Política de Segurança da Informação

Agência Reguladora de Serviços Públicos Concedidos de Transportes Aquaviários, Ferroviários, Metroviários e de Rodovias do Estado do Rio de Janeiro

AGETRANSP

PRESIDENTE

Adolpho Konder

CHEFE DE GABINETE

André Novo

ELABORAÇÃO DO DOCUMENTO

Assessoria Técnica de Informática

Rafael Motta

Política de Segurança da Informação

SUMÁRIO

Política de Segurança da Informação

O Presidente da Agência Reguladora de Serviços Públicos Concedidos de Transportes Aquaviários, Ferroviários, Metroviários e de Rodovias do Estado do Rio de Janeiro (AGETRANSP), no uso das atribuições que lhe são conferidas, emite a seguinte Política de Segurança da Informação, a vigorar a partir da data de sua assinatura, revogando todas as disposições em contrário.

CAPÍTULO I - ESCOPO

Seção I - Propósito

Art. 1 - Esta política visa definir responsabilidades, deveres e penalidades quanto à segurança e à privacidade da informação, bem como promover uma cultura de proteção às informações da AGETRANSP, de seus clientes, de seus fornecedores e de outras partes envolvidas em acordos com a AGETRANSP.

Seção II - Princípios

Art. 2 - 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. 3 - Esta política aplica-se aos servidores, estagiários, fornecedores, trabalhadores terceirizados e às partes envolvidas em acordos (independentemente dos instrumentos administrativos utilizados) com a AGETRANSP.

CAPÍTULO II - REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4 - Esta política foi estabelecida considerando 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);

VI - 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);

VII - Instrução Normativa PRODERJ/PRE nº 02, 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 - 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);

IX - Decreto nº 2.479, de 08 de março de 1979 (Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro);

X - 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 12527, de 18 de novembro de 2011);

XI - Decreto nº 46.730, de 09 de agosto de 2019 (Regulamenta a lei estadual nº 5.427, de 01 de abril de 2009, no que dispõe sobre a produção e tramitação eletrônica de documentos e processos administrativos na Administração Pública Estadual e dá outras providências).

CAPÍTULO III - TERMOS E DEFINIÇÕES

Art. 5 - 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 ou trabalhadores terceirizados, cuja gestão de acesso é feita pela área de tecnologia da informação;

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 realizados por *hackers*;

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

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

VI - Cliente: cidadãos que usufruem do serviço público prestado pela AGETRANSP;

VII - Servidor: servidor público da AGETRANSP, independentemente do regime jurídico de trabalho, que ocupa cargo, emprego ou função públicos, sendo efetivo, temporário ou comissionado;

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

IX - Evento de privacidade da informação: evento de segurança da informação que envolva dados pessoais;

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

XI - Fornecedor: pessoa física ou jurídica, de direito público ou privado, que forneça produto ou serviço à AGETRANSP;

XII - Incidente de privacidade da informação: incidente de segurança da informação que envolva dados pessoais e que possa acarretar risco ou dano relevante aos titulares desses dados;

XIII - Incidente de segurança da informação: evento de segurança da informação que compromete os princípios de segurança da informação;

XIV - Informação sensível: informação que precisa ser protegida contra acesso ou divulgação não autorizados. São as informações com algum grau de sigilo, incluindo as informações pessoais, ou seja, são as informações que não são públicas;

XV - Inteligência de ameaças: coleta, em várias fontes, de informações 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;

XVI - Login: identificação do usuário de um *software* dotada de restrições de segurança, cujo acesso seguro pode ser feito mediante esta identificação e senha;

XVII - Oportunidade de privacidade da informação: oportunidade de segurança da informação que contém dados pessoais;

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

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

XX - Registro de auditoria: registro de texto cronológico e detalhado das ações feitas 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*;

XXI - Risco de privacidade da informação: risco de segurança da informação que contém dados pessoais;

XXII - 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) de um ativo de informação, e cujo impacto potencial seja o comprometimento dos princípios de segurança da informação, impedindo o alcance dos objetivos;

XXIII - Trabalhador terceirizado: a pessoa que realiza o serviço para a AGETRANSP em nome do fornecedor;

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

XXV - Vulnerabilidade técnica: fraqueza em um ativo tecnológico da AGETRANSP, a qual pode ser explorada por uma ameaça.

CAPÍTULO IV - PAPÉIS E RESPONSABILIDADES

Art. 6 - É da 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 - Realizar os treinamentos em segurança e privacidade da informação fornecidos pela AGETRANSP;

IV - Notificar eventos e incidentes de segurança e de privacidade da informação por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, notificar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ.

Art. 7 - É da 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 - Definir e gerenciar os perfis, direitos e níveis de acesso 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 - Segregar funções que representem conflito de interesse nos processos sob sua gestão;

V - Identificar, continuamente, os riscos de segurança e de privacidade da informação associados aos ativos de informação sob sua responsabilidade e notificá-los por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, notificar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ;

V - Após a contratação do fornecedor, garantir, de forma imediata, a disponibilização desta política, a conscientização sobre segurança e privacidade da informação, bem como a assinatura do Termo de Responsabilidade da PSI para cada trabalhador terceirizado;

VI - Solicitar os dispositivos tecnológicos e os acessos básicos lógicos para os trabalhadores terceirizados sob sua gestão, por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, solicitar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ;

VII - Solicitar os acessos físicos para os trabalhadores terceirizados sob sua gestão, por meio do SEI-RJ;

Art. 8 - É da responsabilidade do departamento de Recursos Humanos:

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

II - Solicitar os dispositivos tecnológicos e os acessos básicos lógicos para os novos servidores e estagiários, por meio do sistema de Help Desk e em caso de impossibilidade de acesso a este, solicitar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de Help Desk, e-mail do suporte técnico ou SEI-RJ;

III - Solicitar os acessos físicos para os servidores e estagiários, por meio do SEI-RJ.

Art. 9 - É da responsabilidade da área de Tecnologia da Informação:

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, os direitos e os níveis de acesso 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 - Homologar os dispositivos tecnológicos e os *softwares* para utilização na AGETRANSP;

V - Prover, continuamente, aos dispositivos tecnológicos e *softwares* homologados, os controles necessários para cumprir as diretrizes de segurança e privacidade desta política;

VI - Monitorar o ambiente tecnológico por meio de soluções de monitoramento da disponibilidade, do desempenho e da capacidade dos ativos tecnológicos críticos ao negócio;

VII - Após a contratação, disponibilizar ao servidor ou estagiário, esta política, a conscientização sobre segurança e privacidade da informação, bem como o Termo de Responsabilidade da PSI;

VIII - Prover para servidores, estagiários e trabalhadores terceirizados conscientização e educação tanto em segurança quanto em privacidade da informação de forma contínua, por meio de um plano anual de conscientização e educação — inclusive prover conhecimentos específicos às equipes técnicas.

Art. 10 - É da responsabilidade da equipe de Segurança da Informação:

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.

Art. 11 - É da responsabilidade da equipe de Privacidade da Informação:

I - Mapear, continuamente, as atividades envolvendo tratamento de dados pessoais na AGETRANSP;

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

Art. 12 - É da responsabilidade do Comitê de Segurança e Privacidade da Informação:

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

II - Revisar esta política conforme capítulo VIII;

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

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

a. Recomendar a aplicação de sanção, conforme Termo de Compromisso de Estágio, ao estagiário infrator;

b. Recomendar para o gestor do Contrato a aplicação de sanção, conforme contrato (ou instrumento administrativo equivalente), ao fornecedor, ao trabalhador terceirizado ou a outras partes envolvidas em acordos com a AGETRANSP que tenham cometido a infração;

c. Recomendar para a Corregedoria a abertura de sindicância para processo disciplinar ao servidor infrator.

V - Propor soluções para tratar riscos, oportunidades, eventos e incidentes (seja de segurança, seja de privacidade) identificados na AGETRANSP.

Parágrafo único: este comitê é constituído por representantes da PGA, do departamento de Recursos Humanos, da área de Tecnologia da Informação, da área de Segurança da Informação, Encarregado pela Proteção dos Dados Pessoais e, quando convocada para pauta específica, a Alta Administração.

Art. 13 - É da responsabilidade da Procuradoria Geral da Agência (PGA):

I - Elaborar Termo de Compromisso de Estágio padrão com cláusula que atribua a responsabilidade quanto à segurança e privacidade da informação aos estagiários;

II - Elaborar contrato de trabalho padrão com cláusula que atribua a responsabilidade quanto à segurança e privacidade da informação aos servidores;

III - Elaborar contrato (ou instrumento administrativo equivalente) padrão com cláusula que atribua a responsabilidade quanto à segurança e privacidade da informação aos fornecedores ou a outras partes envolvidas em acordos com a AGETRANSP.

Art. 14 - É da responsabilidade da Corregedoria:

I - Apurar, quando recomendado pelo Comitê de Segurança da Informação, mediante sindicância, as infrações cometidas pelos servidores contra a PSI e contra as cláusulas de segurança e de privacidade da informação constantes nos contratos de trabalho.

Parágrafo único: A aplicação da penalidade de suspensão de até 30 dias é da responsabilidade da Corregedoria.

Art. 15 - É da responsabilidade do presidente da AGETRANSP:

I - Aplicar as sanções aos estagiários diante de infrações cometidas contra esta política quando recomendado pelo Comitê de Segurança da Informação;

II - Aplicar as sanções aos servidores diante de infrações cometidas contra esta política quando recomendado pela Corregedoria;

III - Aplicar as sanções aos fornecedores e a outras partes envolvidas em acordos com a AGETRANSP diante de infrações cometidas contra esta política quando recomendado pelo Comitê de Segurança da Informação.

CAPÍTULO V - DIRETRIZES

Seção I - Gestão de acesso

Art. 16 - A AGETRANSP deve vincular ao Cadastro de Pessoas Físicas (CPF) todos os meios de identificação utilizados para o trabalho — por exemplo, o número de registro, crachá, *login*, certificado, assinatura digital, dado biométrico e reconhecimento facial.

Parágrafo único: As identidades atribuídas a várias pessoas ou atribuídas a entidades não humanas devem ser restringidas, justificadas, aprovadas e controladas pela área de Tecnologia da Informação.

Art. 17 - A AGETRANSP deve bloquear os direitos de acesso caso não ocorra a assinatura do Termo de Responsabilidade da PSI no 1º acesso ao computador.

Art. 18 - A AGETRANSP deve restringir, por meio da definição de perfis de acesso, o acesso à informação e às funções dos *softwares*.

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

Art. 19 - A AGETRANSP deve criar identidades e atribuir direitos de acesso básico mediante solicitação do departamento de Recursos Humanos por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, solicitar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ.

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

Art. 20 - A AGETRANSP deve excluir identidades e revogar direitos de acesso básico mediante solicitação do departamento de Recursos Humanos, por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, solicitar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ;

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

§2 Os direitos de acesso devem ser imediatamente removidos quando se tornarem desnecessários para a AGETRANSP.

Art. 21 - A AGETRANSP deve configurar os direitos de acesso temporários para expirarem de forma automática nas datas definidas, previamente, no momento da solicitação.

Art. 22 - A AGETRANSP deve manter registro de todas as ações referentes às solicitações, autorizações, criações e exclusões de identidade, bem como concessões e revogações dos direitos de acesso.

Art. 23 - A AGETRANSP deve garantir que seus *softwares* exijam senhas complexas conforme critérios abaixo:

I - Todas as senhas de acesso aos *softwares* devem possuir, no mínimo, 8 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.

Art. 24 - 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, número de telefone e afins.

Art. 25 - A AGETRANSP deve implementar, preferencialmente, a autenticação de duplo fator.

Art. 26 - A AGETRANSP deve implementar a expiração de sessão em seus *softwares* que possuam esse recurso.

Art. 27 - A AGETRANSP deve implementar o bloqueio de conta, em caso de digitação errônea da senha por 3 vezes consecutivas, em seus *softwares* que possuam esse recurso.

Art. 28 - A AGETRANSP deve implementar a expiração automática a cada 12 meses, com notificação ao usuário do sistema 5 dias antes, em seus *softwares* que possuam esse recurso.

Parágrafo único: No ato de renovação da senha, não deverá ser aceita senha igual às últimas 10 registradas.

Art. 29 - Nos casos em que a senha inicial é fornecida pelo administrador do *software*, a AGETRANSP deve implementar a exigência de troca da senha no primeiro *login* em seus *softwares* que possuam esse recurso.

Art. 30 - O servidor, estagiário ou trabalhador terceirizado não deve expor, compartilhar ou revelar as senhas para outras pessoas.

Seção II - Uso aceitável dos ativos de informação

Art. 31 - O servidor, estagiário ou trabalhador terceirizado não deve utilizar os ativos de informação da AGETRANSP para fins diferentes dos necessários ao desempenho do seu trabalho.

Art. 32 - O servidor, estagiário ou trabalhador terceirizado deve zelar pelo bom uso dos dispositivos tecnológicos disponibilizados pela AGETRANSP — incluindo não remover, alterar ou acrescentar qualquer tipo de componente interno de *hardware*.

Art. 33 - A AGETRANSP deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga instalar *softwares* não homologados nos dispositivos tecnológicos de propriedade da autarquia.

Art. 34 - A AGETRANSP 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 AGETRANSP.

Art. 35 - A AGETRANSP deve bloquear o uso de mídia removível nos dispositivos tecnológicos de propriedade da autarquia. Conforme necessidade, 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 que possuírem autorização para utilizar mídia removível devem aplicar criptografia nos documentos com informação sensível armazenados no dispositivo em questão.

Art. 36 - A AGETRANSP deve garantir que seus servidores, estagiários ou trabalhadores terceirizados não consigam navegar em sites das seguintes categorias:

I - Propaganda político-partidária;

II - Conteúdo ilegal ou que promova atividade ilegal;

III - Conteúdo de caráter sexual.

Art. 37 - O servidor, estagiário ou trabalhador terceirizado não deve armazenar conteúdo ilegal ou não ético nos ativos de informação da AGETRANSP.

Art. 38 - O servidor, estagiário ou trabalhador terceirizado não deve armazenar conteúdo particular nos ativos de informação de propriedade da AGETRANSP.

Art. 39 - 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.

§1 O servidor, estagiário ou trabalhador terceirizado deve armazenar as informações necessárias para as atividades da AGETRANSP no servidor de arquivos.

Art. 40 - O servidor, estagiário ou trabalhador terceirizado não deve consumir alimentos e bebidas próximo aos ativos de informação.

Art. 41 - A AGETRANSP deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga alterar as configurações de segurança dos ativos tecnológicos de propriedade da autarquia.

Art. 42 - A AGETRANSP deve garantir que o servidor, estagiário ou trabalhador terceirizado não consiga conectar dispositivos tecnológicos não homologados à rede da autarquia.

Art. 43 - O servidor, estagiário ou trabalhador terceirizado deve desligar o computador ao final do expediente, exceto quando a área de Tecnologia da Informação comunicar que, em data determinada, os computadores deverão permanecer ligados para manutenção ou para atualização.

Art. 44 - O servidor, estagiário ou trabalhador terceirizado deve retirar imediatamente da impressora os documentos para os quais tenha solicitado a impressão, caso contenham informações sensíveis.

Art. 45 - A AGETRANSP deve implementar solução tecnológica para inventariar os ativos tecnológicos de propriedade da autarquia.

Art. 46 - A AGETRANSP deve implementar linha de base de configuração para os ativos tecnológicos, incluindo configurações de segurança e privacidade da informação.

Art. 47 - A AGETRANSP deve segregar suas redes, no mínimo, em: domínio de acesso público (rede de visitantes), domínio de estação de trabalho e domínio de computador do tipo servidor.

§1 As comunicações entre essas redes devem estar protegidas com a implementação de um perímetro entre elas.

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

Art. 48 - 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. 49 - 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, em apresentações ou em locais públicos.

Art. 50 - A AGETRANSP deve implementar o bloqueio automático de tela do computador a partir de 2 (dois) minutos de inatividade.

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

Seção III - Trabalho remoto e uso de dispositivos móveis

Art. 51 - Em caso de furto ou roubo de dispositivo móvel de propriedade da AGETRANSP ou de dispositivo pessoal homologado para fins de trabalho, o servidor, estagiário ou trabalhador terceirizado deve notificar imediatamente a autarquia por meio do sistema de *Help Desk* e em caso de impossibilidade de acesso a esse, notificar por meio dos canais na seguinte ordem de preferência: aplicativo móvel do sistema de *Help Desk*, e-mail do suporte técnico ou SEI-RJ — com cópia ao seu superior imediato e à Corregedoria. Assim que possível, também deverá ser registrado o boletim de ocorrência.

Art. 52 - A AGETRANSP deve habilitar o rastreamento de localização e o recurso para limpeza remota nos dispositivos móveis de propriedade da autarquia.

Art. 53 - A AGETRANSP deve garantir que o acesso remoto à sua rede ocorra somente via *Virtual Private Network* (VPN).

Art. 54 - O servidor, estagiário ou trabalhador terceirizado não deve conectar os dispositivos móveis de propriedade da AGETRANSP em redes públicas de Wi-Fi.

Seção IV - Ambiente físico

Art. 55 - Na entrada principal do perímetro da autarquia, a AGETRANSP deve implementar vigilância, portaria ou recepção, bem como catracas com sistemas baseados em cartão de acesso, biometria ou reconhecimento facial.

Art. 56 - Nos arredores do perímetro da autarquia e nos pontos de acesso à entrada principal do escritório a AGETRANSP deve implementar câmeras de segurança com sistema de monitoramento.

Art. 57 - Na entrada principal do escritório, a AGETRANSP deve implementar tranca segura.

Art. 58 - Na entrada principal do escritório, a AGETRANSP deve implementar, recepção e controle de acesso físico com sistemas baseados em cartão de acesso, biometria ou reconhecimento facial.

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

Art. 59 - A AGETRANSP deve prover ao servidor e ao estagiário um meio de identificação visível (por meio do crachá), para que transitem pelo escritório da autarquia.

Art. 60 - A AGETRANSP deve prover aos trabalhadores terceirizados um meio de identificação visível (por meio do crachá) e capaz de diferenciá-los dos servidores e estagiários, para que transitem pelo escritório da autarquia.

Art. 61 - O servidor, estagiário ou trabalhador terceirizado deve utilizar o crachá ao transitar pelo escritório da AGETRANSP.

Art. 62 - Nas subdivisões e salas do escritório onde estejam armazenadas informações sensíveis, a AGETRANSP deve implementar proteções contra acesso não autorizado — mediante sistemas baseados em cartão de acesso, biometria, reconhecimento facial ou chaves.

Art. 63 - Nas salas de cabos, painéis de conexão e pontos terminais, a AGETRANSP deve implementar proteções contra acesso não autorizado

— mediante sistemas baseados em cartão de acesso, biometria, reconhecimento facial ou chaves.

Art. 64 - A AGETRANSP 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 do escritório.

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. 65 - A AGETRANSP deve garantir que seu escritório possua, no mínimo, proteções físicas contra incêndio, inundação, descarga elétrica, explosão e manifestações civis.

Art. 66 - A AGETRANSP deve garantir que a infraestrutura predial de seu escritório 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. 67 - O servidor, estagiário ou trabalhador terceirizado não deve remover, instalar ou movimentar os dispositivos tecnológicos de propriedade da AGETRANSP — com exceção dos dispositivos móveis.

Art. 68 - A AGETRANSP deve garantir que os dispositivos tecnológicos de propriedade da autarquia recebam manutenção com apoio das bases de conhecimento e especificações do fabricante.

Art. 69 - A AGETRANSP, antes da reutilização ou do descarte dos dispositivos tecnológicos, deve sobrescrever de forma segura ou destruir fisicamente os dispositivos de armazenamento.

Art. 70 - Por meio da implementação de redundâncias testadas anualmente, a AGETRANSP deve proteger os seus dispositivos tecnológicos contra indisponibilidade ocasionada por interrupção ou carência no suprimento dos serviços de energia elétrica, telecomunicações e ar-condicionado.

Art. 71 - A AGETRANSP deve proteger o cabeamento de energia e de telecomunicações contra danos e interferências — por meio de passagem em eletrocalhas, cabeamento estruturado e identificação por rótulos nas extremidades do cabeamento.

Seção V - Classificação da informação

Art. 72 - A AGETRANSP deve classificar e rotular as suas informações, quanto ao grau e prazo de sigilo, em: ultrassecreta, secreta ou reservada — para as situações previstas na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Parágrafo único: Para informação pessoal, independentemente da classificação de sigilo atribuída, a AGETRANSP 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 o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Art. 73 - A AGETRANSP deve classificar e rotular as suas informações no SEI-RJ, quanto ao grau de sigilo, em: público, restrito e sigiloso — conforme o disposto no Decreto nº 46.730, de 09 de agosto de 2019.

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

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

§3 Não poderão ser incluídos no SEI-RJ os documentos que possuam informações classificáveis nos níveis de sigilo estabelecidos nos artigos 23 e 24 da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e nos artigos 22, 27, 28 e 29 do Decreto nº 46.205, de 27 de dezembro de 2017.

Seção VI - Transferência da informação

Art. 74 - O servidor, estagiário ou trabalhador terceirizado deve utilizar o e-mail institucional (do domínio da AGETRANSP) para comunicação de assuntos pertinentes à autarquia.

Parágrafo único: O servidor, estagiário ou trabalhador terceirizado não deve utilizar o e-mail particular para comunicação de assuntos pertinentes à autarquia.

Art. 75 - Na utilização do e-mail institucional, o servidor, estagiário ou trabalhador terceirizado não deve:

I - Enviar propagandas, mensagem do tipo 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 corporativo em *sites* ou aplicativos externos, exceto mediante autorização específica da AGETRANSP.

Parágrafo único: Os e-mails corporativos cadastrados em *sites* ou aplicativos externos mediante autorização devem ser estritamente controlados pela AGETRANSP.

Art. 76 - A AGETRANSP deve restringir a permissão de envio simultâneo de mensagens para todos os usuários.

Art. 77 - A AGETRANSP deve garantir que sua solução de e-mail possua detecção e proteção contra código malicioso; 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. 78 - O servidor, estagiário ou trabalhador terceirizado deve aplicar criptografia em anexos de e-mail que contenham informação sensível.

Art. 79 - O servidor, estagiário ou trabalhador terceirizado deve rotular a mensagem eletrônica, antes do envio ou resposta, conforme Seção V do Capítulo V desta política.

Art. 80 - O servidor, estagiário ou trabalhador terceirizado deve proceder com dupla checagem dos remetentes antes do envio de informação sensível, por quaisquer meios de comunicação.

Art. 81 - O servidor, estagiário ou trabalhador terceirizado deve controlar e notificar tanto o envio quanto o recebimento de documentos físicos ou de mídias removíveis com informação sensível. Para transporte, deve-se utilizar envelope opaco sem identificação aparente do conteúdo, mas com a devida classificação do sigilo e, para envio, devem-se utilizar serviços postais homologados pela AGETRANSP.

Seção VII - Privacidade

Art. 82 - A AGETRANSP 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).

§1 A AGETRANSP deve implementar uma Política de Privacidade para informar aos titulares de dados pessoais, a maneira como esses dados são tratados e períodos de armazenamento.

§2 A AGETRANSP deve garantir que o propósito do tratamento dos dados pessoais não é ilícito, por meio do mapeamento e definição das finalidades dos tratamentos.

§3 A AGETRANSP deve garantir que os processos e os *softwares* sejam projetados ou ajustados para que o tratamento dos dados pessoais seja limitado ao necessário para o propósito.

Seção VIII - Códigos maliciosos

Art. 83 - Nos ativos tecnológicos, a AGETRANSP 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 varrer dados recebidos (pela rede ou por mídia removível).

Art. 84 - O servidor, estagiário ou trabalhador terceirizado não deve interromper, nos ativos tecnológicos, a verificação feita pelos *softwares* de proteção contra códigos maliciosos.

Seção IX - Fornecedores

Art. 85 - A AGETRANSP deve acordar com seus fornecedores, em contrato, quais os requisitos de segurança e privacidade da informação necessários, 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 devem ser estendidos, em cláusula específica, à cadeia de suprimento desse fornecedor.

Art. 86 - A AGETRANSP deve implementar processo de *due diligence*.

Seção X - Serviços em nuvem

Art. 87 - A AGETRANSP deve garantir, para cada serviço em nuvem a ser contratado, que as seguintes questões sobre segurança e privacidade da informação estejam 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 à AGETRANSP, diante do término do serviço em nuvem;

V - Localização dos dados e jurisdição.

Art. 88 - A AGETRANSP deve monitorar o uso dos serviços em nuvem, a fim de identificar e tratar riscos, eventos, bem como incidentes (seja de segurança, seja de privacidade da informação).

Seção XI - Incidentes de segurança e de privacidade da informação

Art. 89 - A AGETRANSP deve estabelecer critérios para avaliar quando classificar um evento de segurança ou de privacidade da informação como sendo um incidente de segurança ou de privacidade da informação.

Art. 90 - A AGETRANSP deve estabelecer critérios para avaliar quando o Plano de Continuidade de Negócio deve ser acionado para tratar um incidente de segurança ou de privacidade da informação.

Art. 91 - A AGETRANSP deve estabelecer um processo para gestão de incidentes (seja de segurança, seja 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, a AGETRANSP deve estabelecer fases de contenção, erradicação e recuperação.

Art. 92 - A AGETRANSP deve garantir que os incidentes de segurança e de privacidade da informação possuam registro das ações envolvidas, desde o relato ou detecção até a resolução.

Art. 93 - A AGETRANSP deve estabelecer critérios para avaliar quando será necessária a análise forense de um incidente de segurança ou de privacidade da informação.

Art. 94 - A AGETRANSP deve garantir que as evidências dos incidentes (seja de segurança, seja de privacidade da informação) sejam identificadas, coletadas e preservadas, a fim de embasar as ações tanto disciplinares quanto legais.

Seção XII - Vulnerabilidades técnicas

Art. 95 - A AGETRANSP deve implementar uma solução de varredura de vulnerabilidade técnica, bem como um processo para avaliação contínua, tratamento da vulnerabilidade e verificação da eficácia desse tratamento.

Art. 96 - A AGETRANSP deve implementar um programa de teste de invasão.

Art. 97 - A AGETRANSP deve implementar as atualizações de segurança de *software*.

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

Seção XIII - Inteligência de ameaças

Art. 98 - A AGETRANSP deve produzir inteligência de ameaças a partir da coleta e análise de informações de ameaças — com o objetivo de prevenir, detectar e responder a ameaças cibernéticas.

Seção XIV - Controles criptográficos e gerenciamento de chaves

Art. 99 - A AGETRANSP deve utilizar somente algoritmos de criptografia padronizados.

Art. 100 - A AGETRANSP deve utilizar uma autoridade certificadora confiável para gerenciar suas chaves criptográficas (públicas e privadas).

Art. 101 - A AGETRANSP deve prover condições para a criptografia das informações sensíveis, tanto em seu armazenamento quanto em sua transmissão.

Seção XV - Registro de auditoria

Art. 102 - A AGETRANSP deve garantir que os registros de auditoria dos seus ativos tecnológicos sejam habilitados, alertados, monitorados e analisados.

Art. 103 - Uma vez que os registros de auditoria possuem dado pessoal, a AGETRANSP deve tratá-los em conformidade com as diretrizes da Seção VII do Capítulo V desta política.

Art. 104 - A AGETRANSP deve implementar uma solução de gerenciamento e correlação de eventos de segurança e de privacidade da informação para centralizar e correlacionar os registros de auditoria das atividades dos usuários e dos administradores de *softwares*, das falhas e dos comportamentos atípicos ou anormais dos *softwares*, bem como para alertar eventos de segurança ou de privacidade que requeiram atenção ou ação.

Art. 105 - A AGETRANSP deve proteger os registros de auditoria de seus *softwares*, por meio de cópia de segurança e gestão de acesso.

Art. 106 - A AGETRANSP 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. 107 - A AGETRANSP deve garantir que os registros de auditoria de seus *softwares* sejam sincronizados a partir de uma origem de tempo confiável, para que contenham informação de data/hora consistente.

Seção XVI - Desenvolvimento de *software* interno ou terceirizado

Art. 108 - Para o desenvolvimento de *software* e para cenários de reuso de código, a AGETRANSP deve garantir que sejam adotados: metodologia de desenvolvimento, princípios de codificação segura, princípios de segurança

e privacidade desde a concepção e utilização da técnica de revisão por pares.

Art. 109 - A AGETRANSP 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. 110 - O desenvolvimento de *software* deve ser orientado de modo a evitar, encontrar e corrigir vulnerabilidades, por meio de teste de invasão e teste estático de segurança.

Seção XVII - Cópia de segurança

Art. 111 - A AGETRANSP deve garantir cópia de segurança, incluindo recuperação de desastres.

Art. 112 - A AGETRANSP 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, um esquema (completo, incremental, diferencial), a origem e o destino de armazenamento, a janela de execução, a rotina, bem como a periodicidade do teste de integridade.

Art. 113 - A AGETRANSP deve garantir a proteção, por criptografia, das cópias de segurança de arquivos com informações sensíveis.

Art. 114 - A AGETRANSP deve tratar as cópias de segurança com dados pessoais conforme as diretrizes da Seção VII do Capítulo V desta política.

Seção XVIII - Continuidade do negócio

Art. 115 - A AGETRANSP deve implementar um Plano de Continuidade do Negócio para situações de desastre.

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

Art. 116 - A AGETRANSP 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. 117 - O servidor, estagiário ou trabalhador terceirizado que optar por utilizar o celular pessoal para trabalhar deverá submetê-lo à área de Tecnologia da Informação para, de acordo com os critérios estabelecidos pela AGETRANSP, aplicar as configurações de segurança da informação e homologar os requisitos de segurança da informação para celular.

Art. 118 - O servidor, estagiário ou trabalhador terceirizado que optar por utilizar computador pessoal para trabalhar deverá:

I - Separar o uso pessoal do uso organizacional;

II - Submeter o computador à área de Tecnologia da Informação para, de acordo com os critérios estabelecidos pela AGETRANSP, aplicar as configurações de segurança da informação e homologar os requisitos de segurança da informação para computador pessoal.

Parágrafo único: As diretrizes estabelecidas nesta política devem ser seguidas pelos servidores, estagiários ou trabalhadores terceirizados em seus dispositivos pessoais — com exceção das orientações expressamente direcionadas aos dispositivos de propriedade da AGETRANSP.

CAPÍTULO VI - DOCUMENTOS COMPLEMENTARES

Art. 119 - De modo a viabilizar esta política, devem ser estabelecidos procedimentos para:

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 Ameaças;

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 Solução contra Código Malicioso;

XI - Gestão de Fornecedor;

XII - Gestão de Privacidade;

XIII - Gestão de Continuidade de Negócio;

XIV - Plano de Continuidade de Tecnologia da Informação;

XV - Plano de Disponibilidade de Tecnologia da Informação;

XVI - Plano de Capacidade de Tecnologia da Informação.

CAPÍTULO VII - PROCESSO DISCIPLINAR

Art. 120 - 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. 121 - O Comitê de Segurança da Informação deverá comunicar de imediato ao Órgão Correcional da Agência quanto à inobservância desta política, por parte de servidor, para adoção das providências quanto à deflagração de Procedimento Administrativo de Sindicância.

Art. 122 - 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 2.479/79, de 08 de março de 1979, que aprova o Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro e no Regimento Interno da Agência, no caso de restar comprovada, através do conjunto probatório carreado no curso da apuração, a prática de transgressão disciplinar por parte de servidor.

CAPÍTULO VIII - VIGÊNCIA

Art. 123 - Esta política entrará em vigor na data de sua publicação e deverá ser revisada, quanto à sua pertinência, anualmente ou diante de mudanças com potencial impacto significativo à segurança e à privacidade da informação na AGETRANSP.