

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 1 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

1. Objetivo

O GRUPO TDS estabelece neste documento os requisitos de privacidade e proteção de dados privados da empresa, visando estabelecer diretrizes, controles e direcionamentos para preservar a privacidade e direcionar eventuais riscos associados à operacionalização deste tipo de informação.

2. GRUPO TDS – Definição

O GRUPO TDS é um grupo empresarial formado por duas sociedades distintas, sendo a TDS Informática a controladora.

- I. **TDS Informática S/A**, inscrita no CNPJ 02.231.701/0001-67, tem como principal atividade o tratamento de dados, provedores de serviços de aplicação e de hospedagem na Internet.
- II. **MOBISAFE Sistemas Ltda**, inscrita no CNPJ 14.204.950/0001-42, tem como principal atividade o desenvolvimento de programas de computador, execução de tratamento de dados, controle de provedores de serviços de aplicação e de hospedagem na Internet.

3. Abrangência

Esta política se aplica aos funcionários e prestadores de serviços, bem como a qualquer pessoa com poderes de representação do GRUPO TDS.

4. Referências Normativas

Servem de referência para os procedimentos descritos neste documento, os seguintes documentos:

- ISO/IEC 27701 - Gestão de privacidade de dados
- ISO/IEC 27001 - Gestão de Segurança da Informação
- Lei 13709/18 - Lei Geral de Proteção de Dados
- Lei 14010/20 - Revisão LGPD
- Lei 13853/19 - Criação da autoridade Nacional de Proteção de Dados (ANPD)
- Decreto 10474/20 - Regulamenta a estrutura Regimental da ANPD
- Lei 12965/14 - Marco Civil da Internet
- Decreto 8771/16 - Regulamento do Marco Civil na Internet

5. Privacidade e Proteção de Dados

- A disciplina de Privacidade e Proteção de Dados visa a proteção da vida íntima e privada de um indivíduo, além dos dados privados que identifiquem ou que possam identificar uma pessoa, alinhada ao entendimento das finalidades específicas informadas ao titular no momento da sua coleta.
- Realizar o tratamento adequado e estritamente necessário, sem que haja qualquer tipo de discriminação, para prover o produto ou serviço contratado.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 2 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- Informar e manter a qualidade dos dados privados coletados, aplicando a segurança necessária com mecanismos e processos de prevenção a incidentes de privacidade e segurança da informação.
- Manter a transparência e o acesso facilitado aos titulares dos dados, com responsabilidade e prestando contas sobre o tratamento realizado sobre os dados.

6. Diretrizes

Diretrizes que contemplam a privacidade e proteção de dados privados de pessoas físicas relacionadas que tem ou que em algum momento já tiveram relacionamento com o GRUPO TDS, e que devem ser contempladas nas rotinas que tratam a gestão dos riscos cibernéticos e privacidade.

6.1. Atendimento aos direitos dos titulares

- O atendimento aos direitos dos titulares se dará através de um canal de privacidade, onde serão registradas as solicitações a serem tratadas.
- As solicitações serão recebidas pelo canal de privacidade através do e-mail: tds.privacidade@tdsinfo.com.br, e direcionadas para tratativas nos prazos estabelecidos.
- Os direitos contemplados no canal de privacidade são os previstos abaixo:
 - Consulta de dados
 - Alteração de telefone e/ou e-mail
 - Consulta e revogação de consentimentos
 - Relatório de dados completo
 - Exclusão dos dados
 - Dúvidas e reclamações
 - Oposição à tratamento dos dados
 - Transparência quanto aos dados do titular deve ser seguida em todos os canais da empresa

6.2. Classificação dos dados privados

- Os dados privados são aqueles que identificam ou podem identificar uma pessoa física.
- Os tipos de dados que podem ser mapeados e classificados como privados ou sensíveis são:
 - **Dados Privados**
 - Nome da Pessoa
 - CPF ou quais outros documentos
 - Código de Registro Profissional (exemplo: OAB, CREA)
 - Data de Nascimento
 - Endereço completo (Logradouro, número, complemento, bairro,

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 3 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

cidade, estado, cep, etc.)

- Latitude e longitude de endereço
- Telefone
- E-mail
- Filiação
- Grau de parentesco
- Sexo
- Estado Civil
- Endereços de redes sociais
- Portador de necessidades especiais
- Tipo de deficiência
- Pessoa exposta politicamente (PEP)
- Cargo do PEP a quem se relaciona
- Documento CPF do PEP a quem se relaciona
- Tipo de relacionamento com o PEP (pai, mãe, cônjuge, outro relacionamento)
- Outros dados que sejam vinculados e coletados
- **Dados Financeiros (privados)**
 - Código do Banco
 - Código da Agência
 - Número da conta corrente
 - Número do cartão de crédito
- **Dados de funcionário / prestador (privados)**
 - Cargo do funcionário
 - CBO (Cadastro Nacional de Ocupação)
 - Situação da pessoa (Vivo ou Falecido)
 - Faixa de Renda Salarial Pessoa Física
 - Matrícula do funcionário ou prestador
- **Dados Sensíveis**
 - Religião
 - Orientação sexual / gênero
 - Origem racial / étnica
 - Filiação partidária
 - Filiação sindical
 - Dados referentes à saúde
 - Dados genéticos ou biométricos (se coletados)
- Caso sejam tratados, estes atributos devem ser inventariados, vinculados aos processos, sistemas e a avaliação de proteção dos dados pessoais deve ser periódica.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 4 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- Divergências de utilização de dados privados, falta de enquadramento legal e de finalidade específica, ou mesmo má utilização ou utilização indevida dessas informações são considerados riscos altos ou críticos para a empresa.
- Deve ser validado e acordado junto aos fornecedores da Folha de Pagamentos, Plano de Saúde e Odontológico, Previdência, Alimentação e Transportes, quais dados do titular são coletados e compartilhados entre Controlador e Operador, havendo cláusulas de co-responsabilidade sobre a segurança da informação e privacidade dos dados tratados no contrato de fornecimento dos serviços.

6.3. Limitação da coleta de dados

- A coleta de dados deve considerar a premissa do mínimo necessário para operacionalização da finalidade declarada.
- A coleta dos dados privados deve respeitar a finalidade específica e o enquadramento legal associado vinculado ao inventário de dados.
- Os processos, procedimentos, canais e tecnologias devem considerar o mínimo necessário para operacionalização e sustentação dos objetivos do negócio.
- Os processos, procedimentos, canais e tecnologias, quando utilizarem dados privados ou sensíveis devem respeitar a mínima utilização possível, sem expor dados sem necessidade à consulta.

6.4. Enquadramento e Finalidade praticados

- No âmbito do GRUPO TDS os dados privados tratados são somente dos funcionários contratados.
- O enquadramento legal é “Contrato trabalhista”.
- A finalidade é “Execução de contrato trabalhista”.
- Outras finalidades de uso não previstas neste documento deverão ser avaliadas e aprovadas pela gestão da empresa.

6.5. Limitação do uso

- O acesso a dados privados e sensíveis, em todo o seu ciclo de vida, deve ser restrito, monitorado e controlado pela Segurança da Informação dos fornecedores contratados na prestação de serviços, e também internamente no GRUPO TDS.
- O uso de dados privados deve respeitar a finalidade específica alinhada com o titular, prevendo e considerando o aceite e ciência dos termos de privacidade, e enquadramento legal previsto em inventário de dados.
- O descarte das bases que contém dados privados e sensíveis deve respeitar a política de proteção de dados vigente, de acordo com as legislações e prazos que regulamentam a finalidade de utilização dos dados.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 5 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

6.6. Compartilhamento de dados privados e sensíveis

- Dados privados só podem ser compartilhados entre a TDS e terceiros contratados para execução das atividades contratuais, como por exemplo, Previdência Privada, Vale Alimentação, Folha de Pagamento, Seguro Saúde, Seguro Odontológico, ou qualquer outro contratado para execução de serviços, os quais necessitam dos dados dos funcionários do GRUPO TDS. Todos os contratos firmados com os fornecedores devem ter contempladas as cláusulas inerentes à privacidade de dados (LGPD).
- Qualquer novo dado privado que necessite ser compartilhado, deve ser analisado pela área de Segurança da Informação, antes de ser liberado o seu acesso.
- O formato de compartilhamento de dados privados deve ser criterioso, obedecendo todas as regras e protocolos de Segurança da Informação, de forma a possibilitar consultas pontuais e acesso restrito a dados.
- O compartilhamento somente será possível respeitando o mínimo de dados privados necessários à execução da finalidade pretendida. Não é permitido o compartilhamento massivo e excessivo de dados privados. Qualquer exceção deverá ser analisada e autorizada pela área de Segurança da Informação e Diretoria.
- O compartilhamento de dados sensíveis somente será permitido para a execução de atividades inerentes à execução do objeto do serviço contratado e para atendimento de obrigações legais e regulatórias, sendo vedado qualquer tipo de outro compartilhamento. Exemplo: dados médicos, biométricos, etc.
- O compartilhamento de dados privados em outras situações não previstas nesta normativa, dependem de avaliação e aprovação da Segurança da Informação.
- Não é permitido o envio de informações classificadas como privadas para e-mails pessoais ou com domínio não corporativos, e sem finalidade discriminada.
- O envio de dados via canais não previstos, redes sociais, chats de comunicação, aplicativos de mensagem, podem acarretar em vazamento de dados e estão sujeitos a sanções disciplinares da organização.
- É proibida a coleta de fotos, filmagens ou gravações de áudio não autorizadas contendo dados privados ou sensíveis, acarretando em vazamento de dados e estando sujeitas a sanções disciplinares da organização.

6.7. Bases de dados externas

- É vedada a compra ou venda de bases de dados privados ou o download de bases de dados privados divulgadas em sites de órgãos públicos.
- É permitida a contratação de serviços de dados para a execução de processos de prevenção à fraude, proteção ao crédito e atualização cadastral (como

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 6 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

Serasa, por exemplo), sempre de acordo com as diretrizes e avaliações de Segurança da Informação.

6.8. Retenção e exclusão de dados

- O período de retenção dos dados privados e sensíveis deve respeitar a legislação vigente, de acordo com o tipo de enquadramento e finalidade utilizados na adequação à Lei Geral de Privacidade de Dados (LGPD).
- No caso do GRUPO TDS, como a base de dados privados se refere aos funcionários contratados, este período segue a regulamentação legal da CLT.
- É permitida a retenção de dados privados superiores aos previstos acima detalhados (CLT), para casos de processo judicial em andamento, processo trabalhista em andamento, valores em aberto a serem pagos ao titular e para fins de prevenção à fraudes e combate à lavagem de dinheiro, sendo que neste último caso os dados podem ser migrados para uma base em separado dos sistemas operacionais, com segurança reforçada e acesso restrito às áreas responsáveis.
- A exclusão definitiva dos dados do titular ocorrerá apenas mediante solicitação formal do mesmo no canal apropriado de privacidade, a ser executado após avaliação da viabilidade (cumprimento dos prazos legais regulamentados para finalidade e/ou outros), considerando os critérios estabelecidos no parágrafo anterior.
- A técnica de anonimização de dados será permitida para sistemas que não permitam a exclusão física dos registros.

6.9. Auditoria e conformidade de privacidade

- As áreas de Segurança da Informação e Comitê de Segurança devem prever controles para conformidade à privacidade e proteção de dados.
- O processo de revisão de controles deve ser realizado, pelo menos uma vez ao ano, e os resultados refletidos pela atualização das políticas e normas do GRUPO TDS.
- Os responsáveis pela Segurança da Informação devem prover testes associados ao atendimento regulamentar e de conformidade às leis, políticas e normativas em vigor.
- Os apontamentos e prazos devem respeitar as políticas e normativas, sendo os riscos classificados como: Alto, médio, baixo e informativo.

6.10. Gestão de fluxo de dados

- O ciclo de vida dos dados possui as seguintes fases: coleta, armazenamento, uso, transferência, exclusão/anonimização.
- Em todas as fases, os controles de Segurança da Informação devem estar presentes, e a ausência ou falha destes controles para o fluxo de dados privados

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 7 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

e sensíveis caracteriza um apontamento de alto risco, sendo direcionado este apontamento para a área responsável pelo processo, procedimento, canal específico gerador do risco.

- O fluxo de dados deve considerar as fases oriundas de terceiros e parceiros de serviço, sendo que os mesmos (terceiros e parceiros) devem estar aderentes à privacidade e proteção de dados, e estarem alinhados com as políticas e normas do GRUPO TDS.
- Os processos, tecnologias, procedimentos e pessoas que estejam na operacionalização dos dados privados e sensíveis, devem atender aos requisitos legais em todas as fases do ciclo de vida. Os métodos de comunicação devem estar alinhados com a Segurança da Informação, e legislação em vigor.
- Poderá haver desvio de conformidade e exposição à risco, caso ocorra tráfego de dados em não alinhamento com as normativas, o que poderá acarretar em sanções disciplinares internas.
- O fluxo de dados entre o GRUPO TDS e seus prestadores de serviços deve respeitar o enquadramento e finalidade legal informado no momento da coleta dos dados privados. Em caso de não conformidade o uso e compartilhamento de dados não será permitido.
- A denúncia realizada por qualquer pessoa (funcionários, parceiros, terceiros) sobre eventual desvio de finalidade sobre a utilização dos dados privados, deverá ser encarada como incidente, vulnerabilidade crítica, apontamento de risco crítico, e até mesmo acionamento do plano de gestão de crise (caso seja caracterizado um incidente de vazamento de dados).

6.11. Gestão e Estratégia de Privacidade

- A estratégia de privacidade deve ser revisada anualmente, com o intuito de mapear, identificar e direcionar os riscos à privacidade e proteção de dados privados no GRUPO TDS, através do inventário de dados privados nos processos correlatos.
- A estratégia deve contemplar a forma de atendimento, canais disponibilizados e processo implementado para atendimento aos titulares dos dados privados, observando os aspectos legais e regulatórios vigentes.
- A operação deste atendimento deve ser classificada como crítica, ou seja, não pode apresentar indisponibilidade ao atendimento do titular, sendo consideradas as premissas de horário de atendimento de cada canal.
- É previsto que a estratégia de privacidade, parte integrante da estratégia de Riscos e Compliance, tenha conexão e sinergia com as demais áreas de apoio, como Segurança da Informação, Jurídico, Compliance, Tecnologia da Informação, entre outras. Todos os processos destas áreas devem ter interdependência adequada com esta normativa.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 8 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

6.12. Treinamento, conscientização e engajamento

- Os treinamentos devem ser disponibilizados a toda a organização.
- Executar treinamentos periódicos, comunicados corporativos e/ou abordagens pontuais e direcionadas nas áreas da empresa, sobre o tema de privacidade e proteção de dados.
- Os treinamentos devem ser revisados e reaplicados a cada ano, o que pode ser realizado através de plataforma e-learning, sendo obrigatório a todos os funcionários.
- Os treinamentos devem ser aplicados também como parte do programa de inclusão de novos funcionários e prestadores de serviço.

6.13. Privacy by design

- Considera-se como premissa que o desenvolvimento de qualquer novo processo, desenvolvimento, tecnologia ou canal na empresa, o qual envolve dados privados ou sensíveis, deverá passar pela análise e aprovação da área de Segurança da Informação.
- Em caso da necessidade de tratamento de novos dados privados ou sensíveis, deverá sempre ser considerado o mínimo necessário de dados privados e confidenciais para utilização.
- Novas tecnologias e sistemas que utilizem dados privados e sensíveis, deverão ter mecanismos de rastreabilidade das ações de seus usuários (geração de log's do ciclo de vida), os quais devem conter o mínimo necessário de dados de identificação do titular e rastreabilidade das ações executadas. (Ex: CPF, Nome, Consulta de dados)
- Prever um processo seguro para desenvolvimento de aplicações e canais, com uma preparação adequada da infraestrutura para sustentação, principalmente quando se tratar de solução que possua dados privados e sensíveis.

6.14. Segurança da Informação

- Deve estar envolvida no desenvolvimento de novos canais e sistemas que utilizarão dados privados, tendo a missão de reduzir eventuais riscos de privacidade e proteção de dados associados à nova solução.
- Deve prover as diretrizes para desenho dos componentes de prevenção à risco de vazamento de dados, privacidade, confidencialidade e integridade das informações.
- Deve prover processos e procedimentos a respeito do monitoramento e resposta a incidentes de privacidade e proteção de dados, estando alinhada com as outras áreas da empresa como Jurídico, Compliance e Riscos.
- Deve revisar periodicamente os controles de prevenção e vazamento de dados e comprometimento da segurança das informações privadas e sensíveis.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 9 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- A avaliação de Segurança da Informação quanto a terceiros e parceiros de serviço de dados privados e sensíveis de titulares deve ser limitada à tecnologia associada à contratação.

6.15. Avaliação de maturidade e riscos à privacidade de dados

- O GRUPO TDS deve realizar uma avaliação criteriosa de terceiros e parceiros de serviço dados privados ou sensíveis de titulares, previamente à sua contratação, tendo como premissa a legislação em vigor, processos, procedimentos, normativas e políticas de riscos, proteção de dados e privacidade.
- Na contratação de terceiros deve ser solicitado ao time de Privacidade a avaliação da maturidade de adequação de privacidade, bem como o grau de exposição de eventual risco que o terceiro e a atividade contratada podem acarretar ao GRUPO TDS.
- Esta avaliação deverá ser prevista no contrato com o parceiro ou fornecedor a fim de se ter a garantia na execução do processo contratado.
- A avaliação deverá ser renovada a cada dois anos de vigência da contratação do serviço.
- Os contratos com terceiros que tenham acesso a dados privados ou sensíveis devem possuir cláusulas de privacidade, auditoria, permissão de execução de testes de intrusão, um processo de resposta a incidentes de segurança e privacidade, bem como obrigação de exclusão dos dados compartilhados ao final do contrato, passíveis de rompimento contratual em caso de descumprimento dos acordos firmados entre as partes.
- Em caso de serviços contratados como solução integral (hardware, software, suporte), deverão ser observadas as premissas da política de Proteção de Dados do GRUPO TDS.

7. Processos de Privacidade

7.1. Inventário de Dados

- A área de Recursos Humanos é responsável pelo preenchimento do inventário de dados de todos os processos que envolvem o tratamento de dados privados, pessoais e sensíveis, sejam dados para folha de pagamento, previdência, saúde, odontológicos, alimentação e transporte.
- Na fase de contratação pela TDS, os Currículos e dados recebidos dos candidatos devem ser armazenados de forma segura, atendendo aos princípios da LGPD.
- O enquadramento legal e a finalidade de uso dados no referido processo se dará nos sistemas dos respectivos fornecedores .

7.2. Relatório de Impacto

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 10 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- O relatório de impacto deve ser emitido pela área de Recursos Humanos sempre que solicitado pelo titular dos dados através do Canal de Privacidade.
- O relatório ficará armazenado no GRUPO TDS, o qual poderá ser disponibilizado para a ANPD sempre que solicitado.

7.3. Atendimento aos direitos dos titulares

- Dúvidas, reclamações, solicitação de relatórios ou outras solicitações referentes a privacidade de dados serão atendidas pelo Canal de Privacidade, através de um telefone destinado a este objetivo, com gravação das solicitações efetuadas, ou através do email: tds.privacidade@tdsinfo.com.br.
- Em caso de reclamações de direitos pelo titular, serão atendidas dentro do prazo legal estipulado pela LGPD, de acordo com a avaliação e direcionamentos das respostas pela área responsável.

7.4. Apontamentos de riscos à privacidade

- Avaliação de vulnerabilidades e não conformidades relacionadas ao tema de privacidade nos processos, tecnologias envolvidas nos processos deverão ser registradas e informadas à gestão, com acompanhamento da mitigação dos riscos e homologação das correções efetuadas.

8. Papéis e Responsabilidades

- Diretoria Executiva
 - Avaliar anualmente ou sempre que houver mudança significativa no perfil de risco e privacidade, a eficácia da estrutura de gestão de riscos, informando às partes interessadas os resultados das análises e os planos de ação se necessário.
 - Acompanhar de forma periódica as informações de Segurança da Informação e área de Riscos.
 - Monitorar periodicamente as exposições à riscos assim como os planos de ação ou medidas corretivas, caso necessário.
- Comitê de Segurança
 - Garantir o atendimento às normas publicadas pelos órgãos reguladores.
 - Auxiliar as áreas no atendimento às demandas dos reguladores externos.
 - Acompanhar eventuais fiscalizações de privacidade de dados realizadas pela ANPD ou quaisquer outros reguladores.
 - Recepcionar, analisar e responder questionamentos e *Due Diligences* de parceiros, fornecedores e clientes.
 - Orientar os funcionários a efetuar os treinamentos relacionados à Segurança da Informação.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 11 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- Os participantes do Comitê de Segurança são nomeados na reunião de Assembleia do GRUPO TDS, conforme ata publicada.
- **Segurança da Informação**
 - Propor as políticas e normativas de segurança
 - Zelar pela conformidade das políticas, normas, padrões, procedimentos e regulamentações internas e externas.
 - Revisar e validar periodicamente as políticas e normativas de Segurança da Informação.
 - Avaliar a adequação da Estrutura de Segurança da Informação, dentro de um ciclo máximo de três anos.
 - Recomendar aprimoramentos no ambiente de controles internos.
 - Zelar pelo cumprimento das políticas e normativas do processo de gestão de segurança
 - Prover recomendações relacionadas aos assuntos.
 - Orientar e engajar todas as áreas sobre a gestão de riscos.
 - Analisar e pontuar fatores de riscos internos e externos que levem a possibilidade de incidentes de segurança e privacidade.
 - Analisar os casos submetidos e sugerir à Diretoria o plano de ação, e as melhores soluções face às situações, riscos e custos envolvidos.
- **Gestores das Áreas Operacionais com tratativa de dados privados**
 - Promover controles necessários às atividades sob responsabilidade de suas áreas, inclusive o monitoramento destes controles.
 - Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação e gestão de eventuais riscos.
 - Auxiliar a área de Segurança da Informação, provendo acesso às informações necessárias para análise.
 - Monitorar os serviços terceirizados relevantes para funcionamento das atividades sob sua responsabilidade.
 - Propagar a cultura voltada à Segurança da Informação aos times sob sua gestão.
 - Executar todos os processos de privacidade aplicáveis à execução das atividades da área.
 - Reportar incidentes e desvios de condutas identificados para a gestão de suas áreas de atuação.
 - Estabelecer processos e controles adequados para preservar a segurança da informação e privacidade, no atendimento das políticas e normativos internos do GRUPO TDS.
 - Atuar para prevenir ou responder a riscos e ameaças à segurança e privacidade conforme as normativas estabelecidas.
 - Atuar de forma preventiva, sobre os riscos e possíveis ameaças.

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 12 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

- Tecnologia da Informação
 - Atuar de maneira a reduzir a exposição a riscos e ameaças, atendendo as políticas e normativas do GRUPO TDS.
 - Atentar a desvios e rotinas que possam causar exposição a riscos e ameaças.
 - Observar e alertar a área de Segurança da Informação a eventuais desvios de conduta de profissionais ou parceiros de serviços quanto às políticas e normativas do GRUPO TDS.
- Jurídico
 - O GRUPO TDS conta com uma assessoria jurídica externa.
 - A Assessoria Jurídica deve prover parecer legal sobre situações e temas envolvendo a aplicação da Lei Geral de Proteção de Dados (LGPD), além de fornecer apoio através do serviço de um DPO, para respostas à ANPD no caso de incidentes de privacidade.
 - No caso do GRUPO TDS, como os dados privados (funcionários da empresa) são tratados pelos fornecedores de serviços, o enquadramento será realizado nos sistemas dos fornecedores que fazem o tratamento dos dados privados.
 - Também para avaliação do pedido de exclusão de dados de titulares que não estejam em prazo de retenção legal ou regulatória, os fornecedores de serviços contratados deverão executar os procedimentos correlatos em seus sistemas e reportar ao GRUPO TDS, evidenciando o atendimento às funcionalidades exigidas pela Lei.
- Colaboradores, funcionários, terceiros e parceiros de negócio
 - Seguir as diretrizes estabelecidas.
 - Atuar com as áreas de controle para prevenção e apoio na resposta de eventuais incidentes.
 - Reportar incidentes e desvios de condutas identificados para a gestão de suas áreas de atuação.
 - Identificar e tratar as informações conforme sua classificação e em linha com as políticas e normativas do GRUPO TDS.
 - Ser responsável sobre as informações classificadas como “confidenciais”, “privadas”, “sensíveis”, internas e públicas do GRUPO TDS.

9. Glossário Termos e Definições

- Dado Pessoal: informação relacionada à pessoa física identificada ou identificável. (Dado Privado)
- Dado Pessoal Sensível: dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 13 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

biométrico, quando vinculado a uma pessoa física. (Dado Privado)

- Titular: pessoa física, titular dos dados que a identifica ou que a possam identificar.
- Opt-in: Permissão do titular para receber comunicações gerais por meios físicos ou eletrônicos, destinadas exclusivamente à realização de propaganda ou oferta de produtos e serviços. Não se aplica a finalidade de tratamento de dados que diz respeito à "execução de contrato profissional". Exemplo: execução de contrato CLT, contrato de prestação de serviços, etc.
- Opt-out: Opção do titular, com negativa registrada através de uma página de privacidade (intranet, site, app), pelo não recebimento de comunicações gerais, por meios físicos ou eletrônicos, de propaganda ou oferta de produtos e serviços. Não se aplica para a finalidade de "execução de contrato profissional".
- Consentimento: autorização expressa e formalizada do titular dos dados, quando aplicável para tratamento e compartilhamento dos dados privados, de acordo com a finalidade específica informado no momento da coleta, concedido de forma livre, informada e inequívoca.
- Tratamento de dados: toda operação realizada com dados pessoais como: coleta, produção, recepção, classificação, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação coletada, suas alterações, comunicação, transferência, compartilhamento ou extração, sempre respeitando a finalidade específica informada no momento da coleta.
- Enquadramento legal: realização do tratamento dos dados privados coletados em estrita observância às hipóteses legais previstas no artigo 7º da Lei 13709/18 (LGPD)
- Finalidade: Motivo, devidamente informado ao titular dos dados, pelo qual os dados privados precisam ser coletados (razão justificada de uso).
- Controlador: Responsável Legal por tomar decisões referentes à forma como os dados serão tratados pelo operador, com estrita observância à finalidade informada e dentro de um enquadramento legal.
- Operador: Responsável por efetuar algum tipo de tratamento de dados privados em nome do Controlador e de acordo com suas determinações, práticas, políticas e normas.
- Direito de Esquecimento: Direito do Titular dos dados, mediante solicitação, para que seus dados sejam excluídos ou anonimizados em todos os sistemas, bancos e bases de dados da empresa. O esquecimento pode ser acatado pela empresa e os dados serem eliminados, desde que não haja qualquer outra regulamentação legal que obrigue a manutenção destes dados por outros motivos vinculados à finalidade. Exemplo: legislação trabalhista os dados devem ser mantidos por 35 anos. Neste caso os dados não são apagados, mas a empresa só poderá contatar o titular em caso de ocorrências trabalhistas, como

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 14 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

por exemplo um processo.

- **Expurgo de Dados:** exclusão ou anonimização de dados privados que identificam uma pessoa nas tabelas de sistemas e bancos de dados.
- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis, por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo. Neste caso, a anonimização não é coberta por mascaramento de dados ou criptografia, mas sim pela alteração de um dado privado para um valor que não permita a recuperação do dado de origem. Este mecanismo deve ser utilizado quando por questões estruturais do banco de dados, não seja possível a remoção de um registro completo, mantendo-se a estrutura de dados mas com os dados privados anonimizados.
- **Prazo de retenção legal/regulatória:** período no qual é possível manter os dados de um titular, mesmo mediante solicitação de esquecimento pelo titular, para cumprimento de prazos legais de prescrição e decadência e cumprimento de obrigação regulatória.
- **Inventário de dados:** mapeamento dos processos de negócio da empresa, no qual é mapeado o ciclo de vida dos dados privados nos processos de negócio, com a designação de cada dado privado utilizado, desde sua coleta até o seu eventual expurgo ao final dos prazos legais / regulatórios, passando pelos sistemas e compartilhamentos realizados com terceiros.
- **Relatório de impacto:** relatório que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos à liberdade civil e aos direitos fundamentais dos titulares, bem como das medidas, salvaguardas e mecanismos de mitigação de riscos.
- **Ferramentas de Privacidade:** ferramentas utilizadas nos processos e privacidade para atendimento aos direitos dos titulares e para gestão de riscos à privacidade.
- **Encarregado (DPO) (Data Protection Officer)** - responsável pela proteção de dados pessoais na organização, indicado para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Autoridade Nacional de Proteção de Dados (ANPD):** Órgão da Administração Pública Brasileira responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil.

10. Vigência

Esta política entrará em vigor na data de sua publicação e será revisada periodicamente, com prazo não superior a dois anos, sendo passível de alteração ou atualização sempre que necessário.

11. Datas de Revisão do Documento:

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria

 	POLÍTICA CORPORATIVA	CÓDIGO: TDS-PPD-001	PÁG.: 15 de 15
	Privacidade e Proteção de Dados	Classificação: Pública	Grupo de Acesso: Partes Interessadas

Versão	Revisão por	Data	Aprovador
1.0	Denize Serafim	01/11/2022	Paulo Gerosa
1.1	Denize Serafim	21/10/2024	Gilberto Pierani
1.2	Poliana Amaral	14/02/2025	Gilberto Pierani
1.3	Gisele Klouccek	24/04/2026	Gilberto Pierani

12. Aprovação

Esta política foi revisada e aprovada pelo seguinte destinatário:

GILBERTO CARLOS PIERANI:04794166800

Assinado de forma digital por GILBERTO CARLOS PIERANI:04794166800
Dados: 2026.04.27 15:02:33 -03'00'

Gilberto Carlos Pierani

Diretor Operações

Assinatura Digital

Emissão	Análise	Aprovação
Segurança da Informação	Gerência	Diretoria