



E-BOOK

# SEGURANÇA DA INFORMAÇÃO EM **SOFTWARE TRIBUTÁRIO**

Entenda a importância da **segurança da informação** nas plataformas de **software tributário**.  
Esse é o requisito indispensável para estar em compliance!



# Índice



Introdução..... 03

1. A importância da segurança na informação..... 04

2. A ISO 27001 e os requisitos da segurança da informação..... 04

3. O que prevê e como se preparar para atender a LGPD?..... 05

4. Como estar em *compliance*?..... 07

Conclusão..... 08

Sobre a Thomson Reuters..... 09





# Introdução

A **segurança da informação** é uma política fundamental para conferir maior transparência, agilidade aos processos e, principalmente, proteção aos dados. Especialmente para o setor contábil que lida, diariamente, com tantos números e informações ter a certeza de que a base de dados e as movimentações estão protegidas é indispensável.

Por isso, implementar um Sistema de Gestão de **Segurança da Informação** é tão relevante. Ele contribui para que o departamento contábil e a empresa trabalhem protegidos e ainda traz uma série de outras vantagens, como:

- Manutenção da conformidade legal e regulatória;
- Demonstração de credibilidade e confiança aos clientes;
- Redução da probabilidade de uma falha de segurança.

Essa é uma demanda latente de muitas organizações brasileiras. De acordo com dados da Pesquisa Global de **Segurança da Informação** da PwC, 44% dos respondentes reportaram perda ou dano de informações internas como resultado de um incidente de segurança. O comprometimento de dados de clientes foi apontado por 46% dos entrevistados.

Neste contexto, é necessário pensar em como fortalecer a **segurança da informação** nos departamentos tributários. Ficou interessado e quer saber mais sobre o tema? Preparamos um material completo para orientá-lo no gerenciamento da segurança digital na contabilidade.

Neste e-book, apresentamos a importância da **segurança da informação**, a contribuição da ISO 27001 e as exigências da Lei Geral de Proteção de Dados. Tudo o que você precisa saber para fortalecer a **segurança da informação** no departamento contábil.

Aproveite o e-book: ótima leitura!





## 1. A importância da segurança da informação

Para empresas de diferentes segmentos, a **segurança da informação** é uma área estratégica do negócio. Isso porque o conceito visa garantir a proteção dos dados corporativos e, claro, dos seus clientes também.

No departamento contábil, segurança digital na contabilidade é indispensável para prevenção de ataques cibernéticos, roubo de dados, bem como perdas e danos em sistemas, redes, servidores e dispositivos.

Ao incorporar **tecnologia no departamento tributário**, torna-se possível planejar a estratégia de prevenção de **segurança da informação** nos três pilares Confidencialidade, Integridade e Disponibilidade (CIA – Confidentiality, Integrity and Availability).

Na prática, eles norteiam a análise, o planejamento e a implementação da estratégia de segurança digital na contabilidade. Veja, a seguir, a definição dos principais pilares:

**Confidencialidade:** refere-se à privacidade dos dados. Esse conceito torna o acesso à informação restrito apenas às entidades autorizadas pelo proprietário;

**Integridade:** garante que a informação mantenha as características originais dadas pelo proprietário, impedindo alterações. De outro modo, a integridade também auxilia no controle de mudanças e do ciclo de vida da informação (nascimento, manutenção e destruição);

**Disponibilidade:** assegura a acessibilidade da informação exclusivamente para os usuários autorizados pelo proprietário. O foco é garantir o acesso sempre que preciso, para viabilizar as atividades dos colaboradores em qualquer situação.



## 2. A ISO 27001

Além dos três pilares da **segurança da informação**, os setores contábeis podem contar com outro conceito para embasar a estratégia de proteção digital do departamento: a ISO 27001.

Trata-se de uma norma internacional, publicada pela International Standardization Organization (ISO), que indica como as organizações devem gerenciar a **segurança da informação**. A norma apresenta, inclusive, a metodologia ideal para a implementação deste tipo de política nas empresas.

Publicada pela primeira vez em 2005, a norma foi atualizada em 2013, sendo intitulada, desde então, como ISO/IEC 27001:2013.

As empresas que seguem as diretrizes da **segurança da informação** constantes na norma, podem obter certificação ISO 27001. Para tanto, são avaliadas por um certificador independente. Ele confirma se a organização implementou a **segurança da informação** em conformidade com a ISO 27001, conferindo o selo.

### » Mas, afinal, como a ISO 27001 ajuda na estratégia de segurança da informação?

O principal objetivo da norma é orientar as organizações para que elas consigam proteger os três pilares da informação: confidencialidade, integridade e disponibilidade.

Por isso, a metodologia da ISO 27001 consiste, basicamente, no gerenciamento de riscos. É preciso mapear cada um deles e, na sequência, abordá-los de maneira sistemática. Na prática, são duas etapas:

**Avaliação de risco:** identificar potenciais problemas que podem ocorrer com a informação

**Mitigação ou tratamento de risco:** definir quais demandas devem ser atendidas para prevenir a ocorrência dos potenciais problemas.

Na implementação de uma estratégia consistente de **segurança da informação**, os controles, geralmente, são apresentados como políticas, procedimentos e implementações técnicas, inclusive de softwares e equipamentos.

Além da gestão de múltiplas políticas e procedimentos, vale destacar que a implementação exige também o gerenciamento de processos, proteção legal, recursos humanos, proteção física, entre outros.

Lidar com todos estes aspectos pode parecer complexo. A boa notícia é que a ISO 27001 descreve como encaixar todos os elementos de forma coerente no Sistema de Gestão de **Segurança da Informação** (SGSI).

### Como adotar a ISO 27001?

Depende da estrutura da sua empresa. Muitas vezes, as organizações já possuem todo o hardware e software instalados, mas estão usando-os de forma insegura. Neste caso, a implementação da ISO 27001 consiste, fundamentalmente, na definição de regras organizacionais.

É importante registrá-las em documentos que permaneçam visíveis e acessíveis para todos os colaboradores. A atenção às regras definidas pode evitar muitas brechas na segurança digital da empresa.



## 3. O que prevê e como se preparar para atender a LGPD?

Para orientar o processo de construção de uma política de **segurança da informação**, as empresas também devem se pautar pelas diretrizes da Lei Geral de Proteção de Dados (LGPD). O principal objetivo é aumentar a proteção à privacidade dos indivíduos e empresas, bem como o controle sobre seus próprios dados.

A LGPD é a lei nº 13.709, aprovada em agosto de 2018, tinha vigência prevista a partir de agosto de 2020. Contudo, foi adiada para agosto de 2021.

A LGPD pretende contribuir para um cenário de segurança jurídica. Isso porque padroniza uma série de normas e práticas, que visam garantir a proteção, de forma igualitária, no País e no mundo, aos dados pessoais de todo cidadão residente no Brasil.

As alterações trazidas pela LGPD devem mudar a maneira como as empresas vêm gerenciando as informações pessoais.

Para se adaptar às exigências, será preciso mapear os dados, classificá-los e organizá-los, seguindo a base legal que autoriza o seu tratamento, tornando-os mais seguros.

## Principais diretrizes da LGPD

### Consentimento

Esse é um elemento essencial da LGPD: ter o consentimento do cidadão é a base para tratar seus dados pessoais. Contudo, a lei prevê algumas exceções. É possível tratar dados sem consentimento nas seguintes situações:

- Cumprir uma obrigação legal;
- Executar política pública prevista em lei;
- Realizar estudos via órgão de pesquisa;
- Executar contratos;
- Defender direitos em processo;
- Preservar a vida e a integridade física de uma pessoa;
- Tutelar ações feitas por profissionais das áreas da saúde ou sanitária;
- Prevenir fraudes contra o titular;
- Proteger o crédito;
- Atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

### Automatização com autorização

A lei prevê garantias ao cidadão. Dentre outras ações, ele pode solicitar que seus dados sejam deletados, revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações.

Além disso, o tratamento dos dados deve ser feito considerando alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão.

Se a finalidade de um tratamento, realizado com automatização, for construir um perfil de consumo, o indivíduo deve ser informado. Ele pode, inclusive, intervir, solicitando a revisão do perfil feito por máquinas.

## ANPD e agentes de tratamento

Para fiscalizar e executar punições, quando a LGPD não for cumprida, será criada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A instituição também irá regular e orientar, preventivamente, sobre a aplicação da lei.

Além da ANPD, a Lei Geral de Proteção de Dados Pessoais também determina quais serão os agentes de tratamento de dados e suas funções em cada organização. São eles:

**Controlador:** toma as decisões sobre o tratamento;

**Operador:** realiza o tratamento, em nome do controlador;

**Encarregado:** interage com cidadãos e autoridade nacional. Esse agente poderá ser dispensado, dependendo do tipo ou porte da empresa e do volume de dados.

### Gestão de risco e falhas

Além de gerir a base de dados pessoais, outro desafio colocado pela LGPD é a administração de riscos e falhas, com uma série de boas práticas que precisam ser adotadas para a **segurança da informação**. São algumas delas:

- Redigir normas de governança;
- Medidas preventivas de segurança;
- Elaborar planos de contingência;
- Fazer auditorias;
- Resolver incidentes com agilidade.

Diante de um vazamento de dados, por exemplo, a ANPD e os indivíduos afetados devem ser avisados de imediato. As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil, respeitando o limite de R\$ 50 milhões por infração.

A ANPD deverá definir níveis de penalidade de acordo com a gravidade da falha. Mas, antes de aplicar qualquer sanção, o órgão deverá, claro, alertar e orientar as organizações.





## 4. Tecnologia no departamento tributário: *compliance* em primeiro lugar

Para estruturar uma política de **segurança da informação** consistente dentro de uma empresa, a melhor maneira é seguir as diretrizes da LGPD e da ISO 27001. Afinal, elas apresentam o fundamental sobre o tema. Além disso, as organizações precisam contar com a melhor tecnologia.

Especialmente para alguns departamentos, como o contábil, estar em *compliance* é condição sine qua non para o sucesso dos trabalhos. Com os processos fiscais da empresa organizados e em conformidade com a lei, o setor tem o desafio de gerenciar todos esses dados com a máxima segurança e proteção de dados.

Mas, afinal, como garantir o *compliance* da contabilidade? Qual tipo de recurso pode ajudar?

Usar um **software tributário** em nuvem é uma ótima alternativa! Isso porque a solução oferece uma série de funcionalidades para a gestão da rotina contábil.

Com um sistema em nuvem, como o ONESOURCE Tax One, o setor garante alta disponibilidade dos serviços e dados, sem risco de interrupções.

Além disso, as mudanças tributárias são atualizadas automaticamente na plataforma. Esse é um recurso valioso que, além de evitar erros e garantir o *compliance* tributário, dispensa o trabalho manual de acompanhamento das alterações.

Ao incorporar **tecnologia no departamento tributário** é preciso saber escolher a solução ideal. Um dos principais aspectos a serem avaliados é a segurança do software contábil.

A plataforma deve ter uma política de proteção validada pela ISO 270001, padrão que exige uma gestão adequada das informações dos clientes.

O fato é que investir em um **software tributário** proporciona ao departamento ter o controle total de todos os processos e manter *compliance* fiscal e de **segurança da informação**. Afinal, tão importante quanto ficar em dia com o Fisco é ter a garantia da disponibilidade e da privacidade dos dados.





## Conclusão

Para melhorar o desempenho da empresa e dos setores, o melhor caminho é priorizar a digitalização do negócio, ampliando as camadas de proteção e **segurança da informação**.

Ao incorporar **tecnologia no departamento tributário**, investindo em um sistema contábil com várias funcionalidades e recursos de segurança, a rotina do setor ganha em agilidade e produtividade, mantendo os dados dos clientes protegidos.

A tecnologia também é a melhor aliada para manter o setor tributário em compliance, cumprindo as exigências do Fisco e os padrões de **segurança da informação** predefinidos pela ISO 27001 e pela LGPD.

Sem dúvida alguma, um **software tributário** pode transformar a realidade do departamento, aumentando muito a performance do time fiscal e a qualidade das entregas internas e externas.



## **SOBRE** **THOMSON REUTERS**

A Thomson Reuters opera em mais de 100 países oferecendo notícias e informação para mercados profissionais, além de soluções que dão suporte no gerenciamento de negócios nas áreas de Finanças e Risco, Compliance, Jurídico, Contabilidade e Comércio Exterior.

Nossos clientes confiam em nossos produtos para encontrar respostas e tomar decisões cada vez mais assertivas, assim como buscam por ferramentas tecnológicas que focam na inteligência, praticidade e nos resultados.

As ações da Thomson Reuters estão listadas nas Bolsas de Valores de Toronto e de Nova York (símbolo: TRI). Para mais informações, visite:

[www.thomsonreuters.com.br](http://www.thomsonreuters.com.br)



# THOMSON

[thomsonreuters.com](http://thomsonreuters.com)



the answer company  
**THOMSON REUTERS**