Publicação do primeiro pacote de normas técnicas de regulamentação do Regulamento da Resiliência Operacional Digital do setor financeiro (DORA)

abreuadvogados.com

Com o Regulamento da Resiliência Operacional Digital (DORA), uma série de novas obrigações tornar-se-ão aplicáveis à maioria das Entidades Financeiras.

Nesta atualização, destacamos as regras propostas pelas Autoridades Europeias de Supervisão (AES) no projeto de Normas Técnicas de Regulamentação (NTR) no que diz respeito aos critérios de classificação dos incidentes relacionados com as tecnologias da informação e comunicação (TIC) e aos limiares de materialidade para determinar os principais incidentes relacionados com as TIC que devem ser comunicados à autoridade competente.

Em 17 de janeiro de 2024, as AES publicaram a versão final dos seus projetos de NTR e de normas técnicas de execução (NTE) elaboradas relativamente aos artigos 15, 16(3), 18(3), 28(9) e 28(10) do DORA.

É o primeiro conjunto de normas técnicas no âmbito do DORA, com o objetivo de aumentar a resiliência operacional digital do sector financeiro da UE, reforçando os quadros de gestão de riscos e de comunicação de incidentes das TIC e de terceiros das entidades financeiras

A publicação seguiu-se após uma fase de consulta pública sobre os projetos de normas técnicas de regulamentação e execução realizada no ano passado (ver a nossa nota) e que recolheu 420 contribuições.

As reações à consulta pública conduziram a alterações específicas das normas técnicas de regulamentação, incluindo a simplificação dos requisitos regulatórios inicialmente apresentados, uma maior proporcionalidade e a resposta a preocupações sectoriais específicas.

No que se refere à abordagem de classificação, as AES alteraram o projeto de NTR de modo que as Entidades Financeiras classifiquem os incidentes como graves se o critério "Serviços críticos afetados" for cumprido e, cumulativamente, *(i)* for identificado qualquer acesso malicioso não autorizado à rede e aos sistemas de informação como parte do critério "Perda de dados" ou *(ii)* forem cumpridos os limiares de materialidade de quaisquer outros dois critérios.

No que respeita aos critérios de classificação e respetivos limiares, por sua vez, embora mantendo uma abordagem harmonizada para a classificação de incidentes para todas as Entidades Financeiras no âmbito do DORA, as AES clarificaram os vários aspetos da classificação nos critérios e introduziram alterações nos limiares dos critérios "Clientes, contrapartes financeiras e transações afetadas" e "Perdas de dados" para introduzir uma maior proporcionalidade, abordar questões sectoriais específicas e captar incidentes cibernéticos relevantes.

Por último, para dar resposta às preocupações relativas ao ónus de notificação das Entidades Financeiras, as AES alteraram a abordagem de classificação dos incidentes recorrentes, que se centra agora nos incidentes que ocorreram pelo menos duas vezes, que têm a mesma causa raiz aparente e que teriam preenchido cumulativamente os critérios de classificação dos incidentes. A avaliação da recorrência deverá ser efetuada mensalmente.

O pacote de projetos finais de normas técnicas de regulamentação e execução inclui assim os seguintes documentos:

- NTR sobre o quadro de gestão do risco das TIC (artigo 15.º) e Norma Técnica de Regulamentação sobre o quadro simplificado de gestão do risco das TIC (n.º 3 do artigo 16.º), disponíveis aqui.

  - O projeto de NTR's sobre o quadro de gestão do risco das TIC identifica novos elementos relacionados com a gestão do risco das TIC com vista a harmonizar ferramentas, métodos, processos e políticas.
    Importa destacar que, no âmbito do projeto final as Entidades Financeiras passarão a estar obrigadas a apresentar políticas em áreas como:
    - Gestão de ativos TIC;
    - Cifragem e controlos criptográficos;
    - Gestão de projetos TIC;
    - Aquisição, desenvolvimento e manutenção de sistemas TIC;
    - Segurança física e ambiental;
    - Gestão da identidade;
    - Controlo de acesso;
    - Gestão de incidentes relacionados com as TIC;
    - Continuidade das atividades TIC;
    - Gestão do risco das TIC;
    - Operações TIC;
    - Segurança das redes de gestão;
    - Informações de segurança em trânsito.

    O projeto de NTR identifica igualmente os principais elementos que as entidades financeiras sujeitas ao regime simplificado e de menor escala, risco, dimensão e complexidade terão de ter em vigor, estabelecendo um quadro simplificado de gestão do risco das TIC. As NTR's vêm ainda harmonizar os requisitos de gestão do risco das TIC entre os diferentes sectores financeiros.

- Normas Técnicas de Regulamentação sobre os critérios de classificação dos incidentes relacionados com as TIC (n.º 3 do artigo 18.º), disponíveis aqui.

  - O projeto final de NTR especifica os critérios para a classificação dos incidentes graves relacionados com as TIC, a abordagem a utilizar para os classificar, os limiares de materialidade de cada critério de classificação, os critérios e limiares de materialidade para determinar as ciberameaças significativas, os critérios para as autoridades competentes dos Estados-Membros avaliarem a relevância dos incidentes para outras autoridades competentes e os pormenores dos incidentes a partilhar entre elas. Estabelece também um processo harmonizado de classificação dos relatórios de incidentes em todo o sector financeiro.

    - **Classificação de incidentes**

    A classificação dos incidentes dependerá do preenchimento de critérios tais como "Clientes, contrapartes financeiras e transações afetadas", "Perdas de dados" e "Serviços críticos afetados", "Impacto na reputação", "Duração e tempo de inatividade do serviço", "Distribuição geográfica" e "Impacto económico".

    - **Incidentes recorrentes**

    As AES propõem que vários incidentes, que estejam relacionados em termos de causa, natureza, impacto e serviço em causa, possam ser considerados incidentes graves relacionados com as TIC se, no seu conjunto, cumprirem os critérios de classificação e os limiares de materialidade nos três meses anteriores.

    Por conseguinte, é aconselhável que as Entidades Financeiras não se concentrem apenas nos incidentes que, individualmente, satisfazem os limiares de um incidente grave. Devem também concentrar-se nos incidentes que são menos significativos individualmente, mas que, em conjunto com outros incidentes que ocorrem de forma semelhante, com uma causa e natureza semelhantes, atingem o limiar de um incidente grave.

    Para garantir a proporcionalidade, as AES isentaram os Entidades Financeiras de menor dimensão, nomeadamente os sujeitos ao quadro simplificado de gestão do risco das TIC e as microempresas, das obrigações de comunicação de incidentes recorrentes e alteraram a abordagem de avaliação dos incidentes recorrentes de uma base contínua para uma base mensal.

    - **Impacto nos clientes, contrapartes financeiras e transações**

As AES propõem tratar o "número de clientes", o "número de contrapartes financeiras", a "relevância dos clientes ou contrapartes financeiras" e o "montante ou número de transações" como fatores de desencadeamento alternativos para a comunicação de incidentes.

Por conseguinte, o limiar de materialidade deste critério passará a ser atingido se se verificar uma das seguintes situações:

- 10% de todos os clientes ou 100 000 clientes são afetados pelo incidente;

- 30% de todas as contrapartes financeiras são afetadas pelo incidente;

- 10% do volume de todas as transações, ou um valor mínimo de 15 000 000 euros de transações, são afetados pelo incidente.

As AES especificaram que o "número de clientes afetados" abrange todos os clientes afetados (pessoas singulares ou coletivas) que utilizam os serviços prestados pela Entidade Financeira, quando as AES consideram que o cliente é o beneficiário final do serviço. O termo "número de contrapartes financeiras afetadas" abrange todas as contrapartes financeiras afetadas que tenham celebrado um acordo contratual com a Entidade Financeira.

Para o "número de transações afetadas", a Entidade Financeira deve considerar todas as transações que contenham um montante monetário, em que pelo menos uma parte da transação foi realizada na UE.

No que se refere à relevância de um cliente ou de uma contraparte financeira, a Entidade Financeira deve ter em conta em que medida o impacto no cliente e/ou na contraparte financeira afetará a realização dos objetivos comerciais da Entidade Financeira, bem como o impacto potencial do incidente na eficiência do mercado em geral.

As AES especificaram ainda que, se não for possível determinar o número real de clientes, contrapartes financeiras e/ou transações afetadas (uma vez que tal pode ser difícil por vezes), as Entidades Financeiras devem utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis.

- **Serviços críticos afetados**

As AES sugerem que as Entidades Financeiras devem determinar que um incidente relacionado com as TIC afetou serviços críticos se o incidente tiver afetado serviços ou atividades que exijam autorização, ou serviços TIC que apoiem funções críticas ou importantes da Entidade Financeira.

- **Duração e tempo de inatividade do serviço**

As AES descrevem que tanto a duração de um incidente como o tempo de inatividade do serviço devem poder desencadear este critério de classificação. Assim, propõem que o limiar para este critério seja atingido se a duração do incidente for superior a 24 horas ou o tempo de inatividade do serviço for superior a 2 horas para os serviços TIC que suportam funções críticas.

Se a Entidade Financeira não souber quando é que o incidente ocorreu ou quando é que o tempo de inatividade do serviço começou, deve calcular a ocorrência do incidente ou o início do tempo de inatividade do serviço a partir do momento anterior entre o momento em que foi detetado e o momento em que foi registado a nível da rede/sistema.

- Normas Técnicas de Regulamentação para especificar a política relativa aos serviços de TIC que apoiam funções críticas ou importantes prestados por terceiros prestadores de serviços TIC (artigo 28.º, n.º 10), disponíveis aqui.

  - O projeto de NTR especifica partes das disposições de governação, gestão de riscos e quadro de controlo interno que as entidades financeiras devem ter em vigor relativamente à utilização de prestadores de serviços terceiros de TIC. As disposições visam garantir que as entidades financeiras mantenham o controlo dos seus riscos operacionais, da segurança da informação e da continuidade das atividades ao longo do ciclo de vida das disposições contratuais com esses prestadores de serviços terceiros de TIC.
    Deste modo, será exigido que as entidades financeiras atribuam claramente as responsabilidades internas pela aprovação, gestão, controlo e documentação de acordos contratuais sobre a utilização de serviços TIC fornecidos por prestadores de serviços terceiros de TIC para apoiar as suas funções críticas ou importantes.
    No que respeita aos acordos a nível do grupo, o projeto de NTR exige que a empresa-mãe na UE ou a empresa-mãe num Estado-Membro assegure que a política de utilização de serviços TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços TIC seja implementada de forma coerente nas suas filiais e adequada à aplicação efetiva das NTR a todos os níveis relevantes.

- Normas Técnicas de Execução para estabelecer os modelos para o registo de informações (artigo 28.º, n.º 9), disponíveis aqui.

  - O projeto final de normas de execução estabelece os modelos do registo de informações a manter e atualizar pelas entidades financeiras em relação às suas disposições contratuais com os prestadores de serviços terceiros de TIC.

> O registo de informações é composto por um conjunto de quadros abertos, todos ligados entre si através de chaves específicas diferentes, de modo a formar uma estrutura relacional. O projeto de normas técnicas de execução propõe um conjunto único de modelos, comum a todas as entidades financeiras, subgrupos e grupos, a utilizar para comunicar informações no registo de informações.

Os projetos finais de Normas Técnicas de Regulamentação e Normas Técnicas de Execução foram apresentados à Comissão Europeia para revisão e adoção, que começará agora a trabalhar na sua revisão com o objetivo de adotar estas primeiras normas nos próximos meses.

As entidades abrangidas pelo âmbito de aplicação da DORA (ver aqui a nossa Newsletter) são encorajadas a começar a preparar-se para a sua aplicação, identificando eventuais lacunas na sua governação e nos seus processos de TIC e analisando quais dos seus prestadores de serviços são suscetíveis de serem considerados críticos.

Os requisitos incluem (entre outros) a exigência de implementação de determinadas disposições contratuais nos contratos de prestação de serviços de TIC e a elaboração de diversas políticas e concretização de procedimentos.

Embora o DORA seja aplicável a partir de 17 de janeiro de 2025, as Entidades Financeiras são aconselhadas a tomar já medidas para garantir o seu cumprimento atempado.

Com vista ao cumprimento atempado é importante as Entidades Financeiras começarem a preparar o seu processo de deteção e tratamento de incidentes relacionados com as TIC e manter um registo dos incidentes anteriores relacionados com as TIC, alinhado com os critérios e limiares de materialidade definidos pelas AES.

Se tiver alguma dúvida sobre as informações contidas na presente nota informativa, não hesite em contactar a equipa de Direito Financeiro e TMT da Abreu Advogados.

Thinking about tomorrow? Let's talk today.

Diogo Pereira Duarte – Sócio
diogo.p.duarte@abreuadvogados.com

João Lupi – Associado Sénior
joao.lupi@abreuadvogados.com

Rafael Silva Teopisto – Associado
rafael.s.teopisto@abreuadvogados.com