POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DRM-RJ
DEPARTAMENTO DE RECURSOS MINERAIS

Secretaria de
Desenvolvimento Econômico,
Indústria, Comércio e Serviços

GOVERNO DO ESTADO
RIO DE JANEIRO

DEPARTAMENTO DE RECURSOS MINERAIS DO ESTADO DO RIO DE JANEIRO - DRM-RJ

GOVERNADOR DO ESTADO DO RIO DE JANEIRO

Cláudio Bomfim de Castro e Silva

SECRETARIA DE ESTADO DE DESENVOLVIMENTO ECONÔMICO, INDÚSTRIA, COMÉRCIO E SERVIÇO

Fernanda Pereira Curdi (Interina)

PRESIDENTE DO DEPARTAMENTO DE RECURSOS MINERAIS

Luiz Claudio Almeida Magalhães

DIRETORIA DE ADMINISTRAÇÃO E FINANÇAS

Mariana Cristina Santiago Ouchana

DIRETORIA DE GEOLOGIA

Tulio Márcio Aguiar Oliveira

DIRETORIA DE MINERAÇÃO

Rodrigo Puccini Marques

ELABORAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ASSESSORIA DE INFORMÁTICA

Hélio Edson Da Costa Britto Junior

Fernando Cézar Martins

Alex Sandro Souza Da Costa Junior

SUMÁRIO

CONTROLE DE VERSÕES 5
CAPÍTULO I - ESCOPO 6
Seção I - Propósito 6
Seção II - Princípios 6
Seção III - Abrangência 7
CAPÍTULO II - REFERÊNCIAS LEGAIS E NORMATIVAS 7
CAPÍTULO III - TERMOS E DEFINIÇÕES 9
CAPÍTULO IV - PAPÉIS E RESPONSABILIDADES 12
CAPÍTULO V - DIRETRIZES 17
Seção I - Gestão de acesso 17
Seção II - Uso aceitável dos ativos de informação 20
Seção III - Trabalho remoto e uso de dispositivos móveis 24
Seção IV - Ambiente físico 25
Seção V - Classificação da informação 27
Seção VI - Transferência da informação 28
Seção VII - Privacidade 30
Seção VIII - Códigos maliciosos 30
Seção IX - Fornecedores 31
Seção X - Serviços em nuvem 31
Seção XI - Incidentes de segurança e de privacidade da informação 32
Seção XII - Vulnerabilidades técnicas 33
Seção XIII - Inteligência de ameaças 33
Seção XIV - Controles criptográficos e gerenciamento de chaves 33
Seção XV - Registro de auditoria 34
Seção XVI - Desenvolvimento de *software* interno ou terceirizado 35
Seção XVII - Cópia de segurança 38
Seção XVIII - Continuidade do negócio 39
Seção XIX - Uso de dispositivo pessoal no trabalho 39
CAPÍTULO VI - DOCUMENTOS COMPLEMENTARES 40
CAPÍTULO VII - EXCEÇÕES 41
CAPÍTULO VIII - AVALIAÇÃO DE DESEMPENHO 41
CAPÍTULO IX - PROCESSO DISCIPLINAR 41
CAPÍTULO X - VIGÊNCIA 42

CONTROLE DE VERSÕES

N°	VERSÃO	DATA	ALTERAÇÕES
0.1	Primeira versão para avaliação interna	02/04/2025	N/A
1.0	Versão aprovada pela presidência	12/05/2025	N/A

Obs. Cópias impressas deste documento podem não corresponder à última versão aprovada e em uso. A versão mais atualizada se encontra publicada em: https://rj.gov.br/drm/

Classificação:

Público

Críticas, Sugestões e Correções

Críticas, sugestões e correções a este documento podem ser enviadas para o e-mail informatica@drm.rj.gov.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

O presidente do Departamento de Recursos Minerais do Estado do Rio de Janeiro (DRM-RJ), no uso das atribuições que lhe são conferidas, emite a seguinte Política de Segurança da Informação e Comunicação (POSIC), vigente a partir da data de sua assinatura, revogando-se todas as disposições contrárias.

CAPÍTULO I - ESCOPO

Seção I - Propósito

Art. 1º - Esta política visa definir responsabilidades, deveres e penalidades quanto à segurança e à privacidade da informação, além de promover uma cultura de proteção às informações — sejam elas do DRM-RJ, do governo, do cidadão, de outros órgãos ou entidades, dos fornecedores, bem como de outras partes envolvidas em acordos com a Autarquia.

Seção II - Princípios

Art. 2º - As diretrizes estabelecidas nesta política (para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações) são norteadas pelos princípios de:

I - Confidencialidade: garantia de que a informação está acessível somente para pessoas, entidades ou processos autorizados;

II - Integridade: garantia de que a informação está exata;

III - Disponibilidade: garantia de que, quando preciso, a informação pode ser acessada pelas pessoas, entidades ou processos autorizados;

IV - Autenticidade: garantia de que a entidade é o que alega ser;

V - Legalidade: garantia de que o tratamento da informação ocorre de acordo com a legislação.

Seção III - Abrangência

Art. 3º - Esta política aplica-se aos servidores, estagiários, fornecedores, trabalhadores terceirizados e às partes envolvidas em acordos com o DRM-RJ (independentemente dos instrumentos administrativos utilizados para tal).

CAPÍTULO II - REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º - Esta política foi estabelecida considerando-se as seguintes referências normativas e legais:

I - ISO 27001: 2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de Gestão de Segurança da Informação;

II - ISO 27701: 2019 – Técnicas de segurança para gestão da privacidade da informação;

III - Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

IV - Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

V - Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

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

VII - Instrução Normativa PRODERJ/PRE nº 2, de 28 de abril de 2022 (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);

VIII - Portaria PRODERJ/PRE nº 968 de 05 de agosto de 2022 (institui o Manual de Procedimentos Regulatórios de Segurança da Informação a ser adotado por todas as repartições, técnicas e administrativas, no âmbito do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro – PRODERJ);

IX - Decreto nº 43.583, de 11 de maio de 2012 (Código de Ética Profissional do Servidor Público Civil do Poder Executivo do Estado do Rio de Janeiro);

X - Decreto-Lei nº 220, de 18 de julho de 1975 (Regime Jurídico dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro);

XI - Decreto nº 2.479, de 8 de março de 1979 (Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro);

XII - Decreto nº 46.205, de 27 de dezembro de 2017 (cria o programa de transparência Governo Aberto RJ e regulamenta o procedimento de acesso à informação previsto no inciso XXXIII do artigo 5º, no inciso II do § 3º do artigo 37, e no § 2º do artigo 216 da Constituição da República e na Lei nº 12.527, de 18 de novembro de 2011);

XIII - Decreto nº 46.475, de 25 de outubro de 2018 (regulamenta, no âmbito do Poder Executivo estadual, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, em conformidade ao disposto na Lei nº 12.527, de 18 de novembro de 2011);

XIV - Decreto nº 48.209, de 19 de setembro de 2022 (regulamenta a Lei Estadual nº 5.427, de 1 de abril de 2009, no que dispõe sobre a produção e tramitação eletrônica de documentos e processos administrativos na Administração Pública Estadual e dá outras providências);

XV - Decreto n° 48.891, de 10 de janeiro de 2024 (institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do estado do Rio de Janeiro, em conformidade com a Lei Federal nº 13.709, de 14 de agosto de 2018);

XVI - Portaria DRM nº 40, de 04 de março de 2024 (designa o Gestor de Segurança da Informação, o responsável pelo Tratamento e Resposta a Incidentes, bem como o Encarregado pelo Tratamento de Dados Pessoais, no âmbito do DRM-RJ);

XVII - Portaria DRM nº 49, de 10 de abril de 2025 (estabelece a Política de Privacidade no DRM-RJ);

XVIII - Decreto nº 46.938, de 13 de fevereiro de 2020 (Regimento Interno do DRM-RJ).

CAPÍTULO III - TERMOS E DEFINIÇÕES

Art. 5º - Para os efeitos desta política, entende-se por:

I - Acesso básico: acesso aos ativos de informação que são de uso comum para todos os servidores, estagiários, fornecedores e trabalhadores terceirizados — e cuja gestão de acesso fica sob a responsabilidade da Assessoria de Informática;

II - Ameaça: fator externo com potencial de causar dano a um ativo, intencionalmente ou não, mediante a exploração de uma vulnerabilidade;

III - Ameaça cibernética: ameaça intencional, em ambiente virtual, caracterizada por ações e mecanismos maliciosos aplicados por *hackers*;

IV - Ativo de informação: meios (tecnológicos ou não) de criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte da informação com valor para o DRM-RJ;

V - Ativo tecnológico: componente, físico (dispositivo tecnológico e outros meios físicos) ou não (*softwares*), que integra a infraestrutura tecnológica de propriedade do DRM-RJ ou que foi homologado pela Autarquia para fins de trabalho (dispositivo pessoal);

VI - Cliente: cidadãos que usufruem do serviço público prestado pelo DRM-RJ;

VII - Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

VIII - Evento de privacidade da informação: evento de segurança da informação, o qual envolva dados pessoais;

IX - Evento de segurança da informação: qualquer ocorrência, tecnológica ou não, em que haja violação ou suspeita de violação a esta política ou a seus documentos complementares;

X - Fornecedor: pessoa, física ou jurídica, de direito público ou privado, que forneça produto ou serviço ao DRM-RJ;

XI - Incidente de privacidade da informação: incidente de segurança da informação em que há dados pessoais envolvidos, podendo acarretar risco ou dano relevante aos titulares desses dados;

XII - Incidente de segurança da informação: evento de segurança da informação, o qual comprometa os princípios de segurança da informação;

XIII - Informação sensível: informação com algum grau de sigilo, precisando ser protegida contra acesso ou divulgação não autorizados — ou seja, são as informações não públicas;

XIV - Inteligência de ameaças: coleta de informações (em várias fontes) sobre ameaças cibernéticas, correlacionando-as e analisando-as a fim de compreender suas tendências, padrões e relacionamentos — o que permite, à organização, uma melhoria na detecção e na resposta diante de ataques;

XV - *Login*: identificação do usuário em um *software* dotado de restrições de segurança, cujo acesso seguro ocorre mediante essa identificação e senha;

XVI - Oportunidade de privacidade da informação: oportunidade de segurança relacionada à informação que contém dados pessoais;

XVII - Oportunidade de segurança da informação: efeito positivo da incerteza sobre os objetivos de segurança da informação, em que existe probabilidade de uma força (fator interno) associada a um ativo de informação explorar uma oportunidade (fator externo), para potencializar o alcance dos objetivos de segurança da informação;

XVIII - Processo: sequência de atividades que transformam entradas (insumos) em saídas com valor agregado (serviços ou produtos);

XIX - Registro de auditoria: registro de texto, cronológico e detalhado, sobre as ações executadas em um *software*, para permitir a rastreabilidade de uso, mediante fornecimento de informações sobre quem fez o quê, onde e quando — também conhecido como registro de evento, trilha de auditoria ou *log*;

XX - Risco de privacidade da informação: risco de segurança relacionado à informação que contém dados pessoais;

XXI - Risco de segurança da informação: efeito negativo da incerteza sobre os objetivos de segurança da informação, em que existe probabilidade de uma ameaça (fator externo) explorar uma vulnerabilidade (fator interno), presente em um ativo de informação, para comprometer os princípios de segurança da informação, bem como para impedir o alcance dos objetivos de segurança da informação;

XXII - Servidor: servidor público do DRM-RJ, independentemente do regime jurídico de trabalho ou de qual cargo ocupa, com emprego ou função públicos — sendo efetivo, temporário ou comissionado;

XXIII - Tarefa administrativa: tarefa executada por um usuário com privilégios especiais (*login* de administrador), com a finalidade de gerenciar e controlar a rede, o sistema operacional, o banco de dados ou quaisquer *softwares* e plataformas — incluindo instalar, desinstalar, configurar, gerenciar permissões de usuário, entre outras tarefas críticas à operação e à segurança;

XXIV - Trabalhador terceirizado: pessoa que realiza serviço para o DRM-RJ em nome do fornecedor;

XXV - Usuário: agentes (humanos ou de *software*) que utilizam os ativos tecnológicos;

XXVI - Vulnerabilidade técnica: fraqueza em um ativo tecnológico do DRM-RJ, sendo passível de exploração por uma ameaça.

CAPÍTULO IV - PAPÉIS E RESPONSABILIDADES

Art. 6º - É responsabilidade de cada servidor, estagiário ou trabalhador terceirizado:

I - O prejuízo ou dano que vier a sofrer ou causar, em decorrência do descumprimento das diretrizes desta política;

II - Quaisquer acessos realizados com o seu *login*, uma vez que essa credencial é única, pessoal e intransferível;

III - Participar dos treinamentos em segurança e privacidade da informação, fornecidos pelo DRM-RJ;

IV - Notificar eventos e incidentes (tanto de segurança quanto de privacidade da informação), por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, notificar por meio do SEI-RJ.

Art. 7º - É responsabilidade de cada gestor ou de alguém delegado por ele:

I - Monitorar o cumprimento desta política por parte dos servidores, estagiários ou trabalhadores terceirizados sob sua gestão;

II - Solicitar os dispositivos tecnológicos aos novos servidores e estagiários sob sua gestão, bem como a remoção desses dispositivos ao término do contrato, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ;

III - Definir e gerenciar os perfis, direitos e níveis de acesso, no que se refere aos softwares cuja gestão de acesso está sob sua responsabilidade;

IV - Revisar, semestralmente, os acessos aos softwares cuja gestão de acesso está sob sua responsabilidade;

V - Segregar funções que apresentem conflito de interesse, nos processos sob sua gestão;

VI - Identificar, continuamente, os riscos de segurança e de privacidade da informação associados aos ativos de informação sob sua responsabilidade, bem como notificar tais riscos por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, notificar por meio do SEI-RJ;

VII - Disponibilizar, ao trabalhador terceirizado, após a contratação, esta política, a conscientização sobre segurança e privacidade da informação, bem como o Termo de Responsabilidade de Segurança da Informação para assinatura;

VIII - Solicitar os dispositivos tecnológicos e a concessão dos acessos lógicos básicos para os novos trabalhadores terceirizados sob sua gestão, bem como a remoção dos acessos lógicos básicos ao término do contrato, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ;

IX - Solicitar a concessão dos acessos físicos para os novos trabalhadores terceirizados sob sua gestão, bem como a remoção desses acessos ao término do contrato, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ;

Art. 8º - É responsabilidade da Assessoria de Gestão de Pessoas:

I - Selecionar novos servidores com base em verificação de antecedentes, de acordo com as leis, regulamentos e ética aplicáveis — mediante avaliação proporcional aos riscos de segurança e de privacidade inerentes ao cargo;

II - Solicitar a concessão dos acessos físicos e lógicos básicos necessários aos novos servidores e estagiários, bem como a remoção desses acessos ao término do contrato, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ.

Art. 9º - É responsabilidade da Assessoria de Informática:

I - Restringir, ao mínimo necessário, os privilégios dos administradores e a quantidade de administradores que podem excluir registros de auditoria;

II - Definir e gerenciar os perfis, direitos e níveis de acesso, no que se refere aos *softwares* cuja gestão de acesso está sob sua responsabilidade;

III - Revisar, semestralmente, os acessos aos *softwares* cuja gestão de acesso está sob sua responsabilidade;

IV - Definir requisitos de segurança e privacidade da informação para contratação de fornecedor;

V - Implementar metodologia e princípios de segurança, no desenvolvimento de *software*;

VI - Homologar os dispositivos tecnológicos e os *softwares* para utilização no DRM-RJ;

VII - Prover, continuamente, aos dispositivos tecnológicos e *softwares* homologados, as configurações de segurança necessárias para cumprir as diretrizes de segurança e privacidade desta política;

VIII - Monitorar o ambiente tecnológico, por meio de soluções que verifiquem a disponibilidade, o desempenho e a capacidade dos ativos tecnológicos críticos ao negócio;

IX - Disponibilizar, ao servidor e ao estagiário, após a contratação, esta política, a conscientização sobre segurança e privacidade da informação, bem como o Termo de Responsabilidade de Segurança da Informação para assinatura.

Art. 10 - É responsabilidade do Gestor de Segurança da Informação:

I - Prover, aos servidores, estagiários e trabalhadores terceirizados, contínua conscientização e educação (tanto em segurança quanto em privacidade da informação), por meio de um plano anual correspondente ao tema — inclusive provendo conhecimentos específicos às equipes técnicas;

II - As atribuições definidas na Instrução Normativa PRODERJ/PRE nº 2, de 28 de abril de 2022.

Art. 11 - É atribuição do Responsável pelo Tratamento e Resposta a Incidentes:

I - Identificar e monitorar ameaças cibernéticas, mediante inteligência de ameaças;

II - Identificar e tratar as vulnerabilidades técnicas;

III - Monitorar e tratar os registros de auditoria;

IV - Tratar os incidentes de segurança da informação;

V - As atribuições definidas na Instrução Normativa PRODERJ/PRE nº 2, de 28 de abril de 2022.

Art. 12 - É responsabilidade do Encarregado pelo Tratamento de Dados Pessoais:

I - Mapear, continuamente, as atividades envolvendo tratamento de dados pessoais no DRM-RJ;

II - Assegurar que o tratamento de dados pessoais ocorra em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD);

III - As atribuições definidas na Instrução Normativa PRODERJ/PRE nº 2, de 28 de abril de 2022.

Art. 13 - É responsabilidade do Comitê de Segurança e Privacidade da Informação:

I - Reunir-se anualmente ou diante de um risco, evento ou incidente (seja de segurança, seja de privacidade da informação) que requeira atuação imediata desse comitê;

II - Revisar esta política, conforme “Capítulo X – Vigência”;

III - Avaliar e monitorar, continuamente, os riscos de segurança e de privacidade;

IV - Analisar as infrações a esta política, examinando se o ato em questão causou incidente de segurança ou de privacidade da informação — em caso afirmativo, classificar o incidente e:

a. Recomendar que o presidente, conforme Termo de Compromisso de Estágio, aplique sanção ao estagiário infrator;

b. Recomendar que o presidente, conforme o acordo ou instrumento administrativo vigentes, aplique sanção ao fornecedor, ao trabalhador terceirizado ou às outras partes envolvidas com o DRM-RJ que tenham cometido a infração;

c. Recomendar que o controle interno abra sindicância para apurar a aplicabilidade de um processo disciplinar ao servidor estatutário infrator;

V - Propor soluções para tratar riscos, oportunidades, eventos e incidentes (quer de segurança, quer de privacidade) identificados no DRM-RJ.

Parágrafo único. Esse comitê é constituído por representantes da Assessoria de Gestão de Pessoas, da Assessoria de Informática, do Gestor de Segurança da Informação, do Responsável pelo Tratamento e Resposta a Incidentes, em adição ao Encarregado pelo Tratamento de Dados Pessoais e, quando convocada para pauta específica, à Alta Administração.

Art. 14 - É responsabilidade da Assessoria Jurídica do DRM-RJ:

I - Analisar modelo de Termo de Compromisso de Estágio e recomendar cláusula que atribua, aos estagiários, a responsabilidade quanto à segurança e privacidade da informação;

II - Analisar modelo de Termo de Responsabilidade de Segurança da Informação e recomendar cláusula que atribua, aos servidores, a responsabilidade quanto à segurança e privacidade da informação;

III - Analisar modelo de Termo de Responsabilidade de Segurança da Informação e recomendar cláusula que atribua, aos trabalhadores terceirizados, a responsabilidade quanto à segurança e privacidade da informação;

IV - Analisar modelo de contrato (ou instrumento administrativo equivalente) e recomendar cláusula que atribua, aos fornecedores ou às outras partes envolvidas em acordos com o DRM-RJ, a responsabilidade quanto à segurança e privacidade da informação.

Art. 15 - É responsabilidade do Controle Interno:

I - Apurar, mediante sindicância e quando recomendado pelo Comitê de Segurança da Informação, as infrações cometidas pelos servidores estatutários — seja contra esta política, seja contra as cláusulas de segurança e privacidade da informação constantes no Termo de Responsabilidade de Segurança da Informação.

II - Aplicar, aos servidores estatutários, a penalidade de suspensão observando a legislação pertinente.

Art. 16 - É responsabilidade do presidente do DRM-RJ:

I - Aplicar sanções aos estagiários, quando infrações forem cometidas contra esta política, desde que recomendadas pelo Comitê de Segurança da Informação;

II - Aplicar sanções aos servidores estatutários, quando infrações forem cometidas contra esta política, desde que recomendadas pelo Controle Interno;

III - Aplicar sanções aos fornecedores e aos demais servidores não determinados no inciso II deste artigo em acordos com o DRM-RJ, quando infrações forem cometidas contra esta política, desde que recomendadas pelo Comitê de Segurança da Informação.

CAPÍTULO V - DIRETRIZES

Seção I - Gestão de acesso

Art. 17 - O DRM-RJ deve garantir o vínculo de controle de acesso a uma credencial única pessoal intransferível, restringindo a possibilidade de uso de acesso compartilhado.

Art. 18 - O DRM-RJ deve conceder acessos somente mediante a assinatura do Termo de Responsabilidade de Segurança da Informação.

Art. 19 - O DRM-RJ deve restringir o acesso a informações e a funções dos *softwares*, por meio da definição de perfis de acesso.

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

Art. 20 - O DRM-RJ deve criar identidades e atribuir direitos de acesso básico apenas mediante solicitação da Assessoria de Gestão de Pessoas, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ

Parágrafo único. Os direitos de acesso específicos devem ser atribuídos mediante solicitação do gestor responsável pelo servidor, estagiário ou trabalhador terceirizado.

Art. 21 - O DRM-RJ deve criar identidades de “usuário administrador” apenas para executar tarefas administrativas e criar identidades de “usuário comum” para executar tarefas não administrativas.

Parágrafo único. O servidor, estagiário ou trabalhador terceirizado que possui *login* de “usuário administrador” não deve utilizá-la ao executar tarefas comuns — para isso, deverá utilizar seu *login* de “usuário comum”.

§1º O DRM-RJ deve excluir identidades e revogar direitos de acesso básico mediante solicitação da Assessoria de Gestão de Pessoas, por meio do canal determinado pela organização, em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ.

§2º Os direitos de acesso específicos devem ser revogados mediante solicitação do gestor responsável pelo servidor, estagiário ou trabalhador terceirizado.

§3º Os direitos de acesso devem ser imediatamente removidos quando se tornarem desnecessários para o DRM-RJ.

Art. 22 - O DRM-RJ deve desabilitar, nos seus *softwares*, os *logins* inativos há mais de 45 (quarenta e cinco) dias.

Art. 23 - O DRM-RJ deve configurar os direitos de acesso temporários para expirarem, de forma automática, nas datas definidas no momento da solicitação.

Art. 24 - O DRM-RJ deve manter registro de todas as ações referentes às solicitações, autorizações, criações e exclusões de identidade, bem como às concessões e revogações dos direitos de acesso.

Art. 25 - O DRM-RJ deve garantir que seus *softwares* exijam senhas complexas, conforme critérios abaixo:

I - Todas as senhas de acesso aos *softwares* devem possuir, no mínimo, 8 (oito) caracteres;

II - Todas as senhas de acesso aos *softwares* devem ser constituídas por:

a. Pelo menos 1 (uma) letra minúscula;

b. Pelo menos 1 (uma) letra maiúscula;

c. Pelo menos 1 (um) caractere numérico;

d. Pelo menos 1 (um) caractere especial.

Parágrafo único. Caso algum *software* disponibilizado pelo DRM-RJ não exija automaticamente a referida complexidade nas senhas, o servidor, estagiário ou trabalhador terceirizado é responsável por criar sua senha seguindo os critérios definidos no *caput* deste artigo.

Art. 26 - Em dispositivos tecnológicos que permitem apenas senhas numéricas, o servidor, estagiário ou trabalhador terceirizado não deve criar senhas de fácil identificação — como datas de aniversário, números sequenciais, números de telefone e afins.

Art. 27 - O DRM-RJ deve implementar a autenticação de duplo fator, nos seus *softwares* que possuam esse recurso.

Parágrafo único. As senhas de acesso aos *softwares* que não possuem autenticação de duplo fator implementada, devem ser formadas por, no mínimo, 10 (dez) caracteres.

Art. 28 - O DRM-RJ deve implementar a expiração de sessão, nos seus *softwares* que possuam esse recurso.

Art. 29 - O DRM-RJ deve implementar o bloqueio de *login* em caso de digitação errônea da senha por 5 (cinco) vezes consecutivas, nos seus *softwares* que possuam esse recurso.

Art. 30 - O servidor, estagiário ou trabalhador terceirizado deve alterar ou solicitar alteração de sua senha, imediatamente, caso perceba ou desconfie que tenha sido comprometida, além de notificar como evento de segurança da informação, tal fato ou desconfiança.

Art. 31 - O DRM-RJ deve implementar, nos seus *softwares* que possuam esse recurso, a expiração automática de senha a cada 120 (cento e vinte) dias, com notificação ao usuário do sistema 10 (dez) dias antes da data limite.

Parágrafo único. No ato de renovação da senha, não deverá ser aceita senha igual às últimas 5 (cinco) registradas.

Art. 32 - Caso a senha inicial seja fornecida pelo administrador do *software*, o DRM-RJ deve implementar a exigência de troca da senha no primeiro *login*, em seus *softwares* que possuam esse recurso.

Art. 33 - O servidor, estagiário ou trabalhador terceirizado não deve expor, compartilhar ou revelar as suas senhas para outras pessoas.

Art. 34 - O servidor, estagiário ou trabalhador terceirizado não deve permitir que o navegador de internet armazene as suas senhas.

Art. 35 - O servidor, estagiário ou trabalhador terceirizado não deve transcrever suas senhas em local distinto do cofre de senhas fornecido pelo DRM-RJ.

Seção II - Uso aceitável dos ativos de informação

Art. 36 - O DRM-RJ deve entregar dispositivos móveis ao servidor somente mediante Termo de Acautelamento de Bem Móvel assinado ou outro instrumento equivalente.

Art. 37 - O servidor, estagiário ou trabalhador terceirizado não deve utilizar os ativos de informação do DRM-RJ para fins diferentes dos necessários ao desempenho de suas atividades.

Art. 38 - O servidor, estagiário ou trabalhador terceirizado deve zelar pelo bom uso dos dispositivos tecnológicos disponibilizados pelo DRM-RJ — incluindo não remover, alterar ou acrescentar configuração de segurança, *software* ou componente interno de *hardware*.

Art. 39 - O DRM-RJ deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga instalar *software* nos dispositivos tecnológicos de propriedade da Autarquia.

Art. 40 - O DRM-RJ deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga realizar *download* (seja de *software*, seja de executável) da internet nos dispositivos tecnológicos de propriedade da Autarquia.

Parágrafo único. O servidor, estagiário ou trabalhador terceirizado não deve realizar *download* (seja de *software*, seja de executável) da internet nos dispositivos tecnológicos de propriedade do DRM-RJ.

Art. 41 - O DRM-RJ deve bloquear o uso de mídia removível nos dispositivos tecnológicos de propriedade institucional. Conforme necessário, esse uso poderá ser liberado, com controle estrito e com aplicação da verificação automática (ao inserir a mídia) quanto à existência de códigos maliciosos.

Parágrafo único. Os servidores, estagiários ou trabalhadores terceirizados não devem utilizar mídia removível nos dispositivos tecnológicos de propriedade do DRM-RJ. Contudo, quando possuírem autorização para utilizar tal mídia removível, devem aplicar criptografia aos documentos com informação sensível armazenados no dispositivo em questão.

Art. 42 - O DRM-RJ deve garantir que seus servidores, estagiários ou trabalhadores terceirizados não consigam navegar, nos dispositivos tecnológicos de propriedade institucional, em sites das seguintes categorias:

I - Propaganda político-partidária;

II - Conteúdo ilegal ou que promova atividade ilegal;

III - Conteúdo de caráter sexual.

Parágrafo único. Os servidores, estagiários ou trabalhadores terceirizados não devem navegar, nos dispositivos tecnológicos de propriedade do DRM-RJ, em sites das categorias mencionadas no *caput* deste artigo.

Art. 43 - O servidor, estagiário ou trabalhador terceirizado não deve armazenar conteúdo ilegal ou não ético nos ativos de informação do DRM-RJ.

Art. 44 - O servidor, estagiário ou trabalhador terceirizado não deve armazenar conteúdo particular nos ativos de informação de propriedade do DRM-RJ.

Art. 45 - O servidor, estagiário ou trabalhador terceirizado não deve armazenar localmente as informações necessárias ao trabalho, pois não há cópia de segurança — o que expõe as informações ao risco de perda, em caso de falha no computador.

Parágrafo único. O servidor, estagiário ou trabalhador terceirizado deve armazenar no servidor de arquivos as informações necessárias às atividades do DRM-RJ.

Art. 46 - O servidor, estagiário ou trabalhador terceirizado não deve consumir nem alimentos, nem bebidas se estiver próximo aos ativos de informação.

Art. 47 - O DRM-RJ deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga alterar as configurações de segurança dos ativos tecnológicos de propriedade da Autarquia.

Art. 48 - O DRM-RJ deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga conectar, à rede institucional, dispositivos tecnológicos não homologados.

Parágrafo único. O servidor, estagiário ou trabalhador terceirizado não deve conectar, à rede do DRM-RJ, dispositivos tecnológicos não homologados.

Art. 49 - O servidor, estagiário ou trabalhador terceirizado deve desligar o computador ao final do expediente, exceto quando a Assessoria de Informática comunicar que, em data determinada, os computadores deverão permanecer ligados para manutenção ou para atualização.

Art. 50 - O servidor, estagiário ou trabalhador terceirizado deve retirar da impressora, imediatamente, os documentos para os quais tenha solicitado a impressão, caso contenham informações sensíveis.

Art. 51 - O DRM-RJ deve implementar uma solução tecnológica para inventariar os ativos tecnológicos de propriedade institucional.

Art. 52 - O DRM-RJ deve implementar uma linha de base para a configuração dos ativos tecnológicos, incluindo configurações de segurança e privacidade da informação.

Art. 53 - O DRM-RJ deve segregar suas redes em, no mínimo: domínio de acesso público (rede de visitantes), domínio de estação de trabalho e domínio de computador do tipo servidor.

§1º O tráfego de dados entre essas redes deve ser monitorado, filtrado e controlado por um sistema de segurança.

§2º O acesso à rede de visitantes deverá ser liberado somente para fins de acesso à internet, por meio de um processo de cadastro.

Art. 54 - O servidor, estagiário ou trabalhador terceirizado deve manter as mesas de trabalho limpas — em especial quanto aos papéis e mídias de armazenamento removíveis que contenham informações sensíveis.

Art. 55 - O servidor, estagiário ou trabalhador terceirizado deve proteger a informação sensível exposta na tela de seu dispositivo tecnológico, assegurando que não seja visualizada por pessoas não autorizadas — especialmente em caso de compartilhamento ou *print* da tela, durante fotografias e filmagens, bem como em apresentações ou em locais públicos.

Art. 56 - O servidor, estagiário ou trabalhador terceirizado deve proteger a informação sensível, por meio das seguintes ações:

I - Não discutir assuntos com informação sensível em ambientes públicos, em áreas expostas (elevadores, meios de transporte, restaurantes e afins) ou com terceiros não autorizados;

II - Não publicar assuntos com informação sensível em redes sociais sem a autorização formal do DRM-RJ.

Art. 57 - O DRM-RJ deve implementar o bloqueio automático de tela do computador, a partir de 5 (cinco) minutos de inatividade.

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

Art. 58 - O servidor, estagiário ou trabalhador terceirizado deve descartar documentos, que contenham informação sensível, por meio da trituradora de papel disponibilizada pelo DRM-RJ.

Seção III - Trabalho remoto e uso de dispositivos móveis

Art. 59 - Em caso de furto ou roubo de dispositivo móvel (seja de propriedade do DRM-RJ, seja de dispositivo pessoal homologado para fins de trabalho), o servidor, estagiário ou trabalhador terceirizado deve notificar imediatamente a Autarquia, por meio do canal determinado pela organização, com cópia ao seu superior imediato em caso de impossibilidade de acesso a esse canal, solicitar por meio do SEI-RJ. Assim que possível, a vítima também deverá registrar o boletim de ocorrência.

Art. 60 - O DRM-RJ deve habilitar o rastreamento de localização e o recurso de limpeza remota, nos dispositivos móveis de propriedade institucional.

Art. 61 - O DRM-RJ deve garantir que o acesso remoto à rede institucional ocorra somente via *Virtual Private Network* (VPN).

Art. 62 - O servidor, estagiário ou trabalhador terceirizado não deve conectar os dispositivos móveis de propriedade do DRM-RJ a redes públicas de *Wi-Fi*.

Seção IV - Ambiente físico

Art. 63 - Na entrada principal do perímetro institucional, O DRM-RJ deve garantir o monitoramento da entrada principal, registrando acessos para assegurar o controle de entrada e saída, além de viabilizar a identificação dos visitantes.

Art. 64 - Nos arredores do perímetro institucional e nos pontos de acesso à entrada principal da sede, o DRM-RJ deve implementar câmeras de segurança com sistema de monitoramento.

Art. 65 - Na entrada principal da sede, o DRM-RJ deve implementar tranca segura.

Parágrafo único. A entrada e saída de visitantes, na sede do DRM-RJ, deve ser registrada pela recepção. Além disso, durante a permanência na sede, a visita deve ser acompanhada por um servidor ou estagiário.

Art. 66 - O DRM-RJ deve prover, ao servidor e ao estagiário, um meio de identificação visível (na forma de crachá), para ser utilizado ao transitarem pela sede.

Art. 67 - O DRM-RJ deve prover, aos trabalhadores terceirizados, um meio de identificação visível (na forma de crachá), capaz de diferenciá-los dos servidores, estagiários e visitantes, para ser utilizado ao transitarem pela sede.

Art. 68 - O DRM-RJ deve prover, aos visitantes, um meio de identificação visível (na forma de crachá), capaz de diferenciá-los dos servidores, estagiários e trabalhadores terceirizados, para ser utilizado ao transitarem pela sede.

Art. 69 - Servidores, estagiários, trabalhadores terceirizados ou visitantes devem utilizar o crachá, ao transitar pela sede do DRM-RJ.

Art. 70 - Nas subdivisões e nas salas da sede que armazenam informações sensíveis, o DRM-RJ deve implementar proteções contra acesso não autorizado — mediante sistemas baseados em cartão de acesso, biometria, reconhecimento facial ou chaves.

Art. 71 - Nas salas de cabos, nos painéis de conexão e nos pontos terminais, o DRM-RJ deve implementar proteções contra acesso não autorizado — mediante sistemas baseados em cartão de acesso, biometria, reconhecimento facial ou chaves.

Art. 72 - O DRM-RJ deve isolar a área de carga e descarga (seja de equipamentos, seja de outros materiais) para mitigar o risco de, a partir desse local, ocorrerem acessos não autorizados a áreas restritas da sede.

Parágrafo único. Na área de carga e descarga (seja de equipamentos, seja de outros materiais), deve ser realizada inspeção do material recebido e expedido.

Art. 73 - O DRM-RJ deve garantir que as medidas de proteções físicas sejam implementadas para mitigar os riscos identificados de ameaças físicas e ambientais.

Art. 74 - O DRM-RJ deve garantir que a infraestrutura predial da sua sede possua condições apropriadas para alocar os dispositivos tecnológicos — de forma a minimizar danos causados por poeira, efeitos químicos, variações na umidade do ar e na temperatura, interferência eletromagnética, bem como vandalismo.

Art. 75 - O servidor, estagiário ou trabalhador terceirizado não deve remover, instalar ou movimentar dispositivos tecnológicos de propriedade do DRM-RJ — com exceção dos dispositivos móveis.

§1º A Assessoria de Informática é responsável por remover, instalar ou movimentar os dispositivos tecnológicos de propriedade do DRM-RJ, com exceção dos dispositivos móveis.

§2º Os dispositivos tecnológicos de propriedade do DRM-RJ, com exceção dos dispositivos móveis, somente poderão sair da Autarquia mediante Termo de Autorização de Saída de Material assinado.

Art. 76 - O DRM-RJ deve garantir que os dispositivos tecnológicos de propriedade institucional recebam manutenção, de acordo com as bases de conhecimento e especificações do fabricante.

Art. 77 - Antes de reutilizar ou descartar os dispositivos tecnológicos, o DRM-RJ deve sobrescrever (por meio de formatação) ou destruir fisicamente os dispositivos de armazenamento.

Art. 78 - O DRM-RJ deve planejar medidas de redundância, para que seja possível garantir a continuidade das operações contra indisponibilidade ocasionada por interrupção ou por carência no suprimento dos serviços de energia elétrica, telecomunicações e climatização.

Art. 79 - O DRM-RJ deve garantir a proteção do cabeamento de energia e de telecomunicações, no ambiente institucional, contra danos e interferências.

Seção V - Classificação da informação

Art. 80 - O DRM-RJ deve classificar e rotular as suas informações, quanto ao grau e prazo de sigilo, em: ultrassecreta, secreta ou reservada — para as situações previstas no Decreto nº 46.475, de 25 de outubro de 2018 (que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, no âmbito do Poder Executivo Estadual).

Parágrafo único. Para informação pessoal, independentemente da classificação de sigilo atribuída, o DRM-RJ deve restringir o acesso pelo prazo máximo de 100 anos, a contar da data de produção. Nesse sentido, a informação somente poderá ser acessada por agentes públicos autorizados e pelo próprio titular da informação pessoal — conforme disposto no inciso I, §1º, do art. 52 do Decreto nº 46.475, de 25 de outubro de 2018 (que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, no âmbito do Poder Executivo Estadual).

Art. 81 - O DRM-RJ deve classificar e rotular as informações no SEI-RJ, quanto ao grau de sigilo, em: público, restrito ou sigiloso — conforme o disposto no Decreto nº 48.209, de 19 de setembro de 2022.

§1º Deverão ser classificados como restritos ou sigilosos os documentos e processos que possuam informações pessoais ou que tratem de assunto coberto por sigilo previsto em lei.

§2º Deverão ser classificados como públicos todos os documentos e processos sob os quais não incidam hipótese de sigilo.

§3º Não poderão ser incluídos no SEI-RJ documentos que possuam informações classificáveis nos níveis de sigilo ultrassecreta, secreta ou reservada.

Seção VI - Transferência da informação

Art. 82 - O servidor, estagiário ou trabalhador terceirizado deve utilizar o e-mail institucional (do domínio do DRM-RJ) para comunicação de assuntos pertinentes à Autarquia.

§1º O servidor, estagiário ou trabalhador terceirizado não deve utilizar o e-mail institucional para comunicação de assuntos alheios à Autarquia.

§2º O servidor, estagiário ou trabalhador terceirizado não deve utilizar o e-mail particular para comunicação de assuntos pertinentes à Autarquia.

§3º O servidor, estagiário ou trabalhador terceirizado não deve utilizar linguagem coloquial, nem abreviações, nem gírias nas mensagens enviadas via e-mail institucional.

§4º O servidor, estagiário ou trabalhador terceirizado deve utilizar assinatura no e-mail institucional, seguindo o padrão estabelecido pelo DRM-RJ.

Art. 83 - Ao utilizar o e-mail institucional, o servidor, estagiário ou trabalhador terceirizado não deve:

I - Enviar propagandas, mensagens classificadas como “corrente”, conteúdo ilegal ou não ético, bem como comunicação discriminatória ou ofensiva no que se refere à nacionalidade, à raça, à orientação sexual, à religião ou à opinião política;

II - Enviar arquivo que contenha código malicioso;

III - Enviar conteúdo que viole o direito de propriedade intelectual;

IV - Cadastrar o e-mail institucional em *sites* ou aplicativos externos, exceto mediante autorização formal do DRM-RJ.

Parágrafo único. Os e-mails institucionais cadastrados em *sites* ou aplicativos externos, mediante autorização, devem ser estritamente controlados pelo DRM-RJ.

Art. 84 - O DRM-RJ deve restringir a permissão de envio simultâneo de mensagens a todos os usuários.

Art. 85 - O DRM-RJ deve garantir que a solução de e-mail adotada possua detecção e proteção contra código malicioso; configuração limitando tamanho do anexo; recurso para rotular a informação quanto ao seu grau de sigilo; controles para rastreabilidade e não repúdio; controles contra acesso, cópia, modificação ou destruição não autorizados; além de medidas que impeçam a interceptação, o desvio, a negação de serviço e *Unsolicited Commercial E-mail* (SPAM).

Art. 86 - O servidor, estagiário ou trabalhador terceirizado deve aplicar criptografia em anexos de e-mail que contenham informação sensível.

Art. 87 - O servidor, estagiário ou trabalhador terceirizado deve rotular a mensagem eletrônica, antes do envio ou resposta, conforme indicado na “Seção V – Classificação da informação” do “Capítulo V – Diretrizes” desta política.

Art. 88 - O servidor, estagiário ou trabalhador terceirizado deve proceder com dupla checagem dos destinatários, antes de enviar informação sensível, por quaisquer meios de comunicação.

Art. 89 - O servidor, estagiário ou trabalhador terceirizado deve controlar, bem como notificar ao destinatário ou ao remetente, sempre que enviar ou receber documentos físicos ou mídias removíveis com informação sensível. Para transportar esses ativos, deve-se utilizar envelope opaco, sem identificação aparente do conteúdo, mas com a devida classificação do sigilo. Notadamente, para envio, devem-se utilizar apenas serviços postais homologados pelo DRM-RJ.

Seção VII - Privacidade

Art. 90 - O DRM-RJ deve garantir que toda operação envolvendo dados pessoais ocorra em conformidade com o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

§1º O DRM-RJ deve garantir que o propósito do tratamento dos dados pessoais não seja ilícito, fazendo-o mediante mapeamento e definição das finalidades desses tratamentos.

§2º O DRM-RJ deve implementar uma Política de Privacidade para informar, aos titulares de dados pessoais, a maneira como esses dados são tratados, bem como os períodos de armazenamento.

§3º O DRM-RJ deve garantir que os processos e os *softwares* sejam projetados ou ajustados, a fim de limitar o tratamento dos dados pessoais ao necessário para o propósito pretendido.

Seção VIII - Códigos maliciosos

Art. 91 - Nos ativos tecnológicos, o DRM-RJ deve implementar soluções de proteção contra códigos maliciosos, com medidas de detecção e de prevenção; além de incluir recursos para bloquear sites maliciosos (conhecidos ou suspeitos) e para verificar os dados recebidos (pela rede ou por mídia removível).

Art. 92 - O servidor, estagiário ou trabalhador terceirizado não deve interromper, nos ativos tecnológicos, a verificação feita pelos *softwares* de proteção contra códigos maliciosos.

Art. 93 - O servidor, estagiário ou trabalhador terceirizado não deve clicar em *links* ou anexos suspeitos.

Seção IX - Fornecedores

Art. 94 - O DRM-RJ deve estabelecer um acordo com seus fornecedores, em contrato, sobre quais os requisitos de segurança e privacidade da informação necessários ao serviço, além de atribuir as responsabilidades correspondentes.

Parágrafo único. Os requisitos (tanto de segurança quanto de privacidade da informação) e as responsabilidades acordados, em contrato, com fornecedores de Tecnologia da Informação e Comunicação (TIC) devem ser estendidos, em cláusula específica, à cadeia de suprimento desse fornecedor.

Seção X - Serviços em nuvem

Art. 95 - O DRM-RJ deve garantir, para cada serviço em nuvem a ser contratado, que as seguintes questões sobre segurança e privacidade da informação sejam determinadas:

I - Papéis e responsabilidades, incluindo as responsabilidades compartilhadas e o esforço colaborativo diante de incidentes (seja de segurança, seja de privacidade da informação);

II - Quais controles de segurança e privacidade da informação devem ser aplicados ao serviço em nuvem, bem como especificar quem deve gerenciá-los — abordando, no mínimo, os requisitos de cópia de segurança, proteção contra códigos maliciosos e gestão de acesso;

III - Como obter e utilizar os recursos (seja de segurança, seja de privacidade da informação) fornecidos pelo provedor de serviços em nuvem;

IV - Como retornar as informações ao DRM-RJ, diante do término do serviço em nuvem;

V - Localização dos dados e jurisdição.

Art. 96 - O DRM-RJ deve monitorar o uso dos serviços em nuvem, a fim de identificar e tratar riscos, eventos, bem como incidentes (quer de segurança, quer de privacidade da informação).

Seção XI - Incidentes de segurança e de privacidade da informação

Art. 97 - O DRM-RJ deve estabelecer critérios para avaliar quando classificar um evento (de segurança ou de privacidade da informação) como incidente (de segurança ou de privacidade da informação).

Art. 98 - O DRM-RJ deve estabelecer critérios para avaliar quando o Plano de Continuidade de Negócio deve ser acionado, visando tratar um incidente de segurança ou de privacidade da informação.

Art. 99 - O DRM-RJ deve estabelecer um processo para gestão de incidentes (quer de segurança, quer de privacidade da informação), abordando como detectá-los, priorizá-los, escaloná-los, analisá-los, resolvê-los e comunicá-los, além de estabelecer como serão identificadas e tratadas as lições aprendidas.

Parágrafo único. Na etapa de resolução do incidente, o DRM-RJ deve estabelecer fases de contenção, erradicação e recuperação.

Art. 100 - O DRM-RJ deve garantir que os incidentes (quer de segurança, quer de privacidade da informação) possuam registro das ações envolvidas, desde o relato ou detecção até a resolução.

Art. 101 - O DRM-RJ deve estabelecer critérios para avaliar quando será necessária a análise forense de um incidente de segurança ou de privacidade da informação.

Art. 102 - O DRM-RJ deve garantir que as evidências dos incidentes (quer de segurança, quer de privacidade da informação) sejam identificadas, coletadas e preservadas, a fim de embasar as ações subsequentes (tanto disciplinares quanto legais).

Seção XII - Vulnerabilidades técnicas

Art. 103 - O DRM-RJ deverá implementar um processo de avaliação e tratamento de vulnerabilidades técnicas, além da verificação de eficácia desse tratamento. Para isso poderá implementar uma solução de varredura de vulnerabilidade técnica.

Art. 104 - O DRM-RJ deverá implementar um programa de teste de invasão.

Art. 105 - O DRM-RJ deverá implementar um processo de gerenciamento das atualizações de segurança de *software*.

Parágrafo único. As atualizações de segurança de *software* devem ser controladas pelo processo de gestão de mudança — incluindo o plano de teste e o plano de remediação ou de retrocesso.

Seção XIII - Inteligência de ameaças

Art. 106 - O DRM-RJ deve produzir inteligência de ameaças a partir da coleta e análise de informações relacionadas, as quais podem ser provenientes de diversas fontes, com o objetivo de prevenir, detectar e responder a ameaças cibernéticas.

Seção XIV - Controles criptográficos e gerenciamento de chaves

Art. 107 - O DRM-RJ deve utilizar, somente, algoritmos de criptografia padronizados.

Art. 108 - O DRM-RJ deve utilizar uma Autoridade Certificadora confiável para gerenciar suas chaves criptográficas (públicas e privadas).

Art. 109 - O DRM-RJ deve prover condições para a criptografia das informações sensíveis, tanto em seu armazenamento quanto em sua transmissão.

Art. 110 - O DRM-RJ deve gerenciar o ciclo de vida das chaves criptográficas utilizadas — criação, ativação, desativação, expiração, exclusão, restauração e destruição.

Seção XV - Registro de auditoria

Art. 111 - O DRM-RJ deve garantir que os registros de auditoria dos seus ativos tecnológicos sejam habilitados, retidos, alertados, monitorados e analisados.

Parágrafo único. A retenção mínima dos registros de auditoria deve ser de 90 dias, observadas a necessidade do negócio e as legislações aplicáveis, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 112 - Quando os registros de auditoria possuírem dado pessoal, o DRM-RJ deverá tratá-los em conformidade com as diretrizes da “Seção VII – Privacidade” do “Capítulo V – Diretrizes” desta política.

Art. 113 - O DRM-RJ deve centralizar e correlacionar os registros de auditoria relacionados às atividades dos usuários e dos administradores de *softwares*, em adição às falhas e comportamentos atípicos ou anormais dos *softwares*, bem como alertar eventos de segurança ou de privacidade que requeiram atenção ou ação.

Art. 114 - O DRM-RJ deve proteger os registros de auditoria de seus *softwares*, por meio de cópia de segurança e controle de acesso.

Art. 115 - O DRM-RJ deve garantir que os registros de auditoria de seus *softwares* possuam, no mínimo, os seguintes dados: identificador, dispositivo, ação, origem, usuário e data/hora.

Art. 116 - O DRM-RJ deve garantir que os registros de auditoria de seus *softwares* sejam sincronizados a partir de uma origem de tempo confiável, para que contenham informações consistentes de data/hora.

Seção XVI - Desenvolvimento de *software* interno ou terceirizado

Art. 117 - Para desenvolvimento de *software* e para cenários de reuso de código, o DRM-RJ deve adotar uma ou mais metodologia(s) de desenvolvimento — incluindo a utilização da técnica de revisão por pares.

Art. 118 - Para desenvolvimento de *software* e para cenários de reuso de código, o DRM-RJ deve adotar os seguintes princípios de codificação segura:

I - Segurança por *design*: os requisitos de segurança devem ser identificados desde a concepção;

II - Segurança por padrão (também conhecido como “à prova de falhas” ou “negação por padrão”): a configuração padrão deve ser a mais segura, fornecer a menor funcionalidade, bem como restringir o uso das outras funções, portas, protocolos e serviços;

III - Nenhum *software* obtém 100% de segurança: os controles devem tornar o ataque o mais difícil possível;

IV - Defesa em profundidade: a defesa deve ser fornecida em camadas de controles;

V - Menor privilégio: deve ser concedido o nível mínimo de direitos de acesso, bem como deve ser concedido pelo período mínimo necessário para concluir a operação;

VI - Compartimentalizar: o acesso às informações, para executar determinadas tarefas, deve ser segregado com base na “necessidade de conhecer”;

VII - Separação de privilégios: os componentes, ou processos que requerem privilégios elevados para executar tarefas específicas, devem ser separados dos demais;

VIII - Economia do mecanismo (também conhecido como “mantenha a simplicidade”): os detalhes do *design* e da implementação do *software* devem ser simples e compreensíveis;

IX - Mediação completa: cada solicitação de acesso de um sujeito para um objeto deve ser completamente mediada quanto à verificação dos direitos de acesso;

X - *Design* aberto: a implementação do *design* deve ser independente do *design* em si, a fim de que a segurança não dependa do sigilo da implementação;

XI - Mecanismo menos comum: mecanismos que são comuns a mais de um usuário ou processo, mas que estão em diferentes níveis de privilégio, não devem ser compartilhados;

XII - Aceitabilidade psicológica: a funcionalidade de segurança do *software* deve ser fácil de utilizar, bem como ser transparente para o usuário;

XIII - Usabilidade e gerenciabilidade: a configuração, a administração e a integração de componentes de segurança não devem ser excessivamente complexas ou obscuras;

XIV - Proteja o elo mais fraco: o componente mais fraco (seja o código, seja o serviço, seja uma interface) deve ser identificado e seu risco deve ser mitigado até que adquira um nível aceitável;

XV - Aproveite componentes existentes: componentes de *software*, código e funcionalidade devem ser reutilizados;

XVI - Valide a entrada: as entradas do usuário devem ser validadas, somente, se atenderem ao formato e às restrições esperadas;

XVII - Atenção aos avisos do compilador: o nível de aviso mais alto do compilador deve ser utilizado;

XVIII - Arquitete e projete para políticas de segurança: o *software* deve ser arquitetado e projetado para aplicar as políticas de segurança;

XIX - Sanitize os dados enviados para outros sistemas;

XX - Utilize técnicas eficazes de garantia de qualidade;

XXI - Adote um padrão de codificação seguro para a linguagem e para a plataforma de desenvolvimento utilizados.

Art. 119 - Para desenvolvimento de *software* e para cenários de reuso de código, o DRM-RJ deve adotar os seguintes princípios de privacidade:

I - Proativo e não reativo: agir de forma preventiva, não corretiva;

II - Privacidade por padrão: aplicar configurações mais seguras por padrão;

III - Privacidade incorporada ao projeto: abordagem holística e integrada, a qual será aplicada desde a concepção de qualquer iniciativa de tratamento de dados pessoais;

IV - Funcionalidade total: ao integrar a privacidade a uma tecnologia ou processo, busque não comprometer sua plena funcionalidade;

V - Segurança fim a fim: salvaguardar a privacidade ao longo do ciclo de vida dos dados pessoais;

VI - Visibilidade e transparência: capacidade de demonstrar conformidade e responsabilidade;

VII - Respeito ao usuário de privacidade: garantir os direitos e liberdades dos titulares de dados pessoais.

Art. 120 - O DRM-RJ deve garantir que os ambientes de desenvolvimento, de teste e de produção do *software* sejam separados, dispondo de um repositório seguro, com solução de versionamento.

Art. 121 - O desenvolvimento de *software* deve ser orientado de modo a evitar, encontrar e corrigir vulnerabilidades — por meio de teste de invasão e de teste estático de segurança.

Seção XVII - Cópia de segurança

Art. 122 - O DRM-RJ deve implementar uma solução de cópia de segurança, incluindo solução para recuperação de desastres.

Art. 123 - O DRM-RJ deve segregar, de forma lógica e física, a infraestrutura de rede da solução de cópia de segurança.

Art. 124 - O DRM-RJ deve possuir uma estratégia de cópia de segurança aplicável a cada uma das seguintes categorias de informações:

I - Arquivo;

II - E-mail;

III - Banco de dados;

IV - Aplicação;

V - Máquina virtual;

VI - Imagem de sistema operacional.

Parágrafo único. A estratégia de cópia de segurança deve possuir a definição de retenção, o esquema (completo, incremental ou diferencial), a origem e o destino de armazenamento, a janela de execução, a rotina, bem como a periodicidade dos testes (seja de integridade da cópia de segurança, seja de recuperação de desastre).

Art. 125 - O DRM-RJ deve garantir a proteção, por criptografia, das cópias de segurança de arquivos com informações sensíveis.

Art. 126 - O DRM-RJ deve tratar as cópias de segurança com dados pessoais conforme as diretrizes da “Seção VII – Privacidade” do “Capítulo V – Diretrizes” desta política.

Seção XVIII - Continuidade do negócio

Art. 127 - O DRM-RJ deve implementar um Plano de Continuidade do Negócio para situações de desastres.

Parágrafo único. O Plano de Continuidade do Negócio deve garantir tanto a segurança quanto a privacidade da informação durante a crise.

Art. 128 - O DRM-RJ deve garantir que os ativos tecnológicos possuam redundância suficiente para atender aos requisitos de disponibilidade da informação.

Seção XIX - Uso de dispositivo pessoal no trabalho

Art. 129 - O servidor, estagiário ou trabalhador terceirizado que optar por utilizar o celular pessoal para fins de trabalho deverá submetê-lo à Assessoria de Informática para, de acordo com os critérios estabelecidos pelo DRM-RJ, aplicar as configurações de segurança da informação, bem como homologar os requisitos de segurança da informação aplicáveis a celulares.

Art. 130 - O servidor, estagiário ou trabalhador terceirizado que optar pela utilização do computador pessoal para trabalhar deverá:

I - Segregar o uso pessoal do uso corporativo;

II - Submeter o computador à Assessoria de Informática para, de acordo com os critérios estabelecidos pelo DRM-RJ, aplicar as configurações de segurança da informação, bem como para homologar os requisitos de segurança da informação aplicáveis a computadores pessoais.

Parágrafo único. As diretrizes estabelecidas nesta política devem ser seguidas e aplicadas pelos servidores, estagiários ou trabalhadores terceirizados em seus dispositivos pessoais — exceto quanto às orientações expressamente direcionadas aos dispositivos de propriedade do DRM-RJ.

CAPÍTULO VI - DOCUMENTOS COMPLEMENTARES

Art. 131 - De modo a viabilizar esta política, devem ser estabelecidos os seguintes procedimentos:

I - Gestão de Acesso Físico e Lógico;

II - Gestão de Ativo;

III - Gestão de Mudança;

IV - Gestão de Risco de Segurança e de Privacidade da Informação;

V - Gestão de Vulnerabilidade Técnica;

VI - Gestão de Inteligência de Ameaça;

VII - Gestão de Evento de Segurança e de Privacidade da Informação;

VIII - Gestão de Incidente de Segurança e de Privacidade da Informação;

IX - Gestão de Cópia de Segurança;

X - Gestão de Segurança em Redes;

XI - Gestão de *Software*;

XII - Gestão de Solução contra Código Malicioso;

XIII - Gestão de Segurança e Privacidade da Informação em Serviço Terceirizado;

XIV - Gestão de Privacidade;

XV - Gestão da Continuidade do Negócio;

XVI - Gestão da Informação Documentada;

XVII - Gestão de Seleção e Contratação de Pessoas;

XVIII - Plano de Disponibilidade de Tecnologia da Informação;

XIX - Plano de Capacidade de Tecnologia da Informação;

XX - Plano de Conscientização.

CAPÍTULO VII - EXCEÇÕES

Art. 132 - As exceções a esta política devem ser explicitadas e formalizadas — seja nos documentos complementares, seja nos Termos de Responsabilidade de Segurança da Informação.

Art. 133 - O DRM-RJ deve definir e implementar controles de segurança para minimizar os riscos inerentes às exceções a esta política.

CAPÍTULO VIII - AVALIAÇÃO DE DESEMPENHO

Art. 134 - O DRM-RJ deve definir os objetivos para a segurança e privacidade da informação.

Art. 135 - O DRM-RJ deve definir e implementar indicadores de desempenho para os processos de segurança e privacidade da informação — sendo que tais indicadores devem apoiar o monitoramento dos objetivos.

Art. 136 - O DRM-RJ deve prover um programa de auditoria desta política, seguido de análise crítica do resultado da auditoria.

CAPÍTULO IX - PROCESSO DISCIPLINAR

Art. 137 - Em caso de descumprimento das diretrizes expressas nesta política, o servidor estará sujeito à responsabilização administrativa.

Parágrafo único. A responsabilização administrativa decorrente da inobservância desta política não isenta o servidor de responder civil e penalmente pelas condutas irregulares praticadas.

Art. 138 - O Comitê de Segurança da Informação deverá comunicar, ao controle interno, casos de inobservância a esta política por parte de algum servidor estatutário, para adoção das providências associadas à deflagração de Procedimento Administrativo de Sindicância.

Parágrafo único. São passíveis de aplicação as penas previstas no Decreto-Lei nº 220, de 18 de julho de 1975 (que dispõe sobre o Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro), no Decreto Estadual nº 2.479, de 8 de março de 1979 (que aprova o Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro), bem como no Decreto nº 46.938 de 13 de fevereiro de 2020 (Regimento Interno do DRM-RJ) — no caso de comprovação, por meio do conjunto probatório carreado no curso da apuração, da prática de transgressão disciplinar por parte de servidor estatutário.

CAPÍTULO X - VIGÊNCIA

Art. 139 - Esta política entrará em vigor na data de sua publicação e deverá ser revisada (quanto à sua pertinência, bem como quanto ao seu alinhamento com o planejamento estratégico) anualmente ou diante de mudanças que acarretem um impacto significativo à segurança e à privacidade da informação no DRM-RJ.

Art. 140 - Fica estabelecido o prazo não superior a 180 (cento e oitenta) dias, a contar da data de publicação desta política, para a implementação dos controles previstos em suas diretrizes.