POLÍTICA ORGANIZACIONAL

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02
Diretoria Responsável: Diretoria de Tecnologia da Informação	**Publicado em:** 03/05/2021
Normas vinculadas: ISO 27001, CODEC, NO-SICORP-03	**Revisão até:** 03/05/2024

1. Objetivo

Estabelecer os conceitos, padrões e diretrizes de segurança da informação, visando proteger os dados e informações mantidas pelo Grupo TOTVS, conforme abaixo definido, dos clientes, parceiros, fornecedores e público em geral. O presente documento possui caráter estratégico, com vistas a promover o gerenciamento da segurança das informações do Grupo TOTVS.

Assim, esta Política deve ser entendida como compromisso da administração do Grupo TOTVS com a proteção das informações sob sua custódia.

2. Abrangência

Esta política se aplica a todo o Grupo TOTVS, incluindo empregados, parceiros e colaboradores de fornecedores que estejam a serviço do Grupo TOTVS. A observância desta Política é obrigatória e reflete a legislação e regulamentação aplicáveis acerca dos temas relacionados à Legislação Geral de Proteção de Dados e Segurança da Informação.

Os TOTVERs devem assinar o TE-SICORP-Contrato de Confidencialidade e Outras Avenças, e os colaboradores de fornecedores devem assinar o TE-SICORP-Contrato de Confidencialidade para Fornecedores, ao solicitar a criação de acesso aos ambientes da TOTVS e se comprometerem ao cumprimento da mesma.

3. Definições

CODEC: significa o Código de Ética e Conduta do Grupo TOTVS, documento que tem por objetivo estabelecer os princípios éticos e as regras de conduta que orientam o compromisso do Grupo 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, TOTVERS, prestadores de serviços, fornecedores e parceiros;
Grupo TOTVS: significa a TOTVS S.A., suas subsidiárias, coligadas e controladas diretas e indiretas;
ISO/IEC 27001: significa o 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: significa a lei brasileira nº 13.709/2018, que regulamenta as atividades de Tratamento de Dados Pessoais.
Política de Gestão de Riscos, Controles Internos e Compliance: significa a 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 do Grupo TOTVS.

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02

Segurança da Informação: significa a forma de gerenciar as informações de uma organização. Por meio da preservação de propriedades como: confidencialidade, integridade, disponibilidade, autenticidade e legalidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento;
TOTVER: significa a denominação da TOTVS para se referir aos seus empregados e estagiários.

4. Diretrizes

O Grupo TOTVS é comprometido com a proteção das informações sob sua responsabilidade além de se manter atento à observância da legislação em vigor, bem como do seu estatuto social, do CODEC e demais políticas de governança.

Esta política define de forma clara os conceitos, as diretrizes e responsabilidades a respeito da segurança das informações do Grupo 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 esteja em conformidade com a legislação aplicável; e que os riscos de segurança da informação sejam geridos adequadamente, garanta a confiabilidade das informações e preserve a imagem do Grupo perante o mercado e seus investidores.

4.1. Pilares da Segurança da Informação

A segurança da informação é aqui caracterizada pela preservação dos seguintes pilares:

Confidencialidade: que garante que o acesso às informações do Grupo TOTVS, de seus clientes, fornecedores, parceiros e colaboradores sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;
Integridade: que 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 de fato 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: que 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.

4.2. Aspectos Gerais

As informações (em formato físico ou lógico) e os ambientes tecnológicos do Grupo TOTVS utilizados pelos TOTVERS no exercício profissional são de exclusiva propriedade do Grupo TOTVS, e devem ser utilizados exclusivamente para os fins estabelecidos, e não para uso pessoal;

As informações de clientes devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pelo CODEC (Código de Ética e Conduta do Grupo TOTVS) e das leis aplicáveis;

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02

As informações não-anonimizadas de clientes devem ser utilizadas somente para os fins para os quais foram autorizados para a prestação dos serviços contratados;

Todos os TOTVERs e colaboradores de fornecedores devem ter ciência de que os equipamentos e uso das informações e dos sistemas de informação do Grupo TOTVS podem ser monitorados, sem aviso prévio, e que os registros assim obtidos, em caso de descumprimento das regras estabelecidas, podem servir de evidência para a aplicação de medidas disciplinares;

O Grupo TOTVS mantém um compromisso com o cliente em adotar técnicas e meios de segurança mais adequados e disponíveis em relação à segurança dos dados trafegados, processados e/ou armazenados na nuvem da TOTVS;

Somente profissionais autorizados devem possuir acesso às informações sob responsabilidade do Grupo TOTVS;

Todo processo, sempre que possível, durante seu ciclo de vida deve garantir a segregação de funções por meio da participação de mais de uma pessoa ou equipe;

Informações confidenciais como senhas de acesso e qualquer informação que o profissional possua em seu poder para exercício do seu cargo devem sempre ser mantidas de forma secreta, sendo terminantemente proibido seu compartilhamento;

Os compromissos e responsabilidades relacionados aos pilares da segurança da informação supracitados devem ser amplamente divulgados entre as empresas do Grupo TOTVS fazendo valer firmemente a aplicação das diretrizes aqui descritas;

Essa Política é apoiada por um conjunto de normativos e procedimentos de segurança da informação estabelecidos pelo Grupo TOTVS.

4.3. Gestão de Acessos e Identidade

Os TOTVERs devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de o identificar como responsável por suas ações;

Os acessos lógicos dos TOTVERs e colaboradores de fornecedores devem ser controlados de forma que somente as informações necessárias ao desempenho de suas atividades estejam disponíveis e mediante aprovação formal do gestor imediato e/ou do responsável pelo ambiente acessado, os quais podem devem ser revistos regularmente.

Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades;

O acesso físico dos TOTVERs, colaboradores de fornecedores e visitantes aos locais que possuem recursos tecnológicos da TOTVS, deve ser autorizado e controlado mediante aprovação formal do gestor imediato e/ou do responsável pelo ambiente acessado.

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

Os TOTVERS, ao receber fornecedores ou terceiros nas instalações do Grupo TOTVS, devem sempre acompanhá-los durante todo o período da visita.

4.4. Tratamento da Informação

Para assegurar a proteção adequada às informações da TOTVS, deve-se adotar um método de classificação e rotulagem da informação de acordo com o grau de confidencialidade e criticidade para os negócios do Grupo TOTVS:

- A classificação deve seguir os seguintes rótulos: Restrita, Confidencial, Interna ou Pública, considerando as características relacionadas à informação, nos termos da Norma NO-SICORP-03 - Classificação e Uso das Informações;
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação do Grupo TOTVS em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada; para usos estatísticos sem identificar os clientes; ou para características de sistema disponíveis para o próprio cliente;
- O tratamento de dados pessoais deve estar em conformidade com a legislação de privacidade aplicável (nacional e internacional) e seguir as diretrizes definidas pela Política Geral de Proteção de Dados Pessoais da TOTVS.

4.5. Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

A área de Segurança da Informação de Cloud é responsável por identificar, analisar, avaliar, tratar, monitorar e reportar os riscos de segurança da informação que possam impactar os objetivos da área de Cloud.

A área de Segurança da Informação Corporativa é responsável por identificar, analisar, avaliar, tratar, monitorar e reportar os riscos de segurança da informação que possam impactar os objetivos da área de TI da TOTVS; monitorar o cumprimento dos procedimentos, normas e políticas de segurança da informação na TOTVS como um todo; e quando solicitado, suportar as demais áreas de negócio na gestão dos seus respectivos riscos de segurança da informação.

As áreas de negócio da TOTVS que operam e sustentam produtos e sistemas fora das áreas de TI e Cloud, são responsáveis por identificar, analisar, avaliar, tratar, monitorar e reportar os riscos de segurança da informação que possam impactar os objetivos das suas respectivas áreas, e quando necessário, podem solicitar apoio técnico para as demais áreas de segurança da informação da TOTVS.

Quando os riscos, identificados pelas áreas de negócio ou segurança da informação, puderem impactar os objetivos ou resultados do Grupo TOTVS e/ou dados pessoais sob a custódia da TOTVS, estes devem ser reportados à área de Controles Internos, Gestão de Riscos e Compliance e área de Gestão de Privacidade, respectivamente, que serão responsáveis por verificar se o risco identificado está sendo tratado conforme definido pela Política de Gestão de Riscos, Controles Internos e Compliance e pela Política Geral de Proteção de Dados Pessoais da TOTVS.

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02

Os eventos e incidentes de segurança da informação devem ser identificados por meio de um processo estabelecido, pela área de negócio, para avaliação de eventos que possam afetar o negócio e/ou as estratégias da companhia, e comunicados à área de Segurança da Informação Corporativa, que será responsável por fazer a coordenação das atividades de Resposta a Incidentes, alinhados de forma a preservar e proteger adequadamente o Grupo TOTVS.

Todos os incidentes de Segurança da Informação, assim que detectados pelas áreas de negócio, devem ser imediatamente reportados à área de Segurança da Informação Corporativa, através de e-mail para segurança.informacao@totvs.com.br, para serem devidamente registrados e reportados, à área de Gestão de Privacidade (quando envolver dados pessoais e/ou dados sensíveis), e, dependendo do caso, reportados também à Comissão de Ética e Conduta e ao Comitê de Privacidade de Dados.

4.6. Treinamentos de Conscientização

O Grupo TOTVS deve realizar treinamentos de forma periódica de conscientização em Segurança da Informação utilizando diferentes formatos a fim de abranger diferentes públicos, podendo ser, mas não se limitando a: treinamento presencial, ensino à distância (“EAD”) e campanhas de engenharia social.

5. Responsabilidades

De forma geral, cabe a todos os TOTVERs e colaboradores de fornecedores:

- Cumprir fielmente esta Política, as normas e os procedimentos de segurança da informação da TOTVS;
- Realizar os treinamentos obrigatórios disponibilizados pela TOTVS;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pelo Grupo TOTVS;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Grupo 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 (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 Corporativa sobre qualquer descumprimento ou violação desta Política, através do e-mail: segurança.informacao@totvs.com.br, bem como reportar quaisquer incidentes de Segurança da Informação.

<u>Segurança da Informação Corporativa</u>

- Prover ampla divulgação e revisão desta Política, bem como das Normas e Procedimentos de Segurança da Informação para todos os TOTVERs e colaboradores de fornecedores;
- Promover ações de conscientização sobre Segurança da Informação para todos os TOTVERs;
- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da Segurança da Informação da TOTVS;

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

- Implantar, administrar e monitorar os sistemas e controles sob gerência da área de Segurança da Informação Corporativa da TOTVS;
- Propor eventuais alterações desta Política;
- Identifcar, analisar, avaliar, tratar, monitorar, reportar e registrar os incidentes de segurança na TI;
- Registrar e reportar os incidentes no ambiente corporativo.

Segurança da Informação de Cloud

- Assegurar o funcionamento do Sistema de Gestão de Segurança da Informação de Cloud, conforme as diretrizes da norma ISO 27001;
- 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 da Certificação ISO 27001;
- 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;
- Identifcar, analisar, avaliar, tratar, monitorar, reportar e registrar os incidentes de segurança no ambiente Cloud.

Gestão de Privacidade

- Definir os requisitos de segurança para proteção de dados pessoais e pessoais sensíveis;
- Definir as táticas e estratégias necessárias a fim de manter as operações da TOTVS em conformidade com as legislações de proteção de Dados aplicáveis;
- Receber reclamações e comunicações dos Titulares, solicitações de esclarecimento e adotar medidas corretivas/preventivas;
- Receber e tomar as devidas providências com relação às comunicações para a ANPD;
- Orientar os TOVERS e contratados da TOTVS a respeito das práticas a serem adotadas em relação à proteção de Dados Pessoais;
- Responder às consultas das áreas de negócio, quanto às dúvidas referentes ao Tratamento e Proteção de Dados Pessoais;
- Executar as atribuições determinadas pela TOTVS ou estabelecidas em normas complementares de Proteção de Dados;
- Propor eventuais alterações desta Política.

Sustentação dos Sistemas

- Gerenciar o acesso lógico das ferramentas e sistemas sob sua gestão dentro do Grupo TOTVS;
- 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.

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02

Segurança Patrimonial
- Gerenciar o acesso físico às dependências da TOTVS.

Comitê de Ética e Conduta
- Analisar ocorrências de violações desta Política de Segurança da Informação relatadas; e a aplicação de consequências, quando cabível, respeitadas as atribuições do Comitê de Auditoria acerca dos indicadores de Riscos de Segurança da Informação;
- Solicitar averiguações em equipamentos e sistemas à área de Segurança da Informação Corporativa;
- Direcionar as ocorrências aos Gestores/ Líderes responsáveis para que sejam tomadas as devidas providências;
- Propor eventuais alterações desta política.

Comitê de Auditoria
- Acompanhar os indicadores de incidentes, Riscos e ocorrências de violações de regras desta Política no que toca às rotinas das áreas de Segurança da Informação, reportando seus achados ao Conselho de Administração;
- Avaliar as informações recebidas e monitorar ações quanto a ocorrência de eventos relacionados às questões de segurança da informação, respeitando as características de criticidade definidas para os mesmos;
- Recomendar eventuais alterações desta política propostas pelas respectivas áreas.

Comitê de Governança e Indicação
- Avaliar a presente Política e suas revisões, e apresentar recomendação ao Conselho de Administração da TOTVS quanto à sua aprovação;

Conselho de Administração
- Tomar conhecimento, através do Comitê de Auditoria, sobre o acompanhamento dos incidentes relevantes, indicadores de riscos, submetidos pela Área de Segurança de Informações e ouvido o Comitê de Auditoria, deliberando, quando necessário, para preservação da segurança da informação;
- Aprovar esta política e suas revisões.

6. 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.

7. 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.

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão: 02

8. Aprovações (Documento)

Nome / Cargo	Descrição
Mara Maehara Diretora de Tecnologia da Informação	Elaboração
Ricardo Guerino Diretor de Planejamento, Controladoria, Controles Internos, Riscos e Compliance	Revisão
Claudia Karpat Diretora Jurídica	Revisão
Gustavo Dutra Bastos Vice-Presidente de Plataformas & TI	Revisão
Comitê de Auditoria	Recomendação
Comitê de Governança e Indicação	Recomendação
Conselho de Administração	Aprovação

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