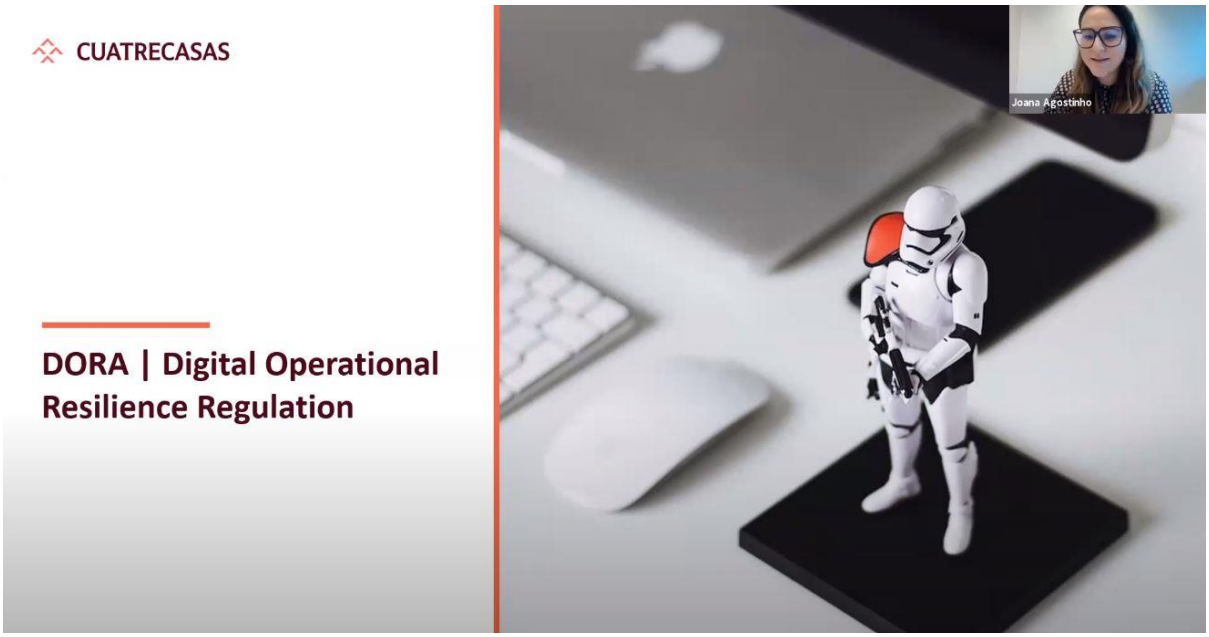
IT2TA de fevereiro: Regulamento DORA | Como navegar na complexidade da sua implementação



No dia 29 de fevereiro o itSMF Portugal realizou mais um It's Time To Talk About. Neste mês recebemos Joana Mota Agostinho, advogada, sócia responsável pela área de Digital Business, Privacy & Cybersecurity da Cuatrecasas.

O Regulamento DORA visa consolidar e atualizar os requisitos para a gestão do risco de TIC que têm sido abordados separadamente em diversos regulamentos e diretivas. Foi publicado no Jornal Oficial da União Europeia a 14 de dezembro de 2022, entrou em vigor a 16 de janeiro de 2023 e **será aplicável a instituições financeiras a partir de 17 de janeiro de 2025 na UE**. Até lá as entidades têm de se preparar para o início da aplicação do DORA. "Percebe-se uma grande tendência para o aumento da *compliance* nestas áreas", afirma Joana Mota Agostinho, cujos serviços incluem novos pacotes regulatórios em matéria de cibersegurança entre as prioridades crescentes de boa parte dos seus clientes.

Os regulamentos comunitários, ao contrário das diretivas, são de aplicação direta nos Estados-membros de forma integrada. O objetivo é, precisamente, criar harmonização nestas matérias entre os Estados-membros. Privacidade e cibersegurança são hoje olhadas como vantagens competitivas – uma visão estratégica do ponto de vista do *top management*. A reformulação de todo o modelo de governo das áreas tecnológicas e dos sistemas de segurança da informação e de gestão do risco tecnológico serão os grandes projetos a desenvolver por todas as entidades que recorrem à tecnologia para a prestação de serviços financeiros e por todos os fornecedores de tecnologia do setor financeiro.

Aliado à componente estratégia de *top management*, o DORA pretende estabelecer um quadro de resiliência operacional digital em todo o setor financeiro da EU e um quadro de supervisão para fornecedores de serviços críticos de TIC a entidades financeiras (todo o setor da EU). Também se aplica aos prestadores de serviços TIC, criando uma preocupação com estas regras "fora de portas".

As principais obrigações a ter em conta são:

- Gestão do risco;

- Resiliência;

- Gestão de terceiros (muito preponderante em todos os novos quadros regulatórios);

- Resposta a incidentes.

No quadro de Gestão do Risco está implicada a *Governance* e o controlo interno das TIC (têm de cumprir com obrigações legais) e o respetivo quadro de gestão terá de ser revisto anualmente, estando sujeito a auditoria interna. Tem de haver um processo de gestão de incidentes, um mecanismo de gestão e notificação de acidentes relacionados com as TIC implementados na organização. **O DORA estende um pouco mais os interesses financeiros do cliente.**

Na resposta a incidentes, devem ser implementados procedimentos e processos adequados para assegurar uma monitorização e acompanhamento de forma integrada dos incidentes relacionados com as TIC, a fim de assegurar que todas as causas são devidamente identificadas e tratadas. Neste contexto, os incidentes considerados "relevantes" têm de ser comunicados à autoridade competente. Voluntariamente, também se pode dar conta destas ameaças ao Banco de Portugal. "Há uma preocupação por parte dos clientes sobre o modelo de reporte. Das conversas que temos tido com as autoridades reguladoras há um grupo de trabalho específico para esta uniformização do documento de segurança", explica Joana Mota Agostinho.

Sobre os programas de testes e resiliência operacional, o DORA introduz um programa obrigatório para entidades financeiras, como parte integrante do **quadro de gestão de riscos TIC, a realizar por entidades independentes internas e externas, a todos os sistemas e aplicações que apoiem funções críticas.**

Já em relação à Gestão do Risco de entidades terceiras, deve ser vista como um todo – fazer um mapeamento de todos os requisitos legais, acautelando tudo o que se quer cumprido em RGPD ou outras políticas internas de que disponham. O DORA exige que as entidades financeiras tenham em vigor disposições contratuais sobre normas de segurança e definam SLAs, mantenham e atualizem um registo de informação em relação a todas as disposições contratuais sobre a utilização de serviços TIC, mantenham contacto regular com as entidades competentes e executem avaliações

específicas relacionadas com a gestão de risco antes de entrarem em novas disposições contratuais.

Os projetos começam sempre com o mapeamento dos requisitos e um *gap analysis* onde se avalia o estado de maturidade da organização, define-se um plano de implementação, calendarização e designação de interlocutores.

O próximo IT2TA realiza-se a 21 de março sobre o tema “Cyber Security Management - Outcome Based Security Program, Priorities and Capacity”.