TOTVS S.A.
CNPJ/MF n.º 53.113.791/0001-22
NIRE 35.300.153.171

ATA DE REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO
REALIZADA EM 3 DE NOVEMBRO DE 2025

1. DATA, HORA E LOCAL: realizada no dia 3 de novembro de 2025, às 13h00min, na sede da TOTVS S.A. ("TOTVS" ou "Companhia"), localizada na Avenida Braz Leme, n.º 1.000, Casa Verde, município de São Paulo, Estado de São Paulo, CEP 02511-000, nos termos do artigo 18 do Estatuto Social e do artigo 16 do Regimento Interno do Conselho de Administração.

2. CONVOCAÇÃO E PRESENÇA: convocação devidamente realizada, nos termos do artigo 18, §1º do Estatuto Social da TOTVS. Presente a totalidade dos membros do Conselho de Administração ("Conselho"), a saber: Ana Claudia Piedade Silveira dos Reis, Edson Georges Nassar, Gilberto Mifano, Guilherme Stocco Filho, Laércio José de Lucena Cosentino e Tania Sztamfater Chocolat. Presentes, como convidados, em parte da reunião: Dennis Herszkowicz, Diretor-Presidente (exceto no IX); Gilsomar Maia Sebastião, Diretor Vice-Presidente Administrativo e Financeiro e Diretor de Relações com Investidores (item 5.IV); Ricardo Guerino, Diretor de Planejamento e Controladoria (item 5.IV); e Sergio Pauperio Serio Filho, Diretor de Relações com Investidores (item 5.IV). Presente ainda, Glaucia Macedo de Sousa, Coordenadora de Governança Corporativa, como ouvinte da reunião.

3. COMPOSIÇÃO DA MESA: Presidente: Laércio José de Lucena Cosentino; Secretária: Téssie Massarão Andrade Simonato.

4. ORDEM DO DIA: (I) Abertura da reunião, incluindo as providências solicitadas referentes a temas de reuniões anteriores; **(II)** Consignar o pedido de renúncia da Conselheira Sra. Maria Letícia de Freitas Costa; Deliberações da pauta: **(III) (a)** eleger a Sra. Isabella de Oliveira Vianna Cavalcanti Wanderley, como membro independente do Conselho de Administração, nos termos do artigo 150, da Lei nº 6.404/1976; **(b)** eleger o novo Vice-Presidente do Conselho de Administração; e **(c)** eleger o novo Coordenador do Comitê de Estratégia; **(IV) (a)** apreciação das Demonstrações Financeiras da Companhia relativas ao 3º trimestre do exercício de 2025, com a revisão trimestral da KPMG Auditores Independentes Ltda. ("KPMG"), acompanhadas do Release de Resultados; **(b)** apresentação de Transação entre Parte Relacionada - TOTVS Techfin S.A. ("TOTVS Techfin"); **(c)** análise do Contrato de locação do espaço complexo Sêneca; **(d)** revisão da Política de Segurança da Informação Corporativa; Temas Informativos: **(V)** Relato dos trabalhos do Comitê de Estratégia ("CE"); **(VI)** Relato dos trabalhos do Comitê de Gente e Remuneração ("CGR"); **(VII)** Relato dos trabalhos do Comitê de Auditoria Estatutário ("CAE"); **(VIII)** Relato do Diretor-Presidente; e **(IX)** Sessão Executiva.

5. APRESENTAÇÕES, DISCUSSÕES E DELIBERAÇÕES:

5.I. Abertura da reunião

O Presidente do Conselho declarou aberta a reunião e passou a palavra à Secretária da mesa, que

apresentou a ordem do dia, descrita no item "4" desta Ata, bem como o status das ações solicitadas em reuniões anteriores. Na oportunidade, a Secretária informou os temas deliberativos a serem tratados e comunicou que todos os materiais de suporte foram disponibilizados no Portal de Governança Corporativa da Companhia.

5.II. Consignar o pedido de renúncia da Conselheira Sra. Maria Letícia de Freitas Costa: o Conselho tomou conhecimento do pedido de renúncia apresentado, em 3 de novembro de 2025, pela Sra. Maria Letícia de Freitas Costa, ao cargo de Vice-Presidente do Conselho de Administração e Membro do Comitê de Estratégia da TOTVS, conforme carta de renúncia arquivada na sede social da Companhia.

5.III. Deliberações sobre a composição do Conselho de Administração e Comitês de Assessoramento

(a) **Eleição de novo membro independente do Conselho de Administração e membro do Comitê de Estratégia**: Considerando a renúncia consignada no item anterior, o Conselho **elegeu**, em substituição, a Sra. Isabella de Oliveira Vianna Cavalcanti Wanderley, brasileira, casada, economista, portadora da Cédula de Identidade RG n.º 34.619.403-9, expedida pela SSP/SP, inscrita no CPF/MF sob o nº 949.606.587-20, com endereço comercial na Avenida Braz Leme, nº 1.000, Casa Verde, Município de São Paulo, Estado de São Paulo, CEP 02.511-000. A Conselheira ora eleita declara, sob as penas da lei, que cumpre todos os requisitos previstos para sua investidura nos cargos de membro independente do Conselho de Administração da Companhia e membro do Comitê de Estratégia, para cumprimento do mandato remanescente que se encerrará na Assembleia Geral Ordinária da Companhia a se realizar em 2026, de acordo com o artigo 150 da Lei nº 6.404/1976. A Conselheira ora eleita tomará posse em seu cargo mediante a assinatura do respectivo Termo de Posse, lavrado no livro de atas de reuniões do Conselho de Administração da Companhia, e da declaração a que se refere a Resolução CVM nº 80/2022.

(b) **Eleição do Vice-Presidente do Conselho de Administração**: nos termos do artigo 17 do Estatuto Social e artigo 10 do Regimento Interno do Conselho de Administração, o Conselho **elegeu**, por unanimidade, com mandato que se encerrará na Assembleia Geral Ordinária de 2026, para o cargo de Vice-Presidente do Conselho de Administração, o Conselheiro Sr. Gilberto Mifano, naturalizado brasileiro, casado, administrador de empresas, inscrito no CPF/MF sob o n.º 566.164.738-72 e portador da Cédula de Identidade RG n.º 3.722.086, expedida pela SSP/SP.

(c) **Eleição do Coordenador do Comitê de Estratégia**: nos termos do artigo 20 do Estatuto Social e dos artigos 22 e 33 do Regimento Interno do Conselho de Administração, o Conselho **elegeu**, por unanimidade, com mandato que se encerrará na Assembleia Geral Ordinária de 2026, para o cargo de Coordenador do Comitê de Estratégia, o Conselheiro Sr. Guilherme Stocco Filho, brasileiro, casado, administrador de empresas, inscrito no CPF/MF sob o n.º 176.649.438-25 e portador da Cédula de Identidade RG n.º 18.288.054, expedida pela SSP/SP.

Para fins de clareza, registra-se a nova composição do Comitê de Estratégia: **(i)** Sr. Guilherme Stocco Filho, brasileiro, casado, administrador de empresas, inscrito no CPF/MF sob n.º 176.649.438-25 e

portador da Cédula de Identidade RG n.º 18.288.054, expedida pela SSP/SP, como Coordenador do Comitê; **(ii)** Sra. Isabella de Oliveira Vianna Cavalcanti Wanderley, acima qualificada, como membro do Comitê; e **(iii)** Sr. Laércio José de Lucena Cosentino, brasileiro, casado, engenheiro eletricista, inscrito no CPF/MF sob n.º 032.737.678-39 e portador da Cédula de Identidade RG n.º 8.347.779, expedida pela SSP/SP, como membro do Comitê.

5.IV. Deliberações

Após as deliberações acerca das matérias acima descritas, o Conselho de Administração deliberou:

(a) com parecer favorável do CAE, o Conselho **aprovou** as Demonstrações Financeiras da Companhia relativas ao 3º trimestre do exercício de 2025, com a revisão trimestral da KPMG, mantendo uma via arquivada na sede social. As Demonstrações Financeiras e o *Release* de Resultados serão divulgados no prazo legal;

(b) com parecer favorável do CAE, o Conselho **aprovou** a Transação entre Partes Relacionadas referente à celebração do *2º Aditivo ao Contrato de Prestação de Serviços de Desenvolvimento, Suporte e Atividades Relacionadas* a ser firmado entre a Companhia e a TOTVS Techfin;

(c) com parecer favorável do CAE, o Conselho **aprovou** a celebração do contrato de locação firmado entre a Companhia e o Pátria Escritórios Fundo de Investimento Imobiliário Responsabilidade Ltda., referente ao Edifício Sêneca; e

(d) com parecer favorável do CAE, o Conselho **aprovou** a revisão da Política de Segurança da Informação Corporativa, que passará a vigorar a partir da presente data, conforme arquivada na sede social e divulgada na página de Relações com Investidores da Companhia.

5.V. Relato dos trabalhos do CE

Feito o relato dos trabalhos do Comitê de Estratégia, com destaque para os debates sobre projetos estratégicos.

5. VI. Relato dos trabalhos do CGR

Feito o relato dos trabalhos do Comitê de Gente e Remuneração, com destaque para as diretrizes iniciais para o processo de metas referente ao exercício de 2026, bem como o processo de avaliação de desempenho da Diretoria Estatutária de 2026.

5. VII. Relato dos trabalhos do CAE

Feito o relato dos trabalhos do Comitê de Auditoria Estatutário, com destaque para os debates acerca dos aspectos gerais da Reforma Tributária, incluindo a adequação da Companhia ao novo sistema tributário.

5. VIII. Relato do Diretor-Presidente

Feito o relato do Diretor-Presidente sobre os principais temas em curso, incluindo os indicadores de acompanhamento do Conselho e os resultados do mês de setembro de 2025.

5.IX. Sessão Executiva

Os membros se reuniram em sessão executiva, sem a presença de convidados.

6. APROVAÇÃO E ASSINATURA DA ATA: nada mais havendo a tratar, o Presidente declarou encerrados os trabalhos. A presente ata foi lida e aprovada, sem ressalvas, por todos os presentes e lavrada em livro próprio.

São Paulo, 3 de novembro de 2025.

Mesa:

_____	_____
Laércio José de Lucena Cosentino Presidente	Téssie Massarão Andrade Simonato Secretária

Conselheiros presentes:

_____	_____
Laércio José de Lucena Cosentino	Ana Claudia Piedade Silveira dos Reis
_____	_____
Edson Georges Nassar	Gilberto Mifano
_____	_____
Guilherme Stocco Filho	Tania Sztamfater Chocolat

POLÍTICA ORGANIZACIONAL

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 **Versão:** 04
Diretoria Responsável: Tecnologia da Informação	**Publicado em:** 03/11/2025
Normas vinculadas: CODEC, NO-SICORP-03, ISO 27001.	**Revisão até:** 03/11/2028

1. Objetivo

A Política de Segurança da Informação Corporativa da TOTVS tem por objetivo estabelecer os conceitos, diretrizes e práticas mínimas a serem seguidas por todas as Unidades de Negócio TOTVS, incluindo novas aquisições e integrações, que garantam a proteção de dados e informações de seus negócios, clientes, Parceiros e público em geral.

O presente documento possui caráter estratégico, com vistas a promover o gerenciamento da segurança das informações da TOTVS. A conformidade com esta política é obrigatória e fundamental para garantir a confidencialidade, integridade e disponibilidade das informações mantidas e tratadas pela TOTVS.

Esta Política demonstra abertamente o compromisso da Diretoria Estatutária e Conselheiros da TOTVS com a proteção das informações sob custódia da companhia, atendimento às leis e regulamentações aplicáveis a seus negócios em todas as suas dimensões, bem como o compromisso de nossas Unidades de Negócio em compreender e atender as necessidades específicas de nossos clientes.

2. Abrangência

Esta Política se aplica a todos os colaboradores, Fornecedores e Parceiros da TOTVS, com exceção das coligadas Techfin (e suas subsidiárias) e Dimensa (e suas subsidiárias), que possuem uma Governança Corporativa independente e seguem Políticas próprias, que não devem se contrapor a esta. A observância desta Política é obrigatória e reflete a legislação e regulamentação aplicáveis acerca dos temas relacionados à legislação referente à Proteção de Dados e Segurança da Informação.

Todas as Unidades de Negócio da TOTVS devem implementar medidas para garantir que colaboradores e, quando necessário, Parceiros, clientes e Fornecedores tenham acesso e comprovem a ciência sobre as diretrizes desta política. Também é dever das Unidades de Negócio, quando se fizer necessário, garantir a assinatura de termos de confidencialidade e não divulgação apropriados para os contratos firmados com empregados, Parceiros e Fornecedores que tenham acesso a dados e informações de propriedade ou sob guarda e responsabilidade da TOTVS.

3. Referências

- Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018.
- ABNT NBR ISO/IEC 27001 – Sistema de Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27701 – Requisitos e Diretrizes para a Gestão da Privacidade da Informação.
- ABNT NBR ISO/IEC 27017 – Segurança da Informação para Serviços de Computação em Nuvem.
- ABNT NBR ISO/IEC 27018 – Segurança da Informação para Proteção de Dados Pessoais em Nuvem.
- Lei de Direitos Autorais (Lei nº 9.610/1998).
- Lei da Propriedade Industrial (Lei nº 9.279/1996).

- Resolução CMN nº 4.893/2021.
- Resolução BCB nº 85/2021.
- Instrução CVM nº 505/2011.
- Instrução CVM nº 617/2019.
- Instrução CVM nº 586/2017.
- Resolução CVM nº 35/2021.
- SUSEP 638.

4. Definições

Acesso Privilegiado: refere-se a autorizações ou direito de acesso a sistemas, funções e recursos que excedam os de um usuário padrão. Uma conta com Acesso Privilegiado é aquela que pode executar funções relevantes para a segurança, que um usuário comum não é autorizado a realizar.
Ativos da Informação: são os dados, sistemas, equipamentos e infraestrutura de tecnologia que possuem valor para a TOTVS e que, portanto, requerem proteção e gestão para garantir sua disponibilidade, integridade e confidencialidade.
CODEC: Código de Ética e Conduta da TOTVS, documento que tem por objetivo estabelecer os princípios éticos e as regras de conduta que orientam o compromisso da TOTVS com a integridade dos seus negócios e relacionamentos internos e externos e se aplica a todos os conselheiros, administradores, acionistas que participem do controle da companhia, colaboradores, prestadores de serviços, Fornecedores e Parceiros.
Colaboradores: profissionais que atuam nas Unidades de Negócio da TOTVS por meio de um contrato de trabalho.
Dados Pessoais: toda informação relacionada a uma pessoa natural identificada ou identificável.
Dados Pessoais Sensíveis: 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.
Dados Sensíveis: informações que, se divulgadas ou acessadas indevidamente, podem comprometer a privacidade, a segurança e a integridade de indivíduos ou da própria organização, incluindo dados pessoais, financeiros e estratégicos.
Evento de Segurança da Informação: é uma ocorrência relacionada a ativos ou ambiente que indica um desvio no comportamento esperado ou um possível comprometimento.
Incidente de Segurança da Informação: um ou uma série de eventos de segurança da informação indesejados ou inesperados que possuem uma probabilidade significativa de comprometer as operações de negócio e ameaçar a Segurança da Informação.
Incidente de Segurança da Informação de alto impacto: incidente de segurança da informação que, ao violar um ou mais pilares de segurança, ameace a continuidade dos negócios, a conformidade legal ou a sobrevivência estratégica da organização, causando danos financeiros ou reputacionais severos e inaceitáveis de acordo com a escala de risco definida pela própria empresa.
ISO/IEC 27001: padrão para sistema de gestão da Segurança da Informação publicado pelo *International Organization for Standardization* e pelo *International Electrotechnical Commission* e descreve como gerenciar a Segurança da Informação em uma organização.
Lei Geral de Proteção de Dados Pessoais ou LGPD: Lei nº 13.709/2018, que regulamenta as atividades de Tratamento de Dados Pessoais.
Política de Gestão de Riscos, Controles Internos e Compliance: política PO-GC-03 que tem por objetivo estabelecer os princípios, as diretrizes e responsabilidades a serem observadas no processo de gestão de riscos corporativos, controles internos e compliance, bem como disseminar a cultura de Gestão de Riscos e o Programa de integridade por todos os níveis da TOTVS.

Segurança da Informação: forma de gerenciar as informações de uma organização mediante a preservação de propriedades como: confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e legalidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento.
Segurança da Informação local: Unidades de Negócio ou áreas internas da TOTVS que possuem uma estrutura de Segurança da Informação própria.
Terceiros/Fornecedores e Parceiros: prestadores de serviço que atuam junto às Unidades de Negócio da TOTVS por meio de contratos estabelecidos com Fornecedores de produtos e serviços.
TOTVS ou Companhia: TOTVS S.A., suas subsidiárias, e controladas diretas e indiretas, com exceção da TechFin (e suas subsidiárias) e Dimensa (e suas subsidiárias).
Unidades de Negócio da TOTVS: TOTVS Gestão e RD Station.
Valor de uma Informação ou Ativo: mensurado através do valor do ativo ou informação em si e do impacto potencial que essa pode gerar ao negócio diante da violação de um ou mais Pilares de Segurança da Informação.

5. Diretrizes

A TOTVS é comprometida com a proteção das informações sob sua responsabilidade, com observância da legislação em vigor, das disposições de seu estatuto social, do CODEC e das demais políticas corporativas.

Esta Política define de forma clara os conceitos, as diretrizes e responsabilidades a respeito da segurança das informações da TOTVS, e das informações de seus clientes que estejam sob a sua custódia; permite que os pilares de Segurança da Informação sejam preservados; que o tratamento de Dados Pessoais e de Dados Pessoais Sensíveis esteja em conformidade com a legislação aplicável e que os riscos de Segurança da Informação sejam geridos adequadamente, de modo a garantir a proteção e confiabilidade das informações e preservação da imagem da TOTVS perante o mercado e seus investidores.

A TOTVS compreende a diversidade de atividades das Unidades de Negócio que a compõem. Desta forma, estabelece os padrões mínimos de segurança a serem adotados, avaliando e aplicando controles adicionais que sejam procedentes para os diferentes cenários de cada uma delas.

Esta Política é apoiada por um conjunto de normativos e procedimentos de Segurança da Informação estabelecidos pela TOTVS.

5.1. Pilares da Segurança da Informação

Caracterizamos a Segurança da Informação pela preservação dos seguintes pilares:

Confidencialidade: garante que o acesso às informações da TOTVS, de seus clientes, Fornecedores, Parceiros e colaboradores sejam obtidos somente por pessoas autorizadas e para fins legítimos e éticos;

Integridade: garante a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados que estejam sob sua responsabilidade;

Disponibilidade: garante que a informação esteja sempre disponível aos profissionais que possuam o acesso necessário para tal; e assegura que os dados estejam disponíveis de acordo com o nível de serviço demandado pelas áreas de negócio e/ou contratado pelos clientes;

Rastreabilidade: garante a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registros das transações e alterações realizadas em seus sistemas e aplicações, permitindo a atribuição inequívoca de autoria das ações;

Legalidade: garante que todos os procedimentos relacionados à informação dentro da empresa sejam feitos de acordo com as leis e normas regulamentares;

Autenticidade: garante que os dados e informações são autênticos e legítimos por meio da autenticação de usuários e sistemas, de forma que seja possível o rastreio, atestando a veracidade das informações, não havendo manipulação ou intervenção externa ou de Terceiros não autorizados.

5.2. Segurança da Informação em Empresas Adquiridas e em Parcerias

A TOTVS, como uma empresa de tecnologia, além de compreender a necessidade de estabelecer padrões de Segurança da Informação sólidos e consistentes, busca implementa-los em todas as suas Unidades de Negócio e operações, considerando e respeitando a natureza específica de cada negócio e as regulamentações aplicáveis a eles, inclusive na utilização de Parceiros de negócios e nas empresas por ela adquiridas. Todas as Unidades de Negócio devem seguir práticas de segurança que atendam às necessidades operacionais e aos requisitos legais pertinentes, alinhadas em qualidade e eficiência com as políticas e procedimentos de segurança da TOTVS. Esse alinhamento assegura uma abordagem coesa e eficaz para a proteção da informação de forma geral e abrangente, promovendo a integridade e a resiliência das operações em todas as unidades.

5.3. Gestão de Riscos - Objetivos e Incidentes de Segurança da Informação

Todas as Unidades de Negócio da TOTVS devem manter um processo de gestão de riscos de Segurança da Informação com o objetivo de identificar, avaliar, tratar e monitorar riscos que possam afetar a confidencialidade, integridade, disponibilidade e privacidade de suas informações e ativos. Esse processo deve ser integrado às práticas gerais de gestão de riscos da empresa e deve garantir que os riscos sejam gerenciados de forma proativa e eficaz.

Devido à natureza dos riscos associados, todas as Unidades de Negócio que atuem no desenvolvimento e disponibilização de serviços de Nuvem devem manter processos específicos para identificar, analisar, avaliar, tratar, monitorar e reportar os riscos de Segurança da Informação que possam impactar os objetivos de suas áreas de Nuvem. As Unidades de Negócio devem ter como base os padrões internacionais para segurança do armazenamento em nuvem, conforme referências citadas neste documento.

Todas as Unidades de Negócio da TOTVS devem manter um canal para reporte, bem como ferramentas de monitoramento de eventos e Incidentes de Segurança da Informação, para avaliação de eventos que possam afetar o negócio e/ou as estratégias da empresa.

Todos os Incidentes de Segurança da Informação das Unidades de Negócio da TOTVS, assim que detectados pelas áreas de negócio, devem ser imediatamente reportados às suas respectivas áreas de Segurança da Informação Corporativa da TOTVS Gestão via csirt@totvs.com.br e Governança de Dados e IA, via dpo@totvs.com.br, quando houver envolvimento de dados pessoais, para serem devidamente registrados e tratados. As Unidades de Negócio devem ainda manter meios para o tratamento de Incidentes envolvendo dados pessoais conforme exigências da Lei Geral de Proteção de Dados Pessoais.

Os Incidentes classificados como de alto impacto ocorridos nas Unidades de Negócios da TOTVS devem, ainda, ser reportados periodicamente ao Comitê de Auditoria Estatutário, por meio do relatório de Incidentes apresentado pelo time de Segurança da Informação Corporativa da TOTVS nas reuniões periódicas, previamente agendadas. Em caso de Incidente com dados pessoais, o Incidente também deve ser reportado ao Comitê de Privacidade de Dados da TOTVS.

5.4. Gestão de Acessos e Identidade

Todas as Unidades de Negócio da TOTVS devem estabelecer e manter um processo de gestão de acessos e identidades que restrinja o acesso a recursos críticos e dados sensíveis apenas a indivíduos autorizados, baseando-se nos princípios de menor privilégio e segregação de funções e assegurando

níveis de acesso consonantes com a necessidade de cada função. A implementação de controles de acesso deve incluir autenticação multifatorial para reforçar a segurança, além de procedimentos claros para a concessão, modificação e revogação de permissões.

Todos os colaboradores e Terceiros que atuam em nome da TOTVS devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de os identificar como responsáveis por suas ações.

Acessos Privilegiados devem ser rigorosamente controlados e monitorados, garantindo que apenas usuários autorizados tenham permissão para acessar sistemas e dados sensíveis, obedecendo às regras de mínimo privilégio. As Unidades de Negócio devem garantir processos de revisão frequentes de acessos privilegiados garantindo a revogação tempestiva deles, assim que forem desnecessários.

A responsabilidade pela manutenção dos acessos de Terceiros, incluindo criação, revisão e revogação, é do gestor ou colaborador responsável pelo contrato com Terceiros. No caso de contratos com empresas terceiras que envolvam múltiplos usuários, cabe ao gestor do contrato garantir que todos os acessos relacionados estejam sempre adequados às atividades executadas, e revogados quando não mais necessários. Essa medida reforça a corresponsabilidade da gestão na Segurança da Informação, complementando os controles executados pela área de acessos.

O acesso físico dos colaboradores, Terceiros e visitantes, deve ser autorizado e controlado por meio da aplicação de processos e controles eficientes que atendam e assegurem a proteção de ambientes e ativos conforme necessidades locais. Os colaboradores que receberem Fornecedores ou Terceiros nas instalações das Unidades de Negócio devem sempre acompanhá-los durante todo o período da visita.

Todas as Unidades de Negócio da TOTVS devem implementar um sistema de monitoramento e verificação contínua das atividades de acesso. Os registros de acesso devem ser mantidos, protegidos e analisados regularmente para detectar e responder a qualquer comportamento anômalo ou suspeito.

Todas as Unidades de Negócio da TOTVS devem realizar a revisão periódica de acessos, minimamente anual para acessos gerais e semestral para acessos privilegiados, para os acessos concedidos aos colaboradores e Terceiros aos seus sistemas e instalações. Para os sistemas e instalações que sejam de gestão centralizada da TOTVS, as Unidades de Negócio incorporadas devem estar atentas aos períodos de revisão, prestando todo auxílio necessário para a realização do processo.

Todos os colaboradores devem receber treinamento contínuo sobre as políticas de acesso e práticas seguras para garantir que compreendam suas responsabilidades e as implicações de segurança associadas ao acesso a dados e sistemas.

5.5. Classificação e Tratamento da Informação

Para assegurar a proteção adequada às informações da TOTVS, todas as Unidades de Negócio devem adotar um método de classificação e rotulagem da informação de acordo com o grau de confidencialidade e criticidade para os negócios da TOTVS:

- As informações devem ser classificadas com base em seu valor, sensibilidade e criticidade. A classificação deve determinar os controles de segurança apropriados para a proteção das informações. Informações confidenciais e críticas devem ser tratadas com os níveis mais altos de segurança e protegidas contra acesso não autorizado, divulgação, alteração e destruição;

- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de Segurança da Informação da TOTVS em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

- As informações coletadas devem ser utilizadas para os fins previamente informados ou contratualmente definidos, podendo ser tratadas para finalidades adicionais desde que compatíveis com a base legal aplicável e devidamente autorizadas;
- O tratamento de Dados Pessoais deve estar em conformidade com a legislação de privacidade aplicável (nacional e/ou internacional) e seguir as diretrizes definidas pela Política de Proteção e Privacidade de Dados Pessoais da TOTVS.

5.6. Gestão dos Ativos da Informação

Todas as Unidades de Negócio da TOTVS devem adotar uma abordagem estruturada e sistemática para a gestão de ativos da informação que inclua sua identificação e classificação. Esses ativos devem ser registrados em um inventário detalhado, com informações mínimas sobre sua importância, localização e proprietário. A classificação deve refletir o valor do ativo e o impacto potencial de sua perda, comprometimento ou destruição.

A manutenção e descarte de ativos de tecnologia da TOTVS deve ser realizada apenas por Parceiros devidamente avaliados e homologados, ou por equipes internas da TOTVS formalmente designadas e capacitadas. As Unidades de Negócio devem manter um controle de entrada e saída de seus equipamentos, bem como termos de consentimento de uso assinados por colaboradores e Terceiros no momento da concessão e coleta de equipamentos.

As Unidades de Negócio da TOTVS devem, ainda, implementar controles de segurança apropriados para proteger os ativos da informação garantindo seu uso e a gestão adequadas, incluindo restrições de acesso, criptografia e medidas de proteção física dos equipamentos, bem como a utilização de controles para monitorar e revisar continuamente a segurança deles, atualizando constantemente políticas, normas e procedimentos para identificação de novas ameaças e vulnerabilidades, garantindo que os ativos permaneçam protegidos contra riscos emergentes. Mídias móveis e portas de equipamentos devem ser gerenciadas a fim de evitar riscos de infecção e vazamentos de informação por tais meios.

5.6.1. Uso aceitável dos ativos da TOTVS

Todos os colaboradores e Terceiros devem zelar pela segurança e proteção dos ativos da informação concedidos pelas Unidades de Negócio da TOTVS para realização de suas atividades, observando as seguintes regras:

- Utilizar os ativos de tecnologia (computadores, dispositivos móveis, sistemas e dados) exclusivamente para fins relacionados ao trabalho, exceto em situações expressamente autorizadas pelo gestor do colaborador, pela área de Segurança da Informação e pela área de TI responsável pela unidade de negócio, em casos específicos e pontuais;
- Somente utilizar ativos para os quais o colaborador foi explicitamente autorizado;
- Não compartilhar credenciais de acesso com Terceiros;
- Proteger informações confidenciais e sensíveis. Não divulgar nem armazenar dados sensíveis em locais não autorizados;
- Utilizar criptografia para proteger dados em trânsito e em repouso;
- Usar senhas fortes e únicas para acessar sistemas e dados. Alterar senhas regularmente e nunca compartilhar credenciais;
- Sempre que possível, utilizar métodos adicionais de autenticação para acessar informações e sistemas;
- Instalar apenas software que tenha sido autorizado, homologado e licenciado pela empresa. Não usar aplicativos não verificados;

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

- Manter seguros o computador e outros dispositivos, disponibilizados pela TOTVS. Usar cadeados e outros dispositivos de segurança quando apropriado;
- Armazenar dispositivos móveis e portáteis em locais seguros quando não estiverem em uso;
- Utilizar dispositivos de armazenamento removíveis autorizados apenas quando necessário e protegê-los com senha e criptografia;
- Armazenar dados em locais designados pela empresa, como pastas seguras na rede corporativa;
- Enviar dados sensíveis por meio de canais seguros e protegidos, como e-mails criptografados;
- Verificar sempre a autenticidade dos destinatários antes de transmitir informações confidenciais;
- Ficar atento a qualquer comportamento ou alerta suspeito e reportar imediatamente ao suporte técnico e/ou ao time de Segurança da Informação;
- Seguir todas as políticas e procedimentos estabelecidos para o uso de tecnologia. Qualquer violação deve ser imediatamente reportada ao departamento de TI da Unidade de Negócio;
- Informar qualquer Incidente de segurança ou uso inadequado dos ativos ao seu supervisor ou ao suporte técnico ou ao time de Segurança da Informação.

5.7. Criptografia

Todas as Unidades de Negócio da TOTVS devem avaliar e adotar práticas de criptografia condizentes com o valor de seus ativos de informação a fim de assegurar a proteção dos dados críticos, sensíveis e confidenciais em repouso ou em trânsito.

A criptografia deve ser aplicada a todas as comunicações eletrônicas expostas a internet e transmissões de dados para evitar acessos não autorizados e garantir que as informações sejam transmitidas de forma segura. Além disso, a criptografia deve também ser empregada durante o processamento de dados para proteger informações temporariamente armazenadas ou manipuladas, assegurando que os dados da TOTVS permaneçam protegidos contra exposições e acessos indevidos.

Todas as Unidades de Negócio da TOTVS devem estabelecer processos seguros para a gestão das chaves criptográficas, incluindo a sua geração, armazenamento e rotação. A seleção de algoritmos deve ser feita com base em uma avaliação contínua das melhores práticas e diretrizes de segurança, garantindo que apenas métodos seguros e aprovados sejam utilizados.

5.8. Segurança Física e do Ambiente

Todas as Unidades de Negócio da TOTVS devem implementar controles de segurança física para suas instalações e ambientes que garantam a integridade e a segurança de equipamentos, sistemas e dados, considerando a implementação de ferramentas para restrição de acesso físico e monitoramento de áreas e instalações sensíveis. Todas as Unidades de Negócio da TOTVS que tenham data centers locais devem ainda contar com equipamentos de monitoramento, climatização e controles anti-incêndio das salas. Os planos para recuperação destes locais devem constar no Plano de Recuperação de Desastres destas Unidades de Negócio.

Além da segurança de acesso, para os data centers, devem também ser consideradas medidas para proteger as instalações contra riscos ambientais e sistemas de controle ambiental para mitigação de possíveis danos a equipamentos e dados da TOTVS. A infraestrutura elétrica deve ser projetada para

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

suportar os requisitos de energia dos sistemas críticos, incluindo a instalação de fontes de energia ininterrupta (UPS) e geradores para garantir a continuidade das operações em caso de falhas na rede elétrica.

5.9. Segurança nas Comunicações

Todas as Unidades de Negócio da TOTVS devem implementar medidas de segurança na transmissão de informações interna e externamente. Comunicações eletrônicas, tanto internas quanto externas, devem ser protegidas contra interceptações e acessos não autorizados. Isso inclui a utilização de protocolos de criptografia, firewalls, sistemas de detecção e prevenção de intrusões, e o monitoramento contínuo das redes para identificar e mitigar ameaças em tempo real, assegurando que os dados transmitidos por redes sejam protegidos de ataques cibernéticos e vazamentos. A comunicação de dados sensíveis e confidenciais deve ser realizada exclusivamente por meios que garantam a segurança e a privacidade.

A segurança das redes deve ser revisada regularmente para garantir que as defesas estejam atualizadas. O acesso às redes e sistemas de comunicação deve ser controlado e restrito a pessoal autorizado, e o uso de dispositivos de rede não autorizados deve ser proibido.

Para prestação de seus serviços, todos os colaboradores e Terceiros devem utilizar apenas comunicadores e sistemas de transmissão de informações devidamente homologados e disponibilizados pela TOTVS. Qualquer violação dessa condição pode ser considerada um Incidente de Segurança da Informação.

5.10. Cópias de segurança e testes de recuperação

Todas as Unidades de Negócio da TOTVS devem estabelecer e manter um processo de geração e testes de cópias de segurança dos seus dados críticos a fim de protegê-los contra a perda e corrupção. Isso inclui a definição clara dos tipos e frequências de backups, o armazenamento e a proteção das cópias de segurança, bem como a documentação dos processos de recuperação e resultados dos testes. É imperativa a realização de cópias de segurança (backups) em períodos regulares e consistentes, abrangendo todos os dados essenciais e sistemas críticos da TOTVS, garantindo seu armazenamento em locais seguros, geograficamente distintos, a fim de assegurar a proteção contra desastres locais.

As Unidades de Negócio devem ainda implementar um programa regular de testes de restauração para verificar a eficácia das cópias de segurança. Os testes de restauração devem ser documentados a fim de garantir a integridade das bases salvaguardadas. A frequência dos testes deve ser baseada na criticidade dos dados e sistemas, e os resultados devem ser revisados para garantir a continuidade dos processos de recuperação.

5.11. Gestão de vulnerabilidades e monitoramento

Todas as Unidades de Negócio da TOTVS devem implementar ferramentas e técnicas de varredura de vulnerabilidades para detectar e classificar falhas de segurança em sistemas e aplicações que possam acarretar riscos para os ativos da informação da TOTVS. As técnicas devem prever processos para identificação, classificação, priorização e remediação das vulnerabilidades. A remediação deve ser baseada no risco e impacto potencial para os ativos e operações das Unidades de Negócio, garantindo que as vulnerabilidades críticas sejam abordadas com a máxima urgência e eficiência.

As Unidades de Negócio da TOTVS devem também garantir o monitoramento contínuo das atividades internas e externas que possam impactar a integridade e a confidencialidade dos sistemas. Todas as Unidades de Negócio da TOTVS devem implementar soluções de monitoramento para detecção e prevenção de intrusões, bem como analisar regularmente logs de eventos coletados para identificar e responder rapidamente a atividades suspeitas ou anômalas.

5.12. Segurança da Informação nas relações com Fornecedores

Todas as Unidades de Negócio da TOTVS devem implementar um processo de avaliação dos riscos associados à contratação de Fornecedores que terão acesso a dados sensíveis ou sistemas críticos da TOTVS.

A avaliação deve verificar a adoção de práticas e controles adequados de Segurança da Informação compatíveis com as exigências regulatórias e a segurança na execução dos serviços contratados, assegurando que estes Fornecedores implementem práticas adequadas de segurança.

O processo deve considerar também a verificação contínua da conformidade com os padrões de segurança por meio do monitoramento dos serviços, auditorias regulares e revisões de relatórios de segurança e a adoção de medidas seguras para o encerramento do contrato, garantindo a remoção segura do acesso dos Fornecedores aos dados e sistemas da TOTVS, bem como recolhimento de ativos da informação concedidos durante a execução do contrato.

5.13. Aquisição e desenvolvimento seguro de sistemas

Todas as Unidades de Negócio da TOTVS devem manter um processo para aquisição e desenvolvimento seguro de softwares que contemple a avaliação de segurança dos Fornecedores e dos produtos oferecidos ou desenvolvidos. Isso inclui verificar a conformidade do software com padrões de segurança, realizar testes de vulnerabilidade e revisar as práticas de segurança do fornecedor para assegurar a qualidade e segurança do software. Além disso, todos os contratos com Fornecedores devem incluir cláusulas de segurança que abordam a proteção dos dados e a responsabilidade em caso de Incidentes de segurança, bem como a possibilidade de fiscalização/auditoria do processo de desenvolvimento, que podem ser substituídas pela apresentação de certificações de segurança da informação, desde que aplicável e que essa sane as dúvidas relacionadas à segurança da informação.

Para o desenvolvimento de softwares além das análises de riscos consideradas para o ciclo de vida de desenvolvimento, a implementação de controles, de segurança e privacidade conforme metodologias de *Privacy by Design* e *Security by Design* durante o desenvolvimento, e a realização de testes de segurança, todas as Unidades de Negócio da TOTVS devem observar as regulamentações e práticas aplicáveis ao tipo de sistema a ser desenvolvido considerando, mas não se limitando a:

- Lei Geral de Proteção de Dados Pessoais (LGPD);
- Instruções de Segurança da Informação da Comissão de Valores Mobiliários – CVM;
- Lei de Direitos Autorais (Lei nº 9.610/1998);
- Lei da Propriedade Industrial (Lei nº 9.279/1996);
- Código de Defesa do Consumidor;
- ISO/IEC 27034;
- NIST Secure Software Development Framework (SSDF);
- ABNT NBR ISO/IEC 27001 – Sistema de Gestão da Segurança da Informação;
- ABNT NBR ISO/IEC 27701 – Requisitos e Diretrizes para a Gestão da Privacidade da Informação.

Todas as Unidades de Negócio da TOTVS devem compreender as necessidades legais, regulamentares e demais particularidades de clientes a fim de desenvolverem sistemas que tragam não apenas a proteção das informações tratadas, mas a sua segurança legal e regulatória. As Unidades de Negócio devem monitorar os cenários a fim de garantir a atualização de sistemas sempre que necessário para atender a alterações no ambiente legislativo.

5.14. Gestão de Incidentes

As Unidades de Negócio da TOTVS devem manter canais de comunicação de Incidentes para atendimento aos colaboradores, Terceiros e a seus clientes. Devem estabelecer e manter um processo para a gestão de Incidentes de Segurança da Informação e privacidade que inclua a identificação, resposta e resolução de Incidentes que possam comprometer a integridade, confidencialidade ou disponibilidade de dados e sistemas. O processo deve incluir planos de resposta a Incidentes e procedimentos claros para a notificação e escalonamento de Incidentes às partes interessadas, comunicação e conhecimento das responsabilidades e do fluxo de comunicação adequado.

Todos os Incidentes tratados devem ser investigados para determinar suas causas e impactos, a fim de que sejam implementadas medidas corretivas e preventivas que mitiguem o risco de recorrências futuras. Os registros de Incidentes e as lições aprendidas devem ser revisados e utilizados para aprimorar continuamente as políticas e os procedimentos de segurança e privacidade.

5.15. Gestão da Continuidade de Negócios

Todas as Unidades de Negócio da TOTVS devem estabelecer e manter um plano de gestão da continuidade de negócios para assegurar a operação contínua e a recuperação eficiente das atividades em caso de Incidentes críticos. O plano deve incluir a identificação e avaliação de riscos que possam afetar as operações, a definição de estratégias para a continuidade dos processos essenciais e a implementação de medidas para minimizar a interrupção dos serviços, bem como a realização de testes e simulações.

As Unidades de Negócio da TOTVS devem garantir que os planos de recuperação de suas atividades levem em consideração, quando necessário, o atendimento dos tempos de retorno e demais necessidades específicas, regulamentares ou contratuais, de seus clientes. As informações para definição dos planos de continuidade e recuperação devem ser avaliadas junto às áreas jurídicas e de Gestão de Riscos da TOTVS.

5.16. Propriedade intelectual

Todas as Unidades de Negócio da TOTVS devem adotar medidas para proteger a propriedade intelectual própria e de Parceiros, assegurando que os direitos de propriedade sejam respeitados e protegidos contra acesso indevido, uso indevido ou divulgação indevidas. As Unidades de Negócio devem assegurar que acordos contratuais com clientes, Parceiros e Fornecedores contenham cláusulas específicas para a proteção de softwares e aplicações, estabelecendo claramente os direitos de propriedade intelectual, proteção contra o uso não autorizado, cópia e a modificação dos softwares e aplicações fornecidos ou utilizados em colaboração.

A TOTVS repudia qualquer tipo de utilização não autorizada e não licenciada de softwares e aplicações e mantém controles para gestão de licenças de uso de todos os sistemas que utiliza. A identificação de situações contrárias a isto deve ser tratada como Incidente de Segurança da Informação.

5.17. Inteligência Artificial (IA)

5.17.1. Utilização de Inteligência Artificial por colaboradores e Terceiros

Todas as Unidades de Negócio da TOTVS devem garantir a utilização segura e ética da Inteligência Artificial (IA) em suas operações, adotando medidas para proteger a integridade, a privacidade e a segurança dos dados compartilhados nestas ferramentas. As Unidades de Negócio devem adotar práticas que garantam utilização de IA seguras com controles de acesso

adequados para garantir que apenas usuários autorizados possam interagir com os sistemas, a fim de minimizar vulnerabilidades e proteger contra possíveis vazamentos de informações e ataques cibernéticos. Todos os colaboradores e Terceiros autorizados a utilizar IA devem ser devidamente capacitados quanto aos riscos e a utilização segura dessas ferramentas.

5.17.2. Desenvolvimento ético e seguro de Inteligência Artificial

No desenvolvimento de IA, todas as Unidades de Negócio da TOTVS devem seguir princípios de segurança e ética para assegurar que os sistemas sejam projetados e implementados de forma responsável, realizando avaliações de risco e testes de segurança para identificar e mitigar possíveis ameaças antes do lançamento. Além disso, o desenvolvimento deve considerar os impactos éticos, garantindo que as soluções de IA não perpetuem preconceitos, não invadam a privacidade e respeitem as regulamentações aplicáveis. Para manter a confiança e a conformidade da utilização e desenvolvimento de IA, todas as Unidades de Negócio da TOTVS devem revisar e atualizar suas políticas de IA regularmente. As práticas de desenvolvimento e utilização devem ser continuamente monitoradas e ajustadas conforme as mudanças tecnológicas e regulamentares sobre o assunto.

5.18. Proteção e privacidade de dados

A TOTVS assume o compromisso fundamental com a privacidade e proteção dos dados de todos os seus *stakeholders* (colaboradores, Fornecedores, Parceiros e clientes). O tratamento de dados pessoais na empresa é regido pelo nosso Programa de Privacidade de Dados, que garante a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com as práticas de segurança e confidencialidade. Para detalhes sobre governança, diretrizes e controles, consulte a Política de Proteção e Privacidade de Dados da TOTVS.

5.19. Conformidade legal, regulatória e contratuais

Todas as Unidades de Negócio da TOTVS devem garantir a conformidade com todas as leis e regulamentações aplicáveis relacionadas à Segurança da Informação e à proteção de dados e as regulações aplicáveis ao cumprimento dos acordos contratuais com os clientes.

As Unidades de Negócio devem manter um processo para monitorar, identificar e entender as obrigações legais e regulamentares específicas para cada jurisdição em que operam, incluindo aquelas relacionadas à privacidade de dados, segurança cibernética e direitos dos indivíduos. As Unidades de Negócio devem implementar controles e práticas que atendam a essas exigências, realizando avaliações regulares para assegurar que suas políticas e procedimentos estejam atualizados e em conformidade com as mudanças nas legislações.

5.20. Auditoria dos Processos de Segurança da Informação

A auditoria interna e externa podem, a qualquer momento, conduzir auditorias nos processos de Segurança da Informação para garantir a eficácia e a conformidade das práticas implementadas pelas Unidades de Negócio da TOTVS. Essas auditorias visam avaliar a aderência às políticas de segurança, identificar vulnerabilidades e verificar a eficácia dos controles e procedimentos estabelecidos. A auditoria pode ser realizada por equipes internas ou externas independentes, sempre buscando uma visão imparcial sobre o estado atual da Segurança da Informação.

5.21. Melhoria Contínua

A TOTVS reforça seu compromisso com a melhoria contínua dos processos de Segurança da Informação, assegurando que as políticas, procedimentos e controles sejam constantemente revisados e aprimorados, alinhados às melhores práticas e garantindo que as práticas e controles evoluam de acordo com as mudanças tecnológicas e os novos desafios de segurança, visando sempre

a continuidade dos negócios e a proteção contra ameaças emergentes. Esse compromisso é evidenciado pela implementação de um ciclo sistemático de avaliação e atualização, que incorpora feedback, resultados de auditorias e lições aprendidas. Ao adotar uma abordagem proativa e adaptativa, fortalece continuamente sua postura de segurança, protegendo de forma eficaz os ativos críticos e garantindo a resiliência organizacional em um ambiente de ameaças em constante evolução.

5.22. Treinamentos de Conscientização

Todas as Unidades de Negócio da TOTVS devem planejar e manter um programa de treinamento e comunicação que garanta a conscientização de todos os seus colaboradores sobre as políticas e práticas de Segurança da Informação, incluindo sessões regulares e reciclagens de treinamento, atualizações sobre novas ameaças e procedimentos, e campanhas contínuas de conscientização para reforçar a importância da segurança de dados. As Unidades de Negócio devem monitorar a eficácia do programa e ajustar as abordagens conforme necessário para assegurar que a cultura de segurança seja disseminada e esteja alinhada com a cultura da TOTVS, melhores práticas e requisitos regulatórios.

Todos os colaboradores e Terceiros, quando aplicável, devem compreender suas responsabilidades individuais na proteção de informações para que estejam preparados para execução de suas atividades, bem como para identificar e responder a Incidentes de segurança.

6. Atribuições

De forma geral, cabe a todos os colaboradores e prestadores de serviço da TOTVS:

- Cumprir fielmente esta Política, as normas e os procedimentos de Segurança da Informação aplicáveis a suas atividades;
- Realizar os treinamentos obrigatórios disponibilizados pelas Unidades de Negócio da TOTVS;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pelo TOTVS;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela TOTVS;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (elevadores, transporte terrestre e aéreo, restaurantes, encontros sociais etc.), incluindo emitir comentários e opiniões em blogs e redes sociais;
- Comunicar imediatamente à área de Segurança da Informação local sobre qualquer descumprimento ou violação desta Política, bem como reportar quaisquer Incidentes de Segurança da Informação.

Times de Segurança da Informação Local

- Prover ampla divulgação desta Política, bem como das Normas e Procedimentos de Segurança da Informação para todos os colaboradores e Terceiros sob a administração e gerência da empresa;
- Promover ações de conscientização sobre Segurança da Informação para todos os colaboradores locais;

- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da Segurança da Informação;
- Implantar, administrar e monitorar os sistemas e controles sob gerência da área de Segurança da Informação local ou, quando aplicável, sob a gerência Corporativa da TOTVS;
- Propor eventuais alterações desta Política;
- Identificar, analisar, avaliar, tratar, monitorar, reportar e registrar os Incidentes de segurança na TI;
- Registrar e reportar os Incidentes no ambiente corporativo.

Equipe de Segurança da Informação de Cloud

- Assegurar o funcionamento do Sistema de Gestão de Segurança e Privacidade da Informação de Cloud, conforme as diretrizes das normas ISO 27001, ISO 27701, ISO 27017 e ISO 27018;
- Definir e implementar requisitos de segurança para novos projetos e iniciativas de Cloud;
- Estruturar e evoluir serviços de segurança para Clientes Cloud;
- Apoiar os Clientes de Cloud em seus questionamentos de auditoria e conformidade, sempre que possível por meio de ferramentas de autosserviço;
- Assegurar a correta identificação e tratamento de Incidentes de segurança de Cloud;
- Gerenciar acessos respeitando os princípios de menor privilégio, segregação de funções e revisão periódica para os ativos administrados por Cloud;
- Mapear e tratar vulnerabilidades de segurança no ambiente sob responsabilidade de Cloud, conforme os objetivos das certificações ISO 27001, ISO 27701, ISO 27017 e ISO 27018;
- Assegurar o correto registro e rastreabilidade de ações para os ativos sob administração de Cloud;
- Sustentar, desenvolver e evoluir tecnologias para a operação de segurança em Cloud;
- Propor eventuais alterações desta Política.

TI/ Sustentação dos Sistemas

- Notificar às áreas de Segurança da Informação quando identificar eventos suspeitos, que possam indicar a ocorrência de Incidentes de Segurança da Informação;
- Homologar e aplicar as melhorias de segurança recomendadas pelas áreas de Segurança da Informação.

Segurança Patrimonial

- Gerenciar o acesso físico às dependências da empresa.

Comissão de Ética e Conduta

- Analisar ocorrências de violações desta Política e a aplicação de consequências, quando cabível, respeitadas as atribuições do Comitê de Auditoria Estatutário acerca dos indicadores de Riscos de Segurança da Informação.

Comitê de Auditoria Estatutário

- Acompanhar os indicadores de Incidentes, Riscos e ocorrências de violações de regras desta Política no tocante às rotinas das áreas de Segurança da Informação, reportando seus resultados ao Conselho de Administração;
- Avaliar as informações recebidas e monitorar ações quanto à ocorrência de eventos relacionados às questões de Segurança da Informação, respeitando a classificação de criticidade definida para os mesmos;
- Avaliar a presente Política e suas revisões, e apresentar recomendações ao Conselho de Administração da TOTVS quanto à sua aprovação.

Conselho de Administração

- Tomar conhecimento, através do Comitê de Auditoria Estatutário, sobre o acompanhamento dos Incidentes relevantes, indicadores de riscos, submetidos pela área de Segurança da Informação e ouvido o Comitê de Auditoria Estatutário, deliberando, quando necessário, para preservação da Segurança da Informação;
- Aprovar esta Política e suas revisões.

7. Ações de Gerenciamento

A área de Segurança da Informação Corporativa deve supervisionar o cumprimento desta Política, encaminhando eventuais casos de descumprimento à Comissão de Ética e Conduta.

8. Gestão de Consequências

Em caso de descumprimento desta Política serão adotadas medidas de gestão de consequências adequadas ao tratamento da desconformidade, devendo, ainda, tal descumprimento ser informado ao Comitê de Auditoria Estatutário.

9. Aprovações

Nome / Cargo	Descrição
Mara Maehara Diretora de Tecnologia da Informação	Elaboração
Marcos Corradi Gerente Executivo de Controles Internos, Riscos e Compliance	Revisão
Patricia Vetri Thomazelli Magalhães Fonseca Diretora Jurídica	Revisão
Gustavo Dutra Bastos Vice-Presidente de Plataformas & TI	Revisão
Dennis Herszkowicz CEO	Revisão
Comitê de Auditoria Estatutário	Recomendação
Conselho de Administração	Aprovação

TOTVS S.A.
Corporate Taxpayers' Id. (CNPJ/MF) No. 53.113.791/0001-22
Company Registry (NIRE) No. 35.300.153.171

MINUTES OF THE BOARD OF DIRECTORS' MEETING
HELD ON NOVEMBER 3rd, 2025

1. DATE, TIME, and PLACE: meeting held on November 3rd, 2025, at 1:00 p.m., at the headquarters of TOTVS S.A. ("TOTVS" or the "Company"), located at Avenida Braz Leme, 1.000, Casa Verde district, city of São Paulo, State of São Paulo, Zip Code 02.511-000, Brazil, pursuant to article 18 of the Company's Bylaws and article 16 of the Charter of the Board of Directors.

2. CALL AND ATTENDANCE: the corresponding call notice was duly sent pursuant to article 18, paragraph 1 of TOTVS's Bylaws. All members of the Board of Directors (the "Board") were present, namely: Ana Claudia Piedade Silveira dos Reis, Edson Georges Nassar, Gilberto Mifano, Guilherme Stocco Filho, Laércio José de Lucena Cosentino and Tania Sztamfater Chocolat. Present as guests for part of the meeting: Dennis Herszkowicz, Chief Executive Officer (except item IX); Gilsomar Maia Sebastião, Chief Financial and Investor Relations Officer (items 5.IV); Ricardo Guerino, Controller and Financial Planning Officer (item 5.IV); and Sergio Pauperio Serio Filho, Investor Relations Officer (item 5.IV). Glaucia Macedo de Sousa, Corporate Governance Coordinator, attended the meeting as a listener.

3. CHAIR AND SECRETARY: Chairman of the Board: Laércio José de Lucena Cosentino; Secretary: Téssie Massarão Andrade Simonato.

4. AGENDA: (I) Opening of the meeting, including the measures requested regarding topics from previous meetings; **(II)** To accept the resignation request of Ms. Maria Letícia de Freitas Costa as Board Member; Deliberatives: **(III) (a)** to elect Ms. Isabella de Oliveira Vianna Cavalcanti Wanderley as an independent member of the Board of Directors, pursuant to Article 150 of Law No. 6.404/1976; **(b)** to elect the new Vice-President of the Board of Directors; and **(c)** to elect the new Strategy Committee Coordinator; **(IV) (a)** review of the Company's Financial Statements for the 3rd quarter of fiscal year 2025, with the quarterly review by KPMG Auditores Independentes Ltda. ("KPMG"), accompanied by the Earnings Release; **(b)** presentation of Related Party Transaction - TOTVS Techfin S.A. ("TOTVS Techfin"); **(c)** analysis of the lease contract for the Sêneca complex space; **(d)** Review of Corporate Information Security Policy; Informative Topics: **(V)** Report on the work of the Strategy Committee ("CE"); **(VI)** Report on the work of the People and Compensation Committee ("CGR"); **(VII)** Report on the work of the Statutory Audit Committee ("CAE"); **(VIII)** Report from the Chief Executive Officer; and **(IX)** Executive Session.

5. PRESENTATION, DISCUSSIONS AND RESOLUTIONS:

5.I. Opening of the meeting

The Chairman of the Board declared the meeting established and gave the floor to the Secretary, who informed the agenda, as described in section "4" of these minutes, as well as the status of the actions

requested at previous meetings. On this occasion, the Secretary reported on the deliberative topics to be discussed and announced that all the support materials had been made available on the Corporate Governance Portal.

5.II. To accept the resignation request of Ms. Maria Letícia de Freitas Costa as Board Member: The Board acknowledged the resignation request submitted on November 3rd, 2025, by Ms. Maria Letícia de Freitas Costa from the position of Vice President of the Board of Directors and Member of the Strategy Committee of TOTVS, as per the resignation letter filed at the Company's headquarters.

5.III. Resolutions on the composition of the Board of Directors and Advisory Committees

(a) **Election of a new independent member of the Board of Directors and member of the Strategy Committee**: Considering the resignation mentioned in the previous item, the Board **elected** Ms. Isabella de Oliveira Vianna Cavalcanti Wanderley, Brazilian citizen, married, economist, bearer of Brazilian identification document ("RG") No. 34.619.403-9, delivered by SSP/SP, registered in CPF/MF under No. 949.606.587-20, with business address at Avenida Braz Leme, nº 1.000, Casa Verde, São Paulo City, State of São Paulo, Zip Code 02.511-000. The newly elected member declares, under penalty of law, that she meets all the requirements for her appointment as an independent member of the Company's Board of Directors and member of the Strategy Committee, to fulfill the remaining term of office, which will end at the Company's Annual General Shareholders' Meeting to be held in 2026, in accordance with Article 150 of Law No. 6,404/1976. The newly elected member will take office upon signing the respective Term of Office, recorded in the minutes book of the Company's Board of Directors, and the declaration referred to in CVM Resolution No. 80/2022.

(b) **Election of the Vice-President of the Board of Directors**: pursuant to Article 17 of the Bylaws and Article 10 of the Internal Regulations of the Board of Directors, the Board unanimously **elected**, with term of office ending at Company's Annual General Shareholders' Meeting to be held in 2026, Mr. Gilberto Mifano, naturalized Brazilian, married, business administrator, registered in CPF/MF under No. 566.164.738-72 and bearer of Brazilian identification document ("RG") No. 3.722.086, delivered by SSP/SP.

(c) **Election of the Strategy Committee Coordinator**: pursuant to Article 20 of the Bylaws and Articles 22 and 33 of the Internal Rules of the Board of Directors, the Board unanimously **elected**, with a term ending at the 2026 Annual General Shareholders' Meeting, to the position of Strategy Committee Coordinator, Mr. Guilherme Stocco Filho, brazilian, married, business administrator, registered in CPF/MF under No. 176.649.438-25 and bearer of Brazilian identification document ("RG") No. 18.288.054, delivered by SSP/SP.

For clarity purposes, the new composition of the Strategy Committee is hereby recorded: **(i)** Mr. Guilherme Stocco Filho, Brazilian, married, business administrator, registered in CPF/MF under No. 176.649.438-25 and bearer of Brazilian identification document ("RG") No. 18.288.054, delivered by SSP/SP, as Committee Coordinator; **(ii)** Ms. Isabella de Oliveira Vianna Cavalcanti Wanderley, above qualified, as a member of the Committee; and **(iii)** Mr. Laércio José de Lucena Cosentino, Brazilian,

married, electrical engineer, registered in CPF/MF under No. 032.737.678-39 and bearer of Brazilian identification document ("RG") No. 8.347.779, delivered by SSP/SP, as a member of the Committee.

5.IV. Resolutions

After the resolutions on the matters described above, the Board of Directors resolved:

(a) with the CAE's favorable opinion, the Board **approved** the Company's Financial Statements for the 3rd quarter of fiscal year 2025, with KPMG's quarterly review, and a copy is filed at the corporate headquarters. The Financial Statements and Earnings Release will be disclosed within the legal deadline;

(b) with the CAE's favorable opinion, the Board **approved** the Related Party Transaction regarding the execution of the 2*nd Amendment to the Agreement for the Provision of Development, Support and Related Services* to be entered into between the Company and TOTVS Techfin**;**

(c) with the CAE's favorable opinion, the Board **approved** the signing of the lease contract of Sêneca Building between the Company and Pátria Escritórios Fundo de Investimento Imobiliário Responsabilidade Ltda.; and

(d) with the CAE's favorable opinion, the Board **approved** the revision of the Corporate Information Security Policy, which will come into effect as of this date, as filed at the Company's headquarter and disclosed on the Company's Investor Relations page**.**

5.V. Report of the CE

The report on the work of the Strategy Committee was presented, highlighting the discussions on strategic projects.

5. VI. Report of the CGR

The report on the work of the People and Compensation Committee was presented, highlighting the initial guidelines for the goal-setting process for the 2026 fiscal year, as well as the performance evaluation process for the Statutory Officers in 2026.

5. VII. Report of the CAE

The report on the work of the Statutory Audit Committee was presented, highlighting the discussions on the general aspects of the Tax Reform, including the Company's compliance with the new tax system.

5. VIII. Report from the CEO

The CEO reported on the main issues underway, including the Board's monitoring indicators and the results for September 2025.

5.IX. Executive Session

The members met in an executive session without the presence of guests.

6. APPROVAL AND SIGNATURE OF THESE MINUTES: there being no further issues to address, the Chairman called the meeting to a close. These minutes were read and approved with no reservations by all those present.

We certify that this is a free translation of the original minutes drawn up in the Company's records.

São Paulo, November 3rd, 2025.

Chair and Secretary:

_____	_____
Laércio José de Lucena Cosentino President	Téssie Massarão Andrade Simonato Secretary

Board members present:

_____	_____
Laércio José de Lucena Cosentino	Ana Claudia Piedade Silveira dos Reis
_____	_____
Edson Georges Nassar	Gilberto Mifano
_____	_____
Guilherme Stocco Filho	Tania Sztamfater Chocolat

ORGANIZATIONAL POLICY

Subject: Corporate Information Security	**Identification:** PO-SICORP-01 **Version:** 04
Board in Charge: Information Technology	**Published on:** 03/11/2025
Related Rules: CODEC, NO-SICORP-03, ISO 27001.	**Review by:** 03/11/2028

1. Purpose

The TOTVS Corporate Information Security Policy aims to establish the concepts, guidelines, and minimum practices to be followed by all TOTVS Business Units, including new acquisitions and integrations, to ensure the protection of data and information belonging to its businesses, customers, Partners, and the general public.

This document was strategically created to promote the management of information security at TOTVS. Compliance with this policy is mandatory and essential to ensure the confidentiality, integrity, and availability of information maintained and processed by TOTVS.

This Policy clearly demonstrates the commitment of the Company's Statutory Board of Directors and Directors to safeguarding information under the Company's custody, complying with all applicable laws and regulations governing its business in every aspect, as well as the commitment of our Business Units to understand and meet our customers' specific needs.

2. Scope

This Policy applies to all TOTVS employees, suppliers, and Partners, except for the Techfin (and its subsidiaries) and Dimensa (and its subsidiaries) affiliates, which maintain independent Corporate Governance and follow their own Policies, provided these do not conflict with this Policy. Compliance with this Policy is mandatory and reflects applicable laws and regulations related to topics concerning Data Protection and Information Security legislation.

All TOTVS Business Units must implement measures to ensure that employees and, when necessary, Partners, customers, and Suppliers have access to and acknowledge awareness of the guidelines outlined in this policy. It is also the responsibility of the Business Units, when necessary, to ensure the execution of appropriate confidentiality and non-disclosure agreements for contracts entered into with employees, Partners, and Suppliers who have access to data and information owned by, or under the custody and responsibility of, TOTVS.

3. References

- General Personal Data Protection Law (LGPD) – Law No. 13.709/2018.
- ABNT NBR ISO/IEC 27001 – Information Security Management System.
- ABNT NBR ISO/IEC 27701 – Requirements and Guidelines for Information Privacy Management.
- ABNT NBR ISO/IEC 27017 – Information Security for Cloud Computing Services.
- ABNT NBR ISO/IEC 27018 – Information Security for the Protection of Personal Data in Cloud Environments.
- Copyright Law (Law No. 9.610/1998).
- Industrial Property Law (Law No. 9.279/1996).
- CMN Resolution No. 4.893/2021.
- BCB Resolution No. 85/2021.
- CVM Instruction No. 505/2011.

- CVM Instruction No. 617/2019.
- CVM Instruction No. 586/2017.
- CVM Resolution No. 35/2021.
- SUSEP 638.

4. Definitions

Brazilian General Personal Data Protection Law or LGPD: Law No. 13.709/2018, which regulates Personal Data Processing activities.
CODEC: TOTVS Code of Ethics and Conduct, a document aimed at establishing the ethical principles and rules of conduct that guide the TOTVS's commitment towards the integrity of its internal and external relationships and business activities, applicable to all directors, officers, shareholders of the company, employees, service providers, Suppliers and Partners.
High-impact Information Security Incident: an information security incident that, by compromising one or more security pillars, threatens business continuity, legal compliance, or the strategic survival of the organization, resulting in severe and unacceptable financial or reputational harm according to the risk scale defined by the company.
Employees: professionals who work in TOTVS Business Units under an employment contract.
Information Assets: are the data, systems, equipment, and technology infrastructure that hold value for TOTVS and therefore require protection and management to ensure their availability, integrity, and confidentiality.
Information Security: a method of managing an organization's information by preserving properties such as confidentiality, integrity, availability, authenticity, traceability, and legality, not limited to computer systems, electronic information, and/or storage systems.
Information Security Event: an occurrence related to assets or the environment that indicates a deviation from expected behavior or a potential compromise.
Information Security Incident: one or a series of undesirable or unexpected information security events that have a significant likelihood of compromising business operations and threatening Information Security.
ISO/IEC 27001: Information Security management system standard published by the *International Organization for Standardization* and *International Electrotechnical Commission*, detailing how to manage Information Security within an organization.
Local Information Security: TOTVS Business Units or internal Areas that maintain their own Information Security structure.
Personal Data: any piece of information related to identified or identifiable individuals.
Privileged Access: refers to authorizations or access rights to systems, functions, and resources that exceed those of a standard user. An account with Privileged Access is one that is authorized to execute security-critical functions that a regular user is not permitted to perform.
Risk Management, Internal Controls, and Compliance Policy: Policy PO-GC-03, which establishes the principles, guidelines, and responsibilities to be followed in the process of corporate risk management, internal controls, and compliance, in addition to promote the culture of Risk Management and the Integrity Program throughout TOTVS.
Sensitive Data: information that, if improperly disclosed or accessed, could compromise the privacy, security, and integrity of individuals or the organization itself, including personal, financial, and strategic data.
Sensitive Personal Data: personal data on racial or ethnic origin, religious beliefs, political opinions, membership to a union or organization of a religious, philosophical, or political nature, data regarding health or sex life, and genetic or biometric data, when linked to an individual.
Third-parties/Suppliers, and Partners: service providers that operate alongside TOTVS Business Units through contracts established with Suppliers of products and services.

TOTVS Business Units: TOTVS Management and RD Station.
TOTVS or Company: TOTVS S.A., its direct and indirect subsidiaries and affiliates, except for TechFin (and its subsidiaries) and Dimensa (and its subsidiaries).
Value of an Asset or Information: measured by the value of the asset or information itself and by the potential impact it may cause to the business in the event of a violation of one or more Information Security Pillars.

5. Guidelines

TOTVS is committed to protecting the information under its responsibility, in strict compliance with applicable laws, the provisions of its bylaws, the CODEC, and other corporate policies.

This Policy clearly defines the concepts, guidelines and responsibilities regarding the security of TOTVS information, as well as the information of its customers under its custody; allows the Information Security pillars to be preserved; ensures that the processing of Personal Data and Sensitive Personal Data is in compliance with applicable laws and regulations and that Information Security risks are managed properly, ensuring the protection and reliability of information and safeguarding TOTVS' image before the market and its investors.

TOTVS recognizes the diversity of activities carried out by its Business Units. Therefore, it establishes the minimum security standards to be adopted, evaluating and applying additional controls that are valid for the different scenarios of each of them.

This Policy is supported by a set of Information Security standards and procedures established by TOTVS.

5.1. Information Security Pillars

We characterize Information Security by preserving the following pillars:

Confidentiality: ensures that access to TOTVS information, as well as that of its customers, Suppliers, Partners, and employees, is granted exclusively to authorized individuals and solely for legitimate and ethical purposes;

Integrity: ensures the accuracy and completeness of information and its processing methods, as well as the integrity of data under the company's responsibility;

Availability: ensures that the information is always available to professionals who actually require access to them, and ensures that the data are available based on the service level required by the business areas and/or contracted by customers;

Traceability: ensures the availability of audit tracks of information and processing means, through records of transactions and changes made in systems and applications, allowing the unequivocal assignment of authorship for each action;

Legality: ensures that all procedures related to information within the company are conducted in compliance with applicable laws and regulatory rules;

Authenticity: ensures that data and information are genuine and legitimate through the authentication of users and systems, enabling traceability and certifying the accuracy of information, with no manipulation or interference from unauthorized external parties or Third Parties.

5.2. Information Security in Acquired Companies and Partnerships

TOTVS, as a technology company, not only recognizes the need to establish robust and consistent Information Security standards, but also strives to implement them across all its Business Units and operations, taking into account and respecting the specific nature of each business and the applicable

regulations, including when engaging with Partners and in companies it acquires. All Business Units must follow security practices that meet operational needs and applicable legal requirements, ensuring quality and efficiency in alignment with TOTVS security policies and procedures. This alignment ensures a cohesive and effective approach to information protection in a general and comprehensive manner, promoting the integrity and resilience of operations in all units.

5.3. Risk Management – Information Security Objectives and Incidents

All TOTVS Business Units must maintain an Information Security risk management process with the objective of identifying, assessing, addressing, and monitoring risks that may affect the confidentiality, integrity, availability, and privacy of their information and assets. This process must be integrated into the company's general risk management practices and must ensure that risks are managed proactively and effectively.

Due to the nature of associated risks, all Business Units involved in the development and provision of Cloud services must maintain specific processes to identify, analyze, assess, address, monitor, and report Information Security risks that may impact the objectives of their Cloud areas. Business Units must adhere to international standards for cloud storage security, as referenced in this document.

All TOTVS Business Units must maintain a channel for reporting, as well as tools for monitoring rvents and Incidents related to Information Security, to enable the evaluation of events that may impact the business and/or the company's strategies.

All Incidents related to Information Security within the Business Units of TOTVS, once identified by the business areas, must be promptly reported to their respective Corporate Information Security areas of TOTVS Management at csirt@totvs.com.br and to the Data and AI Governance team, at dpo@totvs.com.br, when personal data is involved, in order to ensure proper registration and handling. Business Units must also maintain mechanisms for handling Incidents involving personal data, in accordance with the requirements of the General Personal Data Protection Law.

High-impact Incidents occurring within TOTVS Business Units must also be reported periodically to the Statutory Audit Committee, through the Incident report presented by the TOTVS Corporate Information Security team during regularly scheduled meetings. In case of an Incident involving personal data, the Incident must also be reported to the TOTVS Data Privacy Committee.

5.4. Identity and Access Management

All TOTVS Business Units must establish and maintain an access and identity management process that restricts access to critical resources and sensitive data exclusively to authorized individuals, based on the principles of least privilege and segregation of functions, and ensuring access levels are consistent with the need of each role. The implementation of access controls must include multifactor authentication to enhance security, as well as clear procedures for granting, modifying, and revoking permissions.

All employees and Third Parties acting on behalf of TOTVS must have a unique, personal, and non-transferable identification (physical and logical) that enables them to be identified as the person responsible for their actions.

Privileged Access must be strictly controlled and monitored, ensuring that only authorized users are permitted to access systems and sensitive data, in compliance with the principle of least privilege. Business Units must ensure frequent processes for reviewing privileged access, ensuring their timely revocation as soon as they are no longer necessary.

The responsibility for maintaining access for Third Parties, including creation, review, and revocation, lies with the manager or employee responsible for the contract with Third Parties. In matters

involving contracts with third-party companies that include multiple users, it is the responsibility of the contract manager to ensure that all related access is always appropriate to the activities performed and revoked when no longer necessary. This measure reinforces shared responsibility in Information Security management, complementing the controls implemented by the access area.

Physical access for employees, Third Parties, and visitors must be authorized and controlled through the use of efficient processes and controls that meet and ensure the protection of environments and assets according to local needs. Employees who receive Suppliers or Third Parties at Business Unit facilities must always accompany them throughout the entire visit.

All TOTVS Business Units must implement a system for continuous monitoring and verification of access activities. Access records must be maintained, protected, and regularly analyzed to detect and respond to any anomalous or suspicious behavior.

All TOTVS Business Units must perform periodic access reviews—at least annually for general access and semiannually for privileged access—for the access granted to employees and Third Parties to their systems and facilities. For systems and facilities under centralized management by TOTVS, the incorporated Business Units must remain attentive to review periods and provide all necessary support to ensure the completion of the process.

All employees must receive ongoing training on access policies and secure practices to ensure they understand their responsibilities and the security implications associated with accessing data and systems.

5.5. Information Sorting and Processing

To ensure adequate protection of TOTVS information, all Business Units must adopt an information sorting and labeling method based on the level of confidentiality and criticality for TOTVS' business:

- Information must be sorted based on its value, sensitivity, and criticality. Sorting must determine the appropriate security controls for the protection of information. Confidential and critical information must be processed with the highest levels of security and protected from unauthorized access, disclosure, alteration, and destruction;
- All information must be properly protected, in accordance with TOTVS' Information Security guidelines, throughout their entire lifecycle, which includes: generation, handling, storage, transportation, and disposal;
- The information collected must be used for the purposes previously informed or contractually defined, and may be processed for additional purposes as long as they are compatible with the applicable legal basis and duly authorized;
- Personal Data must be processed in accordance with applicable privacy laws and regulations (national and international), in addition to abiding by the guidelines set out in TOTVS' Personal Data Protection and Privacy Policy.

5.6. Information Asset Management

All TOTVS Business Units must adopt a structured and systematic approach to the management of information assets that includes their identification and sorting. These assets must be recorded in a detailed inventory, including at minimum information regarding their significance, location, and owner. The sorting must reflect the value of the asset and the potential impact of its loss, compromise, or destruction.

The maintenance and disposal of Technology assets belonging to TOTVS must be carried out exclusively by duly evaluated and approved Partners, or by formally assigned and qualified internal

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

TOTVS teams. Business Units must maintain a record of equipment check-in and check-out, as well as signed statements of consent for use by employees and Third Parties at the time the equipment is issued and collected.

TOTVS Business Units must also implement appropriate security controls to safeguard information assets, ensuring their proper use and management. This includes access restrictions, encryption, and physical protection measures for equipment, as well as the use of controls to monitor and continuously review their security. Policies, rules, and procedures must be consistently updated to identify new threats and vulnerabilities, ensuring that assets remain protected against emerging risks. Mobile media and equipment ports must be managed to prevent the risk of infection and information leakage through those means.

5.6.1. Acceptable use of TOTVS assets

All employees and Third Parties must ensure the security and protection of the information assets provided by TOTVS Business Units for the execution of their activities, in accordance with the following rules:

- Use technology assets (computers, mobile devices, systems, and data) exclusively for work-related purposes, except in situations expressly authorized by the employee's manager, the Information Security area, and the IT area responsible for the business unit, in specific and exceptional cases;
- Only use assets for which the employee has been explicitly authorized;
- Do not share access credentials with Third parties;
- Protect confidential and sensitive information. Do not disclose or store sensitive data in unauthorized locations;
- Use encryption to protect data in transit and at rest;
- Use strong, unique passwords to access systems and data. Change passwords regularly and never share credentials;
- Whenever possible, use additional authentication methods to access information and systems;
- Install only software that has been authorized, approved, and licensed by the company. Do not use unverified applications;
- Keep computers and other devices provided by TOTVS secure. Use padlocks and other security devices when appropriate;
- Store mobile and portable devices in secure locations when not in use;
- Use authorized removable storage devices only when necessary and protect them with a password and encryption;
- Store data in locations designated by the company, such as secure folders on the corporate network;
- Send sensitive data through secure and protected channels, such as encrypted emails;
- Always verify the authenticity of recipients before transmitting confidential information;
- Remain vigilant for any suspicious behavior or warning and immediately report it to technical support and/or the Information Security team;
- Follow all established policies and procedures for the use of technology. Any breach must be immediately reported to the IT department of the Business Unit;

- Report any Incident related to security or improper use of assets to your supervisor, technical support, or the Information Security team.

5.7. Cryptography

All TOTVS Business Units must assess and implement encryption practices appropriate to the value of their information assets, in order to ensure the protection of critical, sensitive, and confidential data at rest or in transit.

Encryption must be applied to all electronic communications exposed to the internet and data transmissions in order to prevent unauthorized access and to ensure that information is transmitted securely. In addition, encryption must also be employed during data processing to protect temporarily stored or handled information, ensuring that TOTVS data remains protected from undue exposure and access.

All TOTVS Business Units must establish secure processes for the management of cryptographic keys, including their generation, storage, and rotation. The selection of algorithms must be based on an ongoing evaluation of best practices and security guidelines, ensuring that only secure and approved methods are utilized.

5.8. Physical and Environmental Security

All TOTVS Business Units must implement physical security controls for their facilities and environments to ensure the integrity and security of equipment, systems, and data, including the deployment of tools for restricting physical access and monitoring of sensitive areas and facilities. All TOTVS Business Units with local data centers must also be equipped with monitoring devices, climate control systems, and fire prevention controls for the rooms. The recovery plans for these sites must be included in the Disaster Recovery Plan of these Business Units.

In addition to access security, data centers must also implement measures to protect facilities against environmental risks and establish environmental control systems for the mitigation of potential harm to TOTVS equipment and data. The electrical infrastructure must be designed to support the power requirements of critical systems, including the installation of uninterruptible power supply (UPS) devices and generators to ensure operational continuity in the event of power grid failures.

5.9. Communications Security

All TOTVS Business Units must implement security measures for the internal and external transmission of information. Electronic communications, both internal and external, must be protected from interception and unauthorized access. This includes the use of encryption protocols, firewalls, intrusion detection and prevention systems, and the continuous monitoring of networks to identify and mitigate threats in real time, ensuring that data transmitted across networks is protected from cyberattacks and data breaches. The communication of confidential and sensitive data must be carried out exclusively by means that ensure security and privacy.

Network security must be reviewed regularly to ensure that defenses remain up to date. Access to communication networks and systems should be controlled and restricted to authorized personnel, and the use of unauthorized network devices should be prohibited.

For the provision of services, all employees and Third Parties must use only communication devices and information transmission systems that have been duly approved and provided by TOTVS. Any violation of this condition may be considered an Information Security Incident.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

5.10. Backups and recovery tests

All TOTVS Business Units must establish and maintain a process for generating and testing backups of their critical data in order to protect them against loss and corruption. This includes clearly defining the types and frequency of backups, the storage and protection of backups, as well as documentation on recovery processes and test results. It is mandatory to perform backups at regular and consistent intervals, covering all essential data and critical systems belonging to TOTVS, ensuring their storage in secure, geographically separate locations to provide protection against local disasters.

Business Units should also implement a regular restore testing program to verify the effectiveness of backups. Restore tests must be documented in order to ensure the integrity of safeguarded databases. Testing frequency must be determined based on the criticality of data and systems, and the results must be reviewed to ensure the continuity of recovery processes.

5.11. Vulnerability management and monitoring

All TOTVS Business Units of must implement vulnerability scanning tools and techniques to detect and classify security flaws in systems and applications that may pose risks to TOTVS information assets. The techniques must establish processes for the identification, sorting, prioritization, and remediation of vulnerabilities. Remediation must be based on the risk and potential impact to the assets and operations of the Business Units, ensuring that critical vulnerabilities are addressed with the highest urgency and efficiency.

TOTVS Business Units must also ensure the continuous monitoring of internal and external activities that may impact the integrity and confidentiality of the systems. All TOTVS Business Units must implement monitoring solutions for intrusion detection and prevention, as well as regularly analyze collected event logs to promptly identify and respond to suspicious or anomalous activities.

5.12. Information Security in Supplier Relationships

All TOTVS Business Units must implement a risk evaluation process associated with the contracting of Suppliers who will have access to sensitive data or to critical systems belonging to TOTVS.

The evaluation must verify the adoption of appropriate Information Security practices and controls that comply with regulatory requirements and ensure the security in the execution of contracted services, guaranteeing that these Suppliers implement adequate security practices.

The process must also include ongoing verification of compliance with security standards through monitoring of services, regular audits, and reviews of security reports, as well as the adoption of secure measures for contract termination, ensuring the secure removal of Supplier access to TOTVS data and systems, and the collection of information assets provided during contract execution.

5.13. Aquisition and secure development of systems

All TOTVS Business Units must maintain a process for the secure acquisition and development of software that includes the security evaluation of Suppliers and the products offered or developed. This includes verifying software compliance with security standards, performing vulnerability testing, and reviewing the supplier's security practices to ensure software quality and security. Additionally, all contracts with Suppliers must include security clauses addressing data protection and liability in the case of security Incidents, as well as the possibility of oversight/audit during the development process, which may be replaced by the submission of information security certifications, provided that such certifications are applicable and adequately address any information security concerns.

For software development, in addition to the risk assessments considered throughout the development lifecycle, the implementation of security and privacy controls in accordance with *Privacy by Design* and *Security by Design* methodologies during development, and the execution of security

testing, all TOTVS Business Units must comply with applicable regulations and best practices relevant to the type of system being developed, including but not limited to:

- Brazilian General Personal Data Protection Law (LGPD);
- Instructions on Information Security from the Brazilian Securities and Exchange Commission – CVM;
- Copyright Law (Law No. 9.610/1998);
- Industrial Property Law (Law No. 9.279/1996);
- Consumer Protection Code;
- ISO/IEC 27034;
- NIST Secure Software Development Framework (SSDF);
- ABNT NBR ISO/IEC 27001 – Information Security Management System;
- ABNT NBR ISO/IEC 27701 – Requirements and Guidelines for Information Privacy Management.

All TOTVS Business Units must understand the legal, regulatory, and other specific needs of customers in order to develop systems that ensure not only the protection of processed information, but also its legal and regulatory compliance. Business Units must monitor scenarios in order to ensure systems are updated whenever necessary to comply with changes in the legislative environment.

5.14. Incident Management

TOTVS Business Units must maintain communication channels for reporting Incidents to provide service to employees, Third Parties, and their customers. They must establish and maintain a process for the management of Incidents related to Information Security and privacy, encompassing the identification, response, and resolution of Incidents that may compromise the integrity, confidentiality, or availability of data and systems. The process must include response plans for Incidents and clear procedures for notifying and escalating Incidents to stakeholders, as well as communicating and acknowledging the responsibilities and the appropriate communication flow.

All Incidents treated should be investigated to determine their causes and impacts, so that corrective and preventive measures can be implemented to mitigate the risk of future recurrences. Incident records and lessons learned must be reviewed and used to continuously enhance security and privacy policies and procedures.

5.15. Business Continuity Management

All TOTVS Business Units must establish and maintain a business continuity management plan to ensure the continuous operation and efficient recovery of activities in the event of critical Incidents. The plan must include the identification and evaluation of risks that may impact operations, the definition of strategies to ensure the continuity of essential processes, and the deployment of measures to minimize service disruptions, as well as the execution of tests and simulations.

TOTVS Business Units must ensure that the recovery plans for their activities take into account, when necessary, the fulfillment of return timeframes and other specific, regulatory, or contractual needs of their customers. The information required for the development of continuity and recovery plans must be assessed in conjunction with the legal and Risk Management areas at TOTVS.

5.16. Intellectual property

All TOTVS Business Units must implement measures to safeguard both their own intellectual property and that of Partners, ensuring that property rights are respected and protected against unauthorized

access, misuse, or improper disclosure. Business Units must ensure that contractual agreements with customers, Partners, and Suppliers include specific clauses for the protection of software and applications, clearly establishing intellectual property rights, safeguards against unauthorized use, copying, and modification of the software and applications provided or used in collaboration.

TOTVS strictly prohibits any form of unauthorized or unlicensed use of software and applications, and maintains controls for the management of usage licenses for all systems it operates. The identification of situations contrary to this must be treated as an Information Security Incident.

5.17. Artificial Intelligence (AI)

5.17.1. Use of Artificial Intelligence by employees and Third Parties

All TOTVS Business Units must ensure the secure and ethical use of Artificial Intelligence (AI) in their operations, implementing measures to protect the integrity, privacy, and security of data shared within these tools. Business Units must adopt practices that ensure the secure use of AI, implementing appropriate access controls to assure that only authorized users may interact with the systems, in order to minimize vulnerabilities and protect against potential information leaks and cyberattacks. All employees and Third Parties authorized to Use AI must receive proper training regarding the associated risks and the secure use of these tools.

5.17.2. Ethical and secure development of Artificial Intelligence

In AI development, all TOTVS Business Units must follow security and ethical principles to ensure that systems are designed and implemented responsibly, conducting risk evaluations and security testing to identify and mitigate potential threats prior to entry. Additionally, development must consider ethical impacts, ensuring that AI solutions do not perpetuate bias, do not invade privacy, and respect applicable regulations. To maintain trust and ensure compliance in the use and development of AI, all TOTVS Business Units must regularly review and update their AI policies. Development and usage practices must be continuously monitored and adjusted in accordance with technological and regulatory changes related to the subject.

5.18. Data protection and privacy

TOTVS is fundamentally committed to ensuring the privacy and protection of data for all its *stakeholders* (employees, Suppliers, Partners, and customers). The processing of personal data within the company is governed by our Data Privacy Program, which ensures compliance with the General Personal Data Protection Law (LGPD) and with security and confidentiality practices. For details regarding governance, guidelines, and controls, please refer to the TOTVS Data Protection and Privacy Policy.

5.19. Legal, regulatory, and contractual compliance

All Business Units of TOTVS must ensure compliance with all applicable laws and regulations related to Information Security and data protection, as well as the regulations applicable to fulfilling contractual agreements with customers.

Business Units must maintain a process to monitor, identify, and understand the specific legal and regulatory obligations for each jurisdiction in which they operate, including those related to data privacy, cybersecurity, and individual rights. Business Units must implement controls and practices that meet these requirements, conducting regular evaluations to ensure that their policies and procedures are updated and compliant with changes in legislation.

5.20. Information Security Processes Audit

Internal and external audit teams may, at any time, audit Information Security processes to ensure the effectiveness and compliance of the practices implemented by TOTVS Business Units. These audits are intended to assess compliance with security policies, identify vulnerabilities, and verify the effectiveness of established controls and procedures. The audit may be conducted by independent external or internal teams, always seeking an impartial perspective on the current state of Information Security.

5.21. Continuous Improvement

TOTVS reaffirms its commitment to the continuous improvement of Information Security processes, ensuring that policies, procedures, and controls are consistently reviewed and enhanced in alignment with best practices. This approach guarantees that practices and controls evolve in response to technological advancements and emerging security challenges, with the ongoing objective of maintaining business continuity and safeguarding against emerging threats. This commitment is demonstrated by the deployment of a systematic cycle of evaluation and update, which incorporates feedback, audit results, and lessons learned. By adopting a proactive and adaptive approach, it continuously strengthens its security posture, effectively safeguarding critical assets and ensuring organizational resilience in an environment of constantly evolving threats.

5.22. Awareness Training

All Business Units of TOTVS must plan and maintain a training and communication program that ensures the awareness of all their employees regarding Information Security policies and practices. This program must include regular and refresher training sessions, updates on new threats and procedures, and ongoing awareness campaigns to reinforce the importance of data security. Business Units must monitor the effectiveness of the program and adjust approaches as necessary to ensure that the security culture is promoted and aligned with TOTVS' culture, best practices, and regulatory requirements.

All employees and Third Parties, when applicable, must understand their individual responsibilities in safeguarding information to ensure they are prepared for the performance of their activities, as well as to identify and respond to security Incidents.

6. Assignments:

In general, all TOTVS employees and service providers should:

- Faithfully comply with this Policy, the rules and procedures of Information Security applicable to their activities;
- Complete all mandatory training provided by TOTVS Business Units;
- Protect information against any access, tampering, destruction or disclosure not authorized by TOTVS;
- Ensure technological resources, information, and systems at their disposal are used only for the purposes approved by TOTVS;
- Abide by laws and standards that govern intellectual property;
- Refrain from discussing confidential work matters in public settings or exposed areas (elevators, land and air transportation, restaurants, social gatherings, etc.), including sharing comments and opinions in blogs and social media;

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

- Immediately notify the local Information Security area of any noncompliance or violation of this Policy, as well as report any Incidents of Information Security.

Local Information Security Teams

- Ensure broad dissemination of this Policy, as well as all Information Security Standards and Procedures, to all employees and Third Parties under the company's management and oversight;
- Promote awareness initiatives on Information Security for all local employees;
- Propose and manage projects and initiatives related to Information Security management;
- Implement, manage, and monitor systems and controls under the management of the local Information Security area or, when applicable, under the Corporate management of TOTVS;
- Propose eventual changes to this Policy;
- Identify, analyze, review, process, monitor, report and register IT security Incidents;
- Register and report Incidents in the corporate environment.

Cloud Information Security Team

- Ensure the operation of the Cloud Information Security and Privacy Management System, in accordance with the guidelines of the ISO 27001, ISO 27701, ISO 27017, and ISO 27018 standards;
- Define and implement security requirements for new Cloud initiatives and projects;
- Structure and improve security services for Cloud Customers;
- Support Cloud Customers in compliance and audit inquiries, whenever possible, through self-service tools;
- Ensure the correct identification and handling of Cloud security Incidents;
- Manage accesses based on the principle of least privilege, segregation of functions and periodic revision for assets managed via Cloud;
- Map and address security vulnerabilities in the Cloud environment, in accordance with the objectives of the ISO 27001, ISO 27701, ISO 27017, and ISO 27018 certifications;
- Ensure the correct registration and traceability of actions for assets under Cloud management;
- Support, develop and improve technologies for security operation in Cloud;
- Propose eventual changes to this Policy.

IT/System Maintenance

- Notify the Information Security areas upon identifying suspicious events that may indicate the occurrence of Incidents of Information Security;
- Approve and implement security improvements recommended by the Information Security areas.

Property Security

- Manage physical access to the company's facilities.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Ethics and Conduct Committee

- Analyze events of violations of this Policy and the enforcement of consequences, when applicable, in accordance with the duties of the Statutory Audit Committee regarding the indicators of Information Security Risks.

Statutory Audit Committee

- Monitor indicators of Incidents, Risks, and events of violation of the rules of this Policy regarding the routines of the Information Security areas, reporting the findings to the Board of Directors;
- Review the information received and monitor actions regarding the occurrence of events related to Information Security issues, based on the criticality characteristics defined for them;
- Review this Policy and its revisions, and submit recommendations to the TOTVS Board of Directors regarding its approval.

Board of Directors

- Become aware, through the Statutory Audit Committee, of the monitoring of relevant Incidents, risk indicators, submitted by the Information Security area, and listen to the Audit Committee, deliberating, as necessary, in order to safeguard Information Security;
- Approve this policy and revisions hereof.

7. Management Actions

The Corporate Information Security area must ensure compliance with this Policy, referring any cases of noncompliance to the Ethics and Conduct Committee.

8. Consequence Management

In the case of noncompliance with this Policy, management measures with appropriate consequences shall be adopted to address the nonconformity, and the Statutory Audit Committee shall be informed.

9. Approvals

Name/Position	Description
Mara Maehara Information Technology Director	Development
Marcos Corradi Executive Manager of Internal Controls, Risks and Compliance	Review
Patricia Vetri Thomazelli Magalhães Fonseca Legal Officer	Review
Gustavo Dutra Bastos Vice President of Platforms & IT	Review
Dennis Herszkowicz CEO	Review
Statutory Audit Committee	Recommendation
Board of Directors	Approval