ISO 27701: Como a norma se harmoniza com a LGPD e como adequar e certificar sua empresa?

Embora a GDPR esteja em vigor há mais de um ano, é fato que não havia um padrão de certificação definido para a norma ou referenciado pela mesma. Em outras palavras, não existia um padrão ou método endossado.

Este cenário pode ser modificado com o estabelecimento de um importante marco na gestão da proteção de dados ou da privacidade da informação: A edição da norma ISO 27701, publicada em 06 de agosto de 2019. Esta norma é considerada uma baliza para o gerenciamento contínuo dos riscos envolvendo privacidade. Ela estabelece os requisitos e orientações para implantação e manutenção de um PIMS, ou Privacy Information Management System (Sistema de gerenciamento da privacidade da informação), complementando e integrando (ou estendendo) os objetivos e controles da já conhecida ISO 27001.

Para tanto, a nova norma amplia os controles preexistentes, apresentando pontos específicos em relação a privacidade e proteção de dados. Trata-se de uma norma específica para ajudar

empresas a gerirem a privacidade da informação, termo este também trazido pela ISO.

Com efeito, é sabido que a ISO 27001 trata do chamado SGSI (Sistema de gerenciamento de segurança da informação), de modo que tal certificação é condição para que a empresa possa ampliar seu escopo de controles por meio da extensão trazida pela ISO 27701, certificando-se também nesta nova norma. Assim, é necessário ter a certificação ISO 27001 para buscar a nova certificação na extensão em privacidade da informação, nada impedindo que já se reúna esforços para tal no conjunto de normas.

A norma 27701 amplia ou estende os requisitos e orientações trazidas pela ISO 27001 (requisitos) e 27002 (códigos de prática) e é de boa prática a implementação conjunta caso a empresa não tenha avançado em um sistema de gerenciamento de segurança da informação.

Todos os agentes de tratamento, controladores e processadores precisam estar atentos às diretrizes da nova ISO 27701, que estabelece requisitos para um sistema de gerenciamento de informações de privacidade. É de se destacar, que além de estender os controles das normas envolvendo segurança da informação, a ISO também traz anexos que fazem o mapeamento de seus requisitos em comparação com os requisitos de outras

documentações, como as ISO 29100, ISO 29151, ISO 27018 e com a própria GDPR.

De acordo com relatório divulgado pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), subordinado ao Gabinete de Segurança Institucional (GSI), em 2018 foram detectados 20.566 eventos que comprometiam a segurança digital de órgãos federais, sendo que o vazamento de dados corresponde a mais de 20% dos casos apresentados. Considerando o contexto envolvendo a violação de dados, inclusive na área pública, a aplicação da ISO 27701 pode ser considerada um importante passo de adequação e satisfação das diretrizes da GDPR e da LGPD.

Neste panorama, vem sendo anunciada como o "guia do que fazer" para que as empresas se mantenham em conformidade com a GDPR – General Data Protection Regulation e LGPD – Lei Geral de Proteção de Dados.

Estar em conformidade com a norma 27701 é inovar e garantir atendimento aos requisitos de privacidade das principais regulamentações de proteção de dados.

Destaque para o art. 42 da GDPR que trata da questão dos mecanismos de certificação de proteção de dados, como os selos. No entanto, os mecanismos não haviam sido apresentados claramente. Do mesmo modo, no Brasil, a LGPD trata os certificados, selos e códigos de conduta como necessários para a transferência internacional de dados. Além disso,

estabelece que compete a ANPD realizar auditorias ou determinar sua relação no
âmbito da atividade de fiscalização sobre o tratamento de dados pessoais
efetuados pelos agentes de tratamento, incluindo o poder público.

Assim, certificar-se na ISO 27001 e de forma estendida na ISO 27701 poderá ensejar o reconhecimento por parte dos atores interessados e pela própria Autoridade, de que a empresa adota e se preocupa com as melhores práticas no que diz respeito a privacidade da informação.

Estruturar um *Privacy Management System* é assegurar observância aos controles no
tratamento de PII (*Personally Identifiable Information*). Deste modo, as empresas devem
iniciar um plano de ação, incluindo, mas não se limitando a:

1. **Assessment:** Avaliação e revisão do programa de privacidade confrontado com o framework 27701;
2. **Priorização:** Após avaliação, um mapeamento dos pontos prioritários a serem implementados;
3. **Plano de implementação:** Criação do plano de gerenciamento
eficiente da privacidade da informação;
4. **Implementação:** Conscientização, análise dos riscos, benchmarkings, concordância com plano de implementação e ação para
criação prática dos controles;
5. **Auditoria:** Revisão da norma em cotejo com os controles implementados.

Como visto, a recente publicação da
norma ISO 27701 abrirá uma importante oportunidade de certificação não só de
empresas que buscam um mecanismo de renome e consolidação para demonstrarem a

adesão às regras das normas de proteção de dados, como também de profissionais,
que cientes das diretrizes das Leis, saibam utilizar a ISO como instrumento de
certificação e em prestígio da *"accountability"*,
demonstrando que a empresa já possui a dinâmica de um plano de governança em
proteção de dados, em que pese não existir um framework definido por leis e
autoridades, já segue os controles de uma importante norma reconhecida
internacionalmente, fato que pode se tornar
uma tendência.

Em síntese, a ISO 27701 oferece
então, processos e orientações para proteção de dados pessoais, em um sistema
de gestão que envolve melhoria contínua, com possibilidade de ser utilizada
como padrão de certificação, não só por autoridades europeias, mas também no
Brasil. Se a norma vai se tornar sinônimo de certificação LGPD, veremos com o
tempo, o que não impede, como visto, as empresas e profissionais já se
adiantarem à conformidade com o padrão.

A CyberExperts Inteligência Cibernética atua em todas as fases do preparo de empresas e negócios para adequação as extensões da ISO 27701. Igualmente a CyberExperts Academy está com inscrições abertas para o seu treinamento ISSO 27701. Acesse: www.cyberexperts.com.br