POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO E PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO

FEVEREIRO 2024 – 1ª EDIÇÃO

Secretaria de Transformação Digital

GOVERNO DO ESTADO
RIO DE JANEIRO

Secretaria de Transformação Digital

GOVERNO DO ESTADO
RIO DE JANEIRO

SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL – SETD

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO E PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO

FEVEREIRO 2024 – 1ª EDIÇÃO

Sumário

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
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*

1. Da Elaboração

Status do Documento

ELABORAÇÃO	2024
REVISÃO ANUAL	Não
REVISÃO EXTRAORDINÁRIA	-

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

2. Abrangência da Política de Segurança da Informação e Comunicação

2.1. Para os fins do disposto nesta Política, a segurança da informação e comunicação abrange:

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

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

2.3. Os agentes públicos a serviço da Secretaria de Estado de Transformação Digital (SETD) devem observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta Política.

2.4. Integram também a Política as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

2.5. 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.

2.6. No âmbito da presente Política, considera-se:

i. **Acesso**: ato de ingressar, transitar, conhecer, ou consultar dados, ou informações, bem como, a possibilidade de usar os ativos de informação;

ii. **Agente público**: servidores, consultores, estagiários, prestadores de serviços que, por força de contratos, convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas que os tornem autorizados a obter acesso a informações e sistemas da SETD;

iii. **Ameaça**: conjunto de fatores internos, externos, ou causa potencial de um incidente, que pode resultar em comprometimento da segurança dos ativos da organização;

iv. **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a organização;

v. **Ativo Crítico**: ativo do qual a organização depende, em maior ou menor grau, para a continuidade de suas atividades e serviços;

vi. **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, materializadas ou não, bem como, os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

vii. **Autenticação**: confirmação acerca da identidade de um usuário ou sistema para fins de acesso, ou execução de operações. Podem ser utilizados fatores múltiplos de autenticação, a exemplo de certificação digital, informações biométricas, *login* e senha;

viii. **Autenticidade**: garantia de que o dado ou informação é verdadeiro e fidedigno na origem, em trânsito e no destino. Assevera a legitimidade e autoria do dado ou informação;

ix. **Avaliação de riscos**: procedimento de comparar um risco estimado com um critério, visando determinar a sua relevância;

x. **Classificação da informação**: identificação dos níveis de proteção das informações e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

xi. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoas físicas, sistemas, órgãos ou entidades não autorizadas;

xii. **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados para conceder, monitorar ou bloquear o acesso;

xiii. **Credencial de acesso**: recursos que identifiquem univocamente determinado usuário nos mais variados cenários: usuário/senha de rede, crachá, carimbo, correio eletrônico, certificado digital e assinatura GOV.BR;

xiv. **Criptografia**: conjunto de técnicas pelas quais a informação pode ser transformada de sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por alguém não autorizado;

xv. **Criticidade**: grau de importância da informação para a continuidade das atividades e serviços da SETD;

xvi. **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação, materializados ou não, que não lhe pertencem, mas que estão sob sua custódia;

xvii. **Gestor de Segurança da Informação**: é aquele que elabora e atualiza periodicamente os procedimentos de segurança da informação e comunicação da SETD;

xviii. **Responsável pelo Tratamento e Resposta a Incidentes**: é aquele que monitora os recursos de TIC, detecta e realiza as análises dos incidentes de segurança da informação e reporta ao Encarregado pelo Tratamento de Dados Pessoais;

xix. **Encarregado pelo Tratamento de Dados Pessoais**: é aquele que aceita as reclamações e comunicações dos titulares, presta esclarecimentos e adota providências junto à Autoridade Nacional de Proteção de Dados (ANPD);

xx. **Desastre**: catástrofes naturais, pandemias, incêndios, inundações, inacessibilidade ao local de trabalho, falhas nos sistemas de TI, dentre outros;

xxi. **Descarte**: eliminação de informações e documentos, em qualquer tipo de suporte, observando os procedimentos de segurança;

xxii. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

xxiii. **Evento**: ocorrência identificada como uma possível violação da segurança, falha de controles ou uma situação previamente conhecida que possa ter consequências para a segurança da informação;

xxiv. **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

xxv. **Gestão de continuidade dos negócios**: processo que identifica desastres potenciais para uma organização e os possíveis impactos nas operações de negócio, caso esses desastres se concretizem. Esse processo fornece estrutura para que se desenvolva e mantenha o plano de continuidade de negócios, capaz de manter o funcionamento dos processos e salvaguardar a reputação e a marca da organização e suas atividades de valor agregado;

xxvi. **Gestão de Riscos**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

xxvii. **Grau de sigilo**: gradação atribuída aos ativos de informação em decorrência do teor e elementos intrínsecos das informações e dados sigilosos que contenham;

xxviii. **Impacto**: alteração no nível de disponibilidade, integridade, confidencialidade e autenticidade dos serviços e/ou ativos de informação disponíveis para os agentes públicos;

xxix. **Incidentes**: eventos que tenham causado algum dano, colocado em risco algum ativo de informação ou interrompido a execução de alguma atividade por um período;

xxx. **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

xxxi. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada, ou acidental;

xxxii. **Quebra de segurança**: ação ou omissão, intencional ou acidental, resultando no comprometimento da segurança da informação e das comunicações;

xxxiii. **Recursos criptográficos**: sistemas, programas, processos e equipamentos isolados ou em rede que utilizem algoritmo simétrico ou assimétrico para realizar a cifração ou decifração de informações;

xxxiv. **Recursos de TI**: subgrupo dos ativos de informação dedicados à produção, armazenamento, transmissão e processamento de informações; e

xxxv. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. Dos Princípios

3.1. 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, assim como, também o princípio da dignidade da pessoa humana prevista no art. 1^0 inciso III da Constituição da República, e o art. 5^0 da Constituição do Estado do Rio de Janeiro, e também os 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 02, de 28 de abril de 2022, bem como, pela:

i. Confidencialidade;
ii. Integridade;
iii. Disponibilidade;
iv. Autenticidade;
v. Publicidade;
vi. Responsabilidade;
vii. Não repúdio; e
viii. Prevenção.

4. Da Comissão de Segurança da Informação e Comunicação

4.1. Fica estabelecida a Comissão de Segurança da Informação e Comunicação, incumbida de propor, debater, aprimorar e difundir a cultura e aplicação das normas relacionadas à segurança da informação e comunicação no âmbito da SETD.

- A composição da Comissão de Segurança da Informação e Comunicação será a seguinte, preferencialmente:

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.

5. Das Diretrizes

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

II. O uso das informações deverá ser feito apenas para o desempenho das atividades profissionais ou para a geração de políticas públicas.

5.2. Todos os contratos, ou ainda, Acordo de Cooperação Técnicas celebradas pela SETD com prestadores de serviços, ou outros entes, devem conter cláusulas que determinem a observância da Política de Segurança da Informação e Comunicação e seus respectivos documentos, bem como, a manutenção do sigilo de suas informações durante e após sua vigência.

5.3. Todos os servidores, terceiros e/ou fornecedores, em qualquer vínculo, função ou nível hierárquico na SETD, que tenham contato e/ou acesso, de qualquer tipo, aos recursos de tecnologia da informação e comunicação são responsáveis pela segurança, zelo e bom uso dos ativos às quais têm acesso.

5.4. 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.

5.5. Toda informação custodiada em ativos de Tecnologia da Informação e Comunicação, na SETD, ou em terceiros, deve ser protegida para não ser alterada, acessada ou eliminada indevidamente.

5.5.1 A Política de Segurança da Informação e Comunicação trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos vitais da SETD, consoante a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como, os valores éticos e as melhores práticas de Segurança da Informação.

5.5.2 Deverão ser adotados instrumentos de declaração de responsabilidade e compromisso de sigilo e confidencialidade sobre toda e qualquer informação, que seja obtida em razão da relação institucional com a SETD a serem assinados e entregues pelas pessoas previstas nesta diretriz, nas fases de admissão, nomeação e contratação, inclusive por empresas terceiras, em conformidade com o Decreto Estadual 48.891/2024.

5.6. Todas as instalações e equipamentos devem ser protegidos contra acessos não autorizados. As repartições, técnicas e administrativas, devem implementar mecanismos de proteção que impeçam acesso indevido aos ativos de Tecnologia da Informação e Comunicação e às áreas em que se encontram.

5.7. Todos os usuários devem ser orientados a manter em absoluto sigilo suas senhas, sendo vedada a divulgação ou compartilhamento com terceiros, a fim de preservar os ativos de tecnologia da informação.

6. Dos Recursos de Tecnologia da Informação

6.1. 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.

6.2. É terminantemente vedado o uso dos recursos computacionais disponibilizados para armazenar ou transmitir qualquer conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso. A utilização desses recursos deve ser pautada por princípios éticos e legais, respeitando os padrões de conduta estabelecidos pela Secretaria. A responsabilidade pelo cumprimento dessas diretrizes recai sobre cada usuário, que deve zelar pela integridade e reputação da instituição ao empregar os meios tecnológicos disponíveis.

6.3. O uso dos recursos computacionais por parte dos agentes públicos ou de terceiros na rede da SETD está sujeito à monitoração, observando-se rigorosamente os princípios constitucionais e legais aplicáveis. Tal monitoramento visa garantir a segurança, integridade e eficiência dos sistemas, bem como, assegurar a conformidade com as normativas vigentes.

6.4. É expressamente vedado aos agentes públicos ou a terceiros, sem a devida autorização, realizar alterações, sejam físicas ou lógicas, nas estações de trabalho disponibilizadas pela SETD. Tal restrição visa assegurar a estabilidade, segurança e eficiência do ambiente computacional da instituição.

6.5. Os ativos de informação devem ser inventariados e protegidos, além de serem identificados os seus proprietários e/ou custodiantes.

6.6. A implementação de recursos criptográficos é essencial para assegurar a segurança no trânsito e armazenamento das informações, devendo ser considerada conforme a sua classificação específica.

7. Das Normas Complementares

7.1. 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).

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

8. Da Gestão e Continuidade de Negócios

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

8.2. O Plano de Continuidade de Negócios (PCN) da SETD, baseado em metodologias e boas práticas e aprovado pela Comissão de Segurança da Informação e Comunicação, deverá ser desenvolvido, implementado e testado periodicamente, a fim de garantir a continuidade dos serviços críticos, estabelecido pela norma ABNT NBR ISO 22313.

9. Dos Controles de Acesso

9.1. As instalações, equipamentos, redes e sistemas de computadores, com exceção dos sistemas destinados ao atendimento ao público, devem ser dotados de mecanismos apropriados para controle de acesso físico e/ou lógico, a fim de permitir a identificação das pessoas.

9.2. Quando da contratação de colaborador mediante concurso público ou seleção pública, deverá ser prevista em edital e em cláusula contratual uma seleção criteriosa, especificando a obrigatoriedade da apresentação de cópia de certidão negativa criminal (trânsito em julgado), bem como, a assinatura de Termo de Responsabilidade e Confidencialidade, especificado no Anexo desta Política.

9.3. Todos os agentes, colaboradores, consultores ou terceiros da SETD deverão assinar o Termo de Responsabilidade e Confidencialidade, especificado no Anexo desta Política.

9.4. O controle operacional de uma atividade crítica não pode ser exclusivamente atribuído a uma única pessoa.

9.5. Para a utilização dos recursos de TIC da SETD, é indispensável a autenticação por meio de credencial de acesso.

9.6. As credenciais de acesso devem conceder ao portador apenas os níveis de privilégio mínimos necessários para o desempenho de suas funções.

9.7. Equipamentos e *softwares* utilizados na administração dos recursos de TI devem ser protegidos por senha, conhecida exclusivamente pelos responsáveis pela administração desses recursos.

9.8. 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.

9.8.1 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.

9.9. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário, a qualquer tempo, ou por determinação, especialmente quando houver suspeita de sua violação.

9.10. 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. Deverão ser implementados controles de acesso físico para o acesso às dependências da SETD, com a disponibilização de credenciais que permitam o devido acesso, sempre que possível.

9.12. Deverão ser disponibilizadas credenciais de acesso físico também aos visitantes, as quais permitirão o acesso destes às instalações da SETD, sempre mediante A DEVIDA autorização.

9.13. 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.

10. Das Penalidades

10.1. Ações que violem esta política ou quaisquer de suas diretrizes, normas e procedimentos, ou que quebrem os controles de segurança da informação, serão devidamente apuradas e aos responsáveis poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

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

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

11. Das Competências

11.1. A SETD deverá prover os recursos humanos e materiais necessários à aplicação da Política de Segurança.

11.2. Compete ao Gestor de Segurança da Informação dos órgãos e entidades, conforme a Seção I do Art.17 da IN 02 do PRODERJ:

i. Elaborar e atualizar periodicamente os procedimentos de segurança da informação do órgão/entidade que seja responsável;

ii. Implementar e monitorar permanentemente 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. Promover a cultura de segurança da informação no âmbito de atuação do órgão e de seus colaboradores;

iv. Acompanhar eventos e danos decorrentes de incidentes e eventos de segurança da informação;

v. 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;

vi. Propor recursos necessários às ações de segurança da informação, no âmbito de atuação do seu órgão ou entidade; e

vii. Indicar os responsáveis pelo tratamento de resposta a incidentes no âmbito de atuação do órgão.

11.3. O Gestor de Segurança da Informação será designado dentre os servidores públicos civis ou militares ocupantes de cargos efetivos, desde que lotados no órgão ou entidade e com formação ou capacitação técnica compatível às suas atribuições.

11.4. Compete ao Responsável pelo Tratamento e Resposta a Incidentes, conforme a Seção II do Art.17 da IN 02 do PRODERJ:

i. Monitorar os recursos de TIC, detectar e realizar as análises dos incidentes de segurança da informação;

ii. Reportar ao Encarregado pelo Tratamento de Dados Pessoais os incidentes envolvendo tais dados;

iii. Identificar vulnerabilidades;

iv. Receber e propor respostas a notificações relacionadas a incidentes de segurança da informação; e

v. Coordenar e executar atividades de tratamento e resposta a eventos de segurança da informação.

11.5. O Responsável pelo Tratamento e Resposta a Incidentes será designado dentre os servidores públicos civis ou militares ocupantes de cargos efetivos, desde que lotados no órgão ou entidade e com formação ou capacitação técnica compatível às suas atribuições.

11.6. Compete ao Encarregado pelo Tratamento de Dados Pessoais, conforme a Seção III do Art.17 da IN 02 do PRODERJ:

i. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

ii. Receber comunicações da 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. Requerer relatório das áreas responsáveis por tratamento de dados pessoais no âmbito dos órgãos administrativos contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e

vi. Atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, na forma da Lei Federal n.º 13.709/2018 - LGPD.

11.7. Compete à Coordenadoria Administrativa e Recursos Humanos (COOADM) da SETD:

i. Notificar, por meio do SEI-RJ, as áreas responsáveis sobre qualquer alteração de cargo, função ou lotação de funcionários, consultores ou terceiros, bem como, sobre afastamentos destes por períodos superiores a 30 (trinta) dias;

ii. Notificar, por meio do SEI-RJ, as áreas responsáveis sobre o desligamento de funcionários, consultores ou terceiros; e

iii. Promover a capacitação dos agentes públicos para os quesitos referentes as normas de segurança da informação.

12. Das Disposições Finais

12.1. É vedada a utilização de usuário administrador local e unidades de armazenamento USB (*pen drives*, HDs externos etc.) em estações de trabalho, salvo em casos excepcionais, mediante justificativa e preenchimento de "Termo de Responsabilidade e Confidencialidade" e parecer da Comissão de Segurança.

12.2. 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 Anexo desta Política.

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

12.4. Apenas os equipamentos e *softwares* disponibilizados e/ou homologados pelo PRODERJ, ou pela SETD, podem ser instalados e conectados à rede da Secretaria.

12.5. 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.

12.6. Casos excepcionais poderão ser vistos pela Comissão de Segurança da Informação mediante justificativa e preenchimento de Termo de Responsabilidade e Confidencialidade.

13. 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 02, de 28/04/2022, 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 - 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 - 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 dentro do contexto da organização.
ABNT NBR ISO/IEC 27002:2022 - Norma de fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implementação.

Rio de Janeiro, 20 de fevereiro de 2024.

JOSÉ MAURO DE FARIAS JUNIOR
Secretário de Estado

14. Anexo

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO E PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Eu, _____, Matrícula n.º [_____], CPF n.º [_____], RG n.º [_____], Órgão Expedidor [_____], lotado(a) no(a) [_____], doravante denominado simplesmente **FUNCIONÁRIO**, 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 CONFIDENCIALIDADE**, mediante as estipulações consignadas neste instrumento:

1. O **FUNCIONÁRIO** declara expressamente por este ato:

   1.1. Conhecer os termos da Resolução que aprova a Política de Segurança da Informação e demais normas e procedimentos em segurança da informação da **SETD**;

   1.2. Conhecer o Decreto Estadual nº 48.891/2024 e suas obrigações, a qual 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 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

   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 para cumprir os regulamentos apresentados, ciente de que o seu não cumprimento 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 as minhas atividades no ambiente computacional corporativo e 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 em 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 assina nesta data, para que produza seus jurídicos e legais efeitos.

_____, _____/_____/_____.

_____

[ASSINATURA]

ANEXO II

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO E PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO

TERMO DE RESPONSABILIDADE E COMPROMISSO 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 (**SETD**), 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:

I. PARÁGRAFO PRIMEIRO:

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

- Sejam de domínio público à época da comunicação;
- Seja conhecida pela parte receptora antes da comunicação ou caia no domínio público sem culpa da parte receptora; e
- Seja desenvolvida, de modo independente, pela parte receptora, sem uso de informação confidencial.

II. PARÁGRAFO SEGUNDO:

A SETD, e a CONTRATADA devem cumprir a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGDP) e o Decreto Estadual nº 48.891/2024 (Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro), no âmbito da fiscalização, da guarda dos dados e da execução do objeto deste Contrato.

III. 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, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou 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.

IV. 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 de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

V. PARÁGRAFO QUINTO:

A CONTRATADA deve notificar imediatamente, à SETD, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a SETD cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

VI. 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 outra.

VII. 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 48.891/2024, no âmbito da execução deste Contrato.

VIII. PARÁGRAFO OITAVO:

Por ocasião do encerramento deste Contrato, a CONTRATADA deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, fornecer, a 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 desta obrigação.

IX. PARÁGRAFO NONO:

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

X. PARÁGRAFO DÉCIMO:

A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a SETD, ou a terceiros, decorrentes do descumprimento da Lei Federal nº 13.709/2018 ou do Decreto Estadual nº 48.891/2024, não excluindo ou reduzindo essa responsabilidade a fiscalização da SETD em seu acompanhamento.

XI. PARÁGRAFO DÉCIMO PRIMEIRO:

É vedada a utilização ou transferência de dados pessoais, pela CONTRATADA, sem o prévio consentimento, por escrito, da SETD, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro(s) país(es) que for aplicável.

XII. PARÁGRAFO DÉCIMO SEGUNDO:

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 obrigações profissionais de confidencialidade, e cumprir, no tocante à subcontratação, todas as disposições aplicáveis da Lei Federal nº 13.709/2018 e o Decreto Estadual nº 48.891/2024.

XIII. PARÁGRAFO DÉCIMO TERCEIRO:

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, à delegação a CONTRATADA para o tratamento dos dados obtidos.

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 jurídicos e legais efeitos.

_____, _____/_____/_____.

_____

[ASSINATURA]