irretratáveis.

9.7. No caso dos prestadores de serviço, as obrigações relativas ao sigilo de informações deverão ser formalizadas e entregues ao fornecedor pela área contratante, por meio da assinatura do Termo de Responsabilidade e Confidencialidade para Fornecedores e Parceiros, especificado no Apêndice II desta Política.

9.8. A SETD deverá implementar mecanismos de proteção contra acesso não autorizado em suas instalações e equipamentos.

9.9. Os acessos lógicos e físicos de todos os usuários abrangidos neste documento devem ser aprovados, registrados, armazenados e adequados às necessidades inerentes ao respectivo cargo e função na organização.

9.10. A senha é pessoal e intrasferível. Sendo assim, é vedada a divulgação e o compartilhamento de senhas com qualquer outro usuário (interno ou externo), a fim de preservar os ativos da organização.

Parágrafo único: Qualquer utilização dos sistemas e demais recursos de TIC da SETD é de responsabilidade do agente público ao qual estejam associadas as credenciais de acesso utilizadas

9.11. A SETD deverá observar e implementar as orientações técnicas e as melhores práticas de segurança publicadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e outros órgãos competentes, especialmente aquelas relacionadas à mitigação de vulnerabilidades técnicas conhecidas em aplicativos web e sistemas da informação.

9.12. A SETD deve estabelecer um processo para avaliar e gerenciar os riscos e oportunidades associados ao uso de tecnologias emergentes (e.g., Inteligência Artificial, Internet das Coisas, Blockchain, Computação Quântica), desenvolvendo ou adotando normas complementares e realizando análises de risco específicas para sua implementação segura e alinhada aos objetivos estratégicos.

10. NORMAS COMPLEMENTARES

10.1. Com o propósito de assegurar a confidencialidade, disponibilidade e integridade dos ativos de tecnologia, bem como o desenvolvimento de sistemas, páginas e aplicativos, a SETD adotará, a partir de agora, as normas complementares estabelecidas pelo Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ), agente de Direção-Geral do Sistema Estadual de Tecnologia da Informação e Comunicação (SETIC).

10.2. A SETD poderá instituir outras normas complementares não previstas neste artigo, resguardada a disposição do parágrafo anterior.

11. GESTÃO DE ATIVOS

11.1. Todo ativo de informação da SETD deve:

11.1.1. Ser inventariado e protegido;

11.1.2. Possuir identificação da área custodiante; e

11.1.3. Ter suas ameaças, vulnerabilidades e interdependências mapeadas.

11.2. Os ativos de informação organizacionais devem ser equipados com medidas de autoproteção — como antivírus, *firewalls*, criptografia e controle de acesso às configurações. Sendo assim, é vedado ao usuário desabilitar ou alterar as configurações dessas medidas de autoproteção.

11.3. A SETD deve definir regras e processos tanto para solicitação quanto para descarte dos ativos de informação.

Parágrafo único: a SETD deve implementar, caso julgue necessário, um plano de obsolescência programada nos seus ativos de informação, não ultrapassando o período de 5 (cinco) anos.

11.4. A SETD deve definir regras e diretrizes relacionadas ao *backup*, seja dos ativos de rede ou das aplicações que compõem o seu ambiente tecnológico.

12. USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO

12.1. Os recursos de tecnologia da informação vinculadas à SETD são disponibilizados para os usuários como ferramentas de trabalho, devendo ser utilizados, primordialmente, em atividades relacionadas às funções institucionais desempenhadas pela Secretaria.

12.2. A SETD deverá criar mecanismos para garantir que os usuários não consigam instalar softwares não

homologados nos dispositivos tecnológicos da organização.

12.3. É terminantemente vedado o uso dos recursos computacionais disponibilizados para armazenar ou transmitir qualquer conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

12.4. É terminantemente vedado armazenar arquivo que não seja para fins de trabalho nem nos diretórios de rede nem no próprio ativo de informação. Também é proibido transmiti-los por e-mail ou por aplicativos de mensagens instantâneas.

12.5. As informações corporativas devem ser armazenadas na rede corporativa, em local destinado à unidade do usuário, conforme orientação do gestor correspondente — não sendo autorizado armazená-las localmente, no computador.

Parágrafo único: A área de Segurança e Tecnologia da Informação não se responsabilizará por informações armazenadas no disco local dos equipamentos utilizados por usuários, independente do seu cargo e função.

12.6. A SETD deverá implementar mecanismos que garantam que o usuário não consiga alterar as configurações de segurança dos ativos tecnológicos da organização;

12.7. A SETD deverá bloquear o uso de mídia removível nos dispositivos tecnológicos da organização.

Parágrafo único: exceções poderão ser concedidas pela CSIC mediante justificativa plausível e preenchimento do Termo de Responsabilidade disponibilizado no Apêndice III dessa Política.

12.8. A SETD deve segregar suas redes, no mínimo, em: domínio de acesso público (rede de visitantes), domínio de estação de trabalho e domínio de computador do tipo servidor.

12.9. É vedada a utilização em Nuvem (Cloud Computing) que não seja disponibilizada pela SETD.

12.10. O usuário deve manter as mesas de trabalho limpas — em relação aos papéis e mídias de armazenamento removíveis que contenham informações sensíveis.

12.11. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

12.12. A SETD deve implementar o bloqueio automático de tela do computador a partir de 2 (dois) minutos de inatividade.

Parágrafo único: sempre que se ausentar da frente do computador, o servidor, estagiário ou trabalhador terceirizado deve efetuar, imediatamente, o bloqueio do dispositivo ou a desconexão.

13. ACESSO LÓGICO

13.1. A SETD deve criar mecanismos para restringir, por meio da definição de perfis de acesso, o acesso à informação e às funções dos softwares;

Parágrafo único: os perfis de acesso devem ser definidos conforme premissas da necessidade de conhecer, necessidade de uso e menor privilégio (tudo é proibido a menos que expressamente permitido).

13.2. Os pedidos para a concessão de novos acessos ou a remoção de acessos existentes devem ser encaminhados à área de Segurança e Tecnologia da Informação por meio da ferramenta oficial de solicitações da organização.

Parágrafo único: a SETD deve manter registro de todas as ações referentes às solicitações, autorizações, criações e exclusões de identidade, bem como concessões e revogações dos direitos de acesso.

13.3. Todos os acessos devem ser revistos, periodicamente, pelo gerente responsável.

Parágrafo Primeiro: em casos de afastamento, mudança de responsabilidades, lotação ou atribuições dentro da SETD, torna-se necessário realizar uma revisão imediata dos direitos de acesso e uso dos ativos. A Coordenadoria Administrativa de Recursos Humanos (COOADM) é responsável por comunicar aos setores pertinentes para efetuarem as devidas alterações.

Parágrafo Segundo: no momento do desligamento do usuário, todos os direitos de acesso e uso dos ativos de informação a ele atribuídos devem ser encerrados. A Coordenadoria Administrativa de Recursos Humanos (COOADM) é encarregada de notificar os setores responsáveis para procederem com esse desligamento.

13.4. A SETD deve definir e implementar uma política de senhas, a qual deve ser definida pelo gestor do sistema, para todas as suas aplicações.

Parágrafo Primeiro: as senhas da organização devem ser criadas considerando, minimamente, a utilização de 10 caracteres sendo ao menos:

a) 1 (uma) letra maiúscula;

b) 1 (uma) letra minúscula;

c) 1 (um) número; e

d) 1 (um) caractere especial.

Parágrafo Segundo: a SETD deve implementar mecanismos para garantir que todos os usuários realizem a troca das senhas, preferencialmente, a cada 60 (sessenta) dias.

Parágrafo Terceiro: nos casos em que a senha inicial é fornecida pelo administrador do *software*, a SETD deve implementar a exigência de troca da senha no primeiro login em seus *softwares* que possuam esse recurso.

13.5. A SETD deve implementar a autenticação multifator (MFA) como medida de segurança essencial para o acesso aos seus sistemas e dados. A escolha e configuração das soluções de MFA devem considerar a robustez e a resistência a ataques conhecidos, priorizando métodos mais seguros e desencorajando o uso exclusivo de senhas descartáveis via SMS (OTP SMS) quando existirem alternativas mais seguras.

Parágrafo único: A SETD deverá buscar a conscientização de seus usuários sobre a importância da MFA e os riscos associados a tentativas de fraude que busquem contornar esse controle.

13.6. Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores da SETD, exceto nos casos de redes destinadas para tais pessoas, ou em casos previstos na legislação vigente.

14. ACESSO FÍSICO

14.1. A SETD deve implementar, em suas dependências, vigilância, portaria ou recepção, bem como catracas com sistemas baseados em cartão de acesso, biometria ou reconhecimento facial, a fim de detectar acessos não autorizados ou comportamento suspeitos.

Parágrafo único: a entrada e saída de visitantes ao escritório da SETD devem ser registradas pela recepção. Além disso, a visita deve ser guiada pela recepção ao seu destino, bem como pelo servidor, estagiário ou trabalhador terceirizado até a saída do escritório.

14.2. A SETD deve prover meios de identificação visível (por meio de crachás) a todos os servidores, funcionários, estagiários, fornecedores, consultores e visitantes.

Parágrafo único: o uso dos crachás nas dependências da SETD é obrigatório.

14.3. Todos os acessos devem ser revistos, periodicamente, pelo responsável da área.

14.4. Nas subdivisões e salas do escritório onde estejam armazenadas informações sensíveis, a SETD deve implementar proteções contra acesso não autorizado.

14.5. A SETD deve proteger o cabeamento de energia e de telecomunicações contra danos e interferências — por meio de passagem em eletrocalhas, cabeamento estruturado e identificação por rótulos nas extremidades do cabeamento.

14.6. A SETD deve garantir que seu escritório possua, no mínimo, proteções físicas contra incêndio, inundação, descarga elétrica e explosão.

Parágrafo único: os controles implementados deverão ser testados periodicamente dentro do PCN da organização.

15. USO DO E-MAIL E REDE LOCAL

15.1. Não é permitido cadastrar o e-mail corporativo em sites ou aplicativos para utilização pessoal, devendo ele somente ser utilizado estritamente para atividades profissionais relativas a SETD.

15.2. A SETD deve adotar mecanismos para reduzir o recebimento e o envio de mensagens indesejadas (SPAM, *Phishing*, entre outros) que representem risco ou que estejam em desconformidade com os normativos vigentes.

15.3. A internet deve ser utilizada para fins corporativos e inerentes às atividades diárias de cada usuário de informação.

Parágrafo único: Os acessos à internet serão fornecidos conforme o perfil e a necessidade de cada usuário, de modo a permitir a execução das suas atividades e o cumprimento de suas funções na Secretaria.

16. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

16.1. A SETD definirá, em seu Plano de Continuidade de Negócios (PCN), critérios para avaliar quando um evento de segurança da informação deve ser classificado como um incidente de segurança da informação.

16.2. A SETD deve estabelecer, em seu Plano de Continuidade de Negócios (PCN), um processo para a gestão de incidentes de segurança da informação, abordando como detectá-los, priorizá-los, analisá-los, resolvê-los e comunicá-los, além de definir como serão identificadas e tratadas as lições aprendidas.

Parágrafo único: Na fase de resolução do incidente, o PCN deve estabelecer as etapas de contenção, erradicação e recuperação.

16.3. A SETD deve garantir, por meio do seu PCN, que os incidentes de segurança da informação possuam um

registro das ações realizadas — desde o relato ou detecção até a resolução.

16.4. A SETD deve garantir que as evidências dos incidentes de segurança da informação sejam identificadas, coletadas e preservadas, a fim de embasar as ações disciplinares ou legais.

16.5. Em caso de roubo ou furto do equipamento, o colaborador ou terceiro afetado deve imediatamente informar o ocorrido à área de Segurança e Tecnologia da Informação, via procedimento estabelecido, bem como deve registrar o boletim de ocorrência.

16.6. A SETD deve monitorar proativamente o ambiente cibernético da organização, garantindo o tratamento eficiente de incidentes e reduzindo o tempo de resposta.

17. RISCOS DE SEGURANÇA DA INFORMAÇÃO

17.1. A SETD deve definir critérios, em seu Plano de Continuidade de Negócios (PCN), para classificar os riscos de segurança da informação identificados e para avaliar o respectivo nível de impacto para a organização.

17.2. A SETD deve estabelecer um processo para a gestão de riscos de segurança da informação, com um escopo definido que aborde como identificá-los, analisá-los, avaliá-los, tratá-los, monitorá-los e comunicá-los.

Parágrafo único: Na etapa de tratamento dos riscos, a SETD deverá definir critérios para a aceitação dos riscos.

17.3. A SETD deve garantir que o processo de riscos de segurança da informação possua registro das ações realizadas durante todo o ciclo.

18. MONITORAMENTO E AUDITORIA

18.1. Todo usuário de informação, seja interno seja externo, na função de custodiante, está sujeito ao monitoramento e à auditoria de suas ações nos ativos que compõem o ambiente computacional da SETD. Essa medida visa detectar atividades anômalas ou não autorizadas, bem como investigar incidentes, auditorias e demandas da corregedoria — as quais são devidamente autorizadas pela autoridade competente.

19. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

19.1. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento contínuo ou a recuperação antecipada da SETD, quando da ocorrência de indisponibilidade dos recursos de infraestrutura, de tecnologia ou de recursos humanos (isolada ou simultaneamente).

19.2. A SETD deverá implementar um Plano de Continuidade de Negócios (PCN), a fim de garantir a continuidade dos serviços críticos da organização.

Parágrafo Primeiro: O PCN deve ser aprovado pela CSIC.

Parágrafo Segundo: A SETD deve testar, periodicamente, a eficácia do plano desenvolvido.

19.3. A SETD deve garantir que os ativos tecnológicos possuam redundância suficiente para atender aos requisitos de disponibilidade da informação.

19.4. A SETD deve garantir a existência de redundâncias para seus ativos, terceirizados ou não. Além disso, deve assegurar que essas redundâncias sejam testadas periodicamente, para que protejam os dispositivos tecnológicos contra indisponibilidades causadas por interrupções ou por falhas no fornecimento de energia elétrica, de telecomunicações e de ar-condicionado. Por fim, cabe à SETD monitorar a conformidade dos fornecedores com os Acordos de Nível de Serviço (SLAs) estabelecidos e garantir a realização dos testes do Plano de Continuidade de Negócios (PCN), minimizando o impacto nas operações.

20. DAS PENALIDADES

20.1. Serão devidamente apuradas ações que violem esta política ou quaisquer de suas diretrizes, normas e procedimentos, ou ações que descumpram os controles de segurança da informação. Nesses casos, aos responsáveis, poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

20.2. Responsabilizações e penalidades previstas no Plano de Integridade da SETD.

20.3. Responsabilizações e penalidades existentes no Código de Ética e de Conduta Profissional da SETD.

21. VIGÊNCIA

21.1. Esta política entrará em vigor na data de sua publicação.

22. INSTRUMENTOS NORMATIVOS

Lei Federal nº 12.527, de 18/11/2011 - Lei de Acesso à Informação (LAI).
Lei Federal nº 13.709, de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Decreto Estadual nº 48.891, de 10/01/2024 - que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, em conformidade com a LGPD.
Instrução Normativa GSI/PR nº 1, de 27/05/2020, do Gabinete de Segurança Institucional da Presidência da República, publicada no Diário Oficial da União em 28/05/2020 - que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.
Instrução Normativa GSI/PR nº 5, de 30/08/2021, do Gabinete de Segurança Institucional da Presidência da República, publicada no Diário Oficial da União em 31/08/2021 - que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da Administração Pública Federal.
Instrução Normativa PRODERJ/PRE nº 07, de 29/05/2025 - 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.
Portaria PRODERJ/PRE nº 825, de 26/02/2021 - que institui a Política de Governança, a Estratégia da Governança e as normas do Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação (PEDTIC) no âmbito do Poder Executivo da administração pública estadual direta e indireta do estado do Rio de Janeiro.
Portaria PRODERJ/PRE nº 968, de 05/08/2022 - que institui o Manual de Procedimentos Regulatórios de Segurança da Informação a ser adotado por todas as Repartições, Técnicas e Administrativas, no âmbito do PRODERJ.
ABNT NBR ISO/IEC 27001:2022, Versão Corrigida 2023 - norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão da Segurança da Informação no contexto da organização.
ABNT NBR ISO/IEC 27002:2022 - norma que fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientações para implementá-los.
ABNT NBR ISO/IEC 27005:2023 - norma que fornece orientações para uma abordagem de riscos de segurança da informação.
ABNT NBR ISO/IEC 31000:2018 - norma que fornece diretrizes associadas a uma abordagem comum para gerenciar riscos enfrentados pelas organizações.
ABNT NBR ISO/IEC 22301:2020 - norma que especifica a estrutura e os requisitos para implementação e manutenção de um Sistema de Gestão de Continuidade de Negócios (SGCN).

23. APÊNDICES

APÊNDICE I

TERMO DE RESPONSABILIDADE E CONFICENCIALIDADE

Eu, _____, matrícula n.º [_____], CPF n.º [_____], RG n.º [_____], lotado(a) no(a) [_____] , doravante denominado simplesmente **Funcionário**, em razão do meu vínculo com a Secretaria de Estado de Transformação Digital, com sede na Rua da Conceição, nº 69, 25º andar, Centro, Rio de Janeiro/RJ, CEP: 20051-011, doravante denominada **SETD**, firmo o presente **TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE**, mediante as estipulações consignadas neste instrumento:

1. O **Funcionário** declara, expressamente, por este ato:

   1.1.Conhecer os termos da Resolução nº. ____/2025, de ____ de _____ de 2025 (Política de Segurança da Informação) e demais normas e procedimentos relacionados à segurança da informação da **SETD**;

   1.2.Conhecer o Decreto Estadual nº 48.891, de 10 de janeiro de 2024, e suas obrigações;

   1.3.Estar ciente de minhas obrigações quanto à salvaguarda das informações por mim acessadas em virtude de minhas atribuições funcionais na **SETD;**

1.4.Estar em concordância quanto a cumprir os regulamentos apresentados, ciente de que não os cumprir poderá acarretar a aplicação de sanções administrativas, civis e penais, na forma da Lei;

1.5.Estar ciente de que não devo criar expectativa de privacidade em relação às minhas atividades no ambiente computacional corporativo e de que meus acessos poderão ser registrados, auditados ou investigados pela **SETD**, em caso de incidentes de segurança da informação; e

1.6.Estar em concordância quanto a notificar o setor de Pessoal da **SETD** sobre quaisquer circunstâncias que possam tornar falsas, imprecisas ou incompletas as declarações anteriores.

2. Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura.

E, por estar de acordo com o inteiro teor deste Termo, o assino nesta data, para que produza seus efeitos jurídicos e legais.

_____, _____/_____/_____

_____

(ASSINATURA)

APÊNDICE II

TERMO DE RESPONSABILIDADE E COMPROSSIMO DE SIGILO, CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS

A empresa, _____, CNPJ n.º [_____], doravante denominada simplesmente CONTRATADA, em razão do seu vínculo com a Secretaria de Estado de Transformação Digital, com sede na Rua da Conceição, nº 69, 25º andar, Centro, Rio de Janeiro/RJ, CEP: 20051-011, doravante denominada SETD, firma o presente **TERMO DE RESPONSABILIDADE E COMPROMISSO DE SIGILO, CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS**, mediante as estipulações consignadas neste instrumento:

- **PARÁGRAFO PRIMEIRO:**

  A CONTRATADA deverá manter sigilo sobre toda informação confidencial, reservada ou exclusiva (incluindo informações técnicas, de negócio ou financeiras), comunicada pela SETD ou obtida em função da execução do objeto contratado, exceto as informações que:

  - Sejam de domínio público à época da comunicação;
  - Sejam conhecidas pela parte receptora antes da comunicação ou que se tornem disponíveis em domínio público sem culpa da parte receptora; e
  - Sejam desenvolvidas, de modo independente, pela parte receptora, sem uso de informação confidencial.

- **PARÁGRAFO SEGUNDO:**

  A SETD e a CONTRATADA devem cumprir a Lei Federal nº 13.709/2018 e o Decreto Estadual nº 48.991/2024 no âmbito da fiscalização, da guarda dos dados e da execução do objeto deste Contrato.

- **PARÁGRAFO TERCEIRO:**

  A CONTRATADA deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados de guarda e responsabilidade da SETD, na medida em que sejam estritamente necessários para as finalidades deste Contrato. Ainda, a CONTRATADA deve cumprir a legislação aplicável, assegurando que todos os indivíduos acima mencionados estejam sujeitos a compromissos de

confidencialidade ou a obrigações profissionais de confidencialidade; e

A CONTRATADA deve assegurar que todos os empregados, prepostos ou colaboradores assinem o TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE disponibilizado pela SETD.

- **PARÁGRAFO QUARTO:**

Considerando a natureza dos dados tratados, pertinentes ao objeto desta contratação, a SETD e a CONTRATADA deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- **PARÁGRAFO QUINTO:**

A CONTRATADA deve notificar imediatamente, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da SETD, a ocorrência de qualquer incidente de segurança relacionado a dados pessoais por ela tratados. A notificação inicial deve ser realizada por [especificar canal, e.g., e-mail para seguranca@setd.gov.br ou telefone de emergência XXXX-XXXX] e incluir, no mínimo, o tipo de incidente, data/hora estimada, sistemas envolvidos e contato do responsável pela notificação na CONTRATADA. Informações adicionais deverão ser fornecidas para que a SETD cumpra suas obrigações de comunicação à Autoridade Nacional e aos titulares dos dados.

- **PARÁGRAFO SEXTO:**

A SETD e a CONTRATADA devem adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança, quando identificada a responsabilização exclusiva de uma parte e/ou de outra.

- **PARÁGRAFO SÉTIMO:**

A CONTRATADA, na execução dos serviços de plataforma de serviços digitais, deve auxiliar a SETD na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018 e no Decreto Estadual nº 48.991/2024, no âmbito da execução deste Contrato.

- **PARÁGRAFO OITAVO:**

Por ocasião do encerramento deste Contrato, a CONTRATADA deve, imediatamente ou mediante justificativa, em até 10 (dez) dias úteis da data de encerramento, fornecer, à SETD, a base de dados do atendimento, inclusive eventuais cópias de dados pessoais tratados no âmbito do Contrato, certificando por escrito, à SETD, o cumprimento dessa obrigação.

- **PARÁGRAFO NONO:**

A CONTRATADA deve manter registros detalhados de todas as operações de tratamento de dados pessoais realizadas sob este Contrato, em conformidade com a Lei Federal nº 13.709/2018 (LGPD).

- **PARÁGRAFO DÉCIMO:**

A CONTRATADA deve colocar à disposição da SETD, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta CLÁUSULA, bem como deve permitir auditorias e contribuir com elas, incluindo inspeções, pela SETD ou auditor por ela indicado, em relação ao tratamento de dados pessoais do cidadão, acessados na base de dados da SETD.

- **PARÁGRAFO DÉCIMO PRIMEIRO:**

A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados à SETD ou a terceiros, decorrentes do descumprimento da Lei Federal nº 13.709/2018 ou do Decreto Estadual nº 48.991/2024, não excluindo ou reduzindo essa responsabilidade à fiscalização da SETD em seu acompanhamento.

- **PARÁGRAFO DÉCIMO SEGUNDO:**

É vedada a utilização ou transferência de dados pessoais, pela CONTRATADA, sem o prévio consentimento, por escrito, da SETD, e sem a demonstração da observância, pela CONTRATADA, da adequada proteção desses dados e das regulamentações aplicáveis quanto à localização e soberania dos dados. Cabe à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro(s) país(es) aplicáveis.

- **PARÁGRAFO DÉCIMO TERCEIRO:**

A CONTRATADA deve tomar medidas razoáveis para assegurar que empregados, prepostos ou colaboradores, de qualquer subcontratado, que necessitem conhecer/acessar dados pessoais relacionados à execução do contrato, estejam sujeitos a compromissos de confidencialidade ou a obrigações profissionais de confidencialidade. A SETD se reserva o direito de exigir comprovações periódicas ou realizar verificações de conformidade sobre as políticas e práticas de segurança dos subcontratados da CONTRATADA, no que tange ao tratamento de dados da SETD.

- **PARÁGRAFO DÉCIMO QUARTO:**

A SETD é a controladora dos dados gerados pelo contrato na prestação dos serviços realizada pela CONTRATADA, cabendo, por meio de normas e regras a serem definidas pela SETD, a delegação à CONTRATADA para o tratamento dos dados obtidos.

- **PARÁGRAFO DÉCIMO QUINTO:**

O descumprimento de quaisquer das cláusulas deste Termo, incluindo as relativas a sigilo e proteção de dados, poderá acarretar a rescisão contratual imediata, sem prejuízo das sanções administrativas, civis e penais cabíveis, conforme a legislação vigente e o contrato principal.

Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura.

E, por estar de acordo com o inteiro teor deste Termo, o assina nesta data, para que produza seus efeitos jurídicos e legais.

_____, _____/_____/_____

_____

(ASSINATURA)

APÊNDICE III

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DE DISPOSITIVOS REMOVÍVEIS

A utilização de dispositivos de armazenamento removíveis representa uma fonte potencial de infecção para a rede de computadores, sujeita a diversos tipos de *malware*, como vírus, *worms*, *adware*, *spyware*, *ransomware*, *bots*, *rootkits* e outras ameaças maliciosas transmitidas por mídias digitais. Além disso, pode permitir a propagação de dados e informações corporativos para além da rede privada da Secretaria de Estado de Transformação Digital (SETD).

Este termo tem como objetivo atribuir responsabilidade ao usuário descrito abaixo, que concorda expressamente, juntamente com seu gestor imediato, que é sua responsabilidade manter a segurança, integridade e confidencialidade dos dados e informações contidos no dispositivo removível, bem como do equipamento utilizado para conexão e acesso ao dispositivo de armazenamento removível — seja *USB,* seja aqueles de barramentos similares.

Eu, Eu, _____, matrícula n.º [_____], CPF n.º [_____], RG n.º [_____], lotado(a) no(a) [_____] ,declaro ter solicitado permissão para utilizar dispositivos removíveis nos equipamentos de tecnologia da Secretaria de Estado de Transformação Digital (SETD), comprometendo-me a utilizar essa autorização com plena ciência das seguintes condições:

1. São considerados dispositivos móveis aqueles equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, dentre os quais se incluem *USB*, HD Externo, cartões de memória, *notebooks*, *smartphones*, *drives* e similares.
2. O uso de dispositivos móveis removíveis deve ser tratado como exceção absoluta, em razão de potencial vulnerabilidade de segurança dos dados pertencentes à Secretaria de Estado de Transformação Digital (SETD).
3. A utilização de dispositivos móveis removíveis traz responsabilidade direta pelos riscos e impactos

oriundos da utilização desses equipamentos, considerando a possibilidade de vírus e *softwares* maliciosos potencialmente danificarem e corromperem dados e/ou equipamentos tecnológicos da Secretaria de Estado de Transformação Digital (SETD).

4. O uso de dispositivos móveis removíveis deve ser realizado apenas por imperiosa necessidade de trabalho ou por determinação expressa do superior hierárquico, em estrita obediência às determinações de utilização de sistemas.
5. A gravação de dados em dispositivos móveis removíveis deve ser realizada com criteriosa cautela, não devendo ser tratada fora do âmbito profissional nem das atribuições de competência das funções exercidas.
6. O dispositivo móvel removível com dados obtidos dos sistemas governamentais não deve ser, em hipótese alguma, entregue a terceiros.
7. Caso ocorram omissões passíveis de gerar risco ou de comprometer os dados sob guarda da Secretaria de Estado de Transformação Digital (SETD) que estejam armazenados nos dispositivos móveis removíveis, seu portador deverá responder em toda instância por suas consequências.
8. É de integral responsabilidade do portador do dispositivo móvel removível o cuidado pela integridade, confidencialidade e disponibilidade dos dados da Secretaria de Estado de Transformação Digital (SETD) ali armazenados.
9. O acesso à informação armazenada no dispositivo móvel removível, obtida nos equipamentos tecnológicos da Secretaria de Estado de Transformação Digital (SETD), não garante ao portador do dispositivo direitos sobre ela, tampouco, confere-lhe autoridade para liberar acesso a terceiros.
10. A utilização de dispositivos móveis removíveis nos equipamentos tecnológicos da Secretaria de Estado de Transformação Digital (SETD) deve ser pautada nas diretrizes dispostas na Política de Segurança da Informação e da Comunicação, em adição aos Procedimentos de Segurança de Informação.
11. Configura-se descumprimento de normas legais e regulamentares, bem como quebra de sigilo funcional, a divulgação de dados e informações extraídos de banco de dados da Secretaria de Estado de Transformação Digital (SETD) e inseridos no dispositivo móvel removível.
12. Poderão configurar ilícito penal quaisquer condutas em desacordo com as determinações postas pela Comissão de Segurança da Informação e Comunicação, especialmente aquelas tipificadas como crimes contra a Administração Pública, conforme previsto no Código Penal Brasileiro.
13. A utilização de dispositivos móveis removíveis nos equipamentos tecnológicos da Secretaria de Estado de Transformação Digital (SETD) deve ser pautada pelas determinações da Lei de Acesso à Informação (Lei Federal n.º 12.527/20211), Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018) e Decreto Estadual n.º 48.891/2024, que institui a Política de Governança de Dados Pessoais do Estado do Rio de Janeiro.

Por fim, declaro que as informações prestadas acima representam a legítima expressão da verdade e aceito as condições deste Termo de Responsabilidade.

_____, _____/_____/_____

_____

Assinatura do solicitante

Documento assinado eletronicamente por **Larissa Tagarro Fernades**, **Assessora**, em 11/09/2025, às 16:59, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Rua da Conceição, nº 69, 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: 2333-0333 - https://www.rj.gov.br/digital