RISK

ISO 27701: UM SELO DE APROVAÇÃO DE COMPLIANCE COM O RGPD

POR MARIA BEATRIZ FERNANDES

A NORMA ISO 27701, EXTENSÃO DA ISO 27001 ORIENTADA PARA A GESTÃO DA PRIVACIDADE DOS DADOS, PRETENDE GARANTIR AS BOAS PRÁTICAS À LUZ DO REGULAMENTO GERAL PARA A PROTEÇÃO DE DADOS, QUE ENTROU EM VIGOR HÁ QUATRO ANOS.

Na edição de *setembro de 2021 da IT Security virámos o holofote para a ISO 27001*, certificação para a gestão da segurança da informação. Na nova era digital, e com o surgimento de novos conceitos associados à proteção de dados, foi criada a necessidade de os padrões de segurança abrangerem o domínio.

A ISO 27701 pretende "preservar a confidencialidade, integridade e disponibilidade da informação, que é um bem crítico para a operação e para a sobrevivência da organização", reitera Francisco Pimenta, Business Developer na APCER, a Associação Portuguesa de Certificação.

Bruno Marques, Vice-Presidente da Direção da CIIWA – organização que oferece um curso de formação introdutório ao tema chamado "Sinergias, Segurança e Privacidade: ISO 27001 E ISO 27701" – explica que a norma oferece apoio às organizações para "estabelecer um sistema de gestão e a obter sinergias entre estes dois temas decisivos para a confiança digital: Segurança de Informação e Privacidade".

Assim, continua, "o principal objetivo é permitir às organizações desenvolverem estes temas numa lógica de melhoria contínua, traduzindo segurança e privacidade em valor para o seu negócio, por via de uma relação de maior confiança com o mercado" – o "capital reputacional", segundo o responsável da CIIWA.

Segundo Aurélio Maia, Consulting Service Director na Integrity, a ISO 27701 "fornece requisitos e orientações específicas para estabelecer, implementar, manter e melhorar continuamente um *Privacy Information Management System* (PIMS) como uma extensão do *Information Security Management System* (ISMS) definido na ISO 27001". Todos os requisitos e orientações foram escritos de forma que "sejam práticos e utilizáveis por organizações de todos os tamanhos e ambientes culturais", acrescenta o responsável da APCER.

Mas, enquanto um ramificação da 27001, o que é que diferencia a 27701 e qual é a ponte entre ambas? Apesar de a essência ser a mesma, os controlos e requisitos são específicos e únicos para cada um dos padrões (que na 27701 estão refletidos na cláusula 7 e 8). "O principal requisito para certificar a ISO 27701 é, em primeira instância, ter implementada a ISO 27001, sendo esta uma base obrigatória", afir-


BRUNO MARQUES, CIIWA

ma Francisco Pimenta. Desta forma, conta Bruno Marques, "as empresas que já estiverem alinhadas com a ISO 27001 poderão, sem grande esforço adicional, melhorar as suas práticas de gestão da privacidade e proteção de dados".

RGPD

Criada enquanto uma extensão da ISO 27001, a certificação pode ser uma requerida mais-valia para demonstrar a conformidade com o Regulamento Geral para a Proteção de Dados (RGPD) e outros regulamentos de privacidade a nível global, na gestão de riscos relacionados com a informação de identificação pessoal (PII, na sua sigla em inglês).

No que concerne o seu enquadramento na conformidade com o RGPD, é de notar que, em primeiro lugar, o documento "incentiva a criação de esquemas de certificação, com o objetivo de permitir que as organizações demonstrem conformidade" e, num segundo ponto, "que a certificação deve ser voluntária e disponível por meio de um processo transparente", afiança Aurélio Maia.

Nesse sentido, a adoção da norma "está na linha da frente" da *compliance* com o RGPD, uma vez que é uma norma internacionalmente reconhecida, e, por si só, uma extensão de uma norma de segurança da informação – "já amplamente utilizada e madura", reflete o responsável da Integrity.

A norma estabelece uma estrutura para os papéis de gestão de dados pessoais *Controllers* e *Processors* tendo em vista reduzir os riscos associados. Nesse sentido, "a ISO 27701 fornece uma estrutura profícua que permite que as organizações identifiquem consistentemente os riscos de privacidade, requisitos legislativos específicos, bem como tratarem os seus

> "O PRINCIPAL OBJETIVO É PERMITIR ÀS ORGANIZAÇÕES DESENVOLVEREM ESTES TEMAS NUMA LÓGICA DE MELHORIA CONTÍNUA, TRADUZINDO SEGURANÇA E PRIVACIDADE EM VALOR PARA O SEU NEGÓCIO, POR VIA DE UMA RELAÇÃO DE MAIOR CONFIANÇA COM O MERCADO"
>
> BRUNO MARQUES, VICE-PRESIDENTE DA DIREÇÃO DA CIIWA

"O PRINCIPAL REQUISITO PARA CERTIFICAR A ISO 27701 É, EM PRIMEIRA INSTÂNCIA, TER IMPLEMENTADA A ISO 27001, SENDO ESTA UMA BASE OBRIGATÓRIA"

FRANCISCO PIMENTA, APCER

dados pessoais de uma forma responsável", assevera o representante da APCER.

PORQUÊ?

Ao adotarem a norma, as organizações podem criar provas documentais de como lidam e tratam os dados pessoais, demonstrando "eficácia dos processos para identificar, priorizar e gerir riscos de privacidade ao longo da cadeia de tratamento de dados pessoais", afirma Aurélio Maia. Desta forma são facilitados os acordos com parceiros de negócios, que passam a ter garantias do bom tratamento das suas informações privadas, salvaguardando ou estabelecendo uma determinada reputação da organização, garantindo, assim, uma aura de confiança e transparência perante os clientes e os *stakeholders*.

"Desde logo, a adoção da norma ISO 27701 implica que os profissionais envolvidos na implementação do PIMS conheçam bem o âmbito do ISMS que lhe estará associado, bem como toda a estrutura documental e operativa do mesmo. Por essa via, devem saber identificar o conjunto das atividades de tratamento de dados pessoais existentes no referido âmbito, a natureza e tipos de dados envolvidos em cada uma dessas atividades, as entidades e/ou indivíduos envolvidos no respetivo tratamento desses dados, assim como, os respetivos fluxos de dados internos e externos à organização", explica Aurélio Maia.

COMO?

Quanto ao processo de obtenção da certificação, o período de preparação e os custos associados deverão depender de vários fatores, nomeadamente a dimensão, maturidade e complexidade do âmbito do sistema da organização a certificar e o tipo de dados com que trabalham, podendo o processo demorar entre seis meses e um ano. Contudo, é de esperar um valor total de entre cerca de 40 mil e 70 mil euros.

FRANCISCO PIMENTA, BUSINESS DEVELOPER NA APCER

AO ADOTAREM A NORMA, AS ORGANIZAÇÕES PODEM CRIAR PROVAS DOCUMENTAIS DE COMO LIDAM E TRATAM OS DADOS PESSOAIS, DEMONSTRANDO "EFICÁCIA DOS PROCESSOS PARA IDENTIFICAR, PRIORIZAR E GERIR RISCOS DE PRIVACIDADE AO LONGO DA CADEIA DE TRATAMENTO DE DADOS PESSOAIS"

AURÉLIO MAIA, INTEGRITY

AURÉLIO MAIA, CONSULTING SERVICE DIRECTOR NA INTEGRITY

Caso a organização não continue o ciclo de certificação, a 27701 pode caducar. A ISO 27701 implica um período de certificação de três anos, renovável – que contém uma fase de concessão e a fase de renovação, e respetivos acompanhamento que se reflete em várias auditorias anuais pela entidade certificadora, - tendo em vista averiguar o estado da operacionalização e maturidade dos sistemas de gestão de privacidade.

Bruno Marques (CIIWA) afirma que as empresas devem começar por fazer um autoavaliação ao nível da sua maturidade inicial, para que possam depois "desenvolver um planeamento em linha com as boas práticas, alocando os recursos, internos ou externos, necessários para o seu sucesso". Refere, também, que as etapas de preparação, auditoria e certificação são instrumentais para a consolidação de novas práticas organizacionais.

De acordo com o Business Developer da APCER, "é fundamental que a organização realize uma avaliação de GAP com os requisitos da ISO 27701, para definir um plano de ação e, assim, colmatar as situações de incumprimento. Posteriormente deverá realizar um mapeamento dos dados pessoais recolhidos pela organização, com o intuito de entender o seu âmbito e de que forma são utilizados/partilhados.

Mais, "posteriormente, devem ser revistas e atualizadas as políticas de privacidade por forma a garantir as informações necessárias, bem como desenvol-

vidas políticas e procedimentos aplicáveis ao papel da organização. O passo seguinte será de executar o plano de ação, incluindo a avaliação de riscos, a medição e monitorização dos objetivos, auditoria interna e revisão pela gestão. Depois de executados todos estes pontos a organização reúne as condições para avançar para um processo de certificação".

DESAFIOS

Para cumprir com os requisitos do padrão, a organização deverá elaborar uma nova estrutura documental, assim como definir as responsabilidades de cada membro no âmbito dos processos de gestão de privacidade, proceder a identificação, avaliação e tratamento dos riscos associados à proteção de dados pessoais, efetuar os registos de informação exigidos, e, finalmente, operacionalizar o processo e procedimentos relativos à gestão de eventuais ocorrências de violações de dados pessoais, explica o representante da Integrity.

BIANCA MONTECCHI, QUALITY MANAGER DA SISQUAL WFM

> "HOJE, O MERCADO NACIONAL E INTERNACIONAL TEM CADA VEZ MAIS EXIGIDO AOS SEUS FORNECEDORES DIVERSAS GUIDELINES E CERTIFICAÇÕES PARA QUE ESTES POSSAM NÃO SÓ PRESTAR SERVIÇOS DE EXCELÊNCIA, COMO ESTAR ALINHADOS AOS SEUS VALORES CORPORATIVOS"
>
> BIANCA MONTECCHI, SISQUAL WFM

Mas a correta adoção das práticas e mudanças estruturais "dependerá sempre do fator humano. A liderança de topo, com o reconhecimento da importância do tema para o desenvolvimento do negócio, deverá dar o mote, mas será sempre a ação das pessoas e a sua mobilização que ditarão o sucesso desta transformação, rumo a uma cultura de segurança e privacidade de dados. Mobilizar todos para

este esforço colaborativo é provavelmente o maior desafio", reflete Bruno Marques (CIIWA).

QUEM?

A Integer Consulting e a Sisqual WFM fazem parte da lista de organizações certificadas com a ISO 27701. Ambas iniciaram o processo em 2020 – que concluíram em 2021 – e, para ambas, as práticas de proteção da privacidade da informação são transversais à organização.

ARLETE RODRIGUES, INTEGER CONSULTING

> "ALGUNS DOS NOSSOS CLIENTES ATUAIS CONSIDERARAM JÁ ESTE CERTIFICADO COMO UM PRÉ-REQUISITO PARA ESTABELECEREM LAÇOS COMERCIAIS CONNOSCO"
>
> ARLETE RODRIGUES, IMS MANAGER NA INTEGER CONSULTING

Para a Sisqual, que obteve em 2020 as certificações 9001 (Qualidade), 20000 (Gestão de Serviços), 27001 (Segurança da Informação) e declaração de conformidade 27018 (Segurança da Informação em cloud), o processo foi "simples" visto que a já tinha implementado diversos controlos de segurança da informação com a norma 27001, explica Bianca Montecchi, Quality Manager da Sisqual WFM.

Segundo a responsável, a norma é uma ferramenta competitiva e de transmissão de confiança. "Hoje, o mercado nacional e internacional tem cada vez mais exigido aos seus fornecedores diversas *guidelines* e certificações para que estes possam não só prestar serviços de excelência, como estar alinhados aos seus valores corporativos", acrescenta.

"Alguns dos nossos clientes atuais, consideraram já este certificado como um pré-requisito para estabelecerem laços comerciais connosco", completa Arlete Rodrigues, IMS Manager na Integer Consulting. Para a empresa, o processo foi desenvolvido em diversas fases e obtiveram simultaneamente a ISO 27001 e respetiva extensão 27701. Fruto

da implementação, a empresa criou uma área operacional direcionada para o mercado externo focada no tema do RGPD.

"Sendo que a médio prazo esperamos ter o retorno deste investimento, a nossa expectativa é que este certificado venha a contribuir para atrair a atenção de clientes internacionais mais exigentes e com requisitos específicos, garantindo e promovendo o cumprimento eficaz da legislação em vigor", refere a representante da Integer Consulting.

Na adoção das práticas, o fator humano representou o maior desafio – "ligado à aceitação por parte de toda a empresa dos vários procedimentos, novas políticas e instruções de trabalho, tendo-se verificado alguma resistência inicial", explica a responsável da consultora. Adicionalmente, a organização encontrou constrangimentos na gestão da implementação do projeto devido ao facto do *core business* empresa ser a gestão de contratos e de competências "para colocação de consultores em regime de prestação de serviços de outsourcing – o que se mostrou muito exigente e minucioso".

E AGORA?

O Business Developer da APCER comenta: "à medida que a tecnologia vai avançando e os processos que a acompanham vão evoluindo, a tendência é que estes tipos de normas também se adaptem às novas necessidades. Neste momento, a ISO 27001 irá lançar, até ao final do presente ano, uma nova edição, a ISO 27001:2022, onde se irá incluir novos controlos como o Data Masking (para

mascarar dados pessoais e outras informações confidenciais). Creio que a norma ISO 27701 também irá evoluir nesse sentido".

Com a nova era digital em curso e a transformação digital a uma rapidez nunca vista, o "futuro dos negócios passa pela dimensão da confiança", reflete o representante da CIIWA. Remata: "o tema da segurança e privacidade constitui um pilar incontornável. Como qualquer norma ISO, esta já reflete um consenso alargado sobre as boas práticas a aplicar. Todavia, uma vez que a extensão ISO 27701 é recente, terá de ser continuadamente melhorada, como é próprio de todas as normas ISO e perante matérias em constante evolução". ◀