Sumário

1. Objetivo

Esta política tem como objetivo estabelecer as diretrizes e expectativas de segurança da informação no relacionamento entre a **Toro** e seus fornecedores. A segurança da informação é fundamental para proteger os ativos da organização, garantir a conformidade com regulamentações, preservar a reputação e a confiança do cliente, além de manter a continuidade das operações de negócios.

2. Termos e Definições

Termos	Definições
Ativo	Ativo é algo que tem valor para a organização, está sob o seu controle, portanto deve ser protegido.
Políticas de Segurança da Informação	As políticas de segurança da informação são um conjunto de diretrizes, regras, práticas e procedimentos estabelecidos por uma organização para proteger a confidencialidade, integridade e disponibilidade de suas informações e dados. Essas políticas são projetadas para garantir que os ativos de informação da organização sejam devidamente protegidos contra ameaças internas e externas, como ataques cibernéticos, vazamento de informações confidenciais e outros incidentes de segurança.
TISAX	Trusted Information Security Assessment Exchange - O TISAX (Trusted Information Security Assessment Exchange) é um **padrão de segurança de informação** desenvolvido especificamente para a indústria automotiva. Foi criado pela Associação da **Indústria Automotiva Alemã (VDA)** em colaboração com várias montadoras e fornecedores automotivos para estabelecer um processo de avaliação e troca confiável de informações de segurança. O objetivo do TISAX é garantir a **proteção** das informações **confidenciais e sensíveis**, como **dados de design**, tecnologia, propriedade intelectual e informações do cliente, dentro da cadeia de suprimentos automotiva. Ele define requisitos de segurança e padrões para as organizações que lidam com informações sensíveis e também estabelece um processo de avaliação e certificação para garantir a conformidade.

3. Acrônimos

Termos	Definições
LGPD	Lei Geral de Proteção de Dados Pessoais
SI	Segurança da Informação
TISAX	Trusted Information Security Assessment Exchange

4. Confidencialidade dos Dados

- O fornecedor deve reconhecer e concordar que todas as informações e dados fornecidos pela **Toro** são confidenciais e devem ser tratados como tal.
- O fornecedor deve implementar medidas adequadas para proteger os dados confidenciais da **Toro** contra acesso não autorizado, divulgação ou uso indevido.
- O fornecedor não deve divulgar ou compartilhar informações confidenciais da **Toro** com terceiros sem autorização prévia por escrito da **Toro**.

5. Integridade dos Dados

- O fornecedor deve garantir a integridade dos dados da **Toro**, assegurando que eles não sejam alterados, corrompidos ou destruídos de forma não autorizada.
- Todas as alterações nos dados da Toro devem ser devidamente autorizadas, registradas e rastreáveis.
- O fornecedor deve implementar controles de segurança adequados para prevenir a adulteração ou modificação não autorizada dos dados.

6. Disponibilidade dos Dados

- O fornecedor deve garantir a disponibilidade contínua dos dados da **Toro,** minimizando o tempo de inatividade e interrupções nos serviços.
- O fornecedor deve ter procedimentos de backup e recuperação de dados adequados para garantir a disponibilidade dos dados em caso de falhas ou desastres.
- O fornecedor deve notificar imediatamente a **Toro** sobre quaisquer interrupções nos serviços que possam afetar a disponibilidade dos dados.

7. Responsabilidade

- Os fornecedores devem cumprir todas as políticas de segurança da informação estabelecidas pela **Toro**.
- Devem ler e confirmar a ciência das diretrizes de nossa Política de Segurança da Informação.
- Devem nomear um representante responsável pela segurança da informação em sua organização.
- A **Toro** é responsável por comunicar claramente suas políticas de segurança da informação aos fornecedores.
- A **Toro** deve fornecer treinamento e orientação apropriados aos fornecedores quando necessário.
- O fornecedor é responsável por qualquer violação desta política e deve tomar medidas corretivas imediatas para remediar qualquer não conformidade.
- O não cumprimento desta política pode resultar em medidas disciplinares, incluindo rescisão do contrato de fornecimento e responsabilidade legal.

8. Diretrizes e Requisitos para Fornecedores

O fornecedor e os seus colaboradores, funcionários, terceiros e parceiros estão obrigados a:

a) Respeitar todas as diretrizes e políticas fornecidas pela **Toro** em relação à segurança da informação.
b) O fornecedor deve cumprir todas as leis, regulamentos e normas aplicáveis relacionadas à segurança da informação.
c) Os prestadores de serviço devem ser submetidos a uma análise de risco das operações para identificar possíveis vulnerabilidades no processo de prestação de serviço que possam impactar adversamente a segurança da informação e o cumprimento dos requisitos da organização, essa avaliação deve abranger aspectos relevantes para garantir um nível adequado de segurança da informação.
d) A **Toro** pode solicitar, se necessário e para os casos aplicáveis, que o fornecedor seja certificado de acordo com as normas de segurança da informação ISO 27001 ou TISAX.
e) O compromisso em relação à segurança da informação entre a **Toro** e o prestador de serviço deve ser formalizado por meio de um contrato. É essencial que todos os requisitos estabelecidos neste contrato sejam integralmente cumpridos, sujeitos a verificações por parte da Toro a qualquer momento.
f) Os prestadores de serviço devem cumprir todas as políticas de segurança da informação estabelecidas pela **Toro**, devem ler e confirmar a ciência das diretrizes da **Política de Segurança da Informação**. A Toro reserva o direito de auditar periodicamente os sistemas, processos e controles de segurança do fornecedor para garantir a conformidade com esta política.
g) Utilizar as informações da **Toro**, apenas para os fins permitidos pela prestação do serviço, mantendo um nível de confidencialidade alinhado com os requisitos da **Toro**.
h) A obrigação de manter a confidencialidade permanece válida mesmo em caso de cessação do serviço por qualquer motivo. Na medida em que tais informações, dados e suporte de dados não tenham sido geralmente conhecidos de qualquer outra forma ou a **Toro** tenha renunciado por escrito ao direito ao tratamento confidencial.
i) O uso de dados da **Toro** para situações fora do que definido para efeitos de prestação do serviço deve ser considerado uma violação dos acordos entre a **Toro** e o fornecedor.

j) O fornecedor não deve armazenar/copiar dados digitais em seus equipamentos (que sejam de propriedade da **Toro**), a menos que seja estritamente necessário e com autorização devida para a execução do serviço.
k) O fornecedor não deve levar para fora das instalações da **Toro** documentação em papel de propriedade da **Toro,** a menos que seja estritamente necessário e com autorização devida.
l) Não deve deixar inseguras quaisquer cópias de documentos que contenham dados de propriedade da **Toro**(ex. alguns papéis deixados em impressoras e aparelhos de fax).
m) Comunicar imediatamente qualquer possível perda de confidencialidade dos dados da **Toro** ao seu contacto ou pessoa de referência.
n) Os fornecedores devem relatar imediatamente qualquer incidente de segurança ou violação à equipe de segurança da informação da empresa.
o) Fornecer dados a terceiros (incluindo quaisquer subfornecedores) apenas com a aprovação por escrito do proprietário dos dados da **Toro**. O fornecedor é considerado responsável pelo cumprimento dos requisitos contidos neste documento por parte dos subcontratados autorizados.
p) Os prestadores de serviço devem registrar e informar através de questionário fornecido pela **Toro** uma **avaliação** de seus controles de segurança da informação e do nível de aderência aos requisitos da Lei Nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). Caso não cumpram os requisitos, um plano de ação deve ser apresentado.
q) Eliminar os dados adquiridos na sequência da cessão, no final da mesma, se solicitado pela **Toro** nos termos da legislação em vigor.
r) Respeitar quaisquer requisitos legais relativos ao armazenamento e tempo de retenção de dados.
s) Cuidar e informar a todos os trabalhadores as diretrizes de segurança da informação em linha com as obrigações estabelecidas neste documento.;
t) Permitir que a **Toro** realize verificações, mesmo nas instalações do fornecedor, com pessoal próprio ou através de profissionais qualificados, relativamente aos processos, procedimentos, ferramentas utilizadas para garantir o fornecimento acordado, após ter acordado com o fornecedor o calendário e métodos de intervenção.
u) Os fornecedores devem ser identificados e **classificados** (tabela 1) considerando as necessidades de proteção e requisitos de segurança. Classificar fornecedores com base em suas necessidades de segurança da informação é essencial para garantir que os recursos adequados sejam alocados e que os riscos sejam adequadamente gerenciados. Abaixo estão algumas diretrizes gerais para classificar fornecedores com necessidades de segurança da informação entre: **Alta (A), Média (B) e Baixa (C)**:

É crucial para esta avaliação considerar se o trabalho do fornecedor inclui:

1. Obter acesso a informações ou zonas de segurança da empresa com necessidades de proteção alta ou muito altas em termos de confidencialidade; ou
2. Fornecer ou poder modificar informações relevantes com necessidades de proteção de integridade alta ou muito alta; ou
3. Ter influência relevante em processos ou sistemas de TI com necessidades de proteção pelo menos muito altas em termos de disponibilidade (em conformidade com SLAs internos ou relacionados ao cliente).

Tabela 1 – Classificação de Fornecedor

Classificação de fornecedor	Tipo de acesso à informação
Alta (A)	• Fornecedores que lidam com informações altamente sensíveis (**ver tabela 2**), como dados pessoais, financeiros ou de saúde. • Fornecedores que têm acesso a sistemas críticos ou infraestrutura essencial para o funcionamento da organização. • Fornecedores que lidam com informações confidenciais de propriedade intelectual, projetos, etc... • Fornecedores cujas falhas de segurança podem ter um impacto significativo na reputação da empresa ou em sua conformidade legal. Os fornecedores típicos com necessidades de proteção muito elevadas são, por ex.: prestadores de serviços de TI (por exemplo, administradores de domínio), consultores, agências, subcontratantes (por exemplo, designers de CAD, aos quais é necessário transmitir extensos dados de projetos com necessidades de proteção muito elevadas) e fabricantes de protótipos.

	Os fornecedores típicos com necessidades de necessidades de proteção alta, são, por ex.: serviços de limpeza, limpeza autônoma de zonas de segurança relevantes, prestadores de serviços de TI (por exemplo, administradores de bases de dados), consultores, agências e subcontratados (por exemplo, designers de ferramentas a quem os dados do projeto precisam de ser encaminhados).
Média (B)	• Fornecedores que têm acesso a informações não tão críticas quanto as mencionadas no item acima. • Fornecedores que lidam com informações financeiras ou comerciais que, se comprometidas, não devam causar perdas financeiras ou impactar negativamente a operação. • Fornecedores que têm acesso a sistemas ou redes que se explorados não devam comprometer a segurança da empresa.
Baixa (C)	• Fornecedores que lidam com informações de baixa sensibilidade, como informações públicas ou não confidenciais. • Fornecedores cujo acesso aos sistemas e dados da empresa é limitado e de baixo risco. • Fornecedores que não têm acesso a informações críticas ou sistemas essenciais para o funcionamento da organização.

9. Documentação para envio e ciência do fornecedor

a) **Política de segurança da informação**: Compete ao departamento de compras enviar a **Política de Segurança da Informação** ao fornecedor. Obrigatório classe A, B e C.
- **Revisão e Aceitação:** O representante legal do fornecedor deve revisar a Política de Segurança da Informação e esclarecer eventuais dúvidas. Todos os requisitos referentes à Segurança da Informação que constam na política devem ser compreendidos e atendidos.

b) **Contrato de Confidencialidade (NDA) e Privacidade de Dados:** Obrigatório classe (A) Eventualmente aplicável classe (B)
- **Distribuição do Contrato:** Compete ao departamento de Compras fornecer uma cópia do Contrato de Confidencialidade para Fornecedores (NDA) e Privacidade de Dados ao representante legal do fornecedor.
- **Revisão e Aceitação:** O representante legal do fornecedor deve revisar o Contrato de Confidencialidade, esclarecer eventuais dúvidas e assinar o documento para indicar aceitação dos termos.
- **Registro e Arquivamento:** Uma cópia assinada do Contrato de Confidencialidade deve ser arquivada no departamento de Compras.
- **Medidas Corretivas:** Caso seja identificado algum descumprimento do Contrato, serão aplicadas medidas corretivas, que podem incluir revisão do contrato, treinamento adicional ou rescisão do contrato, conforme a gravidade da violação.

c) **Avaliação de Segurança da Informação e Privacidade de Dados (LGPD)** Obrigatório classe (A)
- **Distribuição do formulário:** fornecer o formulário **"Avaliação de SI e LGPD"** da **Toro** ao representante legal do fornecedor.
- **Revisão e Aceitação:** O representante legal do fornecedor deve revisar o formulário, esclarecer eventuais dúvidas, preencher e assinar o documento para verificar a aderência aos requisitos de Segurança da Informação e LGPD.
- **Registro e Arquivamento:** Uma cópia assinada do formulário deve ser arquivada no departamento de Compras.
- **Não atendimento aos requisitos SI e LGPD:** Caso o fornecedor não seja aderente aos requisitos apresentados no formulário de avaliação, deve ser realizada uma análise de risco por um comitê diretivo ou de gestão da **Toro** para aprovação ou não dos serviços em critério de exceção.

Nota: Os documentos Política de Segurança da Informação, Contrato de Confidencialidade (NDA)/Privacidade de Dados e Questionário de SI e LGPD serão compartilhados uma única vez para conhecimento e assinaturas aplicáveis.

Tabela 2 - Exemplo de Informações Sensíveis

Propriedade Intelectual: Informações sobre patentes, segredos comerciais, inovações, projetos de pesquisa e desenvolvimento, know how , entre outros, que são valiosos para empresas e organizações.

Segredos Empresariais: Informações confidenciais sobre operações comerciais, estratégias de negócios, parcerias, planos de marketing e outros detalhes cruciais para o funcionamento de uma empresa.

Informações Governamentais: Dados governamentais sensíveis, como segurança nacional, estratégias de defesa, informações de inteligência e outros dados classificados.

Informações de Clientes: Dados sobre clientes, projetos confidenciais e estratégicos, preferências, históricos de compras e outras informações relacionadas ao relacionamento com clientes.

Dados Pessoais: Informações como nomes, endereços, números de telefone, números de identificação, dados biométricos, informações de saúde, religião, raça, opção sexual, entre outros, que podem identificar uma pessoa.

Informações Médicas: Dados de saúde, históricos médicos, registros de tratamentos e outras informações relacionadas à saúde de uma pessoa.

Informações Profissionais: Detalhes de empregos, salários, históricos profissionais e outras informações relacionadas ao trabalho de uma pessoa.

Informações Financeiras: Detalhes de contas bancárias, números de cartões de crédito, informações de transações financeiras e outros dados relacionados às finanças estratégicas da empresa.

Tecnologia da Informação: Dados de sistemas e aplicativos, configurações de rede, senhas, códigos de acesso, dados de backups e informações de segurança cibernética.

Infraestrutura Crítica: Sistemas de energia, comunicações, transporte e outros sistemas essenciais para as operações da empresa.

Informações Regulamentares e de Conformidade: Documentação relacionada a regulamentos, padrões do setor, licenças, certificações e conformidade legal.

Controle de Revisão do Documento

Edição	Data	Histórico da Revisão	RESP.
00	18/10/24	Publicação inicial.	Renato Dias Rodrigues

APROVAÇÕES

Elaborado	Nome: Renato Dias Rodrigues	DATA:	10/10/2024
Revisado	Nome: Francisco Sousa	DATA:	11/10/2024

Aprovado	Nome: Júlio César Fiori	DATA:	18/10/2024