DEPARTAMENTO DE TRÂNSITO DO ESTADO
DO RIO DE JANEIRO
ATO DO PRESIDENTE

PORTARIA DETRAN/RJ Nº 6739 DE 07 DE JANEIRO DE 2025

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) NO ÂMBITO DO DETRAN-RJ.

O **PRESIDENTE DO DEPARTAMENTO DE TRÂNSITO DO ESTADO DO RIO DE JANEIRO (DETRAN-RJ),** no uso das atribuições que lhe são conferidas, emite a seguinte Política de Segurança da Informação e Comunicação (POSIC), a vigorar a partir da data de sua assinatura, revogando todas as disposições contrárias, tendo em vista o que consta no Processo n° SEI-150016/097829/2024, e

CONSIDERANDO:

- O DECRETO ESTADUAL Nº 2.479, DE 08 DE MARÇO DE 1979 – aprova o regulamento do estatuto dos funcionários públicos civis do poder executivo do estado do Rio de Janeiro;

- A LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997 – Lei do Habeas Data;

- A LEI N.º 12.527, DE 18 DE NOVEMBRO DE 2011 – Lei de Acesso à Informação;

- A LEI Nº 12.965, DE 23 DE JUNHO DE 2014 – Marco Civil da Internet;

- A LEI N.º 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

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

- A INSTRUÇÃO NORMATIVA PRODERJ/PRE N.º 02, DE 28 DE ABRIL DE 2022 – que regulamenta os procedimentos de Segurança da Informação em soluções de Tecnologia da Informação e Comunicação (TIC) a serem adotados pelos órgãos e entidades integrantes da administração direta e indireta do Poder Executivo do Estado do Rio de Janeiro;

- O DECRETO ESTADUAL Nº 48.891, DE 10 DE JANEIRO DE 2024 – que institui a Política de Governança em privacidade de Proteção de Dados Pessoais do Estado do Rio de Janeiro em conformidade com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais -LGPD;

- A NORMA ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de Gestão de Segurança da Informação;

- A NORMA ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança para gestão da privacidade da informação.

RESOLVE:

Art. 1º - Fica instituída a Política de Segurança da Informação e Comunicação (POSIC) no âmbito do Departamento de Trânsito do Estado do Rio de Janeiro.

CAPÍTULO I
DO ESCOPO

Art. 2º - Esta Política de Segurança da Informação e Comunicação (POSIC) define as diretrizes a serem adotadas na gestão de qualquer informação, abrangendo processos e documentos, com objetivo de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações gerenciadas no âmbito do DETRAN-RJ, de modo a apoiar a tomada de decisões, garantindo a transparência e a eficiência organizacional, com a aplicação das legislações e normas técnicas vigentes.

Parágrafo único - Esta Política abrange todo arcabouço documental complementar que versa sobre a privacidade e proteção de dados pessoais.

SEÇÃO II – DA ABRANGÊNCIA

Art. 3º - Esta Política aplica-se aos servidores e colaboradores que integram a estrutura organizacional do DETRAN/RJ, assim como a todos aqueles que, de alguma forma, se relacionam com a Autarquia.

Art. 4º - Os contratos, convênios, acordos e outros instrumentos congêneres devem atender aos requisitos especificados neste documento.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

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

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

II. AMEAÇA - conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

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

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

V. ATIVIDADE CRÍTICA – atividade que deve ser executada visando garantir a consecução de produtos e serviços fundamentais do órgão ou entidade, de forma a atingir os objetivos mais importantes e sensíveis ao tempo;

VI. ATIVO - tudo que tenha valor para a organização, material ou não;

VII. ATIVO DE REDE - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

VIII. ATIVOS DE INFORMAÇÃO - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

IX. ATIVOS DE INFORMAÇÃO PATRIMONIADOS - compreendem todos os equipamentos físicos pertencentes ao DETRAN-RJ, utilizados para armazenamento, processamento e transmissão de informações, identificados, registrados e geridos como patrimônio do órgão. Ativos de Informação Patrimoniados incluem, mas não se limitam a: Computadores, servidores, roteadores, switches, dispositivos de armazenamento, Tablets, notebooks, smartphones e quaisquer outros dispositivos de TIC registrados como patrimônio do DETRAN-RJ;

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

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

XII. AUTENTICAÇÃO DE MULTIFATORES (MFA) - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

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

XIV. AUTORIZAÇÃO - processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence; portanto, autorização é o direito ou a permissão de acesso a um recurso de um sistema;

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

XVI. CELERIDADE – as ações relacionadas à segurança da informação deverão oferecer respostas ágeis para os incidentes e para as vulnerabilidades identificados nos ativos de informação do DETRAN-RJ;

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

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

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

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

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

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

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

XXIV. DADO PESSOAL - informação relacionada à pessoa natural identificada ou identificável;

XXV. DADO PESSOAL SENSÍVEL – “Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XXVI. DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais;

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

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

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

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

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

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

XXXIII. EXCLUSÃO DE ACESSO - processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso;

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

XXXV. GESTÃO DE SEGURANÇA DA INFORMAÇÃO - processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XXXVI. GESTOR DA INFORMAÇÃO – indivíduo responsável pela administração de informações geradas em seu processo de trabalho e/ou ativos de informação relacionados às suas atividades institucionais;

XXXVII. INCIDENTE DE SEGURANÇA - Eventos de segurança da informação indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações, gerados por acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

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

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

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

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

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

XLIII. QUEBRA DE SEGURANÇA – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XLIV. REDE PRIVADA VIRTUAL (VPN) - refere-se à construção de uma rede privada, utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública;

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

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

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

XLVIII. SEGURANÇA DA INFORMAÇÃO (SI) - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XLIX. TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) - ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

L. TRATAMENTO - toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

LI. USUÁRIO DE INFORMAÇÃO - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade, Confidencialidade e Sigilo (TRCS);

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

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

CAPÍTULO III
PRINCÍPIOS

Art. 6º - A Segurança da Informação do DETRAN-RJ deve obedecer aos princípios de acesso, de disponibilidade, de integridade, de confidencialidade, de autenticidade, de legalidade, de privacidade, de auditabilidade, do não repúdio, do interesse público, da defesa do patrimônio público, da impessoalidade, da moralidade, da transparência, da honestidade, da responsabilidade e da prevenção.

Art. 7º - Para os fins dispostos neste documento, a Segurança da Informação abrange:

I - Segurança e defesa cibernética;

II - Segurança física;

III - Proteção de dados organizacionais;

IV - Privacidade;
V - Ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO IV
DIRETRIZES GERAIS

Art. 8º - A Segurança da Informação tem como principal diretriz a proteção da informação, de modo a garantir a continuidade do negócio, a minimização dos riscos e a implementação de melhorias oportunas nos processos do DETRAN-RJ.

Art. 9º - As diretrizes de segurança da informação devem considerar, prioritariamente, os objetivos estratégicos, os processos e os requisitos legais do DETRAN-RJ.

Art. 10 - As diretrizes de segurança da informação descritas no capítulo VII desta política devem ser observadas por todos os servidores, colaboradores e prestadores de serviços que executem atividades vinculadas ao DETRAN-RJ, durante todas as etapas do tratamento da informação: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle.

Art. 11 - O DETRAN-RJ deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, a relevância, a criticidade e a sensibilidade, observando a legislação em vigor.

Art. 12 - Os contratos, convênios, acordos e instrumentos congêneres firmados pelo DETRAN-RJ devem conter cláusulas que determinem a observância dessa política.

CAPÍTULO V
PAPÉIS E RESPONSABILIDADES

Art. 13 - Caberá ao Diretor de Tecnologia da Informação e Comunicação:

I. Atuar como responsável e exercer liderança quanto à melhoria dos processos relacionados ao tema de Segurança da Informação no DETRAN-RJ;

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

III. Criar, assegurar a implantação e monitorar os normativos relacionados à Segurança da Informação, garantindo adequação à legislação do país;

IV. Implementar medidas de monitoramento e conscientização, a fim de assegurar que as áreas afetadas estejam cientes das possíveis consequências (seja para a organização, seja para o titular de dados pessoais) acarretadas por violações à privacidade, às regras de segurança ou aos procedimentos — especialmente aqueles relacionados ao manuseio de dados pessoais;

V. Analisar criticamente as ocorrências de segurança da informação, considerando o cumprimento das políticas de segurança frente ao volume e aos impactos — dos eventos e incidentes de segurança detectados, bem como das mudanças de tecnologias;

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

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

Art. 14 - Caberá ao Gestor de Segurança da Informação:

I. Conscientizar, informar e incentivar os usuários de informação sob a sua supervisão a cumprirem as regras definidas na presente política, atuando como um agente multiplicador;

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

III. Manter, criar, alterar ou excluir as contas de usuários, considerando a respectiva “necessidade do conhecer” para execução das atividades;

IV. Comunicar a Política de Segurança da Informação e Comunicação (POSIC), assim como a Política de Privacidade e Proteção de Dados Pessoais (PPPDP) e a Política de Controle de Acesso (PCA) a terceiros e a fornecedores contratados;

V. Incluir, nas especificações técnicas dos bens ou serviços contratados, regras que protejam a segurança e a privacidade da informação — quando dados pessoais ou dados pessoais sensíveis estiverem envolvidos, requer-se observância às políticas, aos procedimentos internos e às diretrizes específicas sobre o tema.

Art. 15 - Caberá ao Coordenador de Gestão de Pessoas:

I. Garantir que o Termo de Responsabilidade, Confidencialidade e Sigilo (TRCS), os termos de conhecimento da POSIC, PPPDP e PCA, e de responsabilização (tanto da informação quanto dos ativos manuseados) sejam assinados por todo colaborador atuando em prol do DETRAN-RJ;

II. Assegurar que todo colaborador atuando no DETRAN-RJ seja elegível e adequado para sua função e cargo inserido;

III. Monitorar e controlar a realização do curso de Uso Responsável das TICs por todo colaborador que atue em prol do DETRAN-RJ, incluindo a verificação periódica dos certificados de conclusão e a guarda dos registros comprobatórios.

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

Art. 16 - Caberá aos Usuários de Informação:

I. Conhecer e cumprir a POSIC, PPPDP e PCA;

II. Possuir conclusão do curso de Uso Responsável das TICs, quando disponíveis na Escola Virtual de Governo. O curso deverá ser concluído no prazo máximo de 30 (trinta) dias após o início das atividades do colaborador no DETRAN-RJ ou, no caso de colaboradores já em exercício, no prazo de 60 (sessenta) dias a contar da data de publicação desta POSIC.

III. Não divulgar informações não públicas para pessoas não autorizadas, a fim de mitigar possíveis situações que coloquem em risco a segurança e a imagem do DETRAN-RJ;

IV. Utilizar as informações e os recursos tecnológicos em sua posse exclusivamente para os objetivos do DETRAN-RJ, e não para fins pessoais ou de terceiros;

V. Não compartilhar credenciais de acesso ou equipamentos autenticados;

VI. Relatar ao Gestor de Segurança da Informação eventuais incidentes de segurança da informação, bem como suspeitas ou violações desta política e de suas normas complementares.

CAPÍTULO VI
DIRETRIZES DE SEGURANÇA

Art. 17 - Durante a execução das atividades diárias, tanto nas dependências internas quanto externas do DETRAN-RJ, são geradas ou desenvolvidas informações, as quais constituem ativos de informação — essenciais à condução das operações organizacionais e, em última análise, à própria existência do órgão.

Art. 18 - Toda informação custodiada em ativos de Tecnologia da Informação e Comunicação (TIC) no DETRAN-RJ deve possuir cópias de segurança (backups) guardadas em locais seguros, com controle de acesso e tempo de retenção definidos.

Parágrafo Único - O serviço de cópia de segurança não tem amplitude sobre os dados e/ou informações armazenadas fora do Data Center do DETRAN-RJ.

Art. 19 - Toda informação custodiada, gerada ou desenvolvida no DETRAN-RJ deve ser classificada de acordo com seu impacto e sua importância para a organização.

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

Art. 20 - Todos os servidores, terceiros e conveniados, independentemente do vínculo, função ou nível hierárquico no DETRAN-RJ, são responsáveis pela segurança, zelo e bom uso dos ativos aos quais possuem acesso.

§ 1º- O DETRAN-RJ deve adotar instrumentos de autodeclaração de responsabilidade, bem como de compromisso, com o sigilo e com a confidencialidade das informações e dos ativos manuseados pelos usuários;

§ 2º - Os instrumentos de autodeclaração adotados deverão ser considerados como imprescritíveis, irrevogáveis e irretratáveis.

Art. 21 - As instalações e equipamentos devem ser protegidos contra acessos não autorizados, devendo o DETRAN-RJ implementar, nos seus ativos de informação, mecanismos que impeçam acessos indevidos.

Art. 22 - Os acessos lógicos e físicos de todos os usuários abrangidos neste documento devem ser aprovados, registrados, armazenados e adequados às necessidades inerentes ao respectivo cargo e função no DETRAN-RJ.

Art. 23 - A senha é pessoal e intrasferível, sendo vedado seu compartilhamento com terceiros. É imprescindível sua criação com base na combinação em algoritmos fortes aptos a inibir vulnerabilidades e acessos indevidos.

Parágrafo Único - O DETRAN-RJ deve adotar práticas de gerenciamento de senhas tanto para usuário quanto para administrador – forçando a alteração periódica, definindo o critério de complexidade e impedindo a reutilização de senhas antigas.

CAPÍTULO VII
DIRETRIZES DE ESPECÍFICAS

Art. 24 - Para cada diretriz indicada nas seções deste capítulo, deve ser observada a elaboração de procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o entendimento dos usuários da organização.

SEÇÃO I – Gestão de Ativos

Art. 25 - Todo ativo de informação da organização deve:

I. Ser inventariado e protegido;

II. Possuir identificação formal da área e o Diretor Geral/Assessor Chefe responsável;

III. Ter suas ameaças, vulnerabilidades e interdependências mapeadas.

Art. 26 - Toda entrada e saída dos ativos de informação patrimoniados pelo DETRAN-RJ deve ser informada à Diretoria de Tecnologia da Informação e Comunicação.

Art. 27 - O DETRAN-RJ deve definir regras e processos tanto para solicitação quanto para descarte dos ativos organizacionais.

Art. 28 - O DETRAN-RJ deve implementar mecanismos e práticas para gerir seus ativos de forma remota.

Art. 29 - Devem ser implementados os mecanismos de segurança aptos a tutelar os ativos de informação da organização, considerando as camadas de segurança necessárias e proporcionais à criticidade e risco identificados, vendando-se ao usuário desabilitar configurações instaladas para tal finalidade.

Art. 30 - O DETRAN-RJ deve definir regras e diretrizes relacionadas ao backup seja dos ativos de rede, seja das aplicações que compõem o seu ambiente tecnológico.

SEÇÃO II – Segurança Física e do Ambiente

Art. 31 - O acesso às instalações do DETRAN-RJ deve ser controlado por meio de sistemas de controle de acesso.

Art. 32 - As instalações físicas do DETRAN-RJ devem ser continuamente monitoradas e vigiadas, a fim de detectar acessos não autorizados ou comportamento suspeito.

Art. 33 - O DETRAN-RJ deve estabelecer um perímetro de segurança e definir os níveis necessários de segurança para cada área.

Art. 34 - Em todas as áreas de acesso restrito, a organização deve instalar barreiras de proteção adicional com de controle de acesso físico.

Art. 35 - Todos os acessos devem ser revistos, periodicamente, pela Gerência de Segurança da Informação.

Art. 36 - Visitantes e fornecedores que acessarem as instalações do DETRAN-RJ devem ser devidamente identificados e registrados, de forma a garantir a segurança e o controle de acesso às dependências do órgão.

§ 1º - A identificação de visitantes e fornecedores deverá ser realizada mediante apresentação de documento oficial com foto e registro de informações essenciais, tais como nome completo, documento de identificação, empresa representada, horário de entrada e saída, bem como a área ou setor visitado.

§ 2º - A responsabilidade pelo processo de identificação e registro cabe ao setor de segurança e portaria do DETRAN-RJ, que deverá assegurar o cumprimento desta norma e o armazenamento adequado dos registros em conformidade com a legislação vigente de proteção de dados pessoais.

§ 3º - Todos os visitantes e fornecedores devem ser acompanhados por um servidor ou colaborador autorizado durante sua permanência nas dependências do órgão, exceto em casos devidamente autorizados pela chefia do setor responsável.

§ 4º - As informações de identificação coletadas serão mantidas pelo período necessário, respeitando-se as diretrizes de retenção e descarte de dados estabelecidas pela Política de Segurança da Informação e Comunicação e pela Lei Geral de Proteção de Dados Pessoais (LGPD).

SEÇÃO III – Uso dos Recursos Tecnológicos

Art. 37 - Não é permitido instalar softwares não homologados nos equipamentos disponibilizados pelo DETRAN-RJ.

Art. 38 - Os equipamentos devem permanecer com seus lacres de proteção não violados.

Parágrafo Único - Caso seu equipamento esteja sem o lacre ou com o lacre violado, o fato deverá ser relatado imediatamente à Diretoria de Tecnologia da Informação e Comunicação através dos canais oficiais.

Art. 39 - É de responsabilidade do custodiante realizar o backup das informações salvas nos equipamentos que manusear.

Art. 40 - Não é permitido armazenar arquivos que não sejam para fins de trabalho nos diretórios de rede ou nos ativos de informação, nem transmiti-los por e-mail ou aplicativos de mensagens instantâneas.

Art. 41 - As informações corporativas devem ser armazenadas na rede coorporativa, em local destinado à unidade do usuário, conforme orientação do gestor correspondente — não sendo autorizado armazená-las localmente, no computador.

Art. 42 - É proibido cadastrar o e-mail corporativo em sites ou aplicativos para uso pessoal. O e-mail corporativo deve ser utilizado exclusivamente para atividades profissionais.

Art. 43 - O DETRAN deve adotar mecanismos para reduzir o recebimento e o envio de mensagens indesejadas (SPAM, Phishing, entre outros) que representem risco ou estejam em desconformidade com os normativos vigentes.

Art. 44 - A internet deve ser utilizada para fins corporativos e inerentes às atividades diárias de cada usuário de informação.

Parágrafo Único - O DETRAN deve estabelecer diretrizes e responsabilidades quanto ao uso aceitável da internet e das mídias sociais em seu ambiente tecnológico para todos os usuários de informação.

Art. 45 - O DETRAN-RJ deve definir e implementar uma política de senhas, a qual deve ser definida pelo gestor do sistema, para todas as suas aplicações.

SEÇÃO IV – Acesso Lógico

Art. 46 - O DETRAN-RJ deve definir as regras de acesso aos dados — como autenticação multifator de usuário, senhas, criptografia, entre outros mecanismos de segurança. Além disso, a organização deve estabelecer restrições de acesso baseadas em níveis de autorização.

Art. 47 - Todos os acessos devem ser revistos, semestralmente, pelo Gestor de Segurança da Informação.

Parágrafo Único - É de responsabilidade do Coordenador de Gestão de Pessoas informar ao Gestor de Segurança da Informação sobre o desligamento de qualquer usuário da informação para que sejam adotadas as providências de cancelamento dos acessos.

Art. 48 - Todos os acessos concedidos aos usuários de informação deverão estar alinhados a necessidade de conhecer.

SEÇÃO V – Classificação da Informação

Art. 49 - Toda informação armazenada ou mantida no DETRAN-RJ deve ser classificada de acordo com seu valor, requisitos legais, sensibilidade e criticidade.

Art. 50 - O DETRAN-RJ deve, sempre que possível, implementar mecanismos para a classificação obrigatória de todos os seus documentos.

SEÇÃO VI – Mesa e Tela Limpa

Art. 51 - Todo usuário de informação deve armazenar documentos impressos com informações não públicas em local seguro e com controle de acesso, como cofres, armários ou gavetas com chaves.

Art. 52 - Os equipamentos deverão ser desligados ao final do expediente, para que a rotina de atualização de segurança do sistema operacional possa ser executada.

Art. 53 - Todo usuário de informação deve bloquear a tela do seu equipamento ao se ausentar da mesa.

SEÇÃO VII – Monitoramento e Auditoria

Art. 54 - Todo usuário de informação (interno ou externo), na função de custodiante, está sujeito a terem suas ações realizadas nos ativos que compõem o ambiente computacional do DETRAN-RJ auditadas e monitoradas, com o objetivo de detectar atividades anômalas ou não autorizadas, bem como investigar casos relacionados a incidentes, auditorias e ouvidorias.

SEÇÃO VIII – Trabalho Remoto

Art. 55 - O DETRAN-RJ deve criar regras para estabelecer as formas, bem como os limites, de acesso dos seus usuários de informação, quando esses estiverem exercendo atividades de forma remota.

Art. 56 - As diretrizes desta política também deverão ser cumpridas durante o trabalho remoto.

Art. 57 - O DETRAN-RJ deve implementar mecanismos para tornar o uso de VPN obrigatório durante o trabalho remoto.

SEÇÃO IX – Computação em Nuvem

Art. 58 - O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação deve possibilitar que todas as garantias legais atribuídas ao DETRAN sejam respeitadas.

SEÇÃO X – Incidente de Segurança da Informação

Art. 59 - O DETRAN-RJ deve monitorar o ambiente cibernético da organização, para efetuar o tratamento de incidentes de maneira proativa, reduzindo o tempo de resposta a incidentes.

Art. 60 - Em caso de roubo ou furto do equipamento, o colaborador ou o terceiro deve imediatamente informar o ocorrido à Diretoria de Tecnologia da Informação e Comunicação através dos canais oficiais, bem como deve registrar o boletim de ocorrência.

CAPÍTULO VIII
SANÇÕES E PENALIDADES

Art. 61 - O DETRAN-RJ deve descrever as medidas disciplinares cabíveis a serem tomadas em caso de descumprimento desta política.

Art. 62 - Em caso de descumprimento desta POSIC ou das diretrizes expressas nos normativos relacionados à segurança e à privacidade da informação, qualquer colaborador estará sujeito à responsabilização administrativa, civil ou penal.

CAPÍTULO IX
VIGÊNCIA

Art. 63 - Esta política entrará em vigor na data de sua publicação e deverá ser revisada, minimamente, a cada 2 (dois) anos, ou sempre que houver alteração nas diretrizes estabelecidas que impactem as normas de segurança da informação e comunicação.

§ 1º- A responsabilidade pela coordenação e condução do processo de revisão da POSIC será do Gestor de Segurança da Informação, que deverá avaliar a necessidade de ajustes, propor alterações e assegurar que a política permaneça atualizada e adequada aos requisitos legais e institucionais.

§ 2º- A revisão deverá envolver consulta e alinhamento com as áreas responsáveis por segurança, tecnologia da informação e assessoria jurídica, garantindo que todas as modificações propostas estejam em conformidade com as melhores práticas e exigências regulatórias.

§ 3º- Após cada revisão, a versão atualizada da POSIC deverá ser submetida para aprovação pela Presidência do DETRAN-RJ e, uma vez aprovada, será publicada e comunicada a todos os colaboradores.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Art. 64 - A elaboração da POSIC adotou por referência o disposto na legislação e normatização elencada no preâmbulo.

Art. 65 - Os casos omissos e as dúvidas sugeridas na aplicação desta Política serão dirimidos pelo Presidente do DETRAN-RJ.

Art. 66 - Esta portaria entra em vigor na data de sua publicação.

Rio de Janeiro, 07 de janeiro de 2025

GLAUCIO PAZ DA SILVA
Presidente do DETRAN/RJ