itSMF promoveu mesa-redonda sobre impacto das novas normas ISO/IEC 27001 e 27002: 2022

No dia 24 de novembro de 2022 o itSMF apresentou-se em mesa-redonda, com um painel de especialistas, para abordar os temas da segurança da informação, cibersegurança, privacidade e proteção de dados pessoais e analisar o impacto das novas normas ISO/IEC 27001 e 27002: 2022.

Mário Rui Costa (Transponder Consultores; Comissão Técnica CT 191), Hermano Correia (Auditor, Consultant, Trainer, DPO), João Carlos Falcão (Head Information Security, Operational Risk & Data Protection Officer na Itaú BBA) e Luís Azevedo (Diretor de Governação, Risco e Conformidade da RedShift) abordaram, ao longo de uma hora com moderação do vogal do itSMF António Bento, as mudanças e os potenciais impactos das novas normas ISO27001 e ISO27002 que visam dar apoio às organizações nas suas abordagens à gestão do risco e à gestão de ativos, numa **economia digital onde os modelos organizacionais de gestão da cibersegurança e da segurança da informação são cada vez mais preponderantes.**

Para qualquer instituição, estar em conformidade com a norma ISO27001:2022 é assumir um compromisso para com as melhores práticas de gestão da segurança da informação e da cibersegurança ao abrigo de uma norma universalmente reconhecida.

A ISO/IEC 27001 e 27002: 2022 são dois referenciais normativos que trazem várias mudanças, assim como novos controlos, tendo a generalidade dos controlos sido mantida com ajustes e reorganização. O que muda sobretudo é o que está no Anexo A - a lista dos controlos em consonância com a nova ISO/IEC27002 publicada no início deste ano.

Dessa lista de controlos não desapareceu nada de significativo; apenas está tudo "arrumado" de outra maneira. António Bento introduziu o debate referindo que,

agora, algumas empresas começam a perguntar como vai decorrer o período de transição, atendendo ao facto que há mais temas para serem devidamente implementados e a necessitarem de orientações, havendo, por outro lado, algumas práticas que se tornaram mais explícitas.

Mário Rui Costa reconhece, igualmente, que houve "muito poucas alterações" e as que ocorreram verificaram-se no Anexo A. Mudaram pouco os requisitos do que é obrigatório: "continuamos a ter uma norma focada na avaliação do risco e os controlos são sobre isso mesmo".

Na versão anterior havia um conjunto de políticas que já não existem, mas tal não significa que vai deixar de haver políticas. **Deste novo ciclo espera-se, inclusivamente, que traga um melhor controlo de risco.**

Havendo uma preocupação em comunicar o papel da segurança da informação, do ponto de vista da governação haverá condições para se melhorar? Hermano Correia, acredita que as normas são instrumentos que devem orientar as organizações para o foco na norma, que abrange de forma mais alargada e explícita a cibersegurança e a privacidade.

Tudo tem a ver com a cultura e estruturação da organização (desde microempresas a gigantes) e cada uma tem de estabelecer os seus modelos de governação, colocar-se numa atuação mais local ou multinacional, "mas não acredito que traga grandes alterações, embora seja um bom momento de reflexão para as organizações". Trata-se de uma oportunidade que deveria permitir fazer a transição de um modelo para um conjunto de integração com outros referenciais.

E na perspetiva do CISO, num setor muito regulado, poderá haver melhores condições para se integrarem os vários modelos que parecem estar dispersos? João Carlos Falcão acredita que sim, que esta ISO 27001 cresceu na sua maturidade (desde 2005), e vem consolidar um conjunto de "chapéus" que estavam muito dispersos pela quantidade de regulamentação que temos hoje em dia. Esta atualização vem simplificar a visão da forma como as organizações trabalham e como eliminam dados: "vem acrescentar muito às organizações", entende.

E haverá maturidade para se tirar dela um grande potencial? "A importância que se dá a estes temas nas organizações, ainda não é suficiente – faltam recursos humanos que percebam estas situações e que as consigam operacionalizar nas organizações de forma pragmática e eficaz", afirma Luís Azevedo**. Ao nível da 27011, no sistema de gestão em si muda "a ponta do icebergue", mas aparecem alguns controlos novos (e alguns vão dar muito trabalho). Na 27002 estão sugestões de implementação que foram melhoradas e são excelentes para os controlos agora introduzidos.** Mas a forma como estão catalogadas com novas perspetivas permite-nos fazer melhor ainda o trabalho de conformidade com outras *frameworks* ou *standards* ou outras fontes de requisitos com as quais as organizações se vêm cada vez mais confrontadas com a necessidade de cumprir.

Nos Estados Unidos, as empresas, além de quererem trabalhar com a norma 27001, para estarem em conformidade com o mercado europeu, veem nela uma boa forma de arrumar a sua estrutura interna, assente nesta nova estrutura com diferentes perspetivas. Na ISO/IEC27002 há várias perspetivas de arrumação dos controlos que ajudam a observá-los de diferentes perspetivas e ajudam a fazer a ponte com outros controlos. O trabalho foi demorado, mas "muito feliz".

Mário Rui refere que na perspetiva da implementação, as categorias de segurança estão organizadas em quatro grupos, à semelhança do **ITIL 4 apresentando agora numa categorização mais lógica do ponto de vista do alto nível.**

Há uma diferença acentuada entre a ISO/IEC 27001 (as empresas são certificadas por ela) e a ISO/IEC27002 (que funciona como um guia; suporte). "A ISO/IEC 27002 está muito rica e a categorização está feita de forma melhor, refletindo um crescimento naquilo que deve ser um instrumento na procura de maturidade, embora ainda insuficiente", refere Mário Rui Costa. Relativamente à ligação com outras normas e sistemas de gestão, a não ser na questão dos processos, talvez haja uma maior mudança.

A ISO 20000 tem uma maior relação com a 27001 em requisitos como configuração, gestão de alterações e capacidade. "Não devemos olhar para o Anexo A como um caderno de encargos. Não são requisitos (que têm de ser implementados); são controlos (para ajudar a gerir o risco)", esclarece Mário Rui Costa.

Um dos controlos é o *backup*. A ISO/IEC 27001 pode-se implementar sem *backup*, mas dificilmente se consegue fazê-lo. E uma empresa pode ser certificada sem ter esse controlo? "Sim, mas se eu não precisar deste controlo não preciso de o aplicar. Digamos que é muito importante, no entanto, fazer essa consolidação de maturidade para melhor utilização do instrumento. O ideal é que as empresas comecem por menos controlos e ganhem maturidade de acordo com os ciclos de avaliação de risco e que repitam com sucesso esses ciclos", observa Luís Azevedo.

Hermano Correia lembra ainda que a ISO/IEC 27701 é uma norma muito recente no panorama dos referenciais e ainda é pouco conhecida, embora nesta nova realidade venha potenciar a gestão dos programas da privacidade. A 27701 é a norma que ajuda as organizações a estarem mais alinhadas com os referenciais da privacidade: "quando a lei determina nenhuma norma se sobrepõe à lei". "Não concordo que traga obrigatoriedade de segurança de informação nos processos; a melhor abordagem é ver os riscos nos processos", refere.

A ISO/IEC 27701 tem uma ligação com a ISO/IEC 27001 (não existe sozinha) e vai ter de ser revista, garantindo-se que o ajuste é efetivamente feito. A ISO/IEC 27001 está alinhada com a legislação em vigor sobre privacidade e deve-se usar a ISO/IEC27701 como complemento. **"É um anexo e não uma gestão efetiva da privacidade", conclui Hermano Correia.**

João Carlos Falcão sugere que estas duas novas normas podem ajudar à gestão da cibersegurança, na medida em que, depois de se perceber o contexto da organização e os riscos a que está exposta, esta *framework* vai ter o papel de uma *checklist* para que não fiquem "pontas soltas" dentro da organização.

Ambas trazem, efetivamente, crescimento dos controlos de segurança e privacidade. As organizações, através da aplicação desta norma, estão mais preparadas para a ocorrência de novas vulnerabilidades assim como na proteção dos ativos da organização, nomeadamente a introdução de mecanismos de controlos contra a fuga da informação.

Perguntas e Respostas

Quando será possível a certificação por entidade certificadora de acordo com a nova ISO/IEC **27001: 2022?**

Até dezembro de 2023 podem ser feitas auditorias de acordo com a versão atual. A partir de março de 2024 têm de ser segundo a nova versão. E em setembro de 2025 tudo tem de estar em conformidade com a nova versão. Este período de transição deve-se ao facto de ser necessário qualificar os auditores. Antes do final do primeiro trimestre de 2023 não haverá uma certificação acreditada. Só depois de testada (uma certificação não acreditada) será efetivamente feita.

É preciso fazer alguma jurisprudência – afinar entendimentos e alinhar critérios. "Não aceitem tudo o que o auditor disser, defendam o vosso entendimento da norma", acrescenta Hermano Correia.

Como será feita a qualificação dos profissionais? Como é expectável que façam o seu upgrade? Têm de fazer toda uma nova formação novamente ou podem ser feitos novos cursos?

Sejam formações mais ou menos certificadas, vai, por certo haver oferta de caminhos rápidos de atualização de competências porque na essência não há grande necessidade de fazer um caminho completo de estudos para quem precise de ter uma formação mais básica, apenas para perceber o que mudou.