Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão 00
Diretoria Responsável: Diretoria de Tecnologia da Informação	**Publicado em:** 08/06/2017
Normas vinculadas: ISO 27001, CODEC	**Revisão até:** 08/06/2019

1. Objetivo

Estabelecer os conceitos e diretrizes de segurança da informação, visando proteger as informações da TOTVS e de seus clientes. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação da TOTVS. Assim, deve ser entendida como uma declaração formal da Alta Administração acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os colaboradores, estagiários e colaboradores terceirizados da TOTVS.

2. Abrangência

Esta política aplica-se a todas as áreas do Grupo TOTVS (Matriz, Unidades Próprias, Filiais). A observância destas diretrizes é obrigatória e reflete a Governança Corporativa acerca dos temas de Segurança da Informação Corporativa do Grupo TOTVS.
Após a leitura desta Política, os TOTVERs, estagiários e executivos devem assinar o TE-SICORP-Contrato de Confidencialidade e Outras Avenças, e os colaboradores terceirizados devem assinar o TE-SICORP-Contrato de Confidencialidade para Fornecedores, para confirmar que a mensagem da Política foi compreendida e se refletirá em suas atitudes.

3. Definições

Segurança da Informação – Visa a preservar as propriedades de confidencialidade, integridade, disponibilidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento.

TOTVER – Denominação da TOTVS para se referir aos seus colaboradores.

4. Diretrizes

A TOTVS é comprometida com a observância da legislação em vigor aplicável, bem como do Estatuto da Companhia e do Código de Ética e Conduta. E para a condução de suas atividades empresariais é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara que possibilite aderência e conformidade.

Pilares da Segurança da Informação

A segurança da informação é aqui caracterizada pela preservação dos seguintes pilares:
Confidencialidade: A TOTVS visa garantir que o acesso às informações da companhia e de seus clientes sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão 00

Integridade: A TOTVS visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados de clientes que estejam sob sua responsabilidade.
Disponibilidade: A TOTVS visa garantir que a informação esteja sempre disponível aos profissionais que de fato possuam o acesso necessário para tal e assegure que os dados estejam disponíveis de acordo com o nível de acordo de serviço contratado pelos clientes.
Rastreabilidade: A TOTVS visa garantir 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.

Aspectos Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da TOTVS, não podendo ser interpretado como de 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 da TOTVS e das leis vigentes;
- As informações de clientes devem ser utilizadas somente para os fins para os quais foram autorizados;
- Todos os TOTVERs, estagiários e colaboradores terceirizados devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, sem aviso prévio, e que os registros assim obtidos podem servir de evidência para a aplicação de medidas disciplinares;
- A 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.
- Os TOTVERs devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações;
- Somente profissionais autorizados devem possuir acesso as informações da TOTVS e de seus clientes;
- 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;
- Os acessos devem sempre obedecer o critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades;
- Informações confidenciais como senhas e/ou qualquer informação a qual o profissional possua em seu poder durante exercicio do seu cargo devem sempre ser mantidas de forma secreta, sendo terminantemente proibido seu compartilhamento;
- As responsabilidades no que tange a garantia dos 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 normativas e procedimentos de segurança da informação estabelecidos pela TOTVS;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada e/ou para usos estatísticos sem expor os clientes de forma identificável ou para outras características de sistema disponíveis para o próprio cliente.

Gestão de Acessos e Identidade

Os acessos lógicos dos TOTVERs, estagiários e colaboradores terceirizados devem ser controlados de forma que somente às informações necessárias ao desempenho de suas atividades estejam disponíveis, mediante aprovação formal.

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

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão 00

O acesso físico dos TOTVERs, estagiários, colaboradores terceirizados e visitantes aos locais que possuem recursos tecnológicos da TOTVS, deve ser controlados, mediante aprovação formal.

Tratamento da Informação

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

- A classificação deve seguir os seguintes rótulos: Restrita, Confidencial, Interna ou Pública, considerando assim, as necessidades relacionadas ao negócio;
- 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;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada e/ou para usos estatísticos sem expor os clientes de forma identificável ou para outras características de sistema disponíveis para o próprio cliente.

Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

Os riscos devem ser identificados por meio de um processo estabelecido para Avaliação dos Riscos de Segurança da Informação que afetem o negócio e/ou suas estratégias, alinhados com o contexto do negócio de forma a preservar e proteger adequadamente a TOTVS.

Os incidentes de Segurança da Informação devem ser analisados, tratados, registrados, monitorados e reportados ao solicitante e/ou dependendo do caso deve reportar também ao Comitê de Ética e Conduta.

Treinamentos de Conscientização

A TOTVS deve realizar treinamentos de forma regular e periódica de conscientização em Segurança da Informação, e as ações devem possuir diferentes formatos e abranger diferentes públicos, podendo ser mas não se limitando a: Treinamento Presencial ou Regular, EAD e Campanhas de Engenharia Social.

Responsabilidades

De forma geral, cabe a todos os TOTVERs, estagiários e colaboradores terceirizados:

- Cumprir fielmente a 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 pela TOTVS;
- Assegurar que os recursos tecnológicos, as informações e sistemas a 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 (aviões, transporte, restaurantes, encontros sociais, etc), incluindo a emissão de comentários e opiniões em blogs e redes sociais;

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão 00

- Comunicar imediatamente à área de Segurança da Informação sobre qualquer descumprimento ou violação desta Política e/ou Normas ou Procedimentos, através do e-mail: segurança.informacao@totvs.com.br, bem como reportar quaisquer incidentes de Segurança da Informação.

Cabe à área de Segurança da Informação Corporativa:

- Prover ampla divulgação e revisão da Política, Normas e Procedimentos de Segurança da Informação para todos os TOTVERs e colaboradores terceirizados;
- 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;
- Administrar e Monitorar os sistemas e controles aplicados sob gerência da área de Segurança da Informação da TOTVS.

Cabe à área de Segurança da Informação de Cloud:

- Gerenciar o acesso físico ao Data Center;
- Gerenciar o acesso lógico dos clientes de Cloud;
- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da segurança da informação aos clientes da TOTVS;
- Administrar e Monitorar os sistemas e controles aplicados sob gerência da área de Segurança da Informação dos clientes da TOTVS.

Cabe à área de Sustentação TI:

- Gerenciar o acesso lógico das ferramentas e sistemas da operação TOTVS.

Cabe à área de Qualidade:

- Gerenciar o acesso lógico das ferramentas de gestão de atendimento e projetos.

Cabe à área de Segurança Patrimonial:

- Gerenciar o acesso físico as dependencias da TOTVS.

Cabe ao Comitê de Ética e Conduta:

- Analisar ocorrências de violações da Política de Segurança relatadas e suas 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;
- Direcionar as ocorrências aos Gestores/ Líderes responsáveis para que sejam tomadas as devidas providências.

Cabe ao Comitê de Auditoria:

- Recepcionar comunicações sobre eventos importantes;
- Analisar indicadores de Riscos e ocorrências de violações de regras desta Política no que toca às rotinas da área de Segurança da Informação.

Assunto: Segurança da Informação Corporativa	**Identificação:** PO-SICORP-01 Versão 00

Cabe a Conselho de Administração:

- Recepcionar as informações do Comitê de Auditoria sobre os indicadores de riscos e recepcionar comunicações sobre eventos, deliberando quando necessário para preservação da segurança da informação.

5. Ações de Gerenciamento

A área de Segurança da Informação deve supervisionar o cumprimento desta Política, remetendo eventuais casos de descumprimento ao Comitê de Ética e Conduta.

6. Aprovações (Documento)

Nome / Cargo	Descrição
Mara Maehara Diretora de Tecnologia da Informação	Elaboração
Silvio Roberto Reis de Menezes Diretor, Ouvidoria, RCC, Processos, Riscos e Compliance	Revisão
Andre Rizk Diretor Jurídico	Revisão
Weber George Canova Vice Presidente de Tecnologia	Revisão/Recomendação
Comitê de Auditoria	Recomendação
Conselho de Administração	Aprovação

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