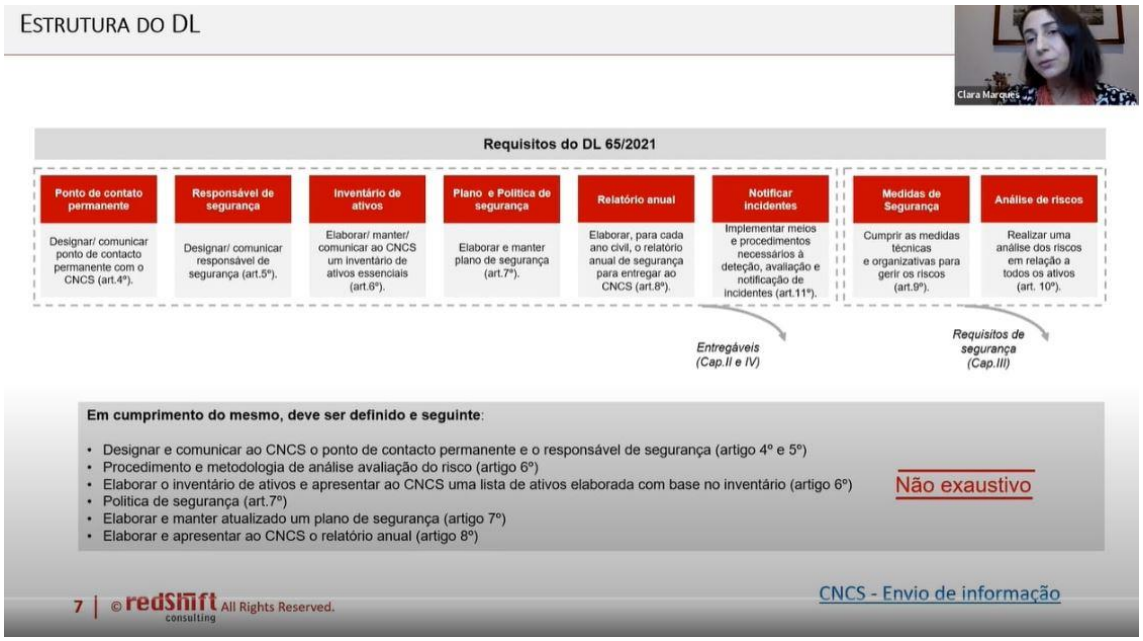
IT2TA sobre o Dec-Lei 65/2021 e o QNRCS - 2 ferramentas impulsionadoras da ciber-resiliência



No dia 23 de março, marcámos encontro com Clara Marques, da redShift, para analisar as principais considerações sobre o Dec-Lei 65/2021 e o QNRCS, duas ferramentas impulsionadoras da ciber-resiliência.

Na sessão ficámos a conhecer melhor o que é o DL 65/2021 e o QNRCS (o Quadro Nacional de Referência para a Cibersegurança, que permite às organizações reduzir o risco associado às ciberameaças das redes e dos sistemas de informação).

Foi feita a transposição da Lei 46/2018 que é baseada na diretiva SIR – Segurança dos Sistemas de Informação e Redes em toda a União Europeia. Este Decreto-Lei é aplicável a todas as entidades da Administração Pública, a prestadores de serviços digitais e operadores de infraestruturas críticas e serviços essenciais. Todas as entidades têm de ter um ponto de contacto permanente (um responsável de segurança) registado no Centro Nacional de Cibersegurança.

Os incidentes nestes domínios têm de ser comunicados de acordo com regras e medidas técnicas adequadas à gestão de riscos.

Ciber-compliance em Portugal

O Quadro Nacional de Referência para a Cibersegurança ajuda a reduzir o risco associado as ciberameaças (faz recomendações) e disponibiliza as bases que devem refletir a realidade organizacional para o modelo de governança neste âmbito. Está divido em cinco objetivos

principais. São eles: - Identificar; Proteger; Detetar; Responder; Recuperar (eventualmente). A estratégia da organização ajuda a endereçar as necessidades do que se pretende proteger.

O CNCS também tem uma segunda ferramenta em complemento: o quadro de avaliação de capacidades de cibersegurança. Inicial, Intermédio ou Avançado são os três níveis de capacidade identificados.

O CERT.pt registou um aumento de 26% no número de incidentes de segurança em 2021, comparando com 2020. Os serviços essenciais são sempre os mais afetados. Segundo a IBM, em janeiro de 2023 Portugal foi o terceiro país europeu com mais ataques informáticos. A maioria destes ataques têm origem na Rússia (quem mais hackeia outras entidades).

Por onde começar?

"Cibersegurança é estar sempre um passo à frente", diz-nos Clara Marques.

A cibersegurança não deve ser vista como um custo, mas sim como um investimento. Primeiro é necessário perceber a aplicabilidade (serei uma entidade abrangida?), fazer uma análise interna e qual o método que vou seguir (faço sozinho ou peço ajuda? Tenho tecnologia obsoleta ou não sei operar a que tenho?), dar início a um processo de pesquisa e, depois, cumprir um plano de ação, envolvendo as pessoas nessa mudança de *mindset* a ocorrer na organização.

Ainda houve um rico período de intervenção do público de onde se destacam algumas questões:

Como as pequenas, médias e microempresas podem responder ao regulamento?

Priorizar um responsável e ponto de contacto e atender ao ativo crítico, que é o que dá suporte ao meu negócio, é dali que vem o meu rendimento, e retiro os proveitos da minha organização – isto é o que deve ser protegido em primeiro lugar. Quando respondo aos controlos da cibersegurança já estou a corresponder às exigências da ISO 27001. A certificação é voluntária, mas tem custos!

Como se processam as coimas de não compliance, considerando os riscos envolvidos?

O próprio quadro não olha só para a organização, mas também para o ecossistema que gravita à volta da mesma (fornecedores). Todos têm de estar de acordo com os padrões de segurança exigidos.

E quem pode fazer o controlo do cumprimento da ISO?

Uma ISO só pode ser auditada e certificada por pessoas capacitadas para o fazer. Se for para certificar, tem de pertencer a entidades certificadoras.

Quando começa a certificabilidade do QNRCS?

Ainda em 2023.

O que mais falta às organizações portuguesas: pessoas, processos ou tecnologia?

Falta-nos um pouco de tudo. Uma empresa quer lucro e, muitas vezes, não estamos conscientes que a cibersegurança é uma necessidade que tem vindo a crescer. Processos, tecnologia e pessoas dependem também da política que as envolve. Enquanto esta evolução não estiver consolidada, as empresas caminham lentamente nesta matéria. O comportamento de um funcionário pode comprometer toda a organização, por isso, a formação em literacia de segurança é fundamental. É um equilíbrio entre os três elementos: pessoas, processos e tecnologia.

Hoje em dia muitas organizações já assumiram o WhatsApp como uma via normal de comunicação. Muitos dados críticos são transferidos por esta via e ninguém as controla. Não temos falta de ferramentas, mas os ataques continuam a acontecer cada vez mais. O que nos falta para passar das ferramentas legais para a sensibilização dos decisores de topo de que a cibersegurança pode ser um problema?

Tudo passa pela literacia digital e geralmente a gestão de topo tem conhecimentos de gestão orientados às finanças e conhecimentos de recursos humanos orientados às pessoas, mas residuais orientados à tecnologia. Aqui tem importância o papel da educação em cibersegurança e literacia digital na liderança.

E nos projetos, no nível operacional, há privacidade *by design*?

Começa a ser integrada, as organizações já vão tendo essa preocupação: segregar ambientes, proteger o código, fazer testes de aceitação, tudo antes das ferramentas serem colocadas ao dispor.

Em maio o itSMF Portugal vai dedicar o debate mensal ao tema da Inteligência Artificial – Sistema de Gestão.