POLÍTICA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO - PGSI				
Tema:	Norma Geral - N-SI-001			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os recursos tecnológicos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO DETRAN|ES

Considerando os princípios, as diretrizes, as responsabilidades e as competências das organizações relacionados ao compartilhamento, ao acesso e à segurança da informação constantes da Lei nº 12.527, Lei de Acesso à Informação - LAI, de 18 de novembro de 2011, bem como da Lei Nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD.

Considerando as diretrizes da Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 12.572/2025, que estabelece o padrão para a segurança da informação na administração pública brasileira

Considerando que as informações geradas internamente, adquiridas ou absorvidas pelo Departamento Estadual de Trânsito do Espírito Santo - DETRAN|ES, no exercício de suas competências legais e regulamentares, são patrimônio da Instituição e, portanto, necessitam ser protegidas.

Considerando que o DETRAN|ES mantém grande volume de informações essenciais ao exercício de suas competências legais e regulamentares e que essas informações devem manter-se íntegras, disponíveis e, quando for o caso, com o sigilo resguardado.

Considerando que a adequada gestão da informação deve nortear todos os processos de trabalho e Unidades do Departamento e ser impulsionada por esta Política Interna de Segurança da Informação;

Considerando as disposições dos Decretos estaduais nº 4922-R, de 09 de julho de 2021 (Política Estadual de Proteção de Dados Pessoais e da Privacidade) e nº 2884-R, de 21 de outubro de 2011 (Política Estadual de Segurança da Informação) a importância da adoção de boas práticas inerentes à proteção da informação, abarcadas pelas normas NBR ISSO/IEC 27001:2022, NBR ISSO/IEC 27002:2022.

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação (PSI) N.SI.001, na forma que segue.

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta política objetiva estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) que transcenda a conformidade técnica, posicionando a segurança como um pilar estratégico para a confiança do cidadão, a proteção de dados pessoais e a soberania do Estado sobre seus ativos de informação.

Parágrafo Único. A implementação da PSI visa assegurar que as informações e seus ativos, possuídos ou custodiados nos sistemas deste DETRAN-ES, são protegidos e utilizados de forma a garantir sua confidencialidade, integridade, disponibilidade e autenticidade, de acordo com a lei.

Art. 3º A Política de Segurança da Informação - PSI se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por nomeação,

designação, contratação, convênio ou qualquer outra forma de investidura ou vínculo, cargo, emprego, função pública ou atividade análoga no âmbito desta Autarquia, e que façam uso de seus recursos materiais e tecnológicos.

Parágrafo único. A PSI estende-se também a todos os Servidores, contratados e instituições ou pessoas credenciadas ou conveniadas, que tratem informações em nome do DETRAN|ES.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para efeito desta Instrução e de suas regulamentações, aplicam-se as seguintes definições:

I. **Agentes de tratamento**: o controlador e o operador;
II. **Anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
III. **Ameaça**: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
IV. **Atividades precípuas**: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim do DETRAN|ES;
V. **Atividades críticas**: atividades precípuas do DETRAN|ES cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, danos à imagem institucional, prejuízo ao Erário, entre outros.
VI. **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a organização.

VII. **Ativo de informação**: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pelo DETRAN|ES.

VIII. **Ativo de processamento**: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas do DETRAN|ES.

IX. **Autenticidade**: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

X. **Autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

XI. **Banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

XII. **Bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

XIII. **Ciclo de vida da informação**: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação, destinação e eliminação.

XIV. **Cifração**: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los.

XV. **Comissão de segurança da informação – CSI**: Grupo de trabalho multidisciplinar permanente, efetivado pela Diretoria Geral do DETRAN|ES, que tem por finalidade tratar questões ligadas à Segurança da Informação.

XVI. **Confidencialidade**: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização.

XVII. **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

XVIII. **Continuidade de negócios**: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

XIX. **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

XX. **Credenciais de Acesso**: Senhas e chaves de acesso a sistemas informáticos.

XXI. **CSI - Comitê Interno de Segurança da Informação**: Órgão estratégico (composto por GTI, Jurídico, RH, DPO, etc.) a ser acionado em incidentes de nível Alto ou Crítico para fornecer orientação e tomar decisões sobre impactos de negócio, legais e de comunicação.

XXII. **Custodiante da Informação**: É a área responsável pela infraestrutura onde a informação é armazenada e processada

XXIII. **Dado anonimizado**: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

XXIV. **Dados Financeiros e Contratuais**: Informações sobre arrecadação de taxas, contratos com fornecedores (operadores, no jargão da LGPD).

XXV. **Dados Operacionais Essenciais**: A base de dados de veículos registrados, o sistema de pontuação e multas, registros de processos administrativos.

XXVI. **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável, incluindo-se o nome, o CPF, o endereço, número da CNH/prontuário e do RENAVAM de milhões de condutores e proprietários de veículos.

XXVII. **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.

XXVIII. **Dado anonimizado**: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

XXIX. **Dados Financeiros e Contratuais**: Informações sobre arrecadação de taxas, contratos com fornecedores (operadores, no jargão da LGPD).

XXX. **Dados Operacionais Essenciais**: A base de dados de veículos registrados, o sistema de pontuação e multas, registros de processos administrativos. A indisponibilidade desses dados paralisa os serviços do órgão.

XXXI. **Data Protection Officer – DPO**: Servidor designado pelo Diretor Geral como o ponto de contato e o elo de comunicação entre os três principais atores do ecossistema de proteção de dados: o Controlador (DETRAN|ES), os Titulares dos Dados (proprietários de veículos e condutores) e a Autoridade Nacional de Proteção de Dados (ANPD).

XXXII. **Decifração**: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

XXXIII. **Disponibilidade**: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada.

XXXIV. **ERISI - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação**: Grupo operacional composto por membros da GTI que tem como atribuição detectar e responder aos incidentes de segurança da informação do DETRAN|ES, bem como recomendar as medidas necessárias para prevenção de incidentes futuros, mediante a capacitação profissional e utilização de tecnologias aplicáveis à segurança da informação.

XXXV. **Eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

XXXVI. **Encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD.

XXXVII. **Gestão de Segurança da Informação**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação.

XXXVIII. **Gestor de Segurança da Informação**: Servidor da GTI, designado para a implementar e gerenciar as políticas, procedimentos e tecnologias que garantem a segurança e privacidade dos dados pessoais de uma organização, assegurando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

XXXIX. **Incidente de segurança em redes computacionais**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XL. **Incidente em segurança da informação**: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação.

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

XLII. **Informação Crítica**: qualquer informação cuja perda de Confidencialidade, Integridade ou Disponibilidade poderia causar impacto severo e inaceitável para o DETRAN|ES, incluindo: Dados pessoais sensíveis; dados operacionais

essenciais; dados financeiros e contratuais; e credenciais de acesso a sistemas.

XLIII. **Integridade**: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário.

XLIV. **Irretratabilidade** (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação.

XLV. **MFA - Autenticação Multifator**: exige que o usuário apresente dois ou mais métodos de verificação diferentes para ter acesso a uma conta, serviço ou sistema.

XLVI. **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

XLVII. **Órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

XLVIII. **Plano de Continuidade do Negócio – PCN**: conjunto estratégico e proativo de processos e procedimentos que a GTI do DETRAN|ES desenvolve para garantir que suas funções críticas possam continuar operando durante e após a ocorrência de um desastre ou uma interrupção significativa.

XLIX. **Política de mesa limpa e tela limpa**: conjunto de diretrizes de segurança da informação projetado para proteger dados sensíveis e confidenciais de uma organização contra acesso não autorizado, roubo ou perda.

L. **Processo de gestão de riscos de ativos de informação e de processamento**: ciclo contínuo e sistemático, alinhado aos objetivos estratégicos do DETRAN|ES, para identificar, analisar, avaliar, tratar e monitorar os riscos que possam comprometer a confidencialidade, a integridade e a disponibilidade das informações.

LI. **Proprietário da Informação**: É o gestor da área de negócio responsável pela geração e manutenção da informação, sendo responsável por solicitar, justificar e revisar periodicamente os acessos de sua equipe, garantindo a aplicação do Princípio do Menor Privilégio.

LII. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

LIII. **Recurso**: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento.

LIV. **Recurso criptográfico**: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

LV. **Rede de computadores**: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros.

LVI. **Relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

LVII. **Risco**: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

LVIII. **Segurança da informação**: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades.

LIX. **Transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

LX. **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

LXI. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

LXII. **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

LXIII. **Trilha de auditoria**: registro cronológico, seguro e detalhado de todos os eventos e ações que ocorrem em um sistema, banco de dados ou ambiente digital que envolva o tratamento de dados pessoais; essencialmente, é um "quem, o quê, quando, onde e por quê" de tudo o que acontece com uma informação pessoal dentro de uma organização.

LXIV. **Uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

LXV. **Usuário**: indivíduo que tem credenciais (login e senha) para acessar e interagir com os sistemas informáticos ou redes do DETRAN|ES.

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

CAPÍTULO II
DOS PRINCÍPIOS

Art. 5º A PSI do DETRAN-ES, alinhada às estratégias desta Instituição e em conformidade com a LGPD e a PNSI, tem como princípios norteadores:

I. Foco na Gestão de Riscos: Adotar a gestão de riscos como pilar para a tomada de decisões em segurança da informação;
II. Garantia dos Direitos Fundamentais: Assegurar a proteção de dados pessoais, a privacidade e o livre acesso à informação, em conformidade com a legislação;
III. Responsabilidade e Prestação de Contas: Garantir que todas as ações de tratamento de dados sejam justificadas e auditáveis;
IV. Segurança como Responsabilidade de Todos: Promover uma cultura organizacional onde cada colaborador e parceiro se reconhece como agente ativo na proteção das informações; e
V. Melhoria Contínua: Manter um ciclo contínuo de avaliação e aprimoramento dos controles e processos de segurança da informação.

CAPÍTULO III
DO ESCOPO

Art. 6º São Objetivos da PSI do DETRAN|ES:

I. Instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação;
II. Proteger os ativos de informação contra todo tipo de ameaça, interna ou externa, intencional ou acidental, garantindo a continuidade dos serviços essenciais à população;
III. Assegurar a conformidade com o arcabouço legal e regulatório vigente; e

IV. Promover a conscientização e a capacitação contínua de recursos humanos em segurança da informação e proteção de dados.

Art. 7º Os destinatários desta PSI, relacionados no artigo 3º, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta instrução.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 8º A operacionalização das diretrizes da PSI do DETRAN|ES, se efetivará por meio das normas superiores e as constantes em seus anexos.

Art. 9º As normas integrantes desta PSI serão homologadas pelo Diretor Geral, publicadas no Portal deste DETRAN|ES, em seção específica intitulada “Segurança da Informação”.

Art. 10. A revisão e a atualização das normas de segurança da informação ocorrerão anualmente ou sempre que se fizer necessário.

SESSÃO I
DA GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 11. Todos os ativos de informação e de processamento do DETRAN|ES, serão inventariados, classificados, atualizados periodicamente, mantidos em condições de uso e terão um responsável designado.

Parágrafo único. Cada ativo de informação e de processamento deverá ter uma unidade responsável, com atribuições claramente definidas.

Art. 12. Toda informação produzida ou custodiada pelo DETRAN-ES deve ser classificada segundo seu grau de confidencialidade, conforme o esquema abaixo, para garantir que os controles de proteção sejam proporcionais à sua sensibilidade.

Nível de Classificação	Definição	Exemplos no Contexto do DETRAN-ES	Requisitos Mínimos de Proteção
Público	Informação que pode ser acessada por qualquer pessoa, sem restrições.	Estatísticas de frota, legislação de trânsito, informações institucionais do site.	Controle de integridade para garantir que não seja alterada indevidamente.
Interno	Informação de uso exclusivo dos colaboradores do DETRAN-ES, cuja divulgação não causa dano direto.	Manuais de procedimento, comunicações internas não sensíveis, relatórios de gestão.	Acesso restrito à rede interna e a usuários autenticados.
Confidencial	Informação cujo acesso não autorizado pode causar dano significativo ao órgão, aos cidadãos ou ao Estado.	Bases de dados RENACH e RENAVAM, dados pessoais de condutores e proprietários, processos administrativos sigilosos.	Criptografia em repouso e em trânsito; controle de acesso baseado em função; registro detalhado de logs de acesso; segregação de redes.
Restrito	Informação altamente sensível, com acesso limitado a um grupo específico de pessoas.	Dados biométricos, laudos médicos e psicológicos, senhas de administração de sistemas críticos.	Todos os controles do nível Confidencial, mais autenticação multifator (MFA) obrigatória e monitoramento proativo de acesso.

Art. 13. Toda e qualquer informação produzida ou custodiada pelo DETRAN|ES deve ser classificada em função do seu grau de confidencialidade, criticidade, disponibilidade, integridade e prazo de retenção, devendo ser protegida, de acordo com a regulamentação de classificação da informação.

Parágrafo único. As informações produzidas por usuários dos sistemas, no exercício de suas funções, são patrimônio intelectual do DETRAN|ES, e não cabe a seus criadores qualquer forma de direito autoral.

Art. 14. É vedado o uso dos ativos do DETRAN|ES para obter proveito pessoal ou de terceiros, bem como para veicular opiniões político-partidárias.

Art. 15. A classificação do nível de sigilo dos dados ou informações deverá ser imposta pelo agente responsável pela sua criação ou manipulação e deverá seguir as especificações prevista na legislação vigente.

Parágrafo único. Na ausência dessa classificação, todas as informações de terceiros que estejam sob a custódia ou processamento do DETRAN|ES devem ser tratadas como possuindo o mais alto grau de sigilo.

SESSÃO II
DO CONTROLE DE ACESSOS A INFORMAÇÃO

Art. 16. O acesso às informações produzidas ou custodiadas pelo DETRAN|ES, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos destinatários desta PSI.

§ 1º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades necessitará de prévia autorização formal.

§ 2º O acesso a informações produzidas ou custodiadas pelo DETRAN|ES que não sejam de domínio público, quando autorizado, será condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 17. Todo usuário deverá possuir identificação pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação.

SEÇÃO III
DA GESTÃO DE RISCOS

Art. 18. Deverá ser estabelecido processo de gestão de riscos de ativos de informação e de processamento do DETRAN|ES, visando à identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação.

Parágrafo único. O Processo de Gestão de Riscos deverá ser acompanhado pela Gerência de Tecnologia da Informação - GTI e revisado periodicamente.

SEÇÃO IV
DA GESTÃO DA CONTINUIDADE DE NEGÓCIOS

Art. 19. A Gerência de Tecnologia da Informação elaborará o Plano de Continuidade de Negócios - PCN que estabeleça procedimentos e defina estrutura mínima de recursos para que se garanta a regularidade do fluxo das informações críticas em momento de crise e salvaguardar o interesse das partes interessadas, a reputação e a marca da Autarquia.

§ 1º O PCN será baseado na ISO 22301, contemplando, pelo menos, os seguintes ciclos:

I. Análise do impacto no negócio;
II. Avaliação de risco;
III. Desenvolvimento de estratégias;
IV. Elaboração e documentação do plano;
V. Testes e exercícios; e
VI. Revisão e melhoria contínua.

Parágrafo único. O Plano de Continuidade de Negócios deverá ser testado e revisado periodicamente.

SEÇÃO V
DO TRATAMENTO DOS INCIDENTES DE REDE

Art. 20. Deverá ser elaborado um Processo de Tratamento e Resposta a Incidentes em Redes de Computadores, visando impedir, interromper ou minimizar o impacto de uma ação maliciosa ou acidental.

§ 1º O Processo descrito no caput deste artigo deverá se basear na ISO 27001 e nas guias National Institute of Standards and Technology – NIST e terá como objetivos:

I. Minimizar o impacto operacional, garantindo que serviços inerentes às atividades deste DETRAN|ES sejam restaurados o mais rápido possível;
II. Proteger os dados dos cidadãos, assegurando a confidencialidade e a integridade dos dados, em conformidade com a LGPD;
III. Preservar a reputação institucional, disponibilizando formas de gerenciar crises de forma transparente e eficaz para manter a confiança do público; e
IV. Cumprir Obrigações Legais, garantindo a correta notificação de incidentes à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, quando necessário.

§ 2º O Processo de Tratamento e Resposta a Incidentes em Redes de Computadores deverá dispor das seguintes fases:

I. Preparação;
II. Detecção e análise;

III. Contenção, erradicação e recuperação; e
IV. Atividades pós-incidente, incluindo a elaboração de relatório final de incidente, a análise da causa raiz, as lições assimiladas e a comunicação aos órgãos de controle, quando necessário.

SEÇÃO VI
DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 21. A gestão de incidentes em segurança da informação tem por objetivo assegurar que fragilidade se incidentes em segurança da informação sejam identificados, permitindo a tomada de ação corretiva em tempo hábil, observando a norma correspondente N-SI-010.

§ 1º É responsabilidade dos usuários:

I. Reportar tempestivamente ao Gestor de Segurança da Informação os incidentes em segurança da informação de que tenham ciência ou suspeita; e
II. Colaborar, em suas áreas de competência, na identificação e no tratamento de incidentes em segurança da informação.

§ 2º É responsabilidade do Gestor de Segurança da Informação:

I. Elaborar e gerir a PSI e Normas Associadas;
II. Implementar e gerir as medidas técnicas de segurança;
III. Liderar o processo de gestão de riscos de segurança;
IV. Coordenar o processo de tratamento e resposta a incidentes;
V. Promover a conscientização e o treinamento em segurança; e
VI. Garantir a segurança desde a concepção (Security by Design).

SESSÃO VII
DA AUDITORIA E CONFORMIDADE

Art. 22. Deverá ser instituído o Plano Anual de Auditoria e Conformidade, para análise do correto cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes.

§ 1º A inclusão no escopo do Plano Anual de Auditoria e Conformidade deve ser realizada, no mínimo, a cada dois anos e deve abranger uma ou mais normas, procedimentos, planos e/ou processos estabelecidos.

§ 2º A GTI será responsável pela elaboração e acompanhamento da regular execução do Plano descrito no *caput* deste artigo.

SESSÃO VIII
DOS SERVIÇOS DE INTERNET, DO CORREIO ELETRÔNICO CORPORATIVO, MÍDIAS SOCIAIS E MENSAGEIROS INSTANTÂNEOS

Art. 23. Na forma dos anexos N-SI-006 e N-SI-008, qualquer informação acessada, transmitida, recebida ou produzida estará sujeita a divulgação e auditoria, resguardados os direitos previstos na LGPD.

Art. 24. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que poderá analisar e, se conveniente e oportuno, monitorar a rede interna, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Art. 25. O monitoramento da rede interna do DETRAN|ES deve ter por objetivo exclusivo a garantia da integridade dos dados e programas, de forma a assegurar a compatibilidade das ações dos usuários com as atribuições legais desta Autarquia.

Parágrafo Único. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor, na forma definida na N-SI-011.

Art. 26. O e-mail institucional deve ser usado apenas para fins relacionados às atividades laborais dos servidores, não devendo ser divulgado ou cadastrado em sites ou serviços relacionados a interesses exclusivamente pessoais.

Art. 27. Os usuários devem adotar todas as medidas que lhes forem possíveis para que suas caixas postais de correio eletrônico não sejam acessadas por terceiros, seja através de dispositivos próprios, alheios, ou pertencentes ao DETRAN|ES.

SESSÃO IX
DO DESENVOLVIMENTO DE SISTEMAS SEGUROS

Art. 28. O desenvolvimento ou melhoria dos softwares do DETRAN|ES deverá contemplar atividades específicas que garantam maior segurança para os sistemas utilizados, de forma a preservar o ambiente tecnológico, assim como prevenir possíveis incidentes de segurança com os dados desses sistemas ou com a infraestrutura utilizada.

Parágrafo único**.** A atuação de empresas contratadas para a atuação nas atividades descritas no *caput* do arquivo, só poderá acontecer se o contrato possuir cláusulas detalhadas e específicas das obrigações da contratada, mediante a elaboração de

Acordo de Processamento de Dados (DPA - Data Processing Agreement), devendo conter, pelo menos:

I. Objeto e Finalidade;
II. Obrigações de Segurança;
III. Confidencialidade;
IV. Proibição de Subcontratação;
V. Cooperação em Incidentes;
VI. Direito de Auditoria;
VII. Controle de Acesso e Segregação de Funções;
VIII. Segurança no Ciclo de Vida do Desenvolvimento;
IX. Devolução e Exclusão Segura dos Dados, após o final do contrato; e
X. Revogação Imediata de Acessos, ao final do processo.

Art. 29. A adoção ou desenvolvimento de ambientes e sistemas contratados, adquiridos, ou desenvolvidos pelo DETRAN|ES, deverá ser previamente avaliados pelas áreas demandantes, em conjunto com os administradores dos ambientes envolvidos, para que se leve em consideração as melhores práticas de segurança da informação aplicáveis aos mesmos, de forma a garantir que sejam seguros.

Art. 30. Todos os requisitos de segurança de ambientes, sistemas ou quaisquer outros ativos ou recursos de informação devem ser identificados previamente à sua implementação e deverão ser testados na fase de avaliação ou desenvolvimento, confirmados na fase de homologação, e continuamente reavaliados durante sua utilização.

Art. 31. Ambientes de desenvolvimento, testes e homologação devem ser segregados entre si e dos ambientes de produção, de forma que impeçam acessos

não autorizados a qualquer desses ambientes e o amplo e irrestrito acesso de desenvolvedores aos ambientes de produção.

Parágrafo único. A GTI poderá disponibilizar acesso aos conteúdos disponibilizados nos ambientes de produção, desde que tais acessos não coloquem em risco a integridade, performance e demais aspectos de segurança dos ambientes de produção.

SESSÃO X
DO USO DE RECURSOS CRIPTOGRAFADOS

Art. 32. Toda a informação classificada como sigilosa, produzida, armazenada ou transmitida pelo DETRAN|ES, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico.

Parágrafo único. A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pela unidade gestora de riscos, ou pela Comissão de Segurança da Informação, ou quando prevista em normativo específico.

SESSÃO XI
DO PROCESSO DE TRATAMENTO DA INFORMAÇÃO

Art. 33. O tratamento da informação deve abranger as políticas, os processos, a práticas e os instrumentos utilizados pelo DETRAN|ES para lidar com a informação ao longo de cada fase do ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Parágrafo único. O conjunto das ações referentes ao tratamento da informação será agrupado nas seguintes fases:

I. Produção e recepção: refere-se à fase inicial do ciclo de vida e compreende produção, recepção ou custódia e classificação da informação;
II. Organizações: refere-se ao armazenamento, arquivamento e controle da informação;
III. uso e disseminação: refere-se à utilização, acesso, reprodução, transporte, transmissão e distribuição da informação;
IV. Destinações: refere-se à fase final do ciclo de vida da informação e compreende avaliação, destinação ou eliminação da informação.

SESSÃO XII
DO ACESSO FÍSICO E SEGURANÇA PATRIMONIAL

Art. 34. A entrada e a saída de bens, equipamentos e demais ativos tecnológicos das dependências do DETRAN|ES devem ser efetuadas com observância aos aspectos de segurança da informação aplicáveis a cada caso e conforme normatizado nas Instruções de Serviço relativas ao controle e gestão de patrimônio publicadas pelo Órgão, visando evitar acessos não autorizados a informações sigilosas armazenadas nesses ativos.

SESSÃO XIII
DO ACESSO LÓGICO E UTILIZAÇÃO DE RECURSOS

Art. 35. Os equipamentos do DETRAN|ES disponibilizados aos usuários (estações de trabalho, notebooks, tablets, smartphones, etc.) devem ser e permanecer configurados de forma a minimizar a probabilidade de incidentes de segurança. Observar norma N-SI-007 sobre Gestão de Identidade.

Art. 36. Não é permitida a conexão de equipamentos pessoais ou de terceiros nas redes locais (cabeadas). Sendo possível tal conexão se necessário à execução das atividades afins.

Art. 37. Autorizações de acesso a sistemas, ambientes e demais recursos devem ser concedidas mediante necessidade e sob o princípio dos privilégios mínimos.

SESSÃO XIV
DO COMPARTILHAMENTO DE INFORMAÇÕES

Art. 38. Dados ou informações só devem ser compartilhados com quem possa ou deva ter acesso aos mesmos, na medida da necessidade e conveniência, na forma das especificações da LGPD.

Art. 39. Senhas de acesso a recursos e ambientes do DETRAN|ES, que precisem ser compartilhadas entre seus administradores ou equipes, devem ser armazenadas criptografadas em sistemas seguros, específicos para este propósito.

SESSÃO XV
DO DESCARTE DE INFORMAÇÕES

Art. 40. Meios, mídias e equipamentos contendo informações confidenciais ou de negócio devem ser instalados, utilizados, armazenados, transportados e descartados de forma segura conforme tabela de temporalidade das atividades e recomendações contidas na norma anexa N-SI-004.

Art. 41. Todos os usuários devem devolver, após o término de suas relações com o DETRAN|ES, todas as mídias eletrônicas ou impressas que possuam quaisquer informações pessoais ou confidenciais pertencentes ao DETRAN|ES ou a terceiros.

CAPÍTULO V
DO ACESSO REMOTO

Art. 42. O acesso remoto a ativos/serviços de informação e recursos computacionais do DETRAN|ES é restrito a usuários que necessitem deste recurso para execução das atividades profissionais.

Art. 43. As diretrizes para acesso remoto a ativos/serviços de informação e recursos computacionais estão descritos no ANEXO N-SI-002 desta política.

CAPÍTULO VI
DA RELAÇÃO COM OS OPERADORES TECNOLÓGICOS

Art. 44. A relação entre o DETRAN|ES, na qualidade de Controlador de dados, com o PRODEST, como principal Operador tecnológico, e demais empresas contratadas que atuam no desenvolvimento ou manutenção de sistemas tecnológicos, será formalizada e gerida ativamente para mitigar riscos e delimitar responsabilidades.

§ 1º Deverá ser estabelecido um Acordo de Nível de Serviço (SLA) focado em segurança, definindo metas de disponibilidade, tempos de resposta a incidentes e canais de comunicação.

§ 2º Será mantida uma matriz de responsabilidade compartilhada, onde o DETRAN|ES define as regras de negócio e acesso, e as contratadas implementam os controles técnicos correspondentes.

CAPÍTULO VII
DOS PAPÉIS E RESPONSABILIDADES

Art. 45. Compete a Gerência de Tecnologia da Informação, além das especificadas nos artigos anteriores:

I. Garantir a implementação desta PSI e o provimento dos ativos de processamento necessários ao seu cumprimento;
II. Garantir que os níveis de acesso lógico concedidos aos usuários estejam adequados aos propósitos do negócio e condizentes com as normas vigentes de segurança da informação;
III. Disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho;
IV. Executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação; e
V. Prover e gerenciar a infraestrutura tecnológica necessária para suportar os controles definidos nesta PSI, em alinhamento com o Gestor de SI.

Art. 46. Compete aos usuários:

I. Ter pleno conhecimento desta PSI;
II. Cumprir as determinações desta Política de Segurança da Informação que sejam aplicáveis e relacionadas ao escopo de suas relações com a autarquia, bem como quaisquer outras obrigações ou termos adicionais relativos à segurança da informação, porventura estabelecidos e formalizados com o DETRAN|ES.
III. Responder por toda atividade executada com o uso de sua identificação;
IV. Proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;

V. Executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

VI. Gerenciar os ativos sob sua responsabilidade, tratando com a devida confidencialidade todas as informações de caráter sigiloso às quais terão acesso ou conhecimento durante a vigência de sua relação com o DETRAN|ES, mesmo após seu encerramento ou extinção do vínculo com a autarquia, por tempo indeterminado ou pelos prazos previstos na legislação em vigor, não as reproduzindo, cedendo, divulgando ou permitindo acesso às mesmas a pessoas não autorizadas a acessá-los ou conhecê-los – à exceção de quando autorizado pelo proprietário da informação, ou se requerido por força de lei ou mandado judicial.

VII. Zelar pela integridade, disponibilidade, autenticidade e legalidade das informações acima citadas, não as utilizando para benefício próprio ou para fins que possam trazer prejuízos de qualquer natureza ao DETRAN|ES, aos seus proprietários ou a terceiros.

VIII. Eximir-se de compartilhar senhas, códigos, tokens, crachás, cartões de acesso ou quaisquer outros meios, credenciais ou dispositivos de autenticação que lhes sejam fornecidos para seu uso exclusivo de serviços, recursos ou ativos gerenciados pelo DETRAN|ES, cuja utilização ocorrerá sob total responsabilidade dos mesmos;

IX. Impedir o acesso a sistemas sob sua administração, sem a devida autorização, conforme N-SI-011;

X. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de TI ou, quando pertinente, à Comissão de Segurança da Informação;

Parágrafo único. Os usuários são responsáveis por seus atos e pelos danos e incidentes provocados pelo mau uso que fizerem das informações e recursos sob suas responsabilidades, sendo aos mesmos imputadas as punições cabíveis.

Art. 47. A Comissão de Segurança da Informação, será composta por, pelo menos: Um representante da GTI, da GJUR, da GV, da GH, da GEOP, da GFIT, da DAFGP e o DPO.

§1º A Comissão terá sua dinâmica de funcionamento especificada pelo Gerente de Tecnologia da informação, que a presidirá.

§ 2º Após a indicação dos membros, pelas respectivas Diretorias, o Diretor Geral, publicará Instrução de Serviço com a relação dos indicados.

Art. 48. É responsabilidade do Comissão de Segurança da Informação:

I. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
II. Requerer às unidades gerenciais do DETRAN|ES informações que considerar relevantes e necessárias à realização de suas atividades;
III. Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do DETRAN|ES.

CAPÍTULO VII
DAS SANÇÕES, PUNIÇÕES E CASOS OMISSOS

Art. 49. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão

passíveis de penalidades que incluem advertência verbal, advertência por escrito e processo administrativo.

Parágrafo único. As sanções administrativas não elidem a aplicação das sanções penais e/ou cíveis, decorrentes da inobservância das obrigações referentes ao tratamento de dados pessoais.

Art. 50. Depois de provocada pela gestão do contrato ou o usuário que identificar possíveis descumprimento de preceitos ou normas relacionadas às atividades de terceiros contratados ou prestadores de serviço, a CSI deverá se manifestar sobre a ocorrência de irregularidade no tratamento dos dados.

Parágrafo único. A manifestação formal da CSI será encaminhada para a gestão do contrato, visando a efetivação das consequências previstas no instrumento contratual.

Art. 51. Os casos omissos serão avaliados pela Comissão de Segurança da Informação para posterior deliberação.

Art. 52. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.

CAPÍTULO IX
DO CONTROLE DE ACESSO LÓGICO

Art. 53. O acesso a sistemas e informações será regido pelo Princípio do Menor Privilégio, garantindo que cada usuário tenha acesso apenas ao que é estritamente necessário para suas funções.

Art. 54. Todo usuário deverá possuir identificação pessoal e intransferível. O uso de senhas fortes é obrigatório, e a Autenticação Multifator (MFA) será exigida para acesso a sistemas críticos e informações classificadas como Confidenciais ou Restritas, a fim de prevenir fraudes e acessos não autorizados.

Art. 55. Deverá existir um processo formal para solicitação, aprovação, revisão periódica e revogação de acessos, garantindo que as permissões sejam sempre atuais e adequadas

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 56. As regras especificadas nesta PSI têm caráter obrigatório, devendo ser observadas por todos os usuários e operadores que utilizem recursos tecnológicos do DETRAN|ES, independente da forma de vínculo estabelecido entre as partes.

Art. 57. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo DETRAN|ES devem observar, no que couber, o constante desta PSI.

Art. 58. A confirmação do conhecimento do inteiro teor deste documento e seus anexos deve ser registrada, em documento próprio, para a concessão de acessos aos sistemas tecnológicos do DETRAN|ES.

Art. 59. Fica alterada a versão anterior da Política de Segurança da Informação do DETRAN|ES, homologada pela IS-N nº 26/2024, passando a produzir efeitos e vincular obrigações, no dia da publicação da nova IS-N, que aprovar os termos deste documento.

ANEXOS

N-SI-002: Acesso Remoto

N-SI-003: BYOD

N-SI-004: Classificação da Informação

N-SI-005: Proteção Contra Códigos Maliciosos

N-SI-006: E-mail e Comunicadores Instantâneos

N-SI-007: Gestão de Identidade

N-SI-008: Internet e Mídias Sociais

N-SI-009: Monitoramento

N-SI-010: Resposta a Incidentes

N-SI-011: Termo de Uso dos Sistemas Internos

N-SI-012: Uso Aceitável dos Ativos de Informação

N-SI-013: Termo de Confidencialidade

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – ACESSO REMOTO				
Tema:	Norma Geral - N-SI-002			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer diretrizes, requisitos e responsabilidades para a solicitação, concessão, uso e monitoramento do acesso remoto aos ativos de informação e recursos computacionais do DETRAN|ES, garantindo a confidencialidade, integridade e disponibilidade das informações, em conformidade com a Política de Gestão de Segurança da Informação (PGSI).

2. DO ESCOPO

Esta norma se aplica a todos os usuários (Servidores, Contratados, Conveniados e usuários) que necessitem de acesso remoto à rede interna do DETRAN|ES, utilizando tanto dispositivos corporativos quanto pessoais (BYOD), conforme o escopo definido na PGSI.

3. DAS DIRETRIZES

O acesso remoto será provido exclusivamente por meio de Conexão de Rede Privada Virtual (VPN), exigindo-se, obrigatoriamente, o uso de Autenticação Multifator (MFA) e de um certificado digital válido.

3.1. DA CONCESSÃO E USO DO ACESSO REMOTO

O acesso remoto é restrito a usuários que necessitem deste recurso para a execução de suas atividades profissionais, mediante justificativa formal aprovada pelo gestor direto.

A concessão do acesso somente será efetivada após a assinatura do "Termo de Responsabilidade de Uso - VPN", disponível no sistema E-Docs.

O acesso para servidores e colaboradores internos terá validade máxima de 1 (um) ano, sendo necessária uma revalidação formal pelo gestor direto ao final do período para sua manutenção.

O acesso para terceiros e prestadores de serviço será limitado ao tempo estritamente necessário para a atividade, não excedendo 60 (sessenta) dias, exigindo um novo processo de solicitação e aprovação para renovação.

O acesso remoto será concedido seguindo o Princípio do Menor Privilégio, garantindo acesso apenas aos recursos mínimos necessários para a execução das atividades laborais.

O usuário é o único e total responsável por toda e qualquer ação executada com suas credenciais de acesso, sendo expressamente proibido o compartilhamento de senhas, tokens de MFA ou certificados.

3.2. DOS REQUISITOS DE SEGURANÇA DO DISPOSITIVO DE ACESSO (ENDPOINT)

Os equipamentos utilizados para acesso remoto (notebooks, desktops, etc.) devem, obrigatoriamente, possuir:

a. Um sistema operacional original e com todas as atualizações de segurança mais recentes aplicadas.
b. Uma solução de proteção contra códigos maliciosos (antivírus/antimalware) ativa e atualizada.
c. Um firewall local ativo e devidamente configurado.
d. Criptografia de disco habilitada (ex: BitLocker ou FileVault), especialmente para dispositivos móveis como notebooks.

É expressamente proibido realizar o acesso remoto a partir de computadores de uso público ou compartilhado (ex: hotéis, cyber ou cafés) e através de redes Wi-Fi públicas não seguras.

3.3. DAS REGRAS DA CONEXÃO E TRATAMENTO DA INFROMAÇÃO

A configuração de split-tunneling na VPN é proibida e todo o tráfego de internet do dispositivo deverá ser roteado através da rede do DETRAN|ES durante a sessão de acesso remoto.

É vedado o armazenamento de informações classificadas como Confidenciais ou Restritas no disco local do dispositivo utilizado para o acesso remoto. Tais informações devem ser manipuladas exclusivamente dentro do ambiente da rede do DETRAN|ES.

A sessão de acesso remoto será automaticamente encerrada após um período predefinido de inatividade.

3.4. DO MONITORAMENTO E RESPOSTA A INCIDENTES

Toda atividade realizada e informações acessadas ou produzidas através do acesso remoto está sujeita a monitoramento e registro de logs para fins de auditoria e segurança, não havendo expectativa de privacidade.

O DETRAN|ES se reserva o direito de, sem aviso prévio, analisar o tráfego e, se necessário, bloquear conexões que apresentem comportamento suspeito ou malicioso.

Durante o monitoramento do acesso remoto a seus ativos/serviços de informação ou recursos computacionais, o DETRAN|ES se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

Em caso de perda, furto, roubo ou qualquer suspeita de comprometimento do dispositivo ou das credenciais de acesso, o usuário deverá notificar imediatamente o Gestor de Segurança da Informação para o bloqueio imediato do acesso.

3.5. DA CONCESSÃO E USO DO ACESSO REMOTO PARA TERCEIROS

O acesso remoto a ativos/serviços de informação e recursos computacionais do DETRAN|ES poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais;

Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:

I. O acesso remoto de terceiros e prestadores de serviço a ativos/serviços de informação ou recursos computacionais do DETRAN|ES somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes, que pode ser elaborada no sistema E-Docs através do modelo SGIS - Termo de Responsabilidade de Uso - VPN;

II. A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado a atividade do terceiro ou prestador de serviço, não excedendo ao máximo de 60 (sessenta) dias tendo de ser renovado após este prazo;

III. O usuário terceiro, bem como a empresa onde o mesmo trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais de acesso remoto;

IV. O acesso remoto de terceiros a ativos/serviços de informação e recursos computacionais do DETRAN|ES será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

V. Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do DETRAN|ES e firewall local ativo;

VI. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possam o acesso remoto ao ambiente do DETRAN|ES habilitado, o usuário responsável deverá informar imediatamente o ocorrido a equipe de segurança da informação.

VII.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade da GTI:

I. Analisar e aprovar tecnicamente as solicitações de acesso remoto, após validação do gestor do solicitante;
II. Gerenciar a infraestrutura de acesso remoto, garantindo a aplicação dos controles de segurança; e
III. Controlar, monitorar e auditar os acessos, tratando incidentes e reportando ao Comitê Interno de Segurança da Informação (CSI), quando pertinente.

4.2. DO GESTOR DIRETO DO USUÁRIO

I. Avaliar e aprovar a necessidade de negócio para a solicitação de acesso remoto de sua equipe; e
II. Realizar a revalidação periódica dos acessos de seus subordinados.

4.3. DO USUÁRIO

I. Cumprir todas as diretrizes desta norma e da PGSI;
II. Zelar pela segurança de suas credenciais e do dispositivo utilizado; e
III. Reportar imediatamente qualquer incidente de segurança.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação e aprovada pelo Comitê Interno de Segurança da Informação (CSI) em conjunto com a Diretoria do DETRAN|ES.

7. DO GLOSSÁRIO

MFA (Multi-Factor Authentication): Autenticação Multifator. Método de segurança que exige que o usuário forneça dois ou mais fatores de verificação para obter acesso a um recurso.

VPN (Virtual Private Network): Rede Privada Virtual. Tecnologia que cria uma conexão segura e criptografada sobre uma rede menos segura, como a internet, para acessar os recursos da rede interna do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – USO SEGURO DE DISPOSITIVOS PESSOAIS				
Tema:	Norma Geral - N-SI-003-BYOD			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação: IS-N nº 32/2025	Vigência: Na data da publicação	

1. DO PROPÓSITO

Estabelecer diretrizes, requisitos e responsabilidades para o uso de dispositivos computacionais pessoais (notebooks, tablets, smartphones) para acessar, processar ou armazenar informações corporativas do DETRAN|ES, equilibrando a flexibilidade para o usuário com a necessidade de proteger os ativos de informação da Autarquia.

2. DO ESCOPO

Esta norma se aplica a todos os usuários (Servidores, Contratados, Conveniados e usuários) que, mediante autorização, utilizem seus dispositivos pessoais para fins de trabalho, em conformidade com a Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

O uso de dispositivos pessoais para acessar recursos da rede interna ou manusear informações classificadas do DETRAN|ES é um privilégio, não um direito, e está condicionado ao cumprimento integral desta norma.

3.1. DAS CONDIÇÕES GERAIS E AUTORIZAÇÃO

A permissão para o uso de dispositivos pessoais é uma prerrogativa das diretorias do DETRAN|ES, mediante solicitação formal com justificativa e aprovação do gestor direto do usuário.

O usuário deverá assinar um "Termo de Responsabilidade para Uso de Dispositivo Pessoal (BYOD)", reconhecendo sua ciência e concordância com todas as regras aqui estabelecidas.

O DETRAN|ES não se responsabiliza por custos de aquisição, manutenção, licenciamento de software, planos de dados ou qualquer outro custo associado ao dispositivo pessoal.

As informações criadas ou manuseadas no exercício da função são de propriedade exclusiva do DETRAN|ES, independentemente do dispositivo utilizado.

3.2. DOS REQUISITOS MÍNIMOS DE SEGURANÇA DO DISPOSITIVO

Para ser autorizado, o dispositivo pessoal deve, obrigatoriamente, atender aos seguintes requisitos:

a. Possuir um mecanismo de bloqueio de tela (senha, PIN, padrão ou biometria) ativado;
b. Ter a criptografia de armazenamento de disco habilitada;
c. Manter o sistema operacional e os aplicativos (especialmente navegador e cliente de e-mail) sempre atualizados com as últimas correções de segurança;
d. Possuir uma solução de proteção contra códigos maliciosos (antivírus/antimalware) ativa e atualizada; e
e. Não possuir sistemas operacionais modificados (jailbreak/rooted).

O acesso a sistemas internos a partir de um dispositivo pessoal está condicionado à instalação de um software de Gerenciamento de Dispositivos Móveis (MDM) ou de Aplicações (MAM) fornecido pelo DETRAN|ES. Este software permitirá a aplicação de políticas de segurança e a remoção seletiva dos dados corporativos.

3.3. DAS REGRAS DE MANUSEIO DA INFORMAÇÃO

É expressamente proibido o armazenamento de informações classificadas como Confidenciais ou Restritas diretamente no armazenamento local do dispositivo pessoal.

Tais informações só poderão ser manuseadas e armazenadas dentro de um "container" seguro e criptografado, gerenciado pela solução de MDM/MAM do DETRAN|ES, que segrega os dados corporativos dos dados pessoais.

É vedada a sincronização ou o backup de dados corporativos em serviços de nuvem pessoais (ex.: iCloud, Google Drive ou Dropbox).

3.4. DOS INCIDENTES DE SEGURANÇA E PERDA DO DISPOSITIVO

Em caso de perda, furto, roubo ou qualquer suspeita de comprometimento do dispositivo pessoal, o usuário tem a obrigação de notificar imediatamente o Gestor de Segurança da Informação.

A notificação imediata é crucial para que a equipe de GTI possa acionar o procedimento de remoção remota (remote wipe) de todos os dados e acessos corporativos contidos no dispositivo, a fim de prevenir vazamentos de informação.

3.5. DO PROCESSO DE DESLIGAMENTO (OFFBOARDING)

Quando o vínculo do usuário com o DETRAN|ES for encerrado, o acesso do dispositivo pessoal será revogado e todos os dados corporativos serão remotamente apagados através da solução de MDM/MAM, como parte do procedimento padrão de desligamento

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade da GTI:

I. Gerenciar a solução de MDM/MAM;
II. Validar tecnicamente as solicitações de uso de BYOD; e
III. Executar os procedimentos de remoção remota de dados em caso de incidentes ou desligamento.

4.2. DO GESTOR DIRETO DO USUÁRIO

I. Avaliar e aprovar a necessidade de negócio para o uso de dispositivo pessoal por sua equipe; e
II. Realizar a revalidação periódica dos acessos de seus subordinados.

4.3. DO USUÁRIO

I. Cumprir todas as diretrizes desta norma e da PGSI;
II. Garantir que seu dispositivo atenda aos requisitos mínimos de segurança; e
III. Reportar imediatamente qualquer incidente de segurança.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação e aprovada pelo Comitê Interno de Segurança da Informação (CSI).

7. DO GLOSSÁRIO

BYOD (Bring Your Own Device): Prática de permitir que os usuários utilizem seus próprios dispositivos pessoais para fins de trabalho.

MDM (Mobile Device Management): Software que permite à organização gerenciar e aplicar políticas de segurança em todo o dispositivo móvel.

MAM (Mobile Application Management): Software que permite gerenciar e proteger apenas as aplicações corporativas e seus dados, sem controlar o dispositivo pessoal como um todo.

Container: Um espaço de trabalho seguro e criptografado no dispositivo que isola os dados e aplicativos corporativos dos pessoais.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – CLASSIFICAÇÃO DA INFORMAÇÃO				
Tema:	Norma Geral - N-SI-004			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação: IS-N nº 32/2025	Vigência: Na data da publicação	

1. DO PROPÓSITO

Estabelecer um sistema padronizado para a classificação dos ativos de informação do DETRAN|ES, definindo os níveis de sensibilidade e as diretrizes obrigatórias para o seu correto manuseio, armazenamento, transmissão e descarte, a fim de garantir que os controles de segurança sejam aplicados de forma proporcional ao valor e à criticidade de cada informação.

2. DO ESCOPO

Esta norma se aplica a todas as informações produzidas, recebidas, processadas ou armazenadas pelo DETRAN|ES, em qualquer formato (digital, impresso ou verbal), e a todos os usuários (Servidores, Contratados, Conveniados e usuários) que tenham acesso a esses ativos, em conformidade com a Política de Gestão de Segurança da Informação (PGSI)

3. DAS DIRETRIZES

3.1. DOS NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação sob a responsabilidade do DETRAN|ES deve ser classificada em um dos quatro níveis definidos no Art. 12 da PGSI, conforme a tabela abaixo:

Nível de Classificação	Definição	Exemplos no Contexto do DETRAN-ES	Requisitos Mínimos de Proteção
Público	Informação que pode ser acessada por qualquer pessoa, sem restrições.	Estatísticas de frota, legislação de trânsito, informações institucionais do site.	Controle de integridade para garantir que não seja alterada indevidamente.
Interno	Informação de uso exclusivo dos colaboradores do DETRAN-ES, cuja divulgação não causa dano direto.	Manuais de procedimento, comunicações internas não sensíveis, relatórios de gestão.	Acesso restrito à rede interna e a usuários autenticados.
Confidencial	Informação cujo acesso não autorizado pode causar dano significativo ao órgão, aos cidadãos ou ao Estado.	Bases de dados RENACH e RENAVAM, dados pessoais de condutores e proprietários, processos administrativos sigilosos.	Criptografia em repouso e em trânsito; controle de acesso baseado em função; registro detalhado de logs de acesso; segregação de redes.
Restrito	Informação altamente sensível, com acesso limitado a um grupo específico de pessoas.	Dados biométricos, laudos médicos e psicológicos, senhas de administração de sistemas críticos.	Todos os controles do nível Confidencial, mais autenticação multifator (MFA) obrigatória e monitoramento proativo de acesso.

3.2. DOS PAPEIS E RESPONSABILIDADES NA CLASSIFICAÇÃO

Proprietário da Informação: É o gestor da área de negócio responsável pela geração e manutenção da informação. Compete a ele:

I. Atribuir a classificação inicial a toda nova informação gerada em sua área;
II. Revisar periodicamente (no mínimo, anualmente) a classificação dos ativos sob sua responsabilidade; e
III. Autorizar o acesso à informação, seguindo o princípio do menor privilégio.

Custodiante da Informação: É a área responsável pela infraestrutura onde a informação é armazenada e processada. Compete a ela implementar e manter os controles de segurança técnicos adequados ao nível de classificação definido pelo Proprietário.

Usuário: indivíduo que tem credenciais (login e senha) para acessar e interagir com os sistemas informáticos ou redes do DETRAN|ES Compete a ele manusear a informação de acordo com sua classificação e as diretrizes desta norma.

3.3. DA ROTULAGEM DA INFORMAÇÃO

Toda informação classificada como Interna, Confidencial ou Restrita deve ser devidamente rotulada para indicar seu nível de sigilo.

Documentos Digitais: Devem conter o rótulo de classificação (ex: "USO INTERNO", "CONFIDENCIAL") no cabeçalho e/ou rodapé de todas as páginas.

E-mails: Mensagens que contenham informações sensíveis devem incluir o rótulo de classificação no início do campo "Assunto".

Documentos Físicos: Devem ser marcados com carimbos ou etiquetas indicando a classificação em local visível.

3.4. DAS DIRETRIZES DE MANUSEIO POR CLASSIFICAÇÃO

O manuseio de informações deve seguir estritamente as regras definidas na tabela abaixo:

Classificação	Armazenamento	Transmissão / Compartilhamento	Impressão	Descarte
Público	Sem restrições.	Sem restrições.	Permitida.	Lixo comum.
Interno	Em repositórios de rede corporativos (não em desktops locais ou dispositivos pessoais).	Permitido apenas para e-mails internos do DETRAN.	ES. Proibido o envio para e-mails pessoais ou serviços de nuvem públicos.	Permitida, com o devido cuidado para não deixar documentos desacompanhados.
Confidencial	Em servidores com controle de acesso restrito e logs de auditoria. Criptografia de disco obrigatória em notebooks.	Transmissão externa apenas quando estritamente necessário, utilizando criptografia de ponta a ponta (e-mail criptografado, portal seguro).	Deve ser evitada. Se necessária, o documento deve ser recolhido da impressora imediatamente e manuseado com sigilo.	Fragmentação em partículas (corte cruzado) ou incineração. Mídias digitais devem ser destruídas fisicamente ou ter os dados apagados de forma segura (wiping).
Restrito	Em ambientes de alta segurança, com segregação de rede e monitoramento proativo de acesso.	Transmissão externa proibida, exceto em casos excepcionais com autorização da Diretoria e uso de canais de comunicação dedicados e criptografados.	Proibida, exceto em situações de extrema necessidade, com autorização formal do Proprietário da Informação e registro do ato.	Mesmos controles do nível Confidencial, com a adição de um registro formal de destruição (log de descarte).

3.5. DA REVISÃO E DESCARTE DA INFORMAÇÃO

O Proprietário da Informação deve reavaliar a classificação de seus ativos de informação anualmente para garantir que ela permaneça adequada.

O descarte de informações deve seguir os prazos definidos na Tabela de Temporalidade de Documentos do DETRAN|ES e os procedimentos de destruição segura detalhados na tabela anterior.

4. DAS SANÇÕES E PUNIÇÕES

O manuseio inadequado de informações classificadas, em desacordo com esta norma, será considerado um incidente de segurança e sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

5. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pela Direção Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

ANEXO I – MODELOS PARA ROTULAGEM DE INFORMAÇÕES

Os padrões a seguir representam os rótulos aprovados que devem ser exibidos nos cabeçalhos e rodapés de documentos de acordo com seu nível de classificação.

Observação: A cor, fonte e tamanho do texto podem ser ajustados para adequação a informação rotulada, desde que mantida a clareza e objetividade da informação

1.1. Cabeçalho

Nível	Rótulo
Informação Pública (Rotulagem opcional)	P *Informação Pública* *Public Information*
Informação Interna	I *Informação Interna* *Internal Information*
Informação Confidencial	C *Informação Confidencial* *Confidential Information*

Tabela 1. Cabeçalho.

Exemplo:

DETRAN | ES

P

Informação Pública

Public Information

1.2. Rodapé

www.detran.es.gov.br

Av. Fernando Ferrari, 1080, Torre Sul do Edifício América, 7°andar, Mata da Praia, Vitória, ES. CEP: 29066-380

Exemplo:

www.detran.es.gov.br

Av. Fernando Ferrari, 1080, Torre Sul do Edifício América, 7°andar, Mata da Praia, Vitória, ES. CEP: 29066-380

ANEXO II – TABELA AÇÃO X CLASSIFICAÇÃO

AÇÃO	CLASSIFICAÇÃO		
	Pública	Interna	Restrita / Confidencial
Cópia / Exclusão	Sem restrições	Sem restrições	Permissão do gestor da informação
Envio por Fax	Sem restrições	Usar folha de rosto padronizada	Usar folha de rosto padronizada
Transmissão em rede pública	Permitido	Permitido	Recomendável comunicação criptografada.
Descarte	Lixo comum	Lixo comum. Recomendável uso de fragmentadora.	Utilizar métodos aprovados conforme anexo desta norma.
Envio a terceiros	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação e termo de confidencialidade assinado pelo terceiro.
Solicitação de direitos de acesso	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação
Correio interno e externo	Envelope comum	Envelope comum	Envio para destinatário específico identificado apenas dentro do envelope.
Rotulagem	Opcional	Na capa e em todas as páginas	Na capa e em todas as páginas.
Registro de Acompanhamento	Opcional	Opcional	Destinatários, cópias efetuadas, localização e endereço de todos que acessaram e destruição.

ANEXO III – MÉTODOS DE DESCARTE PARA INFORMAÇÕES ARMAZENADAS ELETRONICAMENTE

Os métodos a seguir foram selecionados como forma segura de garantir o descarte de informações do Departamento Estadual de Trânsito.

Para todos os métodos que envolvem atividades técnicas, os usuários deverão encaminhar a solicitação para a área de tecnologia da informação.

Método	Descrição	Aplicável a
Sobregravar mídia	Sobregravar dados em mídias de armazenamento magnético com informações não sensíveis por pelo menos 07 vezes. Essa tarefa pode ser executada com o auxílio de software/hardware especializado. Este método não destrói fisicamente a mídia, entretanto destrói todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis, CDR, DVDR e similares;
Destruição física	Destruição física da mídia de armazenamento com o uso de picotadores especializados, pulverizadores ou incineradores. Este método destrói completamente a mídia e todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis. CD, CDR, DVD, DVDR. Este método também é valido para material em suporte físico como impressos e similares;
Desmagnetização	Desmagnetização de mídias como fitas e disquetes. Este método destrói todos os dados.	Fitas e disquetes.
Criptografia de caminho único (One-Way)	Uso de um hash do tipo one-way para criptografar a informação de forma irrecuperável, mesmo que de posse da chave de criptografia. Recomenda-se o uso do hash SHA256. Este método não afeta a mídia e pode ser usado para o descarte seletivo de informações.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis, CDR, DVDR e similares;

PSI – PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS				
Tema:	Norma Geral - N-SI-005			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação: IS-N nº 32/2025	Vigência: Na data da publicação	

1. DO PROPÓSITO

Estabelecer diretrizes, responsabilidades e controles para a proteção dos ativos de informação do DETRAN|ES contra ameaças de códigos maliciosos (malware), como vírus, ransomware, spyware, cavalos de Troia e outros, visando minimizar os riscos de interrupção dos serviços, perdas financeiras e vazamento de dados.

2. DO ESCOPO

Esta norma se aplica a todos os ativos de processamento de informação (estações de trabalho, servidores, notebooks, dispositivos móveis) e a todos os usuários (Servidores, Contratados, Conveniados e usuários) no escopo definido na Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

3.1. ESTRATÉGIA DE PROTEÇÃO DE ENDPOINTS EM CAMADAS

O DETRAN|ES implementará e manterá uma solução de Plataforma de Proteção de Endpoints (EPP - Endpoint Protection Platform) em todos os seus ativos computacionais, incluindo estações de trabalho e servidores.

A solução de EPP deverá, no mínimo, incluir:

a. Antivírus de Nova Geração (NGAV): Utilizando análise comportamental, inteligência artificial e machine learning para detectar e bloquear malwares conhecidos e desconhecidos (dia-zero).
b. Firewall Local: Para controlar o tráfego de rede de entrada e saída do dispositivo.
c. Controle de Dispositivos: Para gerenciar o uso de mídias removíveis (pen drives, HDs externos).

Para servidores e ativos críticos, será implementada uma solução de Detecção e Resposta de Endpoint (EDR - Endpoint Detection and Response) para monitoramento contínuo e resposta rápida a ameaças avançadas.

Apenas as ferramentas homologadas e gerenciadas pela GTI poderão ser utilizadas. É vedada a instalação de outras soluções de segurança pelos usuários

O acesso remoto é restrito a usuários que necessitem deste recurso para a execução de

3.2. SEGURANÇA DE E-MAIL E NAVEGAÇÃO WEB

Todo o tráfego de e-mail do DETRAN|ES será processado por um Gateway de E-mail Seguro, que deverá prover:

a. Filtros avançados contra spam e phishing.
b. Análise de anexos em ambiente seguro e isolado (sandboxing) para detectar malwares antes da entrega.
c. Proteção contra links maliciosos (URL Rewriting/Time-of-Click Protection).

Todo o acesso à internet a partir da rede corporativa passará por um Filtro de Conteúdo Web (Proxy Seguro) para bloquear o acesso a sites maliciosos, fraudulentos ou que não estejam em conformidade com as políticas do DETRAN|ES.

3.3. DAS RESPONSABILIDADES E PREVENÇÃO PARA OS USUÁRIOS

A tecnologia é a primeira linha de defesa, mas o comportamento seguro do usuário é fundamental. Todos os usuários devem:

a. Reportar imediatamente ao Gestor de Segurança da Informação qualquer atividade suspeita, e-mail de phishing, ou suspeita de infecção em seu dispositivo;
b. Não tentar remover ou tratar códigos maliciosos por iniciativa própria. Em caso de suspeita, o dispositivo deve ser desconectado da rede (cabo ou Wi-Fi) e o chamado deve ser aberto imediatamente;
c. Ter extrema cautela com e-mails não solicitados, especialmente aqueles que contenham links ou anexos. Verificar sempre o remetente e, na dúvida, não clicar e reportar;
d. Não desativar ou contornar os controles de segurança implementados pelo DETRAN|ES;
e. Não desenvolver, testar ou armazenar qualquer tipo de código malicioso, a menos que expressamente autorizado em um ambiente de pesquisa isolado e controlado; E
f. Participar ativamente dos treinamentos e campanhas de conscientização em segurança da informação promovidos pelo DETRAN|ES.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

a. Definir a estratégia de proteção contra códigos maliciosos, em alinhamento com a PGSI;

b. Coordenar a resposta a incidentes de segurança relacionados a malware, em conjunto com a GTI; E

c. Promover a cultura de segurança e o programa de conscientização contínua para os usuários

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

a. Implementar, gerenciar e manter as ferramentas de proteção (EPP, EDR, Gateway de E-mail, Filtro Web) em todos os ativos;

b. Garantir que as ferramentas estejam sempre atualizadas e configuradas conforme as diretrizes do Gestor de SI; E

c. Atuar tecnicamente na contenção e erradicação de malwares durante um incidente, sob a coordenação do Gestor de SI.

4.3. DO USUÁRIO

a. Cumprir todas as diretrizes desta norma e da PGSI; e

b. Agir como a primeira linha de vigilância, reportando qualquer atividade suspeita.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pela Direção Geral do DETRAN|ES.

7. DO GLOSSÁRIO

Ameaças: Os ataques a computadores são ações praticadas por softwares projetados com intenções danosas. As consequências são bastante variadas, algumas têm como instrução infectar ou invadir computadores alheios para, em seguida, danificar seus componentes de hardware ou software, através da exclusão de arquivos, alterando o funcionamento da máquina ou até mesmo deixando o computador vulnerável a outros tipos de ataques. Porém existem os que visam os dados do usuário, com a captura de informações sigilosas (senhas e números de cartões de créditos entre outros), além da captura de informações de caráter íntimo.)

Cavalo de Tróia: Qualquer malware que objetiva enganar os usuários sobre sua verdadeira intenção.

Códigos Maliciosos: São códigos de computador ou scripts da Web nocivos, que tem como objetivo criar vulnerabilidades no sistema.

Macros: Uma macro é uma série de comandos que podem ser usados para automatizar uma tarefa repetida e que podem ser executados durante a tarefa.

Malware: Termo genérico para qualquer tipo software malicioso projetado para se infiltrar no seu dispositivo sem o seu conhecimento.

Phishing: É uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito. São comunicações falsificadas que parecem vir de uma fonte confiável.

Ransomware: Tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

Script: Em Informática, script é um conjunto de instruções em código, ou seja, escritas em linguagem de computador.

Vírus: Software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

Worms: Programa semelhante aos vírus, com a diferença de este ser autorreplicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS				
Tema:	Norma Geral - N-SI-006			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação: IS-N nº 32/2025	Vigência: Na data da publicação	

1. DO PROPÓSITO

Estabelecer diretrizes para a utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pelo DETRAN|ES, visando garantir o uso profissional das ferramentas, proteger os ativos de informação contra ameaças externas e internas, e assegurar a conformidade com a Política de Gestão de Segurança da Informação (PGSI).

2. DO ESCOPO

Esta norma se aplica a todos os usuários (Servidores, Contratados, Conveniados e outros Usuários) que utilizam as contas de e-mail e as ferramentas de comunicação instantânea corporativas do DETRAN|ES

3. DAS DIRETRIZES

3.1. DO USO ACEITÁVEL E RESPONSABILIDADES GERAIS

Os serviços de e-mail e comunicadores instantâneos são fornecidos pelo DETRAN|ES exclusivamente para o desempenho de atividades profissionais.

É vedado o uso de qualquer serviço de e-mail ou comunicador instantâneo que não seja o oficialmente fornecido e homologado pelo DETRAN|ES para tratar de assuntos de trabalho.

O usuário é o responsável direto por toda e qualquer comunicação enviada a partir de suas contas corporativas.

É expressamente proibido utilizar as ferramentas de comunicação para:

I. Fins pessoais, comerciais, político-partidários ou que não sejam de interesse do DETRAN|ES.
II. Criar, armazenar ou disseminar conteúdo ilegal, ofensivo, discriminatório, calunioso ou que infrinja a legislação vigente.
III. Falsificar a identidade de outro remetente (spoofing).
IV. Enviar mensagens em massa não solicitadas (spam).

3.2. DA SEGURANÇA DO SERVIÇO DE E-MAIL

Para proteger seus usuários e ativos, o DETRAN|ES implementa um Gateway de E-mail Seguro que realiza, entre outras, as seguintes ações:

I. Filtragem de spam e e-mails com conteúdo malicioso;
II. Análise de anexos em ambiente seguro (sandboxing) para identificar ameaças; e
III. Verificação de links (URLs) para bloquear o acesso a sites de phishing e fraudulentos.

Todo usuário tem a responsabilidade de reportar imediatamente ao Gestor de Segurança da Informação qualquer e-mail suspeito de ser phishing ou conter ameaças,

encaminhando a mensagem como anexo e sem clicar em nenhum link ou baixar arquivos.

É proibido o envio de informações classificadas como Interno, Confidencial ou Restrito para endereços de e-mail externos, exceto quando houver necessidade de negócio e autorização expressa do Proprietário da Informação.

Toda transmissão autorizada de informações classificadas como Confidencial ou Restrito para destinatários externos deve, obrigatoriamente, ser realizada com o uso de criptografia de ponta a ponta ou através de um portal seguro de transferência de arquivos fornecido pelo DETRAN|ES.

3.3. DOS PADRÕES DE ENDEREÇO E ASSINATURA

Os endereços de e-mail seguirão o padrão nome.últimosobrenome@detran.es.gov.br, com exceções gerenciadas pela GTI, para evitar ambiguidades ou situações vexatórias.

Todos os usuários devem configurar a assinatura padrão institucional, seguida do aviso de confidencialidade: “Esta mensagem, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar, copiar o seu conteúdo.”.

Os usuários do serviço de e-mail do DETRAN|ES devem adotar a assinatura padrão, formatada de acordo com o seguinte modelo:

Nome Completo; Departamento; Cargo ; e Telefone

3.4. DA SEGURANÇA DOS COMUNICADORES INSTANTÂNEOS

Apenas a ferramenta de comunicação instantânea homologada, fornecida ou de uso autorizado pelo DETRAN|ES deve ser utilizada para comunicações de trabalho.

É expressamente proibido discutir ou compartilhar qualquer informação classificada (Interno, Confidencial ou Restrito) através de aplicativos de mensagens pessoais ou não oficiais (ex.: WhatsApp, Telegram, etc.).

3.5. DO MONITORAMENTO, RETENÇÃO E PRIVACIDADE

Todas as comunicações realizadas através das ferramentas corporativas do DETRAN|ES estão sujeitas a monitoramento, registro e auditoria para fins de segurança e conformidade, não havendo expectativa de privacidade.

As mensagens de e-mail e de comunicadores instantâneos são consideradas registros oficiais do DETRAN|ES e estão sujeitas às políticas de retenção e arquivamento de dados da Autarquia, conforme a Tabela de Temporalidade de Documentos.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DA SEGURANÇA DA INFORMAÇÃO

I. Definir e revisar esta norma;
II. Coordenar a resposta a incidentes de segurança relacionados a e-mail e comunicadores; e
III. Promover a conscientização sobre os riscos de phishing e uso seguro das ferramentas.

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Implementar e gerenciar as ferramentas de comunicação e os controles técnicos de segurança (Gateway de E-mail, etc.); e
II. Gerenciar a criação e exclusão de contas de usuários.

4.3. DA SUBGERENCIA DE INFRAESTRUTURA E SEGURANÇA DE TI

I. Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pelo DETRAN|ES; e
II. Reportar eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao uso dos serviços de e-mail e comunicadores instantâneos para a equipe de segurança da informação

4.3. DOS USUÁRIOS

I. Cumprir todas as diretrizes desta norma e da PGSI;
II. Reportar imediatamente qualquer incidente de segurança.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

7. DO GLOSSÁRIO

Criptografia de E-mail: Processo de codificar o conteúdo de uma mensagem de e-mail para protegê-la de ser lida por pessoas não autorizadas.
Phishing: Tentativa fraudulenta de obter informações sensíveis (como credenciais de acesso) disfarçando-se como uma entidade confiável em uma comunicação eletrônica.
Sandboxing (Análise em Ambiente Seguro): Técnica de segurança que executa arquivos e links suspeitos em um ambiente virtual isolado para verificar se são maliciosos antes de permitir seu acesso pelo usuário.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – GESTÃO DE IDENTIDADE E ACESSOS				
Tema:	Norma Geral - N-SI-007			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer diretrizes, responsabilidades e procedimentos para a gestão do ciclo de vida das identidades e do controle de acesso aos ativos e sistemas de informação do DETRAN|ES, garantindo que apenas usuários autorizados acessem as informações necessárias para suas funções, em conformidade com o Princípio do Menor Privilégio.

2. DO ESCOPO

Esta norma se aplica a todas as formas de acesso lógico aos recursos de tecnologia da informação do DETRAN|ES e a todos os usuários (Servidores, Contratados, Conveniados e outros Usuários), conforme o escopo definido na Política de Gestão de Segurança da Informação (PGSI) e na N-SI-011.

3. DAS DIRETRIZES

3.1. DO PRINCÍPIOS GERAIS DE ACESSO

Toda conta de acesso é pessoal, intransferível e de responsabilidade exclusiva do usuário, que responderá por todas as atividades nela realizadas.

O acesso aos ativos de informação será concedido com base no Princípio do Menor Privilégio, ou seja, cada usuário terá apenas as permissões estritamente necessárias para o desempenho de suas atribuições.

Usuários com acesso a privilégios administrativos devem possuir uma credencial específica para este propósito, que será utilizada somente para a execução de atividades administrativas. Para as atividades rotineiras, deverá ser utilizada a conta de acesso comum.

3.2. DA AUTENTICAÇÃO

A Autenticação Multifator (MFA) será obrigatória para:

I. Todo e qualquer acesso remoto à rede do DETRAN|ES (VPN).
II. O acesso a sistemas que processem ou armazenem informações classificadas como Confidenciais ou Restritas.
III. Todas as contas com privilégios administrativos.

É dever do usuário zelar pela guarda e sigilo de todos os seus fatores de autenticação (senhas, tokens, celulares cadastrados, etc.).

3.3. DA POLÍTICA DE SENHAS

As senhas são um componente do processo de autenticação e devem seguir os seguintes padrões:

I. Validade: 90 (noventa) dias, com troca obrigatória ao final do período;
II. Complexidade (Contas Não-Administrativas): Mínimo de 08 (oito) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais; e
III. Complexidade (Contas Administrativas): Mínimo de 15 (quinze) caracteres, com a mesma combinação de complexidade.
IV. Deverá ser impedia a reutilização das senhas dos últimos 12 meses.

A conta deverá ser bloqueada, por no mínimo 30 (trinta) minutos, após 05 (cinco) tentativas de acesso com senha inválida.

É vedada a criação de senhas que utilizem informações pessoais óbvias (nomes, datas, placas de veículo) ou sequências lógicas

3.4. DO CICLO DE VIDA DOS ACESSOS

A liberação e manutenção dos acessos aos sistemas informáticos do DETRAN|ES estão definidos na N-SI-011, desta PSI.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DA GERÊNCIA DE RECURSOS HUMANOS

I. Ser o gatilho oficial para os processos de criação e revogação de acessos de servidores e estagiários, comunicando admissões, realocações e desligamentos à GTI.

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Implementar e gerenciar tecnicamente a criação, alteração e revogação dos acessos, conforme solicitado e autorizado;
II. Administrar as ferramentas de controle de acesso e autenticação; E
III. Apoiar o processo de revisão periódica, fornecendo os relatórios de acessos vigentes.

4.3. DOS USUÁRIOS

I. Comunicar à chefia imediata o seu desligamento ou realocação;
II. Suspender, imediatamente, a utilização de acessos ativos, quando de sua movimentação ou desligamento do DETRAN|ES.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – INTERNET E MÍDIAS SOCIAIS				
Tema:	Norma Geral - N-SI-008			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer diretrizes para a utilização segura e profissional do acesso à internet fornecido pelo DETRAN|ES e orientar o comportamento de seus colaboradores em mídias e redes sociais, visando proteger os ativos de informação, a produtividade e a reputação da Autarquia.

2. DO ESCOPO

Esta norma se aplica a todos os usuários (Servidores, Contratados, Conveniados e outros Usuários) que utilizam a infraestrutura de rede do DETRAN|ES para acessar a internet ou que interagem em mídias sociais, seja em canais oficiais ou pessoais, conforme o escopo definido na Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

3.1. DO ACESSO À INTERNET

O acesso à internet fornecido pelo DETRAN|ES é um recurso de trabalho e deve ser utilizado prioritariamente para o desempenho de atividades profissionais.

Para garantir a segurança da rede e a produtividade, todo o tráfego de internet é gerenciado por uma solução de Filtro de Conteúdo Web (Proxy Seguro). Esta ferramenta bloqueia o acesso a sites e categorias de conteúdo que:

I. Representem ameaças à segurança (malware, phishing, etc.).
II. Contenham conteúdo ilegal ou impróprio.
III. Violem as diretrizes de uso aceitável desta norma.

Toda a atividade de navegação na internet está sujeita a monitoramento, acompanhamento e registro de logs para fins de segurança e auditoria, não havendo expectativa de privacidade.

É expressamente proibido o uso da internet do DETRAN|ES para acessar, baixar, armazenar ou distribuir qualquer conteúdo relacionado a:

I. Pornografia, exploração sexual ou conteúdo adulto.
II. Ameaças, assédio, calúnia, difamação ou qualquer forma de discurso de ódio e preconceito.
III. Incitação a crimes, violência ou ao consumo de substâncias ilícitas.
IV. Atividades político-partidárias ou comerciais não relacionadas às atividades do DETRAN|ES.
V. Violação de direitos autorais ou de propriedade intelectual.
VI. Disseminação de códigos maliciosos ou tentativas de contornar os controles de segurança da rede.

É estritamente proibido realizar o upload de qualquer informação classificada como Interna, Confidencial ou Restrita, conforme a N-SI-004, para sites de terceiros, serviços de nuvem pessoais ou qualquer outra plataforma web não homologada pelo DETRAN|ES.

3.2. DO USO DE MÍDIAS E REDES SOCIAIS

Apenas os setores e usuários formalmente designados pela Assessoria de Comunicação podem publicar conteúdo em nome do DETRAN|ES em seus canais oficiais.

Toda publicação oficial deve seguir as diretrizes da política de comunicação institucional.

Ao utilizar mídias sociais em caráter pessoal, todos os usuários devem observar as seguintes regras:

I. É vedado falar em nome do DETRAN|ES, criar perfis ou grupos que utilizem a marca da Autarquia, ou usar sua identidade visual sem autorização expressa.
II. É proibida a publicação de qualquer informação classificada, imagens do ambiente interno de trabalho, ou detalhes sobre processos e colegas que não sejam de conhecimento público.
III. Os usuários que se identificam publicamente como colaboradores do DETRAN|ES em seus perfis pessoais devem zelar pela imagem da Autarquia, mantendo uma conduta profissional e evitando a publicação de conteúdos que possam gerar conflito de interesses ou dano à reputação do órgão.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

I. Definir e revisar, em conjunto com as áreas de Comunicação, Jurídico e RH, as categorias de conteúdo a serem filtradas pela solução de segurança web.
II. Promover a conscientização sobre o uso seguro da internet e das mídias sociais

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Implementar, gerenciar e manter a ferramenta de Filtro de Conteúdo Web.

II. Monitorar o tráfego de rede para identificar e responder a incidentes de segurança..

4.3. DOS USUÁRIOS

I. Cumprir integralmente as diretrizes desta norma.

II. b. Utilizar os recursos de internet de forma responsável e profissional.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – MONITORAMENTO				
Tema:	Norma Geral - N-SI-009			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer diretrizes para o monitoramento contínuo dos ativos de informação e recursos computacionais do DETRAN|ES, com o objetivo de detectar, analisar e permitir a resposta a incidentes de segurança, garantir a conformidade com as políticas internas e a legislação vigente, e produzir evidências para auditorias e investigações.

2. DO ESCOPO

Esta norma se aplica a todos os ativos de informação, sistemas, serviços e recursos computacionais do DETRAN|ES, bem como a todos os usuários (Servidores, Contratados, Conveniados e outros Usuários), conforme o escopo definido na Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

3.1. DOS PRINCÍPIOS DO MONITORAMENTO

Qualquer ativo de informação ou recurso computacional do DETRAN|ES, bem como qualquer outro recurso com acesso aos mesmos, poderá ser monitorado a qualquer momento.

Não há expectativa de privacidade na utilização dos ativos de informação ou recursos computacionais do DETRAN|ES, incluindo a utilização da conta de e-mail corporativa, comunicadores instantâneos e navegação na internet.

Todas as informações trafegadas ou armazenadas nos recursos do DETRAN|ES podem ser interceptadas, gravadas, lidas, copiadas e divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações e resposta a incidentes, em conformidade com a legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD).

3.2. DA GESTÃO DE LOGS DE AUDITORIA

O DETRAN|ES manterá registros (logs) de eventos relevantes para a segurança da informação, incluindo acessos de usuários, atividades de administradores, falhas de autenticação e eventos de sistema.

Os logs de auditoria de sistemas críticos deverão ser centralizados em um repositório seguro para facilitar a correlação e análise de eventos.

Os logs de auditoria deverão ser protegidos contra acesso não autorizado e modificações indevidas.

Os logs de auditoria serão retidos por um período mínimo definido pela GTI em conjunto com o Gestor de Segurança da Informação, a fim de suportar investigações de incidentes e requisitos de conformidade.

3.3. DO MONITORAMENTO DO AMBIENTE FÍSICO

O DETRAN|ES realiza o monitoramento de seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências.

A filmagem tem por objetivo assegurar a segurança física e patrimonial do DETRAN|ES e as câmeras de filmagem deverão estar dispostas de forma a resguardar a dignidade humana, sendo vedada a sua instalação em banheiros e áreas de atendimento médico.

As imagens captadas são de caráter estritamente confidencial e somente poderão ser divulgadas em caso de infração às regras ou à legislação vigente.

É proibido o uso de qualquer dispositivo de gravação audiovisual dentro do perímetro físico do DETRAN|ES, exceto quando formalmente autorizado.

3.4. DO AVISO LEGAL

Um aviso legal será exibido antes de permitir o acesso a ativos de informação ou recursos computacionais do DETRAN|ES, informando sobre o monitoramento e a ausência de expectativa de privacidade.

O texto do aviso será: “Este é um ativo/serviço de informação ou recurso computacional do DETRAN|ES, o qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste sistema, o infrator estará sujeito às sanções cabíveis nas esferas administrativa, cível e penal. Este recurso é monitorado, não havendo expectativa de privacidade na sua utilização. O acesso ou uso deste recurso constitui seu consentimento irrestrito aos termos aqui expostos.”

O acesso a qualquer recurso do DETRAN|ES caracteriza o consentimento irrestrito aos termos do aviso legal.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

I. Definir a estratégia de monitoramento e gestão de logs, alinhada à gestão de riscos;
II. Analisar os dados e logs coletados para identificar padrões, anomalias e possíveis incidentes de segurança; e
III. Coordenar a resposta a incidentes identificados através do monitoramento.

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Implementar, operar e manter as ferramentas e a infraestrutura de monitoramento e centralização de logs;
II. Garantir a integridade e a disponibilidade dos logs de auditoria; E
III. Apoiar o Gestor de Segurança da Informação na investigação técnica de incidentes.

4.3. DOS USUÁRIOS

I. Ter ciência de que suas atividades nos recursos corporativos são monitoradas; e
II. Reportar qualquer atividade suspeita ou incidente de segurança, conforme a PGSI.

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO				
Tema:	Norma Geral - N-SI-010			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer um processo estruturado e sistemático para a gestão de incidentes de segurança da informação, definindo as diretrizes para uma resposta rápida e eficaz, visando minimizar os impactos operacionais, financeiros e reputacionais ao DETRAN|ES, proteger os dados dos cidadãos e garantir o cumprimento das obrigações legais de notificação.

2. DO ESCOPO

Esta norma se aplica a todos os incidentes de segurança da informação, confirmados ou suspeitos, que afetem os ativos, serviços ou recursos computacionais do DETRAN|ES, e envolve todos os usuários, conforme o escopo da Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

3.1. DA DEFINIÇÃO E CLASSIFICAÇÃO DE INCIDENTES

Um incidente de segurança da informação é qualquer evento adverso que tenha impacto negativo, ou potencial para tal, sobre a confidencialidade, integridade ou disponibilidade dos ativos de informação do DETRAN|ES.

Todos os incidentes reportados serão classificados pelo Gestor de Segurança da Informação com base em seu impacto potencial, conforme a matriz abaixo, para determinar a urgência e a escala da resposta:

Nível	Descrição	Gatilho de Resposta
Baixo	Impacto localizado em um único usuário ou sistema não crítico. Sem exposição de dados sensíveis.	Tratamento pela GTI sob coordenação do Gestor de SI.
Médio	Interrupção de um serviço para um setor. Risco de exposição de dados internos.	Ativação da Equipe de Resposta a Incidentes (ERISI).
Alto	Interrupção de um serviço essencial. Exposição de dados pessoais de um grupo de cidadãos.	Ativação da ERISI e comunicação ao Comitê Interno de SI (CSI).
Crítico	Paralisação de serviços críticos. Vazamento massivo de dados pessoais ou sensíveis. Dano reputacional iminente.	Ativação da ERISI e convocação de reunião emergencial do CSI e da Diretoria.

3.2. DAS FASES DO PROCESSO DE RESPOSTA A INCIDENTES

O tratamento de incidentes seguirá a metodologia padrão recomendada por frameworks de cibersegurança (NIST e ISO/IEC 27035) e disporá de um ciclo de vida estruturado em seis fases:

I. **Fase 1**: Preparação: Manter esta norma atualizada, prover ferramentas adequadas para a equipe de resposta e realizar treinamentos e simulações periódicas.

II. **Fase 2**: Detecção e Análise:

Reporte: Todo e qualquer incidente ou suspeita de incidente deve ser imediatamente comunicado ao Gestor de Segurança da Informação, que é o ponto focal para o registro e início do tratamento.

Análise: O Gestor de SI, com apoio da GTI, realiza a triagem inicial, valida a ocorrência e atribui a classificação de criticidade.

III. **Fase 3**: Contenção: A ERISI tomará ações imediatas para isolar os sistemas afetados (ex: desconectar da rede, bloquear contas comprometidas) e impedir que o incidente se espalhe, limitando o dano.

IV. **Fase 4**: Erradicação: A ERISI identificará a causa raiz do incidente (ex: vulnerabilidade, malware) e a removerá completamente do ambiente para evitar a recorrência.

V. **Fase 5**: Recuperação: A ERISI restaurará os sistemas e dados afetados a partir de backups seguros e validará o retorno à operação normal.

VI. **Fase 6**: Pós-Incidente (Lições Aprendidas):

Dentro de 30 dias após a resolução, será elaborado um relatório detalhado do incidente, contendo a análise da causa raiz, as ações tomadas, o impacto real e as lições aprendidas.

As recomendações do relatório deverão ser transformadas em um plano de ação para aprimorar os controles de segurança e prevenir futuros incidentes.

3.3. DA COMUNICAÇÃO LEGAL E TRANSPARÊNCIA

I. **Comunicação Interna**: O Gestor de SI é responsável por manter as partes interessadas internas (gestores, diretoria) informadas sobre o andamento do tratamento de incidentes relevantes.

II. **Comunicação com a ANPD e Titulares de Dados (LGPD)**: Caso um incidente de segurança envolva dados pessoais e possa acarretar risco ou dano relevante aos titulares, o Gestor de Segurança da Informação, cientificará o Encarregado de Dados (DPO) e a Gerência Jurídica, devendo ser iniciado o processo de notificação.

III. **Comunicação Externa e com a Imprensa**: Nenhuma informação sobre incidentes será divulgada externamente sem a aprovação formal da Diretoria,

em alinhamento com a Assessoria de Comunicação, exceto as notificações legalmente obrigatórias.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

I. Ponto focal para o recebimento de todos os reportes de incidentes.
II. Liderar a Equipe de Resposta a Incidentes (ERISI) e coordenar todas as fases do tratamento.
III. Realizar a classificação dos incidentes e a comunicação com as partes interessadas.

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Manifestar-se, por meio da ERISI, quanto a necessidade de execução das ações de contenção, erradicação e recuperação de dados.

4.3. DOS USUÁRIOS

I. Reportar qualquer suspeita ou incidente de segurança, conforme a PGSI.

5. DAS SANÇÕES E PUNIÇÕES

Sanções e punições serão aplicadas conforme previsão legal e na Política de Gestão de Segurança da Informação (PGSI)..

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI - TERMO DE USO DOS SISTEMAS INTERNOS				
Tema:	Norma Geral - N-SI-011			
Emitente	DIREÇÃO GERAL DO DETRAN|ES		Classificação:	Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação: IS-N nº 032/2025	Vigência: Na data da publicação	

1. DO PROPÓSITO

Definir os papéis, responsabilidades e procedimentos para a solicitação, criação, revisão e revogação de perfis de acesso aos sistemas de informação do DETRAN|ES, bem como estabelecer as regras para a utilização aceitável desses recursos, em conformidade com a Política de Gestão de Segurança da Informação (PGSI).

2. DO ESCOPO

Esta norma se aplica a todos os sistemas de informação do DETRAN|ES e a todos os usuários (internos e externos) que necessitem de acesso a eles.

3. DAS DEFINIÇÕES DE TERMOS E ESPECIFICAÇÕES

Com o objetivo de operacionalizar a gestão dos acessos aos sistemas do DETRAN|ES, são especificados os seguintes termos:

a. **Gestor de sistema**: Diretor de área específica, responsável por sistemas informáticos:

I. **Diretor(a) de Habilitação e Veículos - DHV**: Sistemas fornecidos pelo PRODEST ou outra contratada, que interajam com o Registro Nacional de Veículos Automotores – RENAVAM, com o Registro Nacional de Infrações - RENAINF, com o Registro Nacional de Condutores Habilitados - RENACH e sistemas relacionados às atividades da Diretoria.

II. **Diretor(a) de Segurança e Engenharia de Trânsito**: Sistemas fornecidos pelo PRODEST ou outra contratada, que interajam com o Registro Nacional de Acidentes e Estatísticas de Trânsito - RENAEST, Cerco Integrado

Inteligente, Sistema de Talonário Eletrônico (AUTUA) e sistemas relacionados às atividades da Diretoria;

III. **Diretor(a) Administrativo, Financeiro e de Recursos Humanos - DAFGP**: Sistema de gestão de recursos humanos; sistema de ponto eletrônico e sistemas correlatos; e

IV. **Diretor Geral**: Sistemas vinculados às atividades da Gerência de Tecnologia da Informação - GTI e Interfaces de Programação de Aplicações - API de integração com órgãos externos, instituições conveniadas e empresas contratadas.

b. **Usuário Master DETRAN|ES**: Servidor hierarquicamente superior ao interessado no acesso, sendo responsável pela definição, edição, bloqueio, suspensão e exclusão de usuários e a inclusão, substituição ou retirada de um perfil do usuário interno ou externo.

c. **Usuário Master Externo**: Usuário competente pela administração de um sistema por meio da definição, edição, bloqueio, suspensão e exclusão usuário e a inclusão, alteração ou retirada de um perfil do usuário externo, dentro dos limites estabelecidos pelo Gestor de Sistema.

d. **Administrador do Sistema**: Usuário responsável pela operacionalização das especificações dos níveis de acessos dos perfis, na forma das definições passadas pelos gestores dos sistemas.

e. **Usuário Interno**: Servidor ou pessoa que mantenha vínculo funcional com o DETRAN|ES.

f. **Usuário externo**: Usuário vinculado a uma entidade externa, pública ou privada (credenciados, conveniados ou contratados) que utilizem sistema informático do DETRAN|ES.

g. **Perfis de Usuários**: Níveis de acessos que contemplam um conjunto de permissões e ações, estritamente necessárias às atividades desenvolvidas pelo usuário integrante do perfil.

4. DAS ATRIBUIÇÕES DOS PERFIS DE ACESSOS

Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação, definido para cada sistema do DETRAN|ES e suas especificações ficarão a cargo das respectivas Gerências.

As definições dos perfis deverão ser apreciadas pelo respectivo Gestor de Sistema, antes da sua efetivação.

4.1. DA GESTÃO DOS PERFIS DE ACESSO

A criação e atribuição de todos os perfis de acesso devem seguir estritamente o Princípio do Menor Privilégio, concedendo apenas as permissões necessárias para o desempenho da função.

Os perfis de acesso deverão ser revisados continuamente pelos Proprietários da Informação, em um ciclo que não deve ultrapassar 12 (doze) meses, para garantir que as permissões permaneçam relevantes e adequadas.

5. DAS SOLICITAÇÕES PARA CRIAÇÃO DE USUÁRIOS EXTERNOS

A solicitação de criação de Usuário Master externo deverá ser encaminhada por ofício pelo dirigente máximo do órgão, em caso de agente público ou por responsável legal da empresa em caso de credenciados, conveniados ou contratados que por razão do credenciamento, convênio ou contrato necessitarem de acesso aos sistemas do DETRAN|ES.

O dirigente máximo do órgão poderá, na sua solicitação, informar a delegação da competência para criação de novos usuários máster.

Somente o responsável legal da empresa credenciada, conveniada ou contratada poderá solicitar a criação de usuários master para a mesma.

O cadastro de usuário externo deve ser solicitado pelo usuário master no sistema de gestão de acessos do DETRAN|ES e obedecerá às seguintes diretrizes:

a. As credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do DETRAN|ES, devidamente justificadas e previstas no contrato, convênio, acordo de cooperação técnica ou instrumento congênere ou sempre que houver previsão expressa na LGP ou no CTB; e
b. As solicitações de acessos aos sistemas do DETRAN|ES, para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere, devem:
    I. ser formuladas pelo gestor da unidade/área responsável pela gestão do instrumento legal;
    II. ser precedidas de manifestação formal do gestor do correspondente instrumento contratual no DETRAN|ES, versando sobre a conveniência e a regularidade dn concessão dos acessos requeridos; e
    III. ser atendidas somente após aprovação do Gestor de Sistema ou do Diretor Geral do DETRAN|ES.

6. DAS SOLICITAÇÕES PARA CRIAÇÃO DE USUÁRIOS INTERNOS

A disponibilização de acessos a usuários internos, deve ser solicitada pela chefia imediata ao administrador do sistema.

A liberação dos acessos dos estagiários aos sistemas do DETRAN|ES, terá como requisitos ser penal e civilmente imputável; e possuir perfil específico e restrito às atividades do estagiário.

O acesso será concedido mediante solicitação expressa do responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes a realização dos acessos.

O supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas do DETRAN|ES.

O acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

Compete a chefia do servidor/terceirizado solicitar a inclusão de perfis de acesso para desempenho das atividades inerentes ao setor onde esteja lotado.

7. DAS COMPETÊNCIAS DOS USUÁRIOS DOS SISTEMAS

Aos usuários externos e internos compete:

a. Fazer uso dos perfis de acesso atribuídos aos sistemas do DETRAN|ES, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de acesso;
b. Manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas do DETRAN|ES; e
c. Ter conhecimento e estar de acordo com o disposto na LGPD e na PSI do DETRAN | ES IS Nº 26/2024.

8. DAS COMPETÊNCIAS DOS ADMINISTRADORES DOS SISTEMAS

Aos administradores dos sistemas do DETRAN|ES compete:

a. Mediante solicitação da chefia do usuário interno, do Usuário Master DETRAN|ES ou do Usuário Master e manifestação da gerência da área e aprovação do Gestor do sistema criar, editar, bloquear, suspender e excluir um órgão, setor, vínculo, perfil e/ou usuário; e
b. Atuar, em conjunto com as áreas de negócio, a Gerência de Tecnologia da Informação e Administrador do Sistema, no planejamento e execução do processo

de implementação dos sistemas do DETRAN|ES dos quais for designado responsável.

9. DAS RESTRIÇÕES ÀS CONCESSÕES DE ACESSOS

As concessões de acesso aos sistemas do DETRAN|ES são distintas, dessa forma, o usuário poderá obter permissão de acesso apenas à um sistema específico ou a vários sistemas distintos, sob responsabilidade do DETRAN|ES.

O uso indevido de informações acessadas por meio dos sistemas do DETRAN|ES sujeitará o usuário às penalidades previstas na legislação.

Não poderá ser concedido acesso a sistemas informáticos a usuário que não tenha assinado o Termo de Confidencialidade.

Na solicitação de acesso devem ser informados, pelo menos, os seguintes dados do usuário: Nome; CPF; RG; celular; e-mail; número funcional (usuário interno); e demais dados que se fizerem necessários.

A solicitação deve ser individualizada para cada sistema, com a justificativa de utilização.

Sempre que um agente público deixar de pertencer ao quadro de servidores do DETRAN|ES, a Gerência de Recursos Humanos - GRH deverá providenciar a comunicação aos administradores do sistema para que seja providenciada a exclusão dos acessos desses usuários aos sistemas por eles administrados.

Não havendo a disponibilização de sistema próprio para essa atividade, a GRH realizará a comunicação por meio de e-mail, direcionado aos administradores dos sistemas.

Sempre que houver movimentação de setores de um agente público pertencente ao quadro de servidores do DETRAN|ES, a Gerência de Recursos Humanos deverá

comunicar aos administradores do sistema para que excluam os acessos correspondentes aos perfis do antigo setor.

O bloqueio administrativo dos acessos deverá ser solicitado, de forma cautelar, pelo gerente da respectiva área e cientificada à Direção à qual se vincula, nos seguintes casos:

a. Indícios de utilização indevida dos acessos;
b. Cancelamento ou interrupção do vínculo com o DETRAN|ES; e
c. Perda das condições que imputem a necessidade de acessar os sistemas.

O bloqueio administrativo dos acessos a sistemas poderá ser solicitado pela Corregedoria do DETRAN|ES, ao Gestor de Sistema, de forma cautelar, nos casos em que, durante a tramitação de apurações, PAD ou sindicâncias, seja identificado indício de má utilização dos acessos aos sistemas por servidores ou pessoas que mantenham outro vínculo funcional ou contratual com este DETRAN|ES.

10. DOS PARÂMETROS DAS CREDENCIAIS DE ACESSOS

Com relação às credenciais de acesso, deve-se observar que:

a. Deverão ter, no mínimo, oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números).
b. É vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;
c. Podem ser alteradas sempre que preciso;
d. O prazo de validade não deve ultrapassar 90 (noventa) dias; e
e. O usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha.

11. DAS REGRAS PARA UTILIZAÇÃO DAS CREDENCIAIS E PERFIS

Para a utilização das credenciais e perfis, os usuários devem:

a. Ter conhecimento prévio desta Política de Controle de Acesso e preencher os requisitos estabelecidos na mesma;
b. Estar devidamente autorizados a utilizar os sistemas do DETRAN|ES, de acordo com os requisitos estabelecidos nesta Norma;
c. Utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado ou do credenciamento, convênio ou contrato firmado entre as entidades particulares ou públicas e o DETRAN|ES, cumprindo os procedimentos dispostos nesta Norma, sem prejuízo das demais legislações vigentes;
d. Abster-se de divulgar ou compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
e. Abster-se de fazer uso das credenciais de acesso de outros usuários;
f. Fornecer informações acessadas nos sistemas do DETRAN|ES, somente mediante demanda formalizada, de quem tenha competência para tal;
g. Comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa, quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação;
h. Sempre que for necessário, ao afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;
i. Efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e
j. No ato do primeiro acesso, bem como após cada atualização desta Norma, manifestar concordância com os termos dispostos nesta Norma.

12. DAS REGRAS PARA A ESPECIFICAÇÃO DE PERFIS DE ACESSOS

Os gerentes das áreas, responsáveis pela administração dos sistemas do DETRAN|ES, também se responsabilizarão pelas permissões, transações e ações que devem compor cada perfil de acesso.

Os perfis dos usuários e de gestão, concedidos para usuários internos e externos, deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 18 (dezoito) meses.

13. DA AUTENTICAÇÃO DOS USUÁRIOS

O processo de autenticação dos usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do DETRAN|ES e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital, tokens ou outros meios disponíveis).

14. DAS REGRAS DE USO ACEITÁVEL

São condições exigíveis para o uso legal das informações e dados:

I. Todo usuário deve assinar o Termo de Confidencialidade e Manutenção de Sigilo (N-SI-013) antes de receber o acesso.
II. As credenciais de acesso são pessoais e intransferíveis. É expressamente proibido o compartilhamento.
III. O acesso concedido deve ser utilizado única e exclusivamente para as finalidades profissionais designadas.
IV. O usuário deve comunicar imediatamente ao seu gestor e ao Gestor de Segurança da Informação qualquer incidente ou suspeita de violação de suas credenciais.
V. Ao se afastar de sua estação de trabalho, o usuário deve garantir o bloqueio da sessão para impedir o acesso não autorizado.

15. GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – USO ACEITÁVEL DOS ATIVOS DA INFORMAÇÃO				
Tema:	Norma Geral - N-SI-012			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

1. DO PROPÓSITO

Estabelecer diretrizes para o uso seguro e responsável de todos os ativos de informação do DETRAN|ES, visando proteger a confidencialidade, integridade e disponibilidade das informações, garantir a preservação do patrimônio público e orientar a conduta de todos os usuários.

2. DO ESCOPO

Esta norma se aplica a todos os ativos de informação do DETRAN|ES (equipamentos computacionais, mídias de armazenamento, sistemas, impressoras, redes, etc.) e a todos os usuários (Servidores, Contratados, Conveniados e outros Usuários), conforme o escopo da Política de Gestão de Segurança da Informação (PGSI).

3. DAS DIRETRIZES

3.1. DO USO DOS EQUIPAMENTOS COMPUTACIONAIS

Os equipamentos fornecidos pelo DETRAN|ES (desktops, notebooks, etc.) são de propriedade da Autarquia e destinam-se exclusivamente ao desempenho de atividades profissionais.

A manutenção, instalação ou alteração de hardware e software em equipamentos corporativos é atribuição exclusiva da Gerência de Tecnologia da Informação (GTI) ou de terceiros por ela designados.

O uso de equipamentos particulares para fins de trabalho só é permitido mediante autorização formal e deve seguir rigorosamente todas as diretrizes estabelecidas na N-SI-003 - Norma de BYOD.

É proibida a conexão de equipamentos particulares ou não homologados à rede cabeada ou sem fio do DETRAN|ES, sem a prévia autorização do Gestor de Segurança da Informação e da GTI.

3.2. DOS DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEL E NUVEM

O usuário é o responsável direto pela segurança física e lógica dos dispositivos de armazenamento removível (pen drives, HDs externos, etc.) sob sua guarda.

Todos os dispositivos de armazenamento removível fornecidos pelo DETRAN|ES para o transporte de informações classificadas como Confidencial ou Restrito deverão, obrigatoriamente, utilizar criptografia para proteger os dados.

Apenas a solução de armazenamento em nuvem corporativa e homologada pelo DETRAN|ES pode ser utilizada para armazenar arquivos de trabalho. É estritamente proibido o upload de qualquer informação classificada (Interna, Confidencial ou Restrito) para serviços de nuvem pessoais ou de terceiros.

Em caso de perda ou furto de um dispositivo de armazenamento, o usuário deve comunicar imediatamente ao Gestor de Segurança da Informação.

3.3. DA POLÍTICA DE MESA LIMPA E TELA LIMPA

O bloqueio de tela (com senha) deverá ser ativado sempre que o usuário se afastar de sua estação de trabalho, mesmo que por curtos períodos, para impedir o acesso não autorizado.

Documentos físicos, especialmente os classificados como Interno, Confidencial ou Restrito, não devem ser deixados expostos sobre a mesa. Ao final do expediente ou ao se ausentar por longos períodos, o usuário deve guardá-los em local seguro e trancado (gavetas ou armários).

3.4. DA IMPRESSÃO OU MANUSEIO DE DOCUMENTOS

O uso de impressoras e fotocopiadoras deve ser restrito a documentos de interesse do DETRAN|ES.

O usuário deve retirar imediatamente da impressora os documentos que contenham informações classificadas para evitar o acesso indevido.

É vedado o reaproveitamento de papel que contenha informações classificadas como Confidencial ou Restrito. Tais documentos devem ser descartados em fragmentadoras de papel (corte cruzado), conforme as diretrizes da N-SI-004 - Classificação da Informação.

3.5. DA SEGURANÇA FÍSICA

Crachás de identificação ou dispositivos de acessos a sistemas ou a hardwares são pessoais e intransferíveis e devem ser portados de forma visível nas dependências do DETRAN|ES.

Visitantes e terceiros devem ser sempre identificados e acompanhados em áreas de acesso restrito.

É proibido consumir alimentos, bebidas ou fumar em áreas sensíveis, como Data Centers e salas de equipamentos.

4. DOS PAPEIS E RESPONSABILIDADES

4.1. DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

I. Estabelecer e manter esta norma atualizada; e
II. Comunicar ao Comitê Interno de Segurança da Informação (CSI) eventuais violações a esta norma.

4.2. DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

I. Realizar a manutenção e configuração segura dos ativos de TI; e
II. Implementar os controles técnicos necessários, como a criptografia em dispositivos.

4.3. DOS USUÁRIOS

I. Zelar pela preservação e uso adequado de todos os ativos de informação sob sua responsabilidade; e
II. Cumprir integralmente as diretrizes desta norma

5. DAS SANÇÕES E PUNIÇÕES

O descumprimento das diretrizes estabelecidas nesta norma sujeitará o infrator às sanções previstas na Política de Gestão de Segurança da Informação (PGSI) e na legislação vigente.

6. DA GESTÃO DA NORMA

Esta norma será revisada anualmente, ou sempre que necessário, pelo Gestor de Segurança da Informação, aprovada pelo Comitê Interno de Segurança da Informação (CSI) e homologada pelo Diretor Geral do DETRAN|ES.

ELABORAÇÃO E CONTROLE DO DOCUMENTO	
Agente:	Luiz Antonio Uchoa da Silva
Ação:	Revisão
Cargo:	Gerente de Tecnologia da Informação
Contato:	luiz.uchoa@detran.es.gov.br
Agente:	Willian da Conceição Silveira
Ação:	Revisão
Cargo:	Subgerente de Infraestrutura e Segurança de Tecnologia da Informação
Contato:	willian.silveira@detran.es.gov.br

PSI – TERMOS DE CONFIDENCIALIDADE E MANUTENÇÃO DE SIGILO				
Tema:	Norma Geral - N-SI-013			
Emitente	DIREÇÃO GERAL DO DETRAN|ES			Classificação: Uso Interno
Sistema:	Todos os sistemas informáticos do DETRAN|ES			
Versão:	2	Aprovação:	IS-N nº 32/2025	Vigência: Na data da publicação

TERMO DE CONFIDENCIALIDADE E DE MANUTENÇÃO DE SIGILO – TCMS PESSOA FÍSICA

Eu,, [cargo/função], matrícula nº [matrícula], lotado(a) no(a), declaro ter pleno conhecimento da Política de Gestão de Segurança da Informação (PGSI) do DETRAN|ES e de todas as suas normas complementares, e assumo o compromisso pessoal e profissional de manter total confidencialidade e sigilo sobre todas as informações a que tiver acesso em decorrência de minhas funções.

Por este Termo de Confidencialidade e Manutenção de Sigilo, comprometo-me a:

I. Cumprir integralmente a PGSI e todas as suas normas associadas, entendendo que minhas responsabilidades vão além da confidencialidade e incluem o uso seguro de todos os ativos de informação.
II. Não utilizar quaisquer dados ou informações, confidenciais ou não, para gerar benefício próprio ou de terceiros.
III. Não efetuar gravação, extração ou cópia de qualquer informação a que tiver acesso, exceto quando expressamente autorizado e necessário para o desempenho de minhas funções.

IV. Não repassar o conhecimento das informações a que tiver acesso, responsabilizando-me por todas as pessoas que vierem a ter acesso a elas por meu intermédio.

V. Manter minhas credenciais de acesso (usuários, senhas, tokens) em absoluto sigilo, ciente de que são de uso pessoal, intransferível e que sou responsável por todas as atividades realizadas com elas.

VI. Reportar imediatamente ao Gestor de Segurança da Informação qualquer incidente, suspeita de violação de segurança ou perda de minhas credenciais, conforme a N-SI-010 - Resposta a Incidentes.

Zelar pela segurança física e digital dos ativos sob minha guarda, seguindo as diretrizes da N-SI-012 - Uso Aceitável dos Ativos de Informação, incluindo a Política de Mesa Limpa e Tela Limpa.

Definições:

Neste Termo, as seguintes expressões serão assim definidas:

a. Informação: Inclui, mas não se limita, à informação relativa aos dados solicitados e que se encontram sob a guarda do DETRAN|ES.
b. Informação Confidencial: Toda informação, em qualquer formato, não classificada como pública, incluindo dados de processos, planos, informações de cidadãos, dados sob guarda do DETRAN|ES e atos preparatórios.
c. Dados Pessoais: Todas as informações relacionadas à pessoa natural, identificada ou identificável, contidas nos bancos de dados do DETRAN|ES.

Não constituirá "Informação" ou "Informação Confidencial" para os propósitos deste Termo aquela que:

a. Seja de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão da Parte Receptora;
b. Já esteja em poder da Parte Receptora, como resultado de sua própria pesquisa, contanto que a Parte Receptora possa comprovar esse fato;
c. Tenha sido legitimamente recebida de terceiros;
d. Seja revelada em razão de uma ordem válida ou de uma ordem judicial, somente até a extensão de tais ordens, contanto que a Parte Receptora tenha notificado a existência de tal ordem, previamente e por escrito, à Parte Reveladora, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Vigência e Sanções:

A obrigação de confidencialidade e sigilo assumida neste Termo tem validade por prazo indeterminado, mesmo após o encerramento do meu vínculo com o DETRAN|ES.

Pelo não cumprimento do presente Termo, fico ciente de que estarei sujeito(a) a todas as sanções administrativas, cíveis e penais cabíveis, conforme a legislação vigente e a PGSI do DETRAN|ES.

Declaro estar ciente das disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e me obrigo a cumprir suas disposições relativas aos Dados Pessoais a que tiver acesso.

.

Vitória/ES, de de 20 .

_____

Nome/Assinatura

TERMO DE CONFIDENCIALIDADE E DE MANUTENÇÃO DE SIGILO – TCMS PESSOA JURÍDICA

CONTRATO: XXXX

EMPRESA CONTRATADA:

RESPONSÁVEL:

Pelo presente instrumento, a empresa, CNPJ nº [CNPJ], com sede em [Endereço Completo], neste ato representada por seu representante legal, CPF nº, doravante denominada **CONTRATADA**, assume, em caráter irrevogável e irretratável, o compromisso de manter total confidencialidade e sigilo sobre todas as informações do Departamento Estadual de Trânsito do Espírito Santo (DETRAN|ES) a que tiver acesso em virtude do Contrato/Convênio nº [Número do Contrato].

A **CONTRATADA** compromete-se a:

1. Cumprir e fazer cumprir por seus colaboradores, prepostos e eventuais subcontratados a Política de Gestão de Segurança da Informação (PGSI) do DETRAN|ES e todas as suas normas complementares, que declara ter recebido e ter pleno conhecimento.
2. Utilizar as informações confidenciais e dados pessoais acessados única e exclusivamente para a finalidade objeto do contrato, sendo vedado qualquer uso para benefício próprio ou de terceiros.
3. Implementar e manter medidas de segurança técnicas e administrativas aptas a proteger os dados do DETRAN|ES contra acessos não autorizados,

destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito.

4. Garantir que todos os seus colaboradores e prepostos, que terão acesso às informações do DETRAN|ES, assinem um termo de confidencialidade individual, com obrigações no mínimo tão rigorosas quanto as deste documento.
5. Notificar o Gestor de Segurança da Informação do DETRAN|ES e o gestor do contrato sobre qualquer incidente de segurança que afete os dados da Autarquia em, no máximo, 24 (vinte e quatro) horas a partir da ciência do evento.
6. Conceder ao DETRAN|ES, ou a terceiros por ele indicados, o direito de realizar auditorias para verificar o cumprimento das obrigações de segurança aqui estabelecidas.
7. Ao término do contrato, devolver ou destruir de forma segura todos os dados e informações do DETRAN|ES que estiverem em sua posse, emitindo um certificado de destruição, se solicitado.

Vigência e Sanções:

A obrigação de confidencialidade vigerá por prazo indeterminado, mesmo após o término do contrato. O descumprimento deste Termo sujeitará a **CONTRATADA** às sanções contratuais, cíveis, penais e administrativas previstas, sem prejuízo da reparação por perdas e danos causados ao DETRAN|ES ou a terceiros.

Vitória/ES, _____ de _____ de 20____.

[Cargo]

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

GIVALDO VIEIRA DA SILVA
DIRETOR GERAL
DETRAN - DETRAN - GOVES
assinado em 12/09/2025 08:52:24 -03:00

LUIZ ANTONIO UCHOA DA SILVA
GERENTE
GTI - DETRAN - GOVES
assinado em 12/09/2025 08:22:53 -03:00

WILLIAN DA CONCEICAO SILVEIRA
SUBGERENTE
SGIS - DETRAN - GOVES
assinado em 12/09/2025 08:20:26 -03:00

INFORMAÇÕES DO DOCUMENTO
Documento capturado em 12/09/2025 08:52:24 (HORÁRIO DE BRASÍLIA - UTC-3)
por WILLIAN DA CONCEICAO SILVEIRA (SUBGERENTE - SGIS - DETRAN - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: https://e-docs.es.gov.br/d/2025-4WC1HQ