Código **N-SI-001**	**PGSI – DEPARTAMENTO ESTADUAL DE TRÂNSITO DO ESPÍRITO SANTO – DETRAN |ES**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

ANEXOS

Tipo	Nº	Descrição
Norma	N-SI-002	Acesso Remoto
Norma	N-SI-003	BYOD
Norma	N-SI-004	Classificação da Informação
Norma	N-SI-005	Proteção Contra Códigos Maliciosos
Norma	N-SI-006	E-mail e Comunicadores Instantâneos
Norma	N-SI-007	Gestão de Identidade
Norma	N-SI-008	Internet e Mídias Sociais
Norma	N-SI-009	Monitoramento
Norma	N-SI-010	Resposta a Incidentes
Norma	N-SI-011	Termo de Uso dos Sistemas Internos
Norma	N-SI-012	Uso Aceitável dos Ativos de Informação
Norma	N-SI-013	Gestão de Ambientes de Computação em Nuvem
Procedimento	P-SI-001	Termo de Confidencialidade
Procedimento	P-SI-002	Relatório de Impacto a Proteção de Dados Pessoais
Procedimento	P-SI-003	Registro de Operações de Tratamento de Dados Pessoais
Link Web	Lei 13.709 (LGPD)	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

RESOLUÇÃO NORMATIVA Nº XX/20XX

Dispõe sobre a Política de Segurança de Informações do Departamento Estadual de Trânsito do Espírito Santo – PSI – N.SI.001 e dá outras providencias.

O Departamento Estadual de Trânsito do Espírito Santo, no uso das suas atribuições legais e constitucionais;

Considerando o dever de preservar o sigilo imprescindível à segurança da sociedade e do Estado previsto no inciso XXXIII do art. 5º na Constituição Federal;

Considerando a missão de prestar serviços de excelência no atendimento ao cidadão, implementando políticas públicas para um trânsito seguro e humanizado;

Considerando a visão de ser reconhecido pela excelência dos serviços prestados e gestão eficiente dos recursos com valorização da vida e inclusão das pessoas.

Considerando os valores da ética, transparência, responsabilidade social e ambiental, compromisso com a vida, efetividade e humanização.

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

Considerando que o Departamento Estadual de Trânsito do Espírito Santo mantém grande volume de informações essenciais ao exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem manter-se íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

Considerando que as informações são armazenadas em diferentes suportes e veiculadas por diversas formas, tais como meio impresso, eletrônico e magnético, sendo, portanto, vulneráveis a desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando que a adequada gestão da informação precisa nortear todos os processos de trabalho e unidades do Órgão e deve ser impulsionada por política interna de segurança da informação;

Considerando a importância da adoção de boas práticas inerentes à proteção da informação abarcada pelas normas NBR ISSO/IEC 27001:2013, NBR ISSO/IEC 27002:2013;

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, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), bem como na Lei Geral de Proteção de Dados Lei Nº 13.709/2018;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação (PSI) N.SI.001 de acordo com o estabelecido na presente Resolução.

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º. O Departamento Estadual de Trânsito do Espírito Santo institui sua Política de Segurança da Informação (PSI-N.SI.001), objetivando assegurar que as informações e seus ativos, possuídos ou custodiados, serão estabelecidos, protegidos e utilizados de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei.

Art. 3º. A Política de Segurança da Informação se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, cargo, emprego ou função pública no âmbito desta Autarquia, e que façam uso de seus recursos materiais e tecnológicos.

CAPÍTULO I – DOS CONCEITOS E DEFINIÇÕES

Art. 4º. Para efeito desta Resolução 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 Departamento Estadual de Trânsito do Espírito Santo;

V- Atividades críticas: atividades precípuas do Departamento Estadual de Trânsito do Espírito Santo 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 Departamento Estadual de Trânsito do Espírito Santo;

VIII- Ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas do Departamento Estadual de Trânsito do Espírito Santo;

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- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

XI- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XII- Ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação, destinação e eliminação;

XIII- 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;

XIV- Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

XV- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XVI- 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;

XVII- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

XVIII- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

XIX- 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;

XX- 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;

XXI- Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

XXII- Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XXIII- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XXIV- 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);

XXV- 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;

XXVI- 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;

XXVII- 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;

XXVIII- 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;

XXIX- Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

XXX- Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

XXXI- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XXXII- 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; e

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

XXXIV- Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXXV- Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXXVI- Recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXXVII- 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;

XXXVIII- 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;

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

XL- 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;

XLI- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XLII- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XLIII- Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLIV- 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;

XLV- 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;

XLVI- Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas do Departamento Estadual de Trânsito do Espírito Santo.

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

XLVIII- COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do Departamento Estadual de Trânsito do Espírito Santo, que tem por finalidade tratar questões ligadas à Segurança da Informação.

XLIX- Relatório de Impacto a Proteção de Dados Pessoais – Descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, contendo medidas, salvaguardas e mecanismos de mitigação de risco.

CAPÍTULO II – DOS PRINCÍPIOS

Art. 5º. A Política de Segurança da Informação do Departamento Estadual de Trânsito do Espírito Santo, se alinha com às estratégias desta

Instituição e, tem como princípio norteador garantir a integridade, confidencialidade, autenticidade e a disponibilidade das informações processadas dentre outros:

I – Assegurar o uso da informação no interesse da Instituição.

II – Preservar a credibilidade dos ativos de informação.

III - Combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações.

IV - Fomentar a conscientização, capacitação e a educação em segurança da informação.

V - Promover a gestão e continuidade do negócio.

CAPÍTULO III – DOS ESCOPO

Art. 6º São Objetivos da PSI do Departamento Estadual de Trânsito do Espírito Santo:

I- Instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação;

II- Promover ações necessárias à implementação e à manutenção da segurança da informação;

III- combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV- Promover a conscientização e a capacitação de recursos humanos em segurança da informação.

Art. 7º Esta PSI se aplica a todos os, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no âmbito do Departamento Estadual de Trânsito do Espírito Santo.

Parágrafo único. Os destinatários desta PSI, relacionados no caput, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta resolução.

CAPÍTULO IV – DAS DIRETRIZES GERAIS

Art. 8º A operacionalização das diretrizes da Política de Segurança da Informação no Departamento Estadual de Trânsito do Espírito Santo, se efetivará por meio das normas constantes dos anexos desta resolução.

§1º Serão adotadas, para efeito desta resolução e das normas da Política de Segurança da Informação, as definições constantes no artigo 4º desta resolução, bem como do glossário anexo.

§ 2º As normas deverão indicar o público-alvo a que se destinam e serão classificadas como gerais, quando tiverem ampla aplicação ou impacto, ou específicas, quando tiverem aplicação ou impacto restrito.

Parágrafo único: Conforme necessidade e conveniência deste Departamento Estadual de Trânsito do Espírito Santo, as normas elencadas nesta resolução, poderão ser reformuladas e/ou criadas.

Art. 9º Compõem a Política de Segurança da Informação neste, os anexos referentes a pormenorização das normas elencadas nesta resolução, bem como as futuras alterações e/ou criações.

§ 1º As normas que integram a Política de Segurança da Informação serão publicadas pela Comunicação na intranet e no Portal deste Departamento Estadual de Trânsito do Espírito Santo, em seção específica intitulada “Segurança da Informação”.

§ 2º Outras normas poderão ser acrescentadas às constantes dos incisos deste artigo, observados os procedimentos especificados no art. 9º desta resolução.

Art. 10º A revisão e a atualização das normas de segurança da informação ocorrerão sempre que se fizer necessário ou conveniente ao Departamento Estadual de Trânsito do Espírito Santo.

SEÇÃO I – DA GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 11º Todos os ativos de informação e de processamento do Departamento Estadual de Trânsito do Espírito Santo, deverão ser inventariados, classificados, atualizados periodicamente e mantidos em condições de uso;

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

Art. 12º O processo de classificação da informação deverá ser regulamentado e coordenado pela unidade ou comissão responsável pela gestão da informação.

Art. 13º Toda e qualquer informação produzida ou custodiada pelo Departamento Estadual de Trânsito do Espírito Santo 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, no exercício de suas funções, são patrimônio intelectual do Departamento Estadual de Trânsito do Espírito Santo, e não cabe a seus criadores qualquer forma de direito autoral.

Art. 14º É vedado o uso dos ativos do Departamento Estadual de Trânsito do Espírito Santo para obter proveito pessoal ou de terceiros, bem como para veicular opiniões político-partidárias.

Art. 15º Cabe somente ao proprietário da informação classificar seu nível de sigilo. Na ausência dessa classificação, todas as informações de terceiros que estejam sob a custódia ou processamento do Departamento Estadual de Trânsito do Espírito Santo devem ser tratadas como possuindo o mais alto grau de sigilo.

SEÇÃO I – DO CONTROLE DE ACESSOS A INFORMAÇÃO

Art. 16º O acesso às informações produzidas ou custodiadas pelo Departamento Estadual de Trânsito do Espírito Santo 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 Departamento Estadual de Trânsito do Espírito Santo que não sejam de domínio público, quando autorizado, será condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 17º 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. 18º Deverá ser estabelecido Processo de Gestão de Riscos de ativos de informação e de processamento do Departamento Estadual de Trânsito do Espírito Santo, 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 revisado periodicamente.

SEÇÃO IV – DA GESTÃO DA CONTINUIDADE DE NEGÓCIOS

Art. 19º Deverá ser elaborado Plano de Continuidade de Negócios que estabeleça procedimentos e defina estrutura mínima de recursos para que se desenvolva uma resiliência organizacional capaz de garantir o fluxo das informações críticas em momento de crise e salvaguardar o interesse das partes interessadas, a reputação e a marca da organização.

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

SEÇÃO V – DO TRATAMENTO DOS INCIDENTES DE REDE

Art. 20º 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.

SEÇÃO VI – DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 21º 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. Observar norma correspondente N-SI-010.

Parágrafo único. Os usuários são responsáveis por:

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.

SEÇÃO VII – DA AUDITORIA E CONFORMIDADE

Art. 22º Deverá ser incluída no escopo do Plano Anual de Auditoria e Conformidade análise do correto cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes.

Parágrafo único. 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.

SEÇÃO VIII – DOS SERVIÇOS DE INTERNET, DO CORREIO ELETRONICO CORPORATIVO, MIDIAS SOCIAIS E MENSAGEIROS INSTANTANEOS

Art. 23º Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, desde que seja resguardado os direitos previstos nas Lei Geral de Proteção de Dados Nº13.709/2018, ater-se também a norma anexas referentes N-SI-006 e N-SI-008.

Art. 24º O Departamento Estadual de Trânsito do Espírito Santo em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Art. 25º Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, 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. 26º O Departamento Estadual de Trânsito do Espírito Santo ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

Art. 27º O e-mail institucional deve ser usado apenas para fins relacionados ao trabalho, não devendo ser divulgado ou cadastrado em sites ou serviços relacionados a interesses exclusivamente pessoais.

Art. 28º 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 Departamento Estadual de Trânsito do Espírito Santo.

Art. 29º O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

SEÇÃO IX – DO DESENVOLVIMENTO DE SISTEMAS SEGUROS

Art. 30º O Processo de Desenvolvimento de Software do Departamento Estadual de Trânsito do Espírito Santo 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.

Art. 31º A adoção ou desenvolvimento de ambientes e sistemas, sejam tecnológicos ou não, tenham sido contratados, adquiridos, ou desenvolvidos pelo Departamento Estadual de Trânsito do Espírito Santo, deverá ser previamente avaliada pelas áreas requerentes, em conjunto com todos 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. 32º Todos os requisitos de segurança de ambientes, sistemas ou quaisquer outros ativos ou recursos de informação devem ser identificados previamente à implementação dos mesmos e deverão ser testados na fase de avaliação ou desenvolvimento, confirmados na fase de homologação, e continuamente reavaliados durante sua utilização.

Art. 33º 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. Entretanto, os ambientes de desenvolvimento, testes e homologação poderão consumir e ter 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.

SEÇÃO X – DO USO DE RECURSOS CRIPTOGRAFADOS

Art. 34º Toda a informação classificada, como sigilosa, produzida, armazenada ou transmitida pelo Departamento Estadual de Trânsito do Espírito Santo, 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.

SEÇÃO XI – DO PROCESSO DE TRATAMENTO DA INFORMAÇÃO

Art. 35º O tratamento da informação deve abranger as políticas, os processos, a práticas e os instrumentos utilizados pelo Departamento Estadual de Trânsito do Espírito Santo 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.

SEÇÃO XII – DO ACESSO FÍSICO E SEGURANÇA PATRIMONIAL

Art. 36º Usuários somente devem autorizar a entrada de pessoas no Departamento Estadual de Trânsito do Espírito Santo nos casos e ambientes permitidos pela autarquia, desde que possuam os devidos privilégios funcionais ou contratuais para efetuarem e permitirem tais acessos. Nos casos de ambientes restritos, é necessária autorização de um de seus responsáveis.

Art. 37º A entrada e a saída de bens, equipamentos e demais ativos tecnológicos das dependências do Departamento Estadual de Trânsito do Espírito Santo devem ser efetuados 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.

SEÇÃO XIII – DO ACESSO LÓGICO E UTILIZAÇÃO DE RECURSOS

Art. 38º Os equipamentos do Departamento Estadual de Trânsito do Espírito Santo 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. 39º Não é permitida a conexão de equipamentos pessoais ou de terceiros nas redes locais (cabeadas). Terceiros só devem ter acesso aos seus recursos se necessário à execução das atividades afins.

Art. 40º Autorizações de acesso a sistemas, ambientes e demais recursos devem ser concedidas mediante necessidade e sob o princípio dos privilégios mínimos.

SEÇÃO XIV – DO COMPARTILHAMENTO DE INFORMAÇÕES

Art. 41º Dados ou informações só devem ser compartilhados com quem possa ou deva ter acesso aos mesmos.

Art. 42º Senhas de acesso a recursos e ambientes do Departamento Estadual de Trânsito do Espírito Santo que precisem ser compartilhadas entre seus administradores ou equipes devem ser armazenadas criptografadas em sistemas seguros, específicos para este propósito.

Art. 43º O atendimento a solicitações externas de fornecimento de informações pertencentes a entes públicos e custodiadas ou processadas pelo Departamento Estadual de Trânsito do Espírito Santo, quando efetuadas por terceiros ou mesmo por seus próprios proprietários, deve ser efetuado conforme previsto na Lei Geral de Proteção de dados.

SEÇÃO XV – DO DESCARTE DE INFORMAÇÕES

Art. 44º 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. 45º Todos os usuários devem devolver, após o término de suas relações com o Departamento Estadual de Trânsito do Espírito Santo todas as mídias eletrônicas ou impressas que possuam quaisquer informações confidenciais pertencentes ao Departamento Estadual de Trânsito do Espírito Santo ou a terceiros. Nos casos em que não houver essa possibilidade, comprometem-se a efetuar seu descarte seguro.

CAPÍTULO V – DO ACESSO REMOTO

Art. 46º O acesso remoto a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo é

restrito a usuários que necessitem deste recurso para execução das atividades profissionais.

Art. 47º As diretrizes para acesso remoto a ativos/serviços de informação e recursos computacionais estão descritos no ANEXO N-SI-002 desta política.

CAPÍTULO VI – DOS PAPÉIS E RESPONSABILIDADES

Art. 48º Compete a Gerência de Tecnologia da Informação:

I- Apoiar a implementação desta PSI

II- Prover os ativos de processamento necessários ao cumprimento desta PSI;

III- 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;

IV- Disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho;

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

Art. 49º Compete aos usuários:

I- Todos os usuários devem conhecer e 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 Departamento Estadual de Trânsito do Espírito Santo. Observar norma anexa N-SI-012 (Uso Aceitável dos Ativos de Informação).

II- Responder por toda atividade executada com o uso de sua identificação;

III- Ter pleno conhecimento desta PSI;

IV- reportar tempestivamente ao Gestor de Segurança da Informação quaisquer falhas ou indícios de falhas de segurança de que tenha conhecimento ou suspeita;

V- Proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;

VI- Executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

VII- Gerenciar os ativos sob sua responsabilidade

VIII- Todos os usuários devem tratar com a devida CONFIDENCIALIDADE todas as informações de caráter sigiloso às quais terão acesso ou conhecimento durante a vigência de sua relação com o Departamento Estadual de Trânsito do Espírito Santo, 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.

IX- Todos os usuários devem 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 Departamento Estadual de Trânsito do Espírito Santo, aos seus proprietários ou a terceiros.

X- Usuários não devem 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 Departamento Estadual de Trânsito do Espírito Santo, cuja utilização ocorrerá sob total responsabilidade dos mesmos.

XI- Aqueles que utilizem ou administrem sistemas, ambientes ou quaisquer outros ativos ou recursos pertencentes ao Departamento Estadual de Trânsito do Espírito Santo ou por ela gerenciados, não devem permitir que os mesmos sejam acessados por pessoas que não tenham necessidade de efetuarem tais acessos e que não possuam as devidas permissões requeridas para tal.

XII- Os usuários devem se limitar a acessar apenas as informações e recursos necessários à execução das atividades relacionadas ao escopo de suas relações com o Departamento Estadual de Trânsito do Espírito Santo e conforme direitos, privilégios e permissões concedidos para a execução dessas atividades, observando os termos desta PSI e a legislação brasileira em vigor.

XIII- 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.

XIV- 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, ao Comitê Gestor de Segurança da Informação.

Art. 50º Fica constituído o **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI**, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico, Comunicação.

Art. 51º É responsabilidade do CGSI:

I- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
II- Estabelecer as prioridades dos programas institucionais de TI, por meio do alinhamento estratégico das áreas finalísticas, administrativas e acadêmicas com a área de TI, em consonância com o Planejamento Estratégico de Longo Prazo do Departamento Estadual de Trânsito do Espírito Santo.
III- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
IV- Estabelecer as prioridades dos programas institucionais de TI, por meio do alinhamento estratégico das áreas finalísticas, administrativas e acadêmicas com a área de TI, em consonância com o Planejamento Estratégico de Longo Prazo do Departamento Estadual de Trânsito do Espírito Santo.
V- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;
VI- Requerer às unidades gerenciais do Departamento Estadual de Trânsito do Espírito Santo informações que considerar relevantes e necessárias à realização de suas atividades;
VII- Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do Departamento Estadual de Trânsito do Espírito Santo.
VIII- Elaborar através do Controlador, relatório de impacto a proteção de dados pessoais quando necessário, utilizando modelo anexo de procedimento P-SI-01.

CAPÍTULO VII – DAS SANÇÕES, PUNIÇÕES E CASOS OMISSOS

Art. 52º 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.

Art. 53º No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Art. 54º Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao Departamento Estadual de Trânsito do Espírito Santo o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

Art. 55º Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

Art. 56º 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. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do Departamento Estadual de Trânsito do Espírito Santo adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do Departamento Estadual de Trânsito do Espírito Santo.

CAPÍTULO IX - DAS DISPOSIÇÕES FINAIS

Art. 57º Os casos omissos desta PSI serão resolvidos pelas Comissões de Segurança da Informação do Departamento Estadual de Trânsito do Espírito Santo.

Art. 58º Esta PSI é obrigatória a todos os membros do Departamento Estadual de Trânsito do Espírito Santo, os quais terão até XXX de XXXXX de 202X para se adaptarem às regras previstas nesta resolução.

Art. 59º Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet do Departamento Estadual de Trânsito do Espírito Santo.

Art. 60º O descumprimento desta PSI será objeto de apuração pela unidade competente do Órgão e pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 61º Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Departamento Estadual de Trânsito do Espírito Santo devem observar, no que couber, o constante desta PSI.

Art. 62º Ao assinar esta PSI o colaborador ou terceiro concorda com esta e todas as normas anexas.

Art. 63º Esta resolução entra em vigor na data de sua publicação.

Código **N-SI-002**	**PSI – ACESSO REMOTO**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-002** complementa Política Geral de Segurança da Informação, definindo as diretrizes para o acesso remoto a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para o acesso remoto a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo garantindo níveis adequados de proteção aos mesmos.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação

3.2. O acesso se dará através de "*VPN"* junto ao certificado gerado para o acesso.

4. Diretrizes

4.1. Concessão e uso do acesso remoto

4.1.1. O acesso remoto a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo é restrito a usuários que necessitem deste recurso para execução das atividades profissionais;

4.1.2. O acesso remoto dos usuários a serviço a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo 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;

4.1.3. 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 1 (um) ano tendo de ser renovado após este prazo;

4.1.4. A realização do acesso remoto, fora do expediente normal de trabalho, não implicará no pagamento de horas extras ao usuário, excetuando-se casos em que for comprovada a solicitação do trabalho pelo gestor do usuário ou parte autorizada;

4.1.5. O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros de posse de suas credenciais de acesso remoto;

4.1.6. O acesso remoto a ativos/serviços de informação e recursos computacionais da Departamento Estadual de Trânsito do Espírito Santo será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

4.1.7. Equipamentos computacionais utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do Departamento Estadual de Trânsito do Espírito Santo e firewall local ativo;

4.1.8. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possam o acesso remoto ao ambiente do Departamento Estadual de Trânsito do Espírito Santo estar habilitado, o usuário responsável deverá informar imediatamente o ocorrido a equipe de segurança da informação para bloqueio do acesso remoto.

4.2. **Concessão e uso do acesso remoto para terceiros**

4.2.1. O acesso remoto a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais;

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

4.2.2.1. O acesso remoto de terceiros e prestadores de serviço a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo 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;

4.2.2.2. 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;

4.2.2.3. 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;

4.2.2.4. O acesso remoto de terceiros a ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

4.2.2.5. Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do Departamento Estadual de Trânsito do Espírito Santo e firewall local ativo;

4.2.2.6. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possam o acesso remoto ao ambiente do Departamento Estadual de Trânsito do Espírito Santo habilitado, o usuário responsável deverá informar imediatamente o ocorrido a equipe de segurança da informação.

4.3. **Monitoramento do acesso remoto**

4.3.1. Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo está sujeita monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

4.3.2. Durante o monitoramento do acesso remoto a seus ativos/serviços de informação ou recursos computacionais, o Departamento Estadual de Trânsito do Espírito Santo 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.

5. Papéis e Responsabilidades

5.1. **SUBGERÊNCIA DE SEGURANÇA DA INFORMAÇÃO**

5.1.1. É responsabilidade da SUBGERÊNCIA DE SEGURANÇA DA INFORMAÇÃO:

5.1.1.1. Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo;

5.1.1.2. Controlar e monitorar qualquer tipo de acesso remoto fornecido pelo Departamento Estadual de Trânsito do Espírito Santo

5.1.1.3. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-002** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo

9. Glossário

9.1. **VPN – Virtual Privacy Network:** Rede utilizada para conexão com ambiente privado, neste caso a rede do Departamento Estadual de Trânsito do Espírito Santo, com objetivo de utilizar ferramentas que podem ser acessadas apenas internamente.

Código **N-SI-003**	**PSI – BYOD**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-003** complementa Política Geral de Segurança da Informação, definindo as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do Departamento Estadual de Trânsito do Espírito Santo ou para o manuseio de informações do Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do Departamento Estadual de Trânsito do Espírito Santo ou para o manuseio de informações do Departamento Estadual de Trânsito do Espírito Santo.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. **Uso de equipamentos computacionais pessoais no ambiente corporativo**

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;

4.1.2. A seu critério exclusivo, o Departamento Estadual de Trânsito do Espírito Santo poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;

4.1.3. A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da diretoria do Departamento Estadual de Trânsito do Espírito Santo, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade do Departamento Estadual de Trânsito do Espírito Santo;

4.1.4. O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política Geral de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções e punições previstas neste instrumento;

4.1.5. O Departamento Estadual de Trânsito do Espírito Santo não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;

4.1.6. O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos do Departamento Estadual de Trânsito do Espírito Santo não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com o Departamento Estadual de Trânsito do Espírito Santo;

4.1.7. Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações do Departamento Estadual de Trânsito do Espírito Santo, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:

4.1.7.1. O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;

4.1.7.2. Dispositivos de computação pessoal possuem ferramenta para prevenção de códigos maliciosos e garantem que as assinaturas de códigos maliciosos são ser atualizadas em tempo real e executam varreduras diariamente;

4.1.7.3. Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.

5. Papéis e Responsabilidades

5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade do CGSI:

5.1.1.1. Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-003** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

9. Glossário

9.1. **BYOD – Bring your own device:** Descreve uma política adotada por empresas e espaços educacionais que dá aos funcionários, alunos e professores a oportunidade de utilizar os seus próprios aparelhos para acessar dados e informações da companhia em seu local de trabalho e/ou estudo.

Código **N-SI-004**	**PSI – CLASSIFICAÇÃO DA INFORMAÇÃO**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

ANEXOS

Anexo I – Modelo para rotulagem de Informação
Anexo II – Tabela Ação x Classificação
Anexo III – Métodos de Descarte para informações armazenadas eletronicamente

1. Introdução

1.1. A Norma de segurança da informação **N-SI-004** complementa Política Geral de Segurança da Informação, definindo as diretrizes para a classificação, rotulagem, manuseio, guarda e descarte seguro de informações em formato digital ou em suporte físico.

2. Propósito

2.1. Estabelecer diretrizes para a classificação, manuseio e rotulagem dos ativos de informação do Departamento Estadual de Trânsito do Espírito Santo por seus usuários autorizados.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Classificação e rotulagem da Informação

4.1.1. Para efeitos de classificação da informação, o Departamento Estadual de Trânsito do Espírito Santo utiliza as seguintes categorias:

4.1.1.1. **INFORMAÇÃO PÚBLICA**: Informação oficialmente liberada pelo Departamento Estadual de Trânsito do Espírito Santo para o público geral. A divulgação deste tipo de informação não causa problemas ao Departamento Estadual de Trânsito do Espírito Santo ou a seus usuários e colaboradores, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.

4.1.1.2. **INFORMAÇÃO DE USO INTERNO:** Informação liberada exclusivamente para usuários e departamentos específicos do Departamento Estadual de Trânsito do Espírito Santo, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização expressa.

4.1.1.3. **INFORMAÇÃO CONFIDENCIAL:** Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais no Departamento Estadual de Trânsito do Espírito Santo. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para o Departamento Estadual de Trânsito do Espírito Santo e/ou seus usuários e colaboradores, portanto seu compartilhamento deve ser restrito e feito de maneira controlada.

4.1.2. A classificação da informação deverá ser realizada pelos gestores da informação, ou colaboradores designados por estes. Entretanto, a responsabilidade pela assertividade do nível selecionado permanece com o gestor da informação;

4.1.3. Para informações classificadas como **PÚBLICAS**, poderá ser utilizada um rótulo simples, conforme modelos exibidos no Anexo I desta norma;

4.1.4. Para informações classificadas como **USO INTERNO** ou **CONFIDENCIAIS**, deverá constar no rótulo a sua classificação e, quanto o acesso informação for limitado a um setor/departamento específico, o mesmo deverá ser referenciado, conforme modelos exibidos no **Anexo I** desta norma;

4.1.5. Para a rotulagem da informação, devem ser observados os modelos contidos no **Anexo I** desta norma.

4.2. **Manuseio da Informação**

4.2.1. O manuseio da informação do Departamento Estadual de Trânsito do Espírito Santo deverá obedecer às regras definidas na Tabela **Ação x Classificação**, detalhada no **Anexo II** desta norma;

4.2.2. Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas;

4.2.3. Em períodos de ausência da estação de trabalho, documentos em suporte físico devem ser retirados das mesas e de outras áreas de superfície;

4.2.4. Documentos de uso interno ou confidenciais em suporte eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas;

4.2.5. Toda não-conformidade será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

4.3. **Descarte da Informação**

4.3.1. O descarte da informação deve ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original;

4.3.2. O descarte da informação deverá ser realizado conforme os métodos estabelecidos no **Anexo III** desta norma.

5. Papéis e Responsabilidades

5.1. GESTOR DA INFORMAÇÃO

5.1.1. É responsabilidade dos colaboradores apontados como Gestor da Informação:

5.1.1.1. Definir a classificação das informações sob sua responsabilidade com base nas categorias de classificação constantes desta norma, mantendo um registro atualizado dos itens classificados;

5.1.1.2. Controlar as informações geradas em sua área de negócio e atuação;

5.1.1.3. Revisar periodicamente a classificação das informações sob sua guarda.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-001** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

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:

1.2. Rodapé

Exemplo:

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 especifico 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;

Código **N-SI-005**	**PSI – PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-005** complementa Política Geral de Segurança da Informação, definindo as diretrizes para proteção dos ativos/serviços de informação do Departamento Estadual de Trânsito do Espírito Santo contra ameaças e códigos maliciosos de qualquer natureza.

2. Propósito

2.1. Estabelecer diretrizes para a proteção dos ativos/serviços de informação Departamento Estadual de Trânsito do Espírito Santo contra ameaças e códigos maliciosos de qualquer natureza.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Ferramenta de proteção contra códigos maliciosos

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, *Worms*, *Ramsonware, Phishing*, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;

4.1.2. Apenas a ferramenta disponibilizada pela Departamento Estadual de Trânsito do Espírito Santo deve ser utilizada na proteção contra códigos maliciosos;

4.1.3. A ferramenta de proteção contra códigos maliciosos do Departamento Estadual de Trânsito do Espírito Santo adota as seguintes regras de uso:

4.1.3.1. Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;

4.1.3.2. As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;

4.1.3.3. As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

4.1.3.4. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;

4.1.3.5. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;

4.1.4. Caso uma estação de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa do Departamento Estadual de Trânsito do Espírito Santo e de qualquer comunicação com a internet;

4.1.5. Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

4.2. **Prevenção dos usuários contra códigos maliciosos**

4.2.1. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários do Departamento Estadual de Trânsito do Espírito Santo devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;

4.2.2. Os usuários do Departamento Estadual de Trânsito do Espírito Santo devem seguir as seguintes regras para proteção contra códigos maliciosos:

4.2.2.1. Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

4.2.2.2. Reportar imediatamente a área de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;

4.2.2.3. Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;

4.2.2.4. Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pelo Departamento Estadual de Trânsito do Espírito Santo antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;

4.2.2.5. Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de

segurança da informação para validar se o arquivo representa ou não uma ameaça.

5. Papéis e Responsabilidades

5.1. GERENCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da gerência de tecnologia da informação:

5.1.1.1. Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando os mesmos a equipe de segurança da informação, caso necessário.

5.2. SUBGERENCIA DE SEGURANÇA DA INFORMAÇÃO

5.2.1. É responsabilidade da subgerencia de segurança da informação:

5.2.1.1. Garantir que novas modalidades de códigos maliciosos são adequadamente investigadas, tratadas e protegidas pela ferramenta corporativa adotada pelo Departamento Estadual de Trânsito do Espírito Santo;

5.2.1.2. Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários do Departamento Estadual de Trânsito do Espírito Santo.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-005** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

9. Glossário

9.1. **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.

9.2. **Worms:** Um *Worm* é um programa semelhante aos vírus, com a diferença de este ser autorreplicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores.

9.3. **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.

9.4. **Vírus:** Em informática, um vírus de computador é um 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.

9.5. **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.)

9.6. **Códigos Maliciosos:** Código malicioso é um tipo de código de computador ou script da Web nocivo que tem como objetivo criar vulnerabilidades no sistema.

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

9.8. **Ransomware:** Ransomware é um 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.

9.9. **Malware:** Malware é um termo genérico para qualquer tipo software malicioso projetado para se infiltrar no seu dispositivo sem o seu conhecimento.

9.10. **Cavalo de Tróia:** Em computação, um cavalo de Troia é qualquer malware que enganar os usuários sobre sua verdadeira intenção.

Código **N-SI-006**	**PSI – SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-006** complementa Política Geral de Segurança da Informação, definindo as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos fornecidos pelo Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pelo Departamento Estadual de Trânsito do Espírito Santo.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Serviço de E-Mail

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

4.1.2. Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo Departamento Estadual de Trânsito do Espírito Santo;

4.1.3. Quando o usuário fizer uso do serviço de e-mail do Departamento Estadual de Trânsito do Espírito Santo não é permitido:

4.1.3.1. Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do Departamento Estadual de Trânsito do Espírito Santo;

4.1.3.2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;

4.1.3.3. Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do Departamento Estadual de Trânsito do Espírito Santo, excetuando-se quando expressamente autorizados;

4.1.3.4. Inscrever o endereço de e-mail do Departamento Estadual de Trânsito do Espírito Santo em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;

4.1.3.5. Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;

4.1.3.6. Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

4.1.3.7. Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;

4.1.3.8. Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

4.1.3.9. Usar o serviço de e-mail para o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

4.1.4. O serviço de e-mail do Departamento Estadual de Trânsito do Espírito Santo é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;

4.1.5. O monitoramento do serviço de e-mail do Departamento Estadual de Trânsito do Espírito Santo tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;

4.1.6. Durante o monitoramento o Departamento Estadual de Trânsito do Espírito Santo se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail;

4.1.7. O Departamento Estadual de Trânsito do Espírito Santo adota um padrão para criação dos endereços de E-mail sendo composto pelo primeiro nome do empregado, seguido por pontuação e seu último sobrenome, conforme exemplo a seguir:

4.1.7.1. Nome completo do empregado: José Maria da Silva;

4.1.7.2. Email: jose.silva@detran.es.gov.br;

4.1.8. Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão

adotado pelo Departamento Estadual de Trânsito do Espírito Santo, devendo primeiramente ser revisados pela equipe de tecnologia da informação.

4.1.9. Não é permitido o uso de sobrenomes de filiação na composição do endereço de e-mail como, por exemplo, tais como Junior, Filho, Neto, Segundo, Terceiro.

4.1.10. Os usuários do serviço de e-mail do Departamento Estadual de Trânsito do Espírito Santo devem adotar a assinatura padrão, formatada de acordo com o seguinte modelo:

4.1.10.1. Nome Completo
4.1.10.2. Departamento
4.1.10.3. Cargo
4.1.10.4. Telefone

4.1.11. Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:

4.1.11.1. "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."

4.2. **Serviços de Comunicadores instantâneos**

4.2.1. O Departamento Estadual de Trânsito do Espírito Santo fornece o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

4.2.2. Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não seja o oficialmente fornecido pelo Departamento Estadual de Trânsito do Espírito Santo;

4.2.3. Quando o usuário fizer uso do serviço de comunicadores instantâneos do Departamento Estadual de Trânsito do Espírito Santo, não é permitido:

4.2.3.1. Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de interesse do Departamento Estadual de Trânsito do Espírito Santo;

4.2.3.2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;

4.2.3.3. Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para pessoas ou entidades que não fazem parte do domínio corporativo do

Departamento Estadual de Trânsito do Espírito Santo, excetuando-se quando expressamente autorizados;

4.2.3.4. Fazer uso de qualquer técnica forja ou simulação de falsa identidade. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;

4.2.3.5. A interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

4.2.3.6. A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (SPAM) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de comunicadores instantâneos;

4.2.3.7. Usar o serviço de comunicadores instantâneos para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

4.2.3.8. O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, não sendo permitido o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

4.2.4. O serviço de comunicadores instantâneos do Departamento Estadual de Trânsito do Espírito Santo é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;

4.2.5. O monitoramento do serviço de comunicadores instantâneos do Departamento Estadual de Trânsito do Espírito Santo tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;

4.2.6. Durante o monitoramento o Departamento Estadual de Trânsito do Espírito Santo se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de comunicadores instantâneos.

5. Papéis e Responsabilidades

5.1. SUBGERENCIA DE INFRAESTRUTURA E SEGURANÇA DE TI

5.1.1. É responsabilidade da Subgerência de Infraestrutura e Segurança de TI:

5.1.1.1. Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pelo Departamento Estadual de Trânsito do Espírito Santo;

5.1.1.2. 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.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-006** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código **N-SI-007**	**PSI – GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-007** complementa Política Geral de Segurança da Informação, definindo as diretrizes para garantir que o acesso às aos ativos de informação ou sistemas de informação do Departamento Estadual de Trânsito do Espírito Santo garanta níveis adequados de proteção.

2. Propósito

2.1. Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação do Departamento Estadual de Trânsito do Espírito Santo.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Acesso a ativos e sistemas de informação

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;

4.1.2. As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

4.1.3. Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

4.1.4. Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

4.1.4.1. Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo Departamento Estadual de Trânsito do Espírito Santo;

4.1.4.2. Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo Departamento Estadual de Trânsito do Espírito Santo;

4.1.4.3. Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;

4.1.4.4. Informar imediatamente a equipe de segurança caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo;

4.1.5. Usuários que tem acesso autorizado a privilégios administrativas em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

4.1.6. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

4.2. **Senha de acesso**

4.2.1. As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

4.2.2. O Departamento Estadual de Trânsito do Espírito Santo adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:

4.2.2.1. A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;

4.2.2.2. As senhas possuem validade de 90 (noventa) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;

4.2.2.3. As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

4.2.2.4. As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

4.2.2.5. Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo assim por, no mínimo, 30 (trinta) minutos;

4.2.2.6. Os sistemas de informação manterão um histórico das últimas 12 (doze) senhas utilizadas, não permitindo sua reutilização;

4.2.2.7. Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da equipe de tecnologia da informação;

4.2.3. Quando criando uma nova senha, usuários devem estar atentos as seguintes recomendações:

4.2.3.1. Não utilizar nenhuma parte de sua credencial na composição da senha;

4.2.3.2. Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

4.2.3.3. Não utilizar repetição ou sequência de caracteres, números ou letras;

4.2.3.4. Qualquer parte ou variação do nome Departamento Estadual de Trânsito do Espírito Santo;

4.2.3.5. Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

4.3. **Autorização de acesso (privilégios de acesso)**

4.3.1. A autorização e o nível permitido de acesso ativos/serviços de informação do Departamento Estadual de Trânsito do Espírito Santo é feita com base em perfis que definem o nível de privilégio dos usuários.

4.3.2. O acesso à ativos/serviços de informação é fornecido a critério do Departamento Estadual de Trânsito do Espírito Santo, que define permissões baseadas nas necessidades laborais dos usuários;

4.3.3. Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas a equipe de tecnologia da informação.

4.3.4. Toda solicitação deve ser feita a partir do portal de suporte: suporte.detran.es.gov.br

4.3.5. Os usuários devem ainda observar as seguintes diretrizes:

4.3.5.1. A seu critério exclusivo, o Departamento Estadual de Trânsito do Espírito Santo poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto

(nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação ao departamento de tecnologia da informação;

4.3.5.2. É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse do Departamento Estadual de Trânsito do Espírito Santo tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

4.3.5.3. Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) do Departamento Estadual de Trânsito do Espírito Santo.

5. Papéis e Responsabilidades

5.1. **GESTOR DA INFORMAÇÃO**

5.1.1. É responsabilidade dos colaboradores apontados como Gestor da Informação:

5.1.1.1. Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;

5.1.1.2. Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;

5.1.1.3. Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade.

5.2. **DEPARTAMENTO PESSOAL**

5.2.1. É responsabilidade do departamento pessoal (Recursos Humanos):

5.2.1.1. Reportar através do sistema de suporte (suporte.detran.es.gov.br) a inclusão de novos usuários para criação de contas de acesso, utilizando formulário específico para tal.

5.2.1.2. Reportar em tempo hábil o desligamento de empregados do Departamento Estadual de Trânsito do Espírito Santo a equipe de tecnologia da informação para que contas de acesso possam ser revogadas;

5.2.1.3. Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição no Departamento Estadual de Trânsito do Espírito Santo;

5.2.1.4. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

5.3. **GESTORES**

5.3.1. É responsabilidade dos gestores e coordenadores:

5.3.1.1. Solicitar a equipe de tecnologia da informação concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;

5.3.1.2. Informar a equipe de tecnologia da informação quando ao encerramento do contrato com terceiros/prestadores de serviços contratados que tenham a ativos/sistemas de informação.

5.4. **SUBGERENCIA DE INFRAESTRUTURA E SEGURANÇA DE TI**

5.4.1. É responsabilidade da gerência de tecnologia da informação:

5.4.1.1. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de empregados, terceiros/prestadores de serviços;

5.4.1.2. Conceder, quando autorizado, o acesso aos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;

5.4.1.3. Revogar, quando solicitado, o acesso dos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;

5.4.1.4. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de empregados, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-007** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código **N-SI-008**	**PSI – INTERNET E MÍDIAS SOCIAIS**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-008** complementa Política Geral de Segurança da Informação, definindo as diretrizes para utilização segura do acesso à internet fornecido pelo Departamento Estadual de Trânsito do Espírito Santo e do comportamento de colaboradores em mídias e redes sociais.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura do acesso à internet fornecido pelo Departamento Estadual de Trânsito do Espírito Santo e do comportamento de colaboradores em mídias e redes sociais.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Acesso à internet

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;

4.1.2. O acesso à internet é fornecido través da rede corporativa do Departamento Estadual de Trânsito do Espírito Santo.

4.1.3. Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pelo Departamento Estadual de Trânsito do Espírito Santo está sujeita monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

4.1.4. Durante o monitoramento do acesso à internet, o Departamento Estadual de Trânsito do Espírito Santo se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, 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;

4.1.5. Durante o acesso à Internet fornecido pelo Departamento Estadual de Trânsito do Espírito Santo não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:

4.1.5.1. Qualquer espécie de exploração sexual;

4.1.5.2. Qualquer forma de conteúdo adulto, erotismo, pornografia;

4.1.5.3. Qualquer tipo de Pornografia infantil;

4.1.5.4. Qualquer forma de ameaça, chantagem e assédio moral ou sexual;

4.1.5.5. Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

4.1.5.6. Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

4.1.5.7. Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;

4.1.5.8. A prática e/ou a incitação de crimes ou contravenções penais;

4.1.5.9. A prática de propaganda política nacional ou internacional;

4.1.5.10. A prática de quaisquer atividades comerciais desleais;

4.1.5.11. O desrespeito a imagem ou aos direitos de propriedade intelectual do Departamento Estadual de Trânsito do Espírito Santo;

4.1.5.12. A disseminação de códigos maliciosos e ameaças virtuais;

4.1.5.13. Tentativa de expor a infraestrutura computacional do Departamento Estadual de Trânsito do Espírito Santo a ameaças virtuais;

4.1.5.14. Divulgação não autorizada de qualquer informação do Departamento Estadual de Trânsito do Espírito Santo classificada como confidencial ou de uso interno;

4.1.5.15. Uso de sites ou serviços que busquem contornar controles de acesso à internet.

4.2. **Comportamento corporativo em mídias e redes sociais**

4.2.1. A publicação de conteúdo referente ao Departamento Estadual de Trânsito do Espírito Santo em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização;

4.2.2. Quando no uso de suas mídias e redes sociais particulares, empregados, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

4.2.2.1. Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual do Departamento Estadual de Trânsito do Espírito Santo sem autorização prévia e expressa;

4.2.2.2. Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos do Departamento Estadual de Trânsito do Espírito Santo, excetuando-se os canais oficiais da empresa;

4.2.2.3. Não é permitida a publicação de conteúdo ou comentários diretamente relacionados ao Departamento Estadual de Trânsito do Espírito Santo, seus empregados, terceiros contratados e prestadores de serviço;

4.2.2.4. Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo do Departamento Estadual de Trânsito do Espírito Santo sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais;

5. Papéis e Responsabilidades

5.1. GERENCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da gerência de tecnologia da informação:

5.1.1.1. Controlar e monitorar qualquer tipo de acesso à internet fornecido pelo Departamento Estadual de Trânsito do Espírito Santo;

5.1.1.2. Reportar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso internet para a equipe de segurança da informação.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-008** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código N-SI-009	PSI – MONITORAMENTO	Emissão	Classificação Uso interno
		Versão 1.0	Aprovado por:

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-009** complementa Política Geral de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo garantindo o respeito dos usuários às regras estabelecidas na Política Geral de Segurança da Informação, bem como produzir prova de eventual violação das condições constantes da mesma, e na legislação vigente.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. **Monitoramento de ativos/serviços da informação e recursos computacionais**

4.1.1. Qualquer ativo/serviço de informação ou recurso computacional do Departamento Estadual de Trânsito do Espírito Santo, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento;

4.1.2. Todos os ativos/serviços de informação, recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, estão sujeitos à monitoração, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança dos ativos de informações, bem como segurança jurídica do Departamento Estadual de Trânsito do Espírito Santo;

4.1.3. Não há expectativa de privacidade na utilização dos ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo, incluindo a utilização da conta de e-mail corporativa, comunicadores instantâneos e navegação em sites da Internet, através da infraestrutura tecnológica do Departamento Estadual de Trânsito do Espírito Santo;

4.1.4. Todas as informações dos ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo podem ser interceptadas, gravadas, lidas, copiadas e divulgadas por, ou para, pessoas

autorizadas para finalidades oficiais, incluindo investigações criminais. Estas informações incluem dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade.

4.2. **Monitoramento do ambiente físico**

4.2.1. O Departamento Estadual de Trânsito do Espírito Santo faz o monitoramento do seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências;

4.2.2. As câmeras de filmagem estão dispostas de forma a resguardar a dignidade humana, sendo vedada a sua instalação em banheiros, lavabos e na área reservada ao atendimento médico de empregados;

4.2.3. A filmagem descrita nesta norma tem por objetivo assegurar a segurança física do ambiente do Departamento Estadual de Trânsito do Espírito Santo, bem como a sua segurança patrimonial, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, o que o usuário tem ciência expressamente neste ato;

4.2.4. As imagens captadas dentro das dependências do Departamento Estadual de Trânsito do Espírito Santo serão arquivadas conforme procedimento adotado pela instituição e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes em suas políticas e normas e/ou infração de legislação vigente;

4.2.5. O Departamento Estadual de Trânsito do Espírito Santo não permite o uso de qualquer dispositivo de gravação audiovisual dentro do seu perímetro físico, excetuando-se quando o usuário estiver formalmente autorizado.

4.3. **Aviso legal**

4.3.1. O Departamento Estadual de Trânsito do Espírito Santo faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso a ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas pelo Departamento Estadual de Trânsito do Espírito Santo, bem como do monitoramento realizado nos termos desta norma;

4.3.2. O aviso legal deverá ser exibido antes de permitir o acesso a ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo, apresentando o seguinte formato:

4.3.2.1. “Este é um ativo/serviço de informação ou recurso computacional do Departamento Estadual de Trânsito do Espírito Santo, 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 sanções cabíveis nas esferas administrativa, cível e penal, sem prejuízo das demais legislações aplicáveis. Este ativo/serviço de informação ou recurso computacional é monitorado, não havendo expectativa de privacidade na sua utilização. O acesso a este ativo/serviço de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos."

4.3.3. O acesso a qualquer ativo/serviço de informação ou recurso computacional do Departamento Estadual de Trânsito do Espírito Santo ou o uso dos mesmos por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal;

4.3.4. A ausência do aviso legal em qualquer ativo/serviço de informação ou recurso computacional do Departamento Estadual de Trânsito do Espírito Santo não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pelo Departamento Estadual de Trânsito do Espírito Santo.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO:

5.1.1.1. Realizar o monitoramento dos ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo;

5.1.1.2. Tratar eventuais violações das diretrizes de segurança do Departamento Estadual de Trânsito do Espírito Santo identificadas através de ferramentas de monitoramento, e, quando pertinente, reportar as mesmas a equipe de segurança da informação.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-009** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo

Código N-SI-010	**PSI – RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**	Emissão	Classificação Uso interno
		Versão 1.0	Aprovado por:

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-010** complementa Política Geral de Segurança da Informação, definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Incidentes de segurança da informação

4.1.1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

4.1.2. Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;

4.1.3. Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a área de segurança da informação;

4.1.4. A área de segurança da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação;

4.1.5. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança

comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;

4.1.6. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;

4.1.7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

4.2. **Time de resposta a incidentes de segurança da informação**

4.2.1. O time de resposta a incidentes de segurança da informação do Departamento Estadual de Trânsito do Espírito Santo deverá ser composto por, no mínimo, representantes das seguintes áreas:

4.2.1.1. Gerência de tecnologia da informação;

4.2.1.2. Subgerência de Infraestrutura e segurança de TI;

4.2.1.3. Gerência de recursos humanos;

4.2.1.4. Gerência jurídica.

4.2.2. Conforme a natureza do incidente, colaboradores de qualquer setor do Departamento Estadual de Trânsito do Espírito Santo podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

4.3. **Disseminação de informação sobre incidentes de segurança da informação**

4.3.1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas ao Departamento Estadual de Trânsito do Espírito Santo sem aprovação expressa e formal da diretoria.

5. Papéis e Responsabilidades

5.1. **SUBGERENCIA DE INFRAESTRUTURA E SEGURANÇA DE TI**

5.1.1. É responsabilidade da SUBGERENCIA DE INFRAESTRUTURA E SEGURANÇA DE TI:

5.1.1.1. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado

anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;

5.1.1.2. Comunicar prontamente o time de resposta a incidentes de segurança da informação do Departamento Estadual de Trânsito do Espírito Santo sobre eventos e incidentes de segurança.

5.2. **TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

5.2.1. É responsabilidade do TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

5.2.1.1. Apoiar a equipe de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;

5.2.1.2. Aconselhar a diretoria do Departamento Estadual de Trânsito do Espírito Santo sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.

5.3. **COMUNICAÇÃO**

5.3.1. É responsabilidade da GERÊNCIA DE COMUNICAÇÃO:

5.3.1.1. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-010** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código N-SI-011	**PSI – TERMO DE USO DOS SISTEMAS INTERNOS**	Emissão	Classificação Uso interno
		Versão 1.0	Aprovado por:

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

CONSIDERANDO que o Departamento Estadual de Trânsito do Espírito Santo disponibiliza a seus usuários ativos de informação e recursos computacionais exclusivamente para que os mesmos possam desempenhar suas atividades profissionais;

CONSIDERANDO que o Departamento Estadual de Trânsito do Espírito Santo é a única proprietária de todos os ativos de informação e recursos computacionais, dessa forma, sendo responsável por todos os custos com os mesmos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

CONSIDERANDO que o Departamento Estadual de Trânsito do Espírito Santo poderá ser seriamente impactado pela má utilização de seus ativos de informação e recursos computacionais;

DECLARO QUE:

1. Tenho conhecimento e acesso a Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, que se encontram disponíveis no portal corporativo (intranet.detran.es.gov.br) aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;

2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;

3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica do Departamento Estadual de Trânsito do Espírito Santo somente poderá ser utilizada para fins exclusivamente profissionais e relacionados às atividades da organização;

4. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica do Departamento Estadual de Trânsito do Espírito Santo;

5. Estou ciente que violações da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;

6. Comprometo-me a não revelar, fato ou informações de qualquer natureza a que tenha conhecimento por forças das minhas atribuições, mesmo após o encerramento do contrato de trabalho com o Departamento Estadual de Trânsito do Espírito Santo.

_____, ____ de _____ de _____

_____

Nome:

Cargo:

CPF:

Código **N-SI-012**	**PSI – USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação **N-SI-012** complementa Política Geral de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação do Departamento Estadual de Trânsito do Espírito Santo por seus usuários autorizados.

2. Propósito

2.1. Estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação do Departamento Estadual de Trânsito do Espírito Santo por seus usuários autorizados.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Uso de equipamento computacional

4.1.1. O Departamento Estadual de Trânsito do Espírito Santo fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais.

4.1.2. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do Departamento Estadual de Trânsito do Espírito Santo:

4.1.2.1. Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do Departamento Estadual de Trânsito do Espírito Santo, sendo expressamente proibida a utilização para fins particulares;

4.1.2.2. A alteração e/ou a manutenção de qualquer equipamento de propriedade do Departamento Estadual de Trânsito do Espírito Santo é uma atribuição específica do departamento de tecnologia da informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

4.1.2.3. Os equipamentos do Departamento Estadual de Trânsito do Espírito Santo devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

4.1.2.4. Computadores de mesa (*desktops*) ou móveis (*notebooks*) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

4.1.2.5. A desconexão (*log off*) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

4.1.2.6. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

4.1.2.7. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com o Departamento Estadual de Trânsito do Espírito Santo; e

4.1.2.8. Qualquer dano aos equipamentos do Departamento Estadual de Trânsito do Espírito Santo será devidamente analisado pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá ao Departamento Estadual de Trânsito do Espírito Santo exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.

4.1.3. A seu critério exclusivo o Departamento Estadual de Trânsito do Espírito Santo poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção tanto do departamento de tecnologia da informação, quanto da área de segurança da informação de forma a garantir adequação aos requisitos e controles de segurança adotados pela autarquia.

4.1.4. Não é permitida a conexão de equipamentos particulares na rede administrativa do Departamento Estadual de Trânsito do Espírito Santo, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento tanto do departamento de tecnologia da informação, quanto da área de segurança da informação.

4.2. **Dispositivos de Armazenamento Removível**

4.2.1. O Departamento Estadual de Trânsito do Espírito Santo poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes:

4.2.1.1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

4.2.1.2. Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos;

4.2.1.3. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de tecnologia da informação e é obrigatória para todos os equipamentos corporativos; e

4.2.1.4. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente o departamento de segurança patrimonial para que possam ser tomadas as medidas cabíveis.

4.3. **Armazenamento remoto (nuvem)**

4.3.1. O Departamento Estadual de Trânsito do Espírito Santo disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa;

4.3.2. Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela autarquia e homologada pela equipe de segurança da informação do Departamento Estadual de Trânsito do Espírito Santo.

4.4. **Identificação digital**

4.4.1. O Departamento Estadual de Trânsito do Espírito Santo poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:

4.4.1.1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

4.4.1.2. O usuário deverá informar a equipe de segurança da informação sobre qualquer evento ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

4.4.1.3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela Departamento Estadual de Trânsito do Espírito Santo imediatamente revogado;

4.4.1.4. É de responsabilidade da área de segurança da informação prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.

4.5. **Equipamentos de impressão e reprografia**

4.5.1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do Departamento Estadual de Trânsito do Espírito Santo ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

4.5.2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:

4.5.2.1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações do Departamento Estadual de Trânsito do Espírito Santo, classificadas como de uso interno ou confidencial;

4.5.2.2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

4.5.2.3. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pelo Departamento Estadual de Trânsito do Espírito Santo.

4.6. **Segurança física**

4.6.1. As instalações de processamento das informações do Departamento Estadual de Trânsito do Espírito Santo serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

4.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

4.6.2.1. Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

4.6.2.2. Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores do Departamento Estadual de Trânsito do Espírito Santo;

4.6.2.3. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

4.6.2.4. É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis do Departamento Estadual de Trânsito do Espírito Santo;

4.6.2.5. É resguardado ao Departamento Estadual de Trânsito do Espírito Santo o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;

4.6.2.6. É resguardado ao Departamento Estadual de Trânsito do Espírito Santo o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;

4.6.2.7. Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados organização;

4.6.2.8. Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.

5. Papéis e Responsabilidades

5.1. SUBGERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade da Subgerência de Segurança da Informação:

5.1.1.1. Estabelecer e manter atualizados os procedimentos complementares a esta norma;

5.1.1.2. Comunicar ao CGSI eventuais tentativas, bem-sucedidas ou não, de desvio de conduta dos termos dessa norma.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-012** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código N-SI-013	PSI – GESTÃO DE AMBIENTES DE COMPUTAÇÃO EM NUVEM	Emissão	Classificação Uso interno
		Versão 1.0	Aprovado por:

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

1. Introdução

1.1. A Norma de segurança da informação N-SI-013 complementa Política Geral de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do Departamento Estadual de Trânsito do Espírito Santo.

2. Propósito

2.1. Estabelecer diretrizes para contratação e gestão de ambientes de computação em nuvem do Departamento Estadual de Trânsito do Espírito Santo.

3. Escopo

3.1. Esta Norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. O Departamento Estadual de Trânsito do Espírito Santo deve assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas nessa Norma, especialmente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplam a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem.

4.2. O Departamento Estadual de Trânsito do Espírito Santo previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, deve adotar procedimentos que contemplem:

4.2.1. a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

4.2.2. a verificação da capacidade do potencial prestador de serviço de assegurar:

4.2.2.1. o cumprimento da legislação e da regulamentação em vigor;
4.2.2.2. o acesso do Departamento Estadual de Trânsito do Espírito Santo aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
4.2.2.3. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
4.2.2.4. a sua aderência a certificações exigidas pelo Departamento Estadual de Trânsito do Espírito Santo para a prestação do serviço a ser contratado;
4.2.2.5. o acesso do Departamento Estadual de Trânsito do Espírito Santo aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
4.2.2.6. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
4.2.2.7. a identificação e a segregação dos dados dos clientes do Departamento Estadual de Trânsito do Espírito Santo por meio de controles físicos ou lógicos; e
4.2.2.8. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do Departamento Estadual de Trânsito do Espírito Santo.

4.2.3. Na avaliação da relevância do serviço a ser contratado, mencionada no item 4.2.1, o Departamento Estadual de Trânsito do Espírito Santo deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

4.2.4. No caso da execução de aplicativos por meio da internet, o Departamento Estadual de Trânsito do Espírito Santo deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

4.2.5. O Departamento Estadual de Trânsito do Espírito Santo deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos providos nos termos do item 4.2.2.6.

5. Definição de Serviços

5.1. Para os fins do disposto nesta norma, os serviços de computação em nuvem abrangem a disponibilidade ao Departamento Estadual de Trânsito

do Espírito Santo, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

5.1.1. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam ao Departamento Estadual de Trânsito do Espírito Santo implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pelo órgão ou por ele adquiridos;

5.1.2. implantação ou execução de aplicativos desenvolvidos pelo Departamento Estadual de Trânsito do Espírito Santo, ou por ele adquiridos, utilizando recursos computacionais do prestador de serviços; ou

5.1.3. execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

6. Contratação

6.1. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

6.1.1. a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

6.1.2. a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no item 6.1.1;

6.1.3. a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

6.1.4. a obrigatoriedade, em caso de extinção do contrato, de:

6.1.4.1. transferência dos dados citados no item 6.1.1 ao novo prestador de serviços ou ao Departamento Estadual de Trânsito do Espírito Santo; e

6.1.4.2. exclusão dos dados citados no item 6.1.1 pela empresa contratada substituída, após a transferência dos dados prevista no item 6.1.4.1 e a confirmação da integridade e da disponibilidade dos dados recebidos;

6.1.5. o acesso do Departamento Estadual de Trânsito do Espírito Santo a:

6.1.5.1. informações fornecidas pela empresa contratada, visando verificar o cumprimento do disposto nos itens 6.1.1, 6.1.2 e 6.1.3;

6.1.5.2. informações relativas às certificações e aos relatórios de auditoria especializada, citados nos itens 4.2.2.4 e 4.2.2.5; e

6.1.5.3. informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no item 4.2.2.6;

6.1.6. a obrigação de a empresa contratada notificar o Departamento Estadual de Trânsito do Espírito Santo sobre a subcontratação de serviços relevantes para a instituição;

6.1.7. a obrigação de a empresa contratada manter o Departamento Estadual de Trânsito do Espírito Santo permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

7. Sanções e Punições

7.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

8. Revisões

8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

9. Gestão da Norma

9.1. A norma N-SI-013 é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria do Departamento Estadual de Trânsito do Espírito Santo.

Código **P-SI-001**	**PSI – TERMO DE CONFIDENCIALIDADE**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

CONTRATO: XXXX

EMPRESA CONTRATADA:

RESPONSÁVEL:

Eu _____, nacionalidade, estado civil, profissão, inscrito(a) no CPF n xxx.xxx.xxx-xx,

Abaixo firmado, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas e outras relacionadas à prestação de serviços para o Departamento Estadual de Trânsito do Espirito Santo, a que tiver acesso durante a Execução dos Serviços, conforme o artigo 5º do Decreto Estadual nº 2830-R/2011, como segue: "...Observar as normas da Política de Segurança e da Política da Qualidade do CONTRATANTE, dentre as quais: Manter, por tempo indeterminado ou até autorização em contrário do CONTRATANTE, a devida confidencialidade, requerida ou não, de quaisquer dados e/ou informações pertencentes ao DETRAN ou por ele tratados ou custodiados e aos quais a CONTRATADA e seus representantes terão acesso ou conhecimento, incluindo aqueles relativos aos negócios existentes ou em desenvolvimento pelas partes, seja verbalmente, por escrito ou visualmente (inclusive mantendo sigilo interno, quando aplicável, necessário ou solicitado), não os comercializando, reproduzindo, cedendo ou divulgando para pessoas não autorizadas a acessá-los ou conhece-los, no todo ou em parte, direta ou indiretamente, sejam quais forem os meios ou formas utilizados – exceto quando necessário, justificável e autorizado pelo CONTRATANTE; Cumprir e fazer cumprir por seus representantes, a qualquer tempo, os controles da PSI (Política de Segurança da Informação) do DETRAN|ES que sejam aplicáveis e/ou que possuam correlação direta ou indireta com a presente contratação, incluindo aqueles afetos à execução do objeto do presente contrato, desde que os mesmos e suas alterações sejam fornecidos à CONTRATADA ou informados à mesma pelo gestor do contrato, via divulgação através de canais aos quais a CONTRATADA tenha acesso e/ou conforme estabelecido contratualmente (se aplicável);...".

Por este Termo de Confidencialidade compromete-se:

1. a não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para uso de terceiros;

2. a não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso relacionada à prestação de serviço acima mencionada;

3. a não se apropriar para si ou para outrem de material confidencial e/ou sigiloso que venha a ser disponível através da prestação de serviço ora mencionada;

4. a não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

5. a garantir que as informações confidenciais serão utilizadas apenas para o propósito deste projeto e que serão divulgadas apenas para seus colaboradores envolvidos respeitando o princípio do privilégio mínimo.

6. a CONTRATADA concorda que todas as informações sigilosas permanecem como propriedade da CONTRATANTE e que este pode utilizá-las para qualquer propósito sem nenhuma obrigação para com a CONTRATADA.

7. a CONTRATADA concorda que todos os resultados dos trabalhos prestados por ela à CONTRATANTE, inclusive os decorrentes de especificações técnicas, desenhos, criações ou aspectos particulares dos serviços prestados, são reconhecidos, irrestritamente, neste ato, como de exclusiva propriedade da CONTRATANTE, não podendo a CONTRATADA reivindicar qualquer direito inerente à propriedade intelectual.

8. a CONTRATADA concorda ter ciência de que este acordo ou qualquer informação sigilosa entregue pela CONTRATANTE a ela, não poderá ser interpretado como concessão a qualquer direito ou licença relativa à propriedade intelectual à CONTRATADA.

A vigência da obrigação de confidencialidade assumida por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público pelo poder público, ou ainda, mediante autorização escrita, concedida pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Código **P-SI-002**	**PSI – RELATÓRIO DE IMPACTO A PROTEÇÃO DE DADOS PESSOAIS**	**Emissão**	**Classificação** **Uso interno**
		Versão **1.0**	**Aprovado por:**

Controle do Documento			
Nome:	**Ação:**	**Cargo:**	**Contato:**
Carlos Augusto Diniz	Criação	Subgerente de Infraestrutura e Segurança de TI (SGIS)	carlos.diniz@detran.es.gov.br
Luiz Antônio Uchoa da Silva	Revisão	Gerente de TI (GTI)	luiz.uchoa@detran.es.gov.br

Sumário

1. Introdução

Este Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) permitirá analisar de forma sistemática e completa como o seu projeto ou sistema impactará a privacidade dos titulares afetados pelo tratamento de seus dados pessoais.

Este modelo foi projetado para incorporar os requisitos legais da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

Este relatório tem por objetivo:

- Demonstrar proativamente a Autoridade Nacional de Proteção de Dados (ANPD) que o tratamento de dados pessoais realizado pelo Departamento Estadual de Trânsito do Espírito Santo está em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD);
- Identificar possíveis riscos à proteção dos Dados Pessoais tratados e proativamente minimizá-los através da seleção e aplicação dos controles necessários.

A realização do RIPDP é um requisito legal sob a LGPD, principalmente se o processamento proposto estiver usando novas tecnologias e representar um alto risco para os dados pessoais dos titulares.

Uma pré-avaliação deve ser realizada para identificar se essa avaliação completa é ou não necessária.

2. Sumário do Projeto

Informações básicas do Projeto:							
ID:		**Nome:**					
Descrição em alto nível:							
Diretoria:							
Patrocinadores							
Nome:				**Cargo**			
Nome:				**Cargo**			
Nome:				**Cargo**			
Gerente do Projeto							
Nome:				**Cargo**			
Cronograma macro:							
Data início:		**Data conclusão:**			**Situação:**		

Informações adicionais:		
Existem terceiros envolvidos ou associados ao projeto:	**Sim**	**Não**
Este RIPDP cobre múltiplos projetos:	**Sim**	**Não**

Observações:

3. Questionário de validação do RIPDP

Essas perguntas têm como objetivo validar se um RIPDP é necessário.

Responder "**sim**" a qualquer uma dessas perguntas é uma indicação de que um RIPDP deve ser realizado. É importante concluir o RIPDP para projetos que já estão em execução, onde as perguntas de triagem podem ser aplicadas.

Importante: Conforme o andamento do projeto, especialmente quando ocorrerem mudanças significativa no escopo, pode ser necessário revalidar respostas.

Instruções:		
▪ Para todas as perguntas abaixo marque "**sim**" ou "**não**"; ▪ Todas as perguntas precisam ser respondidas; ▪ Em caso de dúvidas, entre em contato com o **Encarregado pelo Tratamento de Dados Pessoais (DPO)**.		
Pergunta:	**Sim**	**Não**
1. Será realizado o tratamento de qualquer tipo de Dados Pessoais em larga escala?		
2. Será realizado o tratamento de dados pessoais sensíveis dos titulares, incluindo informações 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?		
3. Será realizado o tratamento Dados pessoais sobre indivíduos vulneráveis?		
4. Será realizado o monitoramento sistemático de titulares de dados pessoais?		
5. O projeto incluirá a avaliação (Perfilização) ou pontuação (*Scoring*) dos titulares de dados pessoais?		
6. Conjuntos de dados pessoais serão combinados ou enriquecidos?		
7. Existe possibilidade de que o tratamento de dados pessoais pretendido impeça que titulares exerçam um direito ou usem um serviço ou contrato?		
8. Existirá transferência de dados pessoais para fora do território nacional brasileiro?		
9. Durante o tratamento Dados pessoais será empregado soluções tecnológicas ou organizacionais inovadoras?		
10. O projeto incluirá o uso de Dados Pessoais para tomada de decisão automatizada com efeito legal ou significativamente similar?		

Importante: Se você respondeu "**sim**" a pelo menos um dos itens acima, siga para as próximas etapas do RIPDP. Caso tenha respondido "não" para todas as perguntas, não é necessário realizar o RIPDP, mas arquive esse formulário como evidência de sua análise.

4. Relatório de Impacto à Proteção de Dados Pessoais (RIPDP)

Etapa 1: Identificação da necessidade do RIPDP
▪ Explique o que o projeto pretende alcançar, quais serão os benefícios para o Departamento Estadual de Trânsito do Espírito Santo, para os titulares e para outras partes interessadas. ▪ Caso necessário vincule outros documentos relevantes relacionados ao projeto, por exemplo, uma proposta de projeto. ▪ Resuma também porque a necessidade de um RIPDP foi identificada com base nas suas respostas do questionário de validação do RIPDP.

Etapa 2: Descrição do tratamento de Dados Pessoais
Etapa 2.1: Descreva a natureza do tratamento dos Dados Pessoais ▪ Explique como os Dados Pessoais são coletados, usados, armazenados e excluídos; ▪ Detalhe todas as fontes dos Dados Pessoais; ▪ Explique todos os casos em que Dados Pessoais são compartilhados, incluindo com quem o dado é compartilhado, seu tipo, e qual o motivo do compartilhamento; ▪ Informe se existem tipos de tratamento de Dados Pessoais identificados como de alto risco provável; ▪ Inclua o um diagrama de fluxo de Dados Pessoais ou outra maneira de descrever fluxos de Dados Pessoais. .

Etapa 2: Descrição do tratamento de Dados Pessoais

Etapa 2.2: Descreva o escopo do tratamento dos Dados Pessoais

Por favor informe:

- A natureza dos Dados Pessoais tratados no projeto;
- Se ocorre o tratamento de Dados Pessoais sensíveis;
- O volume estimado de Dados Pessoais coletados e usados;
- A frequência pretendida de coleta de Dados Pessoais;
- O período de retenção pretendido para os Dados Pessoais;
- Uma estimativa de quantos titulares são afetados pelo tratamento;
- A área geográfica abrangida no tratamento.

Etapa 2: Descrição do tratamento de Dados Pessoais
Etapa 2.3: Descreva o contexto do tratamento dos Dados Pessoais Por favor informe: ▪ Qual é a natureza do relacionamento do Departamento Estadual de Trânsito do Espírito Santo com os titulares de Dados Pessoais? ▪ Qual o nível de controle os titulares terão sobre seus Dados Pessoais tratados? ▪ Os titulares já esperam que o Departamento Estadual de Trânsito do Espírito Santo faça esse tipo de tratamento de Dados Pessoais? ▪ Dentre os titulares de Dados Pessoais se incluem crianças ou outros grupos vulneráveis? ▪ Existem preocupações anteriores ou falhas de segurança já relatadas nesse tipo de tratamento? ▪ O tratamento realizado no Dados Pessoais é considerado inovador ou usa tecnologias inovadoras? ▪ Qual é o estado atual da tecnologia empregada no tratamento dos Dados Pessoais? ▪ Existem questões atuais de interesse público que precisam ser consideradas para este tratamento? O código de conduta ou as certificações do Departamento Estadual de Trânsito do Espírito Santo são relevantes para este tratamento?

Etapa 2: Descrição do tratamento de Dados Pessoais
Etapa 2.4: Descreva o propósito do tratamento dos Dados Pessoais Por favor informe: ▪ Quais os objetivos do Departamento Estadual de Trânsito do Espírito Santo no tratamento destes Dados Pessoais? ▪ Qual é o efeito pretendido sobre os titulares dos Dados Pessoais tratados? ▪ Quais são os benefícios do tratamento para o Departamento Estadual de Trânsito do Espírito Santo em um contexto geral?

Etapa 3: Consulta as partes relevantes para o tratamento de Dados Pessoais
Por favor informe: ▪ Como e quando o Departamento Estadual de Trânsito do Espírito Santo buscou as opiniões dos titulares para o tratamento dos seus Dados Pessoais? Caso isso não tenha sido feito, justifique por que não foi necessário fazê-lo. ▪ Foram consideradas áreas ou diretorias do Departamento Estadual de Trânsito do Espírito Santo para validar o tratamento pretendido para os Dados Pessoais? ▪ Existiu a necessidade de pedir ajuda ou informações aos operadores que realizam tratamento de Dados Pessoais em nome do Departamento Estadual de Trânsito do Espírito Santo? ▪ O Departamento Estadual de Trânsito do Espírito Santo consultou especialistas em Segurança da Informação ou outros especialistas para validar o tratamento pretendido para os Dados Pessoais?

Etapa 4: Descrição das medidas de conformidade e proporcionalidade para o tratamento de Dados Pessoais
Por favor informe: ▪ Qual são as bases legais usadas pelo Departamento Estadual de Trânsito do Espírito Santo para este tratamento de Dados Pessoais? ▪ Como o Departamento Estadual de Trânsito do Espírito Santo garante que o tratamento dos Dados Pessoais realmente alcança seu objetivo? ▪ Foi validado se existe outra maneira de alcançar o mesmo resultado sem a realização deste tratamento? ▪ Como o Departamento Estadual de Trânsito do Espírito Santo pretende segregar funções conflitantes durante o tratamento de Dados Pessoais? ▪ Como o Departamento Estadual de Trânsito do Espírito Santo pretende garantir a qualidade e a minimização dos dados? ▪ Que informação o Departamento Estadual de Trânsito do Espírito Santo dará aos titulares a respeito do tratamento de seus Dados Pessoais? ▪ Como o Departamento Estadual de Trânsito do Espírito Santo ajudará a apoiar os direitos dos titulares? ▪ Que medidas o Departamento Estadual de Trânsito do Espírito Santo pretende tomar para garantir a conformidade dos operadores envolvidos no tratamento? ▪ Como o Departamento Estadual de Trânsito do Espírito Santo pretende proteger Dados Pessoais durante transferências internacionais?

Etapa 5: Identificação, análise e avaliação dos riscos no tratamento de Dados Pessoais

Instruções:

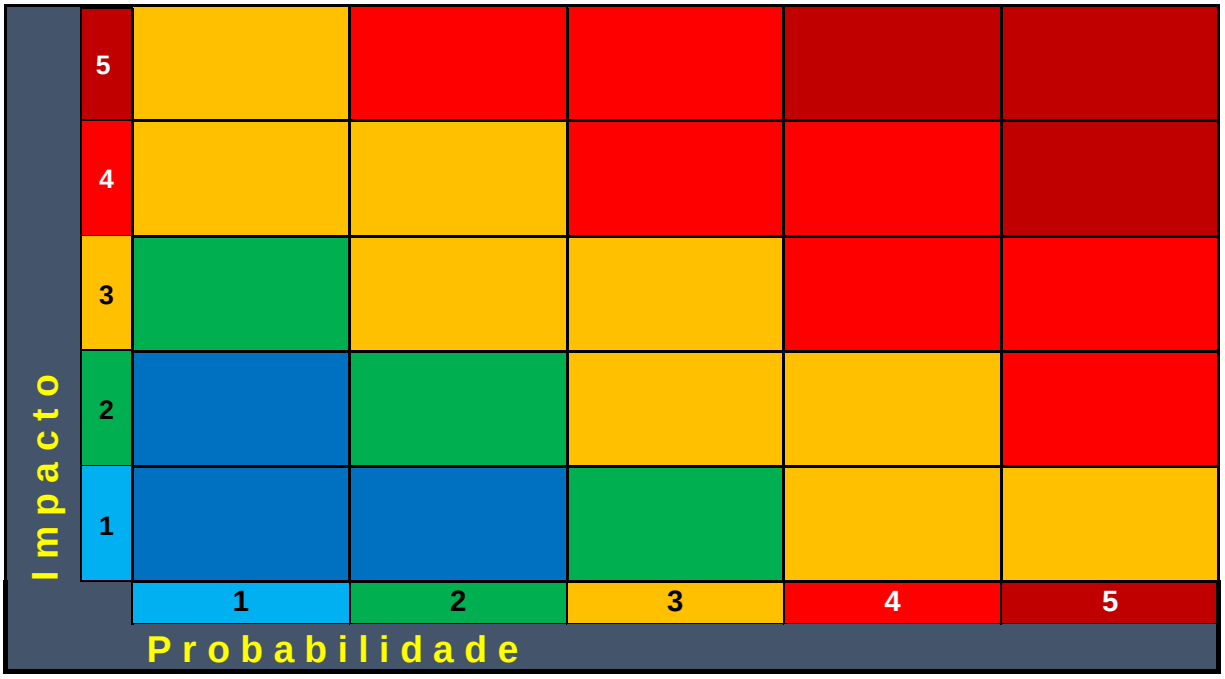
- **IDR:** Identificador único do risco;
- **Descrição:** Detalhamento básico do risco;
- **Probabilidade:** Probabilidade associada de ocorrência do evento causador do risco;
- **Impacto:** consequências da concretização do risco
- **Risco:** Combinação da Probabilidade e Impacto do evento gerador do risco.

Para a análise da Probabilidade, Impacto e Nível de Risco use os níveis:

Probabilidade		Impacto	
Nível	**Descrição**	**Nível**	**Descrição**
Muito baixa	Possibilidade remota de ocorrência	**Muito baixo**	Pouco ou nenhum impacto para titulares
Baixa	Ocorrência improvável	**Baixo**	Impacto não tem efeitos relevantes para titulares
Média	Ocorrência é provável	**Médio**	Impacto com efeitos relevantes para titulares
Alta	Ocorrência altamente provável	**Alto**	Impacto inaceitável para titulares
Muito alta	Ocorrência praticamente certa	**Muito alto**	Impacto catastrófico para titulares

IDR	Descrição	Probabilidade	Impacto	Nível do Risco

Etapa 5: Identificação, análise e avaliação dos riscos no tratamento de Dados Pessoais
Preencha a matriz de riscos abaixo usando o IDR e Nível de Risco:



Etapa 6: Identificação das medidas usadas para tratar os riscos no tratamento de Dados Pessoais

Instruções:

- **IDR:** Identificador único do risco;
- **Descrição:** Descreva a medida ou controle que será utilizado para tratamento do risco;
- **Estratégia:** Descreva qual estratégia de tratamento de risco a medida ou controle implementa (Reduzir, Evitar, Transferir, Aceitar);
- **Aprovado:** Informe se a medida ou controle foi aprovado.

IDR	Descrição da medida ou controle	Estratégia	Risco residual	Estado

Etapa 7: Assinatura e registro dos resultados e conclusões do RIPDP
Instruções: ▪ Preencha todos os campos abaixo. Nenhum item poderá ser deixado sem resposta.

Recomendações do Encarregado pelo Tratamento de Dados Pessoais:		
Nome completo	**Assinatura**	**Data**

Recomendações do Encarregado pelo Tratamento de Dados Pessoais aceitas ou negadas por:		
Nome completo	**Assinatura**	**Data**
Caso as recomendações do Encarregado pelo Tratamento de Dados Pessoais tenham sido negadas justifique:		

Controles ou medidas para tratamento de Riscos no Tratamento de Dados Pessoais aceitos ou negadas por:			
Nome completo	**Cargo**	**Assinatura**	**Data**
Caso Controles ou medidas não tenham sido aceitos justifique:			

Etapa 7: Assinatura e registro dos resultados e conclusões do RIPDP
Instruções: ▪ Preencha todos os campos abaixo. Nenhum item poderá ser deixado sem resposta.

Validade deste RIPDP:	
Este RIPDP será revisado por:	

Este Relatório de Impacto a Proteção de Dados Pessoais foi revisado e aprovado por:			
Nome completo	**Cargo**	**Assinatura**	**Data**

Registro das operações de tratamento de Dados Pessoais

v 1.0

Informações básicas do Controlador				CONTROLE DE VERSÃO	
Nome e detalhes de contato		**Encarregado pelo Tratamento de Dados Pessoais**			
Controlador		**Nome / Sobrenome**		**Elaborado por**	
Endereço		**Endereço**		**Aprovado por**	
E-mail		**E-mail**		**Data de elaboração**	
Telefone		**Telefone**		**Validade**	

INFORMAÇÕES OBRIGATÓRIAS

Responsável pelo preenchimento		Dados Pessoais tratados			Duração do
Nome e sobrenome	**Departamento**	**Finalidade específica de tratamento (Propósito)**	**Dados Pessoais tratados**	**Forma do tratamento**	**Prazo de retenção**
Carlos Augusto Diniz	TI	Folha de Pagamento	Nome/Sobrenome RG CPF Título Eleitoral Certificado Militar PIS/Pasep Carteira de Trabalho Certidão de Nascimento ou de Casamento Filiação Sexo Data de Nascimento Nacionalidade Naturalidade Estado Civil Escolaridade Endereço residencial Certidão de Nascimento de dependentes (benefícios e imposto de renda) Cargo Remuneração CBO do Cargo Regime Trabalhista Categoria e Tipo de Vínculo Empregatício	Calcular e creditar remunerações e benefícios dos empregados usando a solução **xxxxxxxxx**	10 anos

tratamento	Compartilhamento		Identificação da base legal	Transferência Internacional de Dados Pe	
Existe descarte após prazo de retenção?	**Com quem os Dados Pessoais são compartilhados?**	**Qual a finalidade específica do compartilhamento?**	**Qual a base legal usada para tratamento dos Dados Pessoais?**	**Existe transferência internacional de Dados Pessoais?**	**Para qual país Dados Pessoais são transferidos?**
Não	Fornecedor do Software	Realizar o calculo da folha de pagamento em solução online	**Cumprimento de Obrigação Legal** (Calculo da Folha de pagamento dos empregados)	Não	Não

essoais	Natureza dos Dados Pessoais Tratados			Detalhes sobre titulares	
Controles para transferências excepcionais de Dados Pessoais para países terceiros ou organizações internacionais (se aplicável)	**Categorias de Dados Pessoais tratados**	**São tratados dados de crianças e adolescentes?**	**Há tratamento de dados adicionais que podem representar risco para titulares (e.g. dados financeiros)?**	**Quem são os titulares?**	**Qual a natureza do relacionamento com os titulares?**
Não	Dados pessoais comuns	Sim. Certidão de Nascimento de dependentes (benefícios e imposto de renda) pode incluir crianças e adolescentes.	Sim. Dados de contato e Remuneração (Risco de Fraude / Roubo de Identidade)	Empregados / Dependentes de empregados	Empregador >> Empregado

	INFORMAÇÕES COMPLEMENTARES				
	Detalhes do Operador		Segurança da Informação		Interesse
Como os Dados Pessoais são coletados (fonte)?	Operador	Encarregado do Operador (contato)	Medidas de Segurança da Informação adotadas (técnicas e administrativas)	Responsável	Interesses legítimos do controlador para o tratamento de DP (se aplicável)
Dados são coletados através do sistema xxx, do Contrato de Trabalho e da Recepção de documentos do Titular durante fases iniciais da contratação					

legítimo	Direitos do Titular	Decisão automatizada		Consentimento		Localização dos
Relatório de avaliação de interesses legítimos (se aplicável)	Direitos disponíveis para titulares neste tratamento	Existe de tomada de decisão automatizada neste tratamento?	Critérios e procedimentos utilizados para a decisão automatizada (se aplicável)	Este tratamento de Dados Pessoais é realizado com base no consentimento?	Onde o consentimento é registrado? (se aplicável)	Local de armazenamento

Dados Pessoais	Relatório de Impacto a Proteção de Dados Pessoais			Incidentes e violações de Dados Pessoais	
Forma de armazenamento	Foi identificada a necessidade de se realizar um RIPDP?	Status do RIPDP (se aplicável)	Local de armazenamento do RIPDP (se aplicável)	Existe histórico de incidente ou violação de Dados Pessoais?	Registro da violação de Dados Pessoais