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