

Norma de Retenção e Descarte de Dados

Compromissos da Trucks Control com o tempo de guarda, o arquivamento e a eliminação segura dos dados tratados em seus produtos e serviços de rastreamento, telemetria e gestão de frotas.

Campo	Conteúdo
Código	NO-SI-003
Versão	1.0
Classificação	Público
Tipo de documento	Norma
Área responsável	Segurança da Informação
Público destinatário	Clientes contratantes, usuários dos sistemas e titulares de dados pessoais
Data de publicação	11/09/2026
Próxima revisão	Anual ou antes, em caso de mudança legal, contratual ou tecnológica relevante
Canal de privacidade	lgpd@tcsat.com.br
Canal de incidentes	csi@tcsat.com.br

1. Objetivo

Esta norma tem por objetivo tornar públicos os critérios adotados pela Trucks Control para definir por quanto tempo os dados são mantidos, o que ocorre quando esse prazo termina e como a eliminação é executada, validada e comprovada, assegurando que a guarda seja limitada ao necessário e que o descarte seja seguro, rastreável e irreversível.

A Trucks Control trata dados para operar soluções de rastreamento, telemetria, videomonitoramento e gestão de frotas. Esses dados sustentam a prestação do serviço, a segurança das operações dos clientes e o cumprimento de obrigações legais e contratuais. Guardar dados por tempo indeterminado aumenta o risco para todos os envolvidos, motivo pelo qual a retenção controlada é tratada como requisito de negócio e não apenas como exigência regulatória.

1.1 Compromisso com a legalidade e com as normas aplicáveis

A Trucks Control assume o compromisso de cumprir integralmente a legislação, as normas técnicas e os regulamentos aplicáveis à sua atividade, bem como as obrigações contratuais assumidas com clientes, parceiros e fornecedores. Esse compromisso alcança de forma expressa a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, a Lei nº 12.965/2014, Marco Civil da Internet, e as resoluções da Autoridade Nacional de Proteção de Dados, entre elas a Resolução CD/ANPD nº 15/2024.

Havendo exigência legal, regulatória ou contratual mais restritiva do que o previsto neste documento, prevalece a exigência mais restritiva.

1.2 O que você encontra aqui

- Os critérios usados para definir prazos de retenção.
- A tabela de prazos de referência por categoria de dado.
- O que ocorre ao final do prazo e em quais situações a eliminação é suspensa.
- Como a eliminação é executada, validada e evidenciada, inclusive quando envolve fornecedores e serviços em nuvem.
- Como solicitar informações, eliminação ou devolução de dados.

2. Escopo e abrangência

Esta norma aplica-se a todos os dados criados, coletados, recebidos, acessados, transmitidos, armazenados, processados, arquivados ou eliminados pela Trucks Control, independentemente do formato, do local ou da tecnologia utilizada. Não há exceção por formato ou por ambiente: planilhas, mensagens, arquivos locais, backups, ambientes de teste e documentos impressos seguem as mesmas regras.

2.1 Dimensões de abrangência

Dimensão	Abrangência
Categorias de dados	Dados cadastrais e contratuais de clientes e usuários; dados pessoais de titulares, incluindo condutores; dados de veículos, placas, localização, telemetria, eventos e comandos; imagens de videomonitoramento; registros de acesso e de segurança; dados financeiros, fiscais e de fornecedores.
Ambientes	Sistemas e serviços prestados aos clientes, centros de dados, ambientes em nuvem, integrações e interfaces de programação, estações de trabalho, dispositivos móveis, mídias, plataformas de colaboração e documentos físicos.
Pessoas alcançadas	Colaboradores, administradores, estagiários, temporários, prestadores, fornecedores, parceiros e terceiros que tratem dados em nome da Trucks Control, todos vinculados às mesmas obrigações de retenção e descarte.
Destinatários do documento	Clientes contratantes, usuários dos sistemas e titulares de dados pessoais, que podem consultar esta norma para compreender prazos, destinações e canais de solicitação.

2.2 Os dois papéis da Trucks Control

O tempo de guarda e a decisão sobre a eliminação dependem do papel exercido pela Trucks Control em cada tratamento.

Papel	O que significa na prática
Controladora	A Trucks Control define as finalidades e os meios do tratamento, por exemplo em dados cadastrais de contratantes, registros fiscais, dados de fornecedores e comunicações institucionais. Nesses casos, os prazos desta norma são aplicados diretamente.
Operadora	A Trucks Control trata dados em nome do cliente contratante, que atua como controlador, por exemplo dados de veículos, rotas, condutores, eventos e telemetria. Nesses casos, a norma de retenção e descarte de dados é o padrão para todos os contratos dos serviços ofertados.

Importante para titulares. Quando os dados forem tratados em nome de um cliente contratante, a Trucks Control não responde diretamente ao titular sem seguir o fluxo contratual e a orientação do controlador. A solicitação continua sendo recebida e encaminhada, conforme descrito na seção 9.

3. Princípios que orientam a retenção e o descarte

Nenhum dado permanece no ambiente da Trucks Control sem finalidade, responsável identificado, classificação, local de armazenamento definido e regra de retenção compatível com o risco. A partir dessa regra central, aplicam-se os princípios abaixo.

Princípio	Aplicação
Finalidade e necessidade	São coletados e utilizados somente os dados adequados, relevantes e necessários para finalidade legítima, informada e autorizada.
Retenção controlada	Os dados são mantidos pelo prazo legal, contratual ou de negócio aprovado, e eliminados de forma segura ao final.
Minimização	Cópias, campos, exportações e exposição são reduzidas ao mínimo necessário, com separação entre ambientes, clientes e finalidades incompatíveis.
Responsabilidade definida	Todo conjunto de dados possui um responsável de negócio e um responsável técnico identificados, encarregados de decidir e executar a retenção e o descarte.
Rastreabilidade	Operações relevantes produzem registros suficientes para auditoria, investigação e prestação de contas, inclusive as eliminações.
Proteção desde a concepção	Requisitos de segurança e privacidade são incorporados desde a aquisição, o projeto ou a mudança, com configurações restritivas como padrão.

4. Como os prazos são definidos

Cada categoria de dado possui um prazo registrado na Matriz de Retenção de Dados da Trucks Control. A definição desse prazo considera, de forma combinada:

- Obrigação legal ou regulatória aplicável;
- O contrato firmado com o cliente e a instrução válida do cliente controlador;
- Prazos de prescrição e necessidade de defesa de direitos;
- Requisitos de continuidade do serviço e de recuperação;
- Valor legítimo do dado para o negócio e para a operação do cliente;
- Risco associado à manutenção do dado.

Para os dados dos sistemas e serviços comercializados pela Trucks Control, adota-se como referência operacional o prazo de cinco anos, ressalvado prazo legal ou contratual superior ou prazo específico aprovado na Matriz de Retenção.

Esse prazo de referência não se aplica automaticamente a todas as categorias. Logs, documentos fiscais e trabalhistas, registros de segurança, imagens de videomonitoramento, backups e dados pessoais podem exigir tratamento distinto, conforme a tabela da seção 5.

Regra de prevalência. Havendo conflito entre esta norma, o contrato, uma obrigação legal ou regulatória aplica-se sempre o requisito mais restritivo, com registro formal da decisão e participação das áreas de Segurança da Informação e Jurídico ou do Encarregado da Proteção de Dados, conforme a natureza do dado.

5. Tabela de prazos de retenção

A tabela consolida os prazos de referência adotados pela Trucks Control. Um mesmo sistema pode conter categorias de dados com prazos diferentes, e cada linha é detalhada na Matriz de Retenção oficial.

Categoria de dados	Finalidade e exemplos	Prazo de referência	Termo inicial e exceções
Cadastrais e contratuais de clientes e usuários	Identificação, contato, prestação de serviços, contrato, solicitações e relacionamento.	Durante a relação e, em regra, até 5 anos após o término.	Contados do encerramento da relação. A ampliação ocorre somente por obrigação legal ou defesa de direitos documentada.
Financeiros, fiscais e de faturamento	Pagamentos, cobrança, dados bancários necessários, notas fiscais, boletos e conciliação.	Prazo legal aplicável, em regra 5 anos.	Contados do encerramento do exercício fiscal, observadas as legislações fiscal, contábil e regulatória e eventual bloqueio para auditoria ou defesa de direitos.
Rastreamento e telemetria vinculáveis a pessoa natural	Localização, trajetos, eventos, placas, identificadores de veículo, suporte e auditoria.	Até 5 anos.	Contados do recebimento no banco de dados. O contrato ou a instrução válida do cliente controlador pode definir prazo distinto.
Videomonitoramento vinculável a pessoa natural	Imagens e eventos da solução de vídeo rastreamento e de segurança operacional.	Até 6 meses.	Contados do recebimento. A preservação por prazo maior ocorre somente em caso de incidente, investigação, obrigação legal ou defesa de direitos.

Filial Administrativa

Trucks Control – Serviços e Logística Ltda – Av. Tiradentes 501 – 10º Andar – Torre 2 – CEP 86.070-545
Fone: (43) 3378-3500 | Whatsapp (43) 99914-0020 – lgpd@tcsat.com.br

Logs de acesso a aplicações	IP, usuário, data e hora, autenticação e eventos de acesso, para segurança, prevenção a fraude e rastreabilidade.	No mínimo 6 meses, podendo ser superior quando necessário e permitido.	Contados da geração do registro, observados o Marco Civil da Internet, os contratos, a criticidade e os requisitos de investigação.
Cookies, analytics e preferências digitais	Funcionamento do site, segurança, estatísticas, personalização e comunicação.	Até a revogação, o término da finalidade ou 24 meses, conforme a categoria.	Cookies de sessão podem expirar antes. Cookies não essenciais observam o consentimento e a configuração aprovada.
Fornecedores, parceiros e prepostos	Cadastro, contrato, compras, pagamentos, avaliação prévia e relacionamento.	Durante a relação e, em regra, até 5 anos após o término.	Contados do encerramento. Obrigações fiscais, contratuais ou defesa de direitos podem exigir prazo específico.
Videomonitoramento e controle de acesso físico	Imagens, visitantes, credenciais e registros de entrada e saída para segurança patrimonial.	Em regra até 6 meses.	Contados da captura ou do acesso, com preservação quando houver vínculo com incidente, investigação, obrigação legal ou defesa de direitos.
Marketing e comunicação	Preferências, interações, pesquisas, campanhas e comunicações institucionais ou comerciais.	Até a revogação do consentimento, a oposição ou o término da finalidade.	Aplica-se o evento que ocorrer primeiro, salvo fundamento documentado para conservação residual mínima.

Como ler estes prazos. Os prazos são referências e não autorizam retenção automática. Prevalecem a obrigação legal ou regulatória, o contrato, a instrução válida do cliente controlador, o bloqueio para investigação ou defesa de direitos e a necessidade demonstrada. Encerrada a justificativa, os dados são eliminados, anonimizados ou bloqueados, conforme aplicável.

Sempre que o prazo depender de contrato, instrução do cliente controlador, obrigação legal ou defesa de direitos, a evidência desse fundamento permanece vinculada ao registro do ativo de dados. Toda retenção superior ao prazo padrão é revisada periodicamente e encerrada quando a justificativa cessa.

6. O que acontece quando o prazo termina

Ao atingir o prazo de retenção, o responsável pelos dados autoriza formalmente uma entre três destinações. A ausência de decisão não autoriza a manutenção indefinida dos dados.

Destinação	Quando é aplicada
Eliminação	Quando não há finalidade, obrigação legal, previsão contratual ou bloqueio que justifique a manutenção. É a destinação padrão.
Anonimização	Quando a informação ainda tem utilidade estatística ou de melhoria do serviço, mas não exige o dado identificável. É aplicada somente quando a técnica e o contexto reduzem efetivamente a possibilidade de reidentificação. A pseudonimização não equivale à anonimização e permanece sujeita à proteção de dados pessoais.
Arquivamento justificado	Quando há fundamento documentado para guarda prolongada. O arquivo permanente exige fundamento, responsável, proteção, revisão de acesso e avaliação periódica da necessidade.

6.1 Situações em que a eliminação é suspensa

A eliminação é suspensa, de forma registrada e até liberação formal, quando os dados estiverem sujeitos a investigação, auditoria, litígio, obrigação de preservação ou incidente de segurança. A suspensão é temporária, vinculada ao seu fundamento, e encerra-se assim que a justificativa deixa de existir.

7. Como a eliminação é executada

A eliminação abrange cópias ativas, exportações, réplicas, ambientes não produtivos e, conforme o ciclo técnico de cada tecnologia, os backups. O resultado é irreversível ou torna a recuperação inviável em nível de esforço compatível com a sensibilidade dos dados.

O processo segue etapas formais:

- Confirmação do término da finalidade e do prazo de retenção, da inexistência de bloqueio legal ou contratual e da autoridade para eliminar;
- Identificação de todas as localizações, cópias, integrações, subprocessadores e mídias afetadas;
- Seleção do método de limpeza, purga ou destruição compatível com a classificação e a tecnologia, tendo como referência a diretriz NIST 800-88 rev. 2 para sanitização de mídias;
- Execução por pessoa autorizada, com segregação de função ou validação independente no caso de dados classificados como restritos;
- Registro de escopo, método, data, responsável, resultado e evidência, com obtenção de certificado do fornecedor quando a destruição for terceirizada;

- Atualização do inventário, dos contratos, dos repositórios e dos registros de tratamento após a conclusão.

7.1 Eliminação em nuvem, SaaS e fornecedores

Quando a eliminação depende de recursos de fornecedor, nuvem, software como serviço ou infraestrutura terceirizada, a Trucks Control obtém evidência suficiente da execução e da validação e, quando aplicável, certificado ou declaração de sanitização contendo escopo, método, data, ambiente, responsável e limitações conhecidas.

Antes da contratação, fornecedores são avaliados quanto a segurança, privacidade, continuidade, localização dos dados, portabilidade, eliminação, registros, criptografia, subcontratação e resposta a incidentes.

7.2 Backups

Os backups possuem frequência, retenção, imutabilidade, localização e criptografia definidas conforme a criticidade, os objetivos de recuperação, o contrato e a análise de risco. Backups expirados são excluídos de forma controlada, preservando retenções legais e contratuais e eventuais bloqueios por litígio.

Por natureza técnica, um dado eliminado do ambiente produtivo pode permanecer em cópias de segurança até o encerramento do ciclo de retenção do backup correspondente. Durante esse intervalo, o dado permanece protegido, com acesso restrito e criptografia, e não é utilizado para nenhuma finalidade operacional.

7.3 Cópias temporárias e ambientes de apoio

- Evidências retiradas do ambiente para suporte e diagnóstico possuem prazo de descarte definido, com preferência por mascaramento e sessões temporárias.
- Ambientes de desenvolvimento, teste e homologação utilizam dados sintéticos ou anonimizados. O uso de dados reais exige necessidade comprovada, aprovação formal, minimização, mascaramento, acesso restrito, prazo e descarte.
- Exportações e cópias locais são reduzidas ao mínimo e, quando indispensáveis, registram autorização, finalidade, destinatário, prazo e descarte.
- Compartilhamentos externos possuem base contratual, finalidade, destinatário, prazo de acesso, requisitos de segurança e obrigação de devolução ou eliminação.

8. Encerramento do contrato

Quando a Trucks Control atua como operadora, a eliminação ou a devolução dos dados ao final da relação segue o contrato e a instrução documentada do cliente controlador. A Trucks Control não mantém cópia para finalidade própria sem fundamento válido e autorização aplicável.

No encerramento de uma relação contratual, são executadas a revogação de acessos, a exportação dos dados necessários, a confirmação da eliminação e a preservação das evidências correspondentes.

Antes de solicitar a eliminação. Recomenda-se que o cliente verifique previamente suas próprias obrigações de guarda, como exigências fiscais, trabalhistas, regulatórias ou de defesa em processos, uma vez que a eliminação executada é irreversível e de responsabilidade do controlador.

9. Direitos dos titulares e canais de atendimento

Titulares de dados pessoais, incluindo condutores e usuários dos sistemas, podem solicitar informações sobre o tratamento de seus dados e exercer os direitos previstos na Lei Geral de Proteção de Dados, entre eles confirmação da existência de tratamento, acesso, correção, anonimização, bloqueio, eliminação e portabilidade, nos limites legais.

Situação	Encaminhamento
Dados em que a Trucks Control é controladora	A solicitação é recebida, verificada quanto à identidade do solicitante e respondida diretamente pela Trucks Control, nos prazos legais.
Dados tratados em nome de um cliente contratante	A solicitação é recebida e encaminhada ao cliente controlador, que decide sobre o atendimento. A Trucks Control apoia a resposta conforme o contrato e a instrução recebida.
Solicitação de eliminação com obrigação legal pendente	A eliminação pode ser recusada ou postergada quando houver obrigação legal, regulatória, contratual ou necessidade de defesa de direitos, hipótese em que o fundamento é informado ao solicitante.

Canal	Finalidade
lgpd@tcsat.com.br	Solicitações de titulares, dúvidas sobre privacidade, retenção, eliminação e exercício de direitos.
csi@tcsat.com.br	Comunicação de suspeita ou confirmação de incidente de segurança envolvendo dados.

10. Proteção dos dados durante o período de guarda

A retenção segura depende dos controles aplicados enquanto o dado existe. Durante todo o período de guarda, a Trucks Control mantém, de forma proporcional à classificação e ao risco:

- Segregação lógica dos dados por cliente, impedindo que consultas, relatórios, interfaces de integração ou rotinas administrativas misturem contextos sem autorização ou finalidade;
- Tratamento de localização, rotas, placas, identificadores de veículos, condutores, eventos e telemetria como dados no mínimo confidenciais quando associáveis a pessoa, operação ou cliente;

- Criptografia em trânsito e em repouso para dados confidenciais e restritos, backups e transferências externas, com gestão controlada de chaves e segredos;
- Acesso concedido pelo critério do menor privilégio e da necessidade de saber, com identidade individual, autenticação multifator e revisão periódica;
- Registro de acessos administrativos, exportações, comandos, mudanças de permissão e consultas em massa, com identificação do usuário e do contexto;
- Monitoramento de padrões anômalos, como volume incomum, consulta em massa, acesso fora do perfil e tentativas de extração;
- Gestão de vulnerabilidades, processo contínuo de identificar, avaliar e corrigir falhas de segurança em sistemas e redes para evitar invasões e vazamentos de dados antes que sejam explorados.
- Backup, recuperação e testes de restauração compatíveis com os objetivos de continuidade aprovados.

Soluções de inteligência artificial utilizadas para tratar, gerar, resumir, classificar ou inferir informações permanecem sujeitas às mesmas regras de classificação, retenção e responsabilidade, com configurações que impeçam treinamento indevido, retenção incompatível e compartilhamento não autorizado.

11. Incidentes envolvendo dados

Suspeitas ou confirmações de perda, acesso indevido, alteração, indisponibilidade, envio incorreto, vazamento, exposição pública ou eliminação indevida de dados devem ser comunicadas imediatamente pelo canal csi@tcsat.com.br.

Quando o incidente envolver dados pessoais e puder acarretar risco ou dano relevante, é realizada a comunicação à Autoridade Nacional de Proteção de Dados e aos titulares observando o prazo de três dias úteis previsto na Resolução CD/ANPD nº 15/2024, ressalvado prazo específico aplicável.

12. Referências legais e normativas

Referência	Aplicação
Lei nº 13.709/2018	Lei Geral de Proteção de Dados Pessoais, com alterações posteriores.
Lei nº 12.965/2014	Marco Civil da Internet, quando aplicável aos serviços e registros tratados.
Resolução CD/ANPD nº 15/2024	Regulamento de comunicação de incidente de segurança.
ABNT NBR ISO/IEC 27001:2022	Sistema de gestão da segurança da informação.
ABNT NBR ISO/IEC 27002:2022	Controles de segurança da informação, com destaque para exclusão, mascaramento e prevenção de vazamento de dados.
ISO/IEC 27701:2025	Sistema de gestão de informações de privacidade.

Referência	Aplicação
ISO/IEC 27017:2015 e ISO/IEC 27018:2019	Controles de segurança e proteção de informações pessoais em serviços de nuvem.
ABNT NBR ISO 22301:2019	Sistema de gestão de continuidade de negócios.
ABNT NBR ISO 9001:2015	Sistema de gestão da qualidade, aplicável ao controle de documentos e registros, à padronização dos processos e à melhoria contínua.
NIST SP 800-88 Rev. 2:2025	Diretrizes para sanitização de mídias.

14. Glossário

Termo	Significado
Retenção	Período durante o qual os dados e seus registros são mantidos antes do arquivamento ou da eliminação.
Eliminação	Exclusão dos dados de forma irreversível ou que torne a recuperação inviável no nível de esforço compatível com a sensibilidade da informação.
Sanitização	Processo destinado a tornar inviável a recuperação dos dados em uma mídia, por limpeza, purga ou destruição apropriada ao risco.
Anonimização	Uso de meios técnicos razoáveis e disponíveis no momento do tratamento para retirar a possibilidade de associação, direta ou indireta, a uma pessoa.
Pseudonimização	Tratamento em que o dado deixa de ser diretamente atribuível a um titular sem informação adicional mantida separadamente e protegida. Continua sujeito à proteção de dados pessoais.
Mascaramento	Técnica que reduz a exposição do valor original por substituição, ocultação ou apresentação parcial, preservando apenas a utilidade necessária.
Controlador	Quem decide sobre as finalidades e os meios do tratamento de dados pessoais.
Operador	Quem trata dados pessoais em nome do controlador, seguindo suas instruções.
Titular	Pessoa natural a quem se referem os dados pessoais tratados.
Dados de cliente	Dados fornecidos, gerados ou tratados em razão da prestação de serviços, incluindo dados de usuários, veículos, placas, localização, telemetria, eventos, comandos, registros e integrações.

15. Vigência, revisão e atualizações

Esta norma entra em vigor na data de sua publicação e permanece válida até substituição por versão posterior. A revisão ocorre no mínimo anualmente e sempre que houver mudança legal, regulatória, contratual ou tecnológica relevante.

Alterações são publicadas nos canais oficiais da Trucks Control com indicação da versão e da data. Em caso de divergência entre este documento e o contrato firmado com o cliente ou uma obrigação legal aplicável, prevalece o requisito mais restritivo.

Controle de versões	Descrição	Aprovador por
Versão 1.0	Publicação inicial da versão pública, derivada da Norma de Gestão de Dados NO-SI-008, versão 1.0.	Augusto Carvalho – Diretoria de Tecnologia

Dúvidas sobre este documento podem ser encaminhadas para lgpd@tcsat.com.br.