Regulamento DORA
Entender as normas técnicas

Regulatory Technical Standards sobre os critérios para a classificação de incidentes relacionados com as Tecnologias da Informação e Comunicação (TIC)

Em junho de 2023, foi publicada a primeira vaga de Drafts das RTS (Regulatory Technical Standards) e ITS (Implementing Technical Standard) pelas Autoridades Europeias de Supervisão. O objetivo destes Policy Products adicionais é o de fornecer especificações detalhadas e orientações sobre como determinadas disposições do Regulamento Comunitário devem ser implementadas em toda a União Europeia.

Estes Policy Products têm como objetivos:

- Harmonizar a aplicação das regras e regulamentações no setor financeiro;
- Abranger aspetos como requisitos de relatórios, gestão de riscos, obrigações de divulgação e outros aspetos operacionais relacionados com os serviços financeiros;
- Reforçar a transparência, a proteção do consumidor e a estabilidade do sistema financeiro.

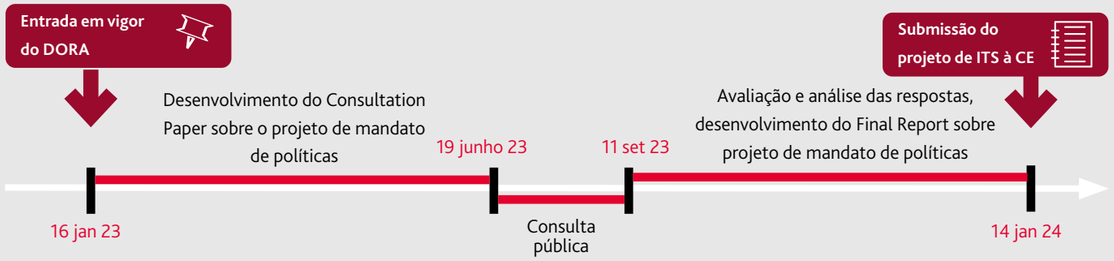
Âmbito e Prazos

O primeiro conjunto de Policy Products publicado para consulta e inclui:

- RTS para especificar a política sobre serviços de TIC realizados por fornecedores terceiros de TIC (Artigo 28 (10))
- RTS sobre critérios para a classificação de incidentes relacionados com as TIC (Artigo 18 (3))
- ITS para estabelecer os modelos para o registo de informações (Art.28 (9))
- RTS sobre estrutura de gestão de riscos de TIC (Artigo 15) e RTS sobre estrutura simplificada de gestão de riscos de TIC (Artigo 16 (3))

Temos o prazer de partilhar uma análise aprofundada, realizada pela BDO, sobre o conteúdo dos RTS sobre os Critérios para a

O cronograma atual prevê que seja publicada até 16 de janeiro de 2024 uma versão final deste RTS.



RTS sobre critérios para a classificação de incidentes relacionados com as TIC

No atual cenário digital, o setor financeiro desempenha um papel fundamental na garantia da resiliência operacional e da cibersegurança. Para lidar com os desafios em constante evolução apresentados por incidentes relacionados com as TIC, a União Europeia introduziu o Regulamento (UE) 2022/2554 sobre a resiliência operacional digital para o setor financeiro. Este RTS tem como objetivo harmonizar e simplificar os requisitos de relato de incidentes em diversos tipos de entidades financeiras,

Principais Objetivos

Este RTS enfatiza diversos objetivos críticos:

- **Harmonização e Simplificação:** O DORA procura estabelecer padrões uniformes para a classificação, gestão e relato de incidentes relacionados com as TIC. O âmbito do DORA abrange uma ampla gama de entidades financeiras, desde bancos tradicionais até Fintechs emergentes.
- **Proporcionalidade:** Reconhecendo a natureza diversificada e os perfis de risco das entidades financeiras, o DORA enfatiza a proporcionalidade. Adequa os critérios e os limites de materialidade para garantir que sejam equitativos para entidades de diferentes dimensões e perfis de risco, ao mesmo tempo que minimiza as obrigações de relato para instituições financeiras de menor dimensão.
- **Continuidade e Alinhamento:** O RTS baseia-se em estruturas existentes de relato de incidentes, assegurando uma transição suave para as entidades financeiras que já estavam sujeitas a requisitos de relato. Aproveita disposições de diretrizes estabelecidas, como as Diretrizes da EBA sobre o relato de incidentes de carácter severo ao abrigo da PSD2, promovendo alinhamento e consistência.
- **Consistência com Estruturas de Risco Operacional:** Dada a interconexão entre o DORA e as estruturas existentes, há um esforço concertado para manter a consistência, especialmente no que diz respeito à avaliação do impacto económico. Esse alinhamento visa evitar requisitos conflituantes e facilitar uma abordagem abrangente ao risco operacional.

Critérios de Classificação e Limites de Materialidade

Um dos aspetos fundamentais do RTS é o estabelecimento de critérios de classificação claros e abrangentes e limites de materialidade. Estes critérios são essenciais para determinar a gravidade dos incidentes e orientar respostas adequadas. Para equilibrar a precisão e praticidade,os critérios são concebidos para serem interdependentes, refletindo a natureza, escala e complexidade dos serviços oferecidos pelas diversas entidades financeiras.

Incidentes Severos e Ciberameaças

O RTS introduz uma abordagem qualitativa e quantitativa para identificar incidentes de carácter severo, enfatizando a importância do impacto de um incidente. Incidentes severos são determinados com base numa combinação de critérios primários e secundários, abrangendo fatores como o número de clientes afetados, perdas de dados e impacto reputacional.

Dados Primários

Clientes / Contrapartes Financeiras

- Limiares Relativos: 10% do número total de clientes, contrapartes que utilizam o serviço afetado
- Limiar absoluto: 50 000 clientes afetados

Transações Afetadas

- Limiar Relativo: 10% do volume de transações
- Limiar Absoluto: Valor de transações de 15 000 000 €

Perda de Dados

- Limiar Binário (resposta sim/não): qualquer perda de dados críticos relacionados com disponibilidade, autenticidade, integridade ou confidencialidade

Serviços Críticos Afetados

- Limiar Binário (resposta sim/não): Impacto em qualquer serviço crítico e se o incidente escalou à direção ou ao órgão de gestão

Dados Secundários

Impacto na Reputação

Limiar Binário (resposta sim/não):

- Por exemplo, com base na atração de atenção mediática, nas reclamações recebidas de vários clientes ou contrapartes financeiras, incumprimento dos requisitos regulamentares ou
- Perda de clientes ou contrapartes financeiras

Duração e Tempo de Inatividade do Serviço

- Limiar Quantitativo: tempo de inatividade de funções críticas superior a 2 horas
- Duração: Limiar Quantitativo: 24 horas calendário

Distribuição geográfica

- Limiar Binário Dependente (resposta sim/não), indicando se o incidente teve um impacto relevante em dois ou mais Estados-Membros

Impacto Económico

- Limiar Absoluto Único: 100 000 € ou mais para os custos brutos diretos e indiretos e perdas incorridas pelo incidente

Adicionalmente, o RTS aborda o tema das ciberameaças significativas, reconhecendo o seu potencial para perturbar funções críticas. As entidades financeiras são encorajadas a reportar voluntariamente essas ameaças, possibilitando uma abordagem proativa à cibersegurança.

Estrutura de Reporte

As entidades financeiras sujeitas às disposições do DORA são obrigadas a aderir a uma estrutura de reporte de três níveis, que inclui uma notificação inicial, relatórios intercalares e relatórios finais. Esta abordagem estruturada garante um reporte atempado e abrangente, facilitando uma resposta eficiente a incidentes.

Incidentes Recorrentes

Reconhecendo que incidentes recorrentes podem indicar deficiências subjacentes, o RTS aborda a agregação de incidentes menores ao longo de um período definido. Se esses incidentes tiverem uma causa, natureza e impacto comuns são considerados coletivamente como importantes (major), promovendo uma visão holística da gestão de riscos.

Relevância para as Autoridades Competentes

O RTS também enfatiza a importância da troca de informações entre as autoridades competentes nos diferentes Estados-Membros da UE. O regulamento delineia critérios para avaliar a relevância dos incidentes importantes para as autoridades noutras jurisdições, promovendo a cooperação transfronteiriça e salvaguardando a estabilidade do setor financeiro.

Em resumo, o RTS fornece um quadro padrão para classificação de incidentes relacionados com as TIC sob o DORA. Ao estabelecer limites de materialidade para incidentes importantes e criar um protocolo claro para relatar ciberameaças significativas, permite que entidades financeiras giram e respondam efetivamente a incidentes de maneira consistente. Este quadro é projetado para atender às necessidades e perfis de risco únicos de várias entidades financeiras, ao mesmo tempo que promove um compromisso coletivo com a resiliência operacional e a cibersegurança dentro do setor. À medida que as instituições financeiras navegam pelo cenário digital em evolução, esses padrões destacam-se como uma ferramenta vital para garantir a integridade e estabilidade das operações digitais no setor financeiro.

De que forma a BDO poderá ajudar?

Insight

Avaliamos em que medida o regulamento DORA se aplica à sua organização

Assessment

Realizamos uma gap analysis do DORA e avaliamos o seu nível atual de conformidade, considerando os drafts das normas RTS e ITS disponíveis.

Roadmap

Definimos um roadmap de segurança prioritizado que inclua requisitos específicos do DORA para a sua organização, mas que também esteja alinhado com a conformidade de outras legislações e regulamentações aplicáveis.

Remediation & Implementation

Auxiliamos com a gestão de projetos e/ou execução prática do roadmap de segurança através de, por exemplo, implementação de políticas e procedimentos chave, realização de testes de resiliência, gestão de testes de intrusão e implementação de recomendações subsequentes, condução de avaliações de risco de terceiros/ fornecedores, etc

PARA MAIS INFORMAÇÕES:

MÁRIO SILVESTRE NETO
Partner
+351 937 997 003
silvestre.neto@bdo.pt

ANTÓNIO JORGE PINTO
Manager
+351 937 990 031
antonio.pinto@bdo.pt

RICARDO VIDAL MOREIRA
Manager
+351 912 942 258
ricardo.moreira@bdo.pt