IT Insight SECURITY

#23 ABRIL 2025

COMO NAVEGAR ENTRE A COMPLEXIDADE REGULATÓRIA

visionware

por João Ledo,
Team Leader Ethics & Compliance, VisionWare

HABEMUS LEI DA CIBERSEGURANÇA

O DIPLOMA CONHECIDO EM FEVEREIRO DE 2025, AINDA QUE EM PROPOSTA, CONCRETIZA A ÂNSIA DO SETOR EM CIMENTAR O CONCEITO DE CIBERSEGURANÇA NO PANORAMA POLÍTICO E LEGISLATIVO EM PORTUGAL.

Tarefa facilitada pelo entorno público do tema e pela tração que o conceito vai colhendo de inúmeras chamadas mediáticas. Aguça a curiosidade do leitor, o incidente de segurança ocorrido naquela multinacional, a indisponibilidade de determinada app ou a inoperabilidade de um qualquer website governamental, mas afinal, como é que a cibersegurança faz prática em realidades dimensionadas? O âmbito de aplicação da proposta de lei lança obrigações mundanas a empresas de média dimensão que até à data não pensaram sobre o tema. Esse âmbito de aplicação alargado emanado pela diretiva comunitária impacta o estado-membro e as suas Organizações com novos e atuais desafios, muito próprios do tempo em que vivemos.

Na Europa, as soluções fugazes de segurança cibernética formatam-se em propostas comerciais vãs ao ritmo da cozedura da Diretiva NIS2 (em processo de transposição para o nosso ordenamento jurídico), do Cyber Resilience Act ou do regulamento DORA – Digital Operational Resilience Act. A relação referencial entre diplomas emaranhados impele a Autoridade de Controlo Nacional a fazer-se próxima das Organizações, não devendo servir como mero entreposto de notificações de incidentes de

JOÃO LEDO, VISIONWARE

segurança. Espera o tecido empresarial colher do CNCS – Centro Nacional de Cibersegurança - um acompanhamento itinerante, sensível às dificuldades daqueles que só na presente Era se confrontam com estes temas, e serão muitos, por força da catalogação dos anexos I e II desta proposta de Lei.

Os conceitos basilares da Segurança da Informação, a relação com fornecedores, a lógica de gestão de risco ou a continuidade do negócio, não estancada por qualquer embate, constituem-se como preceitos bê-á-bá que urge conhecer. O processo de implementação será convertido para muitas empresas impactadas num processo de conhecimento e realização simultânea com laivos de vertigem, contudo, o processo é holístico, paulatino e integral. Trazer stress ao processo será assentar em alicerces muito brandos, a construção de um sistema de gestão da cibersegurança que se pretende pleno e frutífero. Os números conhecidos aliás por via do "Relatório de Cibersegurança em Portugal" (2024) duplicam os vetores de análise e triplicam os alertas em matemática. O caminho é sobretudo cultural e de identificação clara, com padrões de cumprimento e de conformidade. Deseja-se uma identificação orgânica, ponderada e alinhada com a gestão de topo que vai investir no tema, seja na aquisição de produtos e serviços, seja nos próprios recursos. O fator humano é o ativo mais frágil e aquele cuja conduta negligente poderá fazer desabar a construção remediativa, assente em soluções fósforo.

O ROSI – *Return on Security Investment* – que mede o benefício que o investimento em segurança traz para a organização, e o investimento específico em implementação especializada e em formação de ativos humanos, lança a reflexão sobre três indicadores de relevo, nomeadamente: 1) custos de implementação de medidas de cibersegurança, conforme indicado no art.º 27 da proposta de lei, versus os custos de um incidente de segurança (como diz o ditado popular, "casa arrombada, trancas à porta"); 2) o valor economizado pela não ocorrência de incidentes, a valorização da ação preventiva e do investimento planeado; e 3), a relação entre os ativos da Organização, a sua valorização, e o investimento estratégico da Entidade, ao jeito de… perante o que temos, o investimento é parco ou substancial? O marasmo político e governamental que paira em todo o território compactua com a morosidade que estas matérias, ainda consideradas de nicho, colhem.

Estou certo de que o tempo da password no "post-it" já passou e de que só com o compromisso sério de todos os *players*, este tema se efetivará em calendário de ações da gestão de topo, no que diz respeito à adoção das medidas do art.º 27, as quais irão impactar toda a Organização, realinhando-a. Espera-se e recomenda-se, que assim seja.

O regime sancionatório, com produção de efeitos a 24 meses, é suficientemente distante para sujeitar o processo a um comportamento simulado em tema tão urgente. Saibam as entidades ponderar sobre os argumentos que lhes servem, na assunção de um plano estratégico de cumprimento normativo. Não à lei da bala, mas sim, à lei da cibersegurança. ◀