ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Regulamento relativo à resiliência operacional digital (DORA)

Enquadramento, implementação e desafios para a supervisão

Sessão de esclarecimento destinada ao mercado

10 de janeiro de 2025

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

ABERTURA

Dra. Ana Cristina Santos

Departamento de Supervisão Prudencial de Empresas de Seguros

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

RESILIÊNCIA OPERACIONAL DIGITAL PARA O SETOR FINANCEIRO: ENQUADRAMENTO REGULATÓRIO

Dra. Maria Lúcia Brito

Departamento de Política Regulatória

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Resiliência operacional digital do setor financeiro

Regulamento (UE) 2554/2022 («Regulamento DORA»)

- **Harmonização**: estabelece um quadro de resiliência operacional digital comum ao setor financeiro, prevendo regras específicas relativas à gestão do risco associado às TIC*, à notificação de incidentes de carácter severo relacionados com as TIC, aos testes de resiliência operacional digital, bem como à gestão do risco associado às TIC devido a terceiros
- **Produção de efeitos**: 17 de janeiro de 2025
- ***Lex specialis*** relativamente à Diretiva (UE) 2022/2555

Diretiva (UE) 2556/2022

- **Alterações às diretivas enquadradores dos subsetores financeiros**: de modo a garantir a coerência com o Regulamento DORA, quanto à aplicação de requisitos relativos à resiliência operacional digital

* Tecnologias de informação e comunicação

Aplicação do Regulamento DORA

20 tipos de entidades financeiras abrangidas, incluindo:

- Empresas de seguros e de resseguros
- Instituições de realização de planos de pensões profissionais
- Mediadores de seguros, de resseguros e de seguros a título acessório

De acordo com o princípio da proporcionalidade:

- Aplicação e supervisão tendo em conta a dimensão e perfil de risco global das entidades financeiras, bem como a natureza, escala e complexidade dos seus serviços, atividades e operações

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Pilares do Regulamento DORA

Entidades financeiras

Gestão do risco associado às TIC	Reporte de incidentes de carácter severo relacionados com as TIC	Testes de resiliência operacional digital	Gestão do risco devido a terceiros	Partilha de informação
• Requisitos de governação • Quadro de gestão do risco associado às TIC	• Classificação • Comunicação	• Teste dos sistemas e ferramentas no domínio das TIC • Testes de penetração baseados em ameaças (TLPT)	• Registo de Informações • Acordos contratuais celebrados com terceiros prestadores de serviços de TIC	• Acordos de partilha de informações específicas e sensíveis relativas a ciberameaças
			ICT CTPP* • Quadro de superintendência dos terceiros prestadores de serviços de TIC críticos	

Regras de cooperação **entre as autoridades competentes** e regras de supervisão e execução **pelas autoridades competentes**

* ICT CTPP = *information and communication technology critical third-party providers*

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Quadro de superintendência

COMITÉ CONJUNTO (*JOINT COMMITTEE*)

- Composto por ESA (membros), Comissão Europeia (COM) e ESRB (observadores)
- Atualização anual da lista de CTPPs
- Reporte anual ao Parlamento Europeu, Conselho e COM sobre o Trabalho do *Oversight Framework*

FÓRUM DE SUPERINTENDÊNCIA (*OVERSIGHT FORUM*)

- Composto pelos presidentes das ESA, um representante de alto nível das autoridades competentes (NCA) e um observador, administradores executivos das ESA, autoridades adicionais relevantes, autoridades NIS, BCE, ESRB, ENISA e COM
- Subcomité do *Joint Committee*
- Preparação de propostas de posições a assumir pelo *Joint Committee*
- Discussão regular sobre riscos e vulnerabilidades associados às TIC e promoção de abordagens comuns para a monitorização dos riscos
- Discussão das recomendações dirigidas a CTPPs preparadas pelo LO

CONSELHO DE SUPERVISORES (*BOARD OF SUPERVISORS*)

- Aprovação dos CTPPs designados, da nomeação do LO e dos relatórios sobre atividades de superintendência (3 BoS)
- Aprovação de atos e decisões relativos aos CTPP sobre a superintendência do LO (BoS do LO)

AUTORIDADE FISCALIZADORA PRINCIPAL (*LEAD OVERSEER* - LO)

- Uma ESA (EBA, ESMA, EIOPA), dependendo da atividade do CTPP nos diferentes setores
- Concretização da superintendência dos CTPP

REDE DE SUPERINTENDÊNCIA CONJUNTA (*JOINT OVERSIGHT NETWORK*)

- Composta pelos LO, podendo ser solicitado aconselhamento ao BCE e à ENISA
- Coordena as atividades do LO (protocolo de superintendência)

EQUIPA DE AVALIAÇÃO CONJUNTA (*JOINT EXAMINATION TEAM* - JET)

- Compostas por *staff* das ESA, autoridades competentes e autoridades NIS (numa base voluntária)
- Apoio ao LO nas investigações gerais e nas inspeções *on-site* a CTTP

Fonte: JC SC DOR

Estrutura de governação dos Regulamentos das ESA

Estrutura de governação introduzida pelo DORA

Funções introduzidas pelo DORA

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Mandatos regulatórios

ICT risk framework (Chapter II)

- **RTS** on ICT Risk Management framework (Art. 15.º) [Regulamento Delegado (UE) 2024/1774, 13/03/2024]
- **RTS** on simplified risk management framework (Art. 16.º/3) [Regulamento Delegado (UE) 2024/1774, 13/03/2024]
- **Joint Guidelines** on estimation of aggregated annual costs and losses caused by major ICT-related incidents (Art. 11.º/11)

ICT related incident management classification and reporting (Chapter III)

- **RTS** on criteria for the classification of ICT related incidents (Art. 18.º/3) [Regulamento Delegado (UE) 2024/1772, 13/03/2024]
- **RTS** to specify the reporting of major ICT-related incidents [(Art. 20.º/a)]
- **ITS** to establish the reporting details for major ICT related incidents [(Art. 20.º/b)]
- **Feasibility report** on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21.º)

Digital Operational Resilience Testing (Chapter IV)

- **RTS** to specify threat led penetration testing (Art. 26.º/11)

Oversight framework (Chapter V.II)

- **Call for advice** on criticality criteria (Art. 31.º/6) and fees (Art. 43.º/2) [Regulamentos Delegados (UE) 2024/1502 e 2024/1505 da Comissão, 22/02/2024]
- **Joint Guidelines** on the oversight cooperation and information exchange between the ESAs and the competent authorities under DORA Regulation (EU) 2022/2554 (Art. 32.º/7)
- **RTS** on Oversight harmonisation [Art. 41.º/1/a), b), d)] e **RTS** on JETs [Art. 41.º/1/c)]

Third-party risk management (Chapter V.I)

- **ITS** to establish the templates of register of information (Art. 28.º/9) [Regulamento de Execução (UE) 2024/2956 da Comissão, 29/11/2024]
- **RTS** to specify the policy on ICT services performed by third-party (Art. 28.º/10) [Regulamento Delegado (UE) 2024/1773, 13/03/2024]
- **RTS** to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art. 30.º/5)

A azul turquesa: documentos já publicados

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

IMPLEMENTAÇÃO DO REGULAMENTO DORA: MANDATOS REGULATÓRIOS E DESAFIOS PARA A SUPERVISÃO

Dra. Ana Moitinho Byrne

Departamento de Análise de Riscos e Solvência

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Governação e organização

Quadro de governação interna e de controlo para gestão eficaz e prudente do risco associado às TIC a fim de alcançar um elevado nível de resiliência operacional digital

Responsabilidades do **órgão de administração**

Criação de um **cargo para monitorizar os acordos** celebrados com terceiros prestadores de serviços de TIC relativos à utilização de serviços de TIC

Atualização dos **conhecimentos e competências** dos membros do órgão de administração para **compreensão e avaliação do risco associado às TIC**

Disposições do Regulamento DORA

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Governação e organização

Responsabilidades do órgão de administração

- Políticas de segurança de informação (disponibilidade, autenticidade, integridade e confidencialidade dos dados)
- Competências e responsabilidades claras para todas as funções relacionadas com as TIC
- Estratégia de resiliência operacional digital (incluindo tolerância ao risco associado às TIC)
- Política de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC
- Planos de auditoria interna das TIC
- Programas de sensibilização para a segurança das TIC
- Política em matéria de acordos relativos à utilização de serviços de TIC prestados por terceiros
- Canais de comunicação a nível institucional (informação sobre acordos com terceiros prestadores de serviços de TIC)

Disposições do Regulamento DORA

AUTORIDADE DE SUPERVISÃO DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Quadro de gestão do risco associado às TIC

Estratégias, políticas, procedimentos, protocolos e ferramentas de TIC

Função de controlo independente, para gestão e supervisão do risco associado às TIC

Documentação e revisão anual (no mínimo)

Auditorias internas periódicas e subsequente verificação e correção dos resultados

Estratégia de resiliência operacional digital

Disposições do Regulamento DORA

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Quadro de gestão do risco associado às TIC

Estratégias, políticas, procedimentos, protocolos e ferramentas de TIC

- Elementos gerais das **políticas, procedimentos, protocolos e ferramentas**, incluindo políticas de segurança das TIC
- Detalhes das **políticas e procedimentos**: de gestão do risco associado às TIC; de gestão dos ativos de TIC; de gestão do funcionamento (operação) das TIC
- Detalhes das **políticas**: em matéria de encriptação e controlos criptográficos, incluindo a gestão das chaves criptográficas; de gestão dos projetos de TIC; que regula a aquisição, desenvolvimento e manutenção dos sistemas de TIC; de segurança física e ambiental
- Detalhes dos **procedimentos**: para gerir a capacidade e o desempenho; para gerir as vulnerabilidades e correções informáticas; de segurança dos dados e dos sistemas; de gestão das alterações das TIC
- Detalhes das **políticas, procedimentos, protocolos e ferramentas**: em matéria de segurança das redes; de proteção das informações em trânsito
- Requisitos de **registo** (*logs*)

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Quadro de gestão do risco associado às TIC

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Quadro de gestão do risco associado às TIC

- **Outras disposições do Regulamento (UE) 2024/1774**
  - Políticas e procedimentos no âmbito do controlo da gestão dos direitos de acesso
  - Política em matéria de incidentes relacionados com as TIC
  - Funções e responsabilidades para detetar e responder eficazmente a incidentes e atividades anómalas relacionados com as TIC
  - Detalhes da política de continuidade das atividades no domínio das TIC
  - Requisitos dos testes dos planos de continuidade das atividades no domínio das TIC
  - Detalhes dos planos de resposta e recuperação no domínio das TIC
  - Formato e conteúdos do relatório sobre a revisão do quadro de gestão do risco associado às TIC

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco associado às TIC

Quadro simplificado de gestão do risco associado às TIC

- Ao nível nacional, abrange as pequenas instituições de realização de planos de pensões profissionais (i.e., com mais de 15 participantes e menos de 100 participantes)
- Os requisitos consideram a escala, o risco, a dimensão e a complexidade das entidades financeiras
- Abrange os seguintes requisitos:
  - Governação e organização
  - Outros elementos dos sistemas, protocolos e ferramentas para minimizar o impacto do risco associado às TIC
  - Gestão da continuidade das atividades no domínio das TIC
  - Relatório sobre a revisão do quadro simplificado de gestão do risco associado às TIC

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Requisitos gerais

- Estabelecer e implementar um processo para detetar, gerir e notificar os incidentes relacionados com as TIC
- Registar todos os incidentes relacionados com as TIC, bem como as ciberameaças significativas
- Monitorizar, tratar e acompanhar de forma coerente e integrada os incidentes relacionados com as TIC
- Classificar os incidentes de carácter severo relacionados com as TIC com base nos critérios do Regulamento (UE) 2024/1772

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

- Número e/ou relevância dos **clientes ou contrapartes financeiras** afetados e número de **transações** afetadas
- Impacto em termos de **reputação**
- **Duração do incidente**, incluindo tempo de indisponibilidade do serviço
- **Distribuição geográfica** relativamente às áreas afetadas pelo incidente, incluindo outros Estados-membros
- **Perdas de dados**
- **Criticalidade** dos serviços afetados
- **Impacto económico**

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Número e/ou relevância dos **clientes ou contrapartes financeiras** afetados e número de **transações** afetadas

- Clientes pessoas singulares ou coletivas ou contrapartes financeiras que tenham celebrado um acordo contratual impossibilitados de usufruir dos serviços prestados pela entidade financeira afetada durante o incidente
- Transações que envolvam um valor monetário e em que pelo menos uma parte da transação seja realizada na União
- **Limiares de materialidade**: número de clientes afetados superior a 10% ou a 100 000; número de contrapartes financeiras afetadas superior a 30%; número de transações afetadas superior a 10% do número médio diário de transações; transações afetadas superior a 10% do valor médio diário das transações; afetação de clientes ou contrapartes financeiras que tenham sido identificados como relevantes

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Impacto em termos de **reputação**

- Incidente noticiado nos meios de comunicação social
- Incidente deu origem a queixas repetidas de diferentes clientes ou contrapartes financeiras
- Impossibilidade ou potencial impossibilidade de cumprir obrigações regulatórias em resultado do incidente
- Perda ou provável perda de clientes ou contrapartes financeiras em resultado do incidente
- **Limiar de materialidade**: preenchimento de qualquer das condições acima

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Duração do incidente, incluindo tempo de indisponibilidade do serviço

- Duração: desde o momento da ocorrência do incidente até à sua resolução
- Em caso de impossibilidade de detetar o momento da ocorrência, pode ser considerado o momento da deteção
- Indisponibilidade: desde o momento em que o serviço se tornou total ou parcialmente indisponível até ao restabelecimento das atividades ou operações regulares
- Em caso de impossibilidade de detetar o momento da indisponibilidade, pode ser considerado o momento da deteção
- **Limiares de materialidade**: duração do incidente superior a 24h; tempo de indisponibilidade do serviço superior a 2h para serviços de TIC que apoiam funções críticas ou importantes

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Distribuição geográfica relativamente às áreas afetadas pelo incidente, incluindo outros Estados-membros

- Impacto transfronteiriço do incidente, incluindo:
  - Clientes e contrapartes financeiras de outros Estados-membros
  - Sucursais ou outras entidades financeiras pertencentes ao grupo que exerçam atividades noutros Estados-membros
- **Limiar de materialidade**: impacto em dois ou mais Estados-membros

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Perdas de dados

- Disponibilidade: dados temporária ou permanentemente inacessíveis ou inutilizáveis
- Autenticidade: comprometimento da fiabilidade da fonte dos dados
- Integridade: alteração não autorizada dos dados que os tornou inexatos ou incompletos
- Confidencialidade: acesso ou divulgação dos dados a uma parte ou sistema não autorizado
- **Limiares de materialidade**: impacto na disponibilidade, autenticidade, integridade ou confidencialidade que possam ter consequências negativas para a realização dos objetivos da entidade financeira ou para a sua capacidade de cumprir obrigações regulatórias; qualquer acesso bem-sucedido, mal-intencionado e não autorizado não abrangido pelo critério anterior, sempre que esse acesso possa resultar em perdas de dados

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Criticalidade dos serviços afetados

- Afetação de serviços de TIC ou sistemas de rede e de informação que apoiam funções críticas ou importantes
- Afetação de serviços financeiros prestados pela entidade financeira que exijam autorização, registo ou que sejam supervisionados pelas autoridades competentes
- Acesso bem-sucedido, mal-intencionado e não autorizado aos sistemas de rede e de informação da entidade financeira (**limiar de materialidade**)

AUTORIDADE DE SUPERVISÃO DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

Impacto económico

- Determinação dos custos e perdas diretos e indiretos incorridos em resultado do incidente, incluindo:
  - Fundos ou ativos financeiros expropriados, incluindo furto
  - Custos de substituição e relocalização de *software*, *hardware* ou infraestruturas
  - Custos com pessoal
  - Taxas por incumprimento de obrigações contratuais
  - Custos de reparação e indemnização
  - Prejuízos resultantes da perda de receitas
  - Custos de comunicação e com consultoria
- **Limiar de materialidade**: custos e perdas excedem (ou podem vir a exceder) 100 000 EUR

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Classificação de incidentes relacionados com as TIC

- Incidentes de carácter severo:
  - Qualquer acesso bem-sucedido, mal-intencionado e não autorizado que possa resultar em perdas de dados
  - Alcance de pelo menos dois dos restantes limiares de materialidade
  - Incidentes recorrentes que, não sendo individualmente considerados de carácter severo, tenham ocorrido pelo menos duas vezes num período de seis meses, têm a mesma causa aparente, preenchem coletivamente os critérios para serem considerados de carácter severo
- Ciberameaças significativas

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Notificação de incidentes de carácter severo relacionados com as TIC

Comunicação às autoridades competentes

- Notificação inicial, relatório intercalar e relatório final (prazos a definir em norma técnica de regulamentação, ainda não publicada)
- Notificação voluntária de ameaças significativas
- Harmonização de conteúdos e modelos (a definir em norma técnica de execução, ainda não publicada)

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

IMPLEMENTAÇÃO DO REGULAMENTO DORA: MANDATOS REGULATÓRIOS E DESAFIOS PARA A SUPERVISÃO

Dr. Tiago Silva

Departamento de Supervisão Prudencial de Empresas de Seguros

AUTORIDADE DE SUPERVISÃO DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

- **Artigos 28.º a 44.º do Regulamento DORA**

Princípios gerais	Acordos contratuais	Quadro de superintendência
• Total responsabilização por parte das entidades financeiras • Estratégia de gestão do risco de terceiros • Registo de informação • Avaliação do risco de concentração • Proporcionalidade	• Descrição das funções e serviços • Indicação da localização/armazenamento dos dados • Obrigação do prestador de serviços de TIC prestar assistência • Direito de acesso, inspeção e auditoria	• Designação pelas Autoridades Europeias de Supervisão (ESA) • Autoridade fiscalizadora principal tem o poder de monitorizar e emitir recomendações • Fórum de superintendência que permite cooperação entre setores

- Regulamento Delegado (UE) 2024/1773 que especifica a política de utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC
- Regulamento de Execução (UE) 2024/2956 que estabelece os modelos do registo de informações
- RTS que especifica os elementos que devem permitir à entidade financeira determinar e avaliar quando proceder à subcontratação de serviços de TIC de apoio a funções críticas ou importantes (ao abrigo do n.º 5 do artigo 30.º do DORA)

- Regulamento Delegado (UE) 2024/1502 que especifica os critérios para a designação dos terceiros prestadores de serviços de TIC críticos
- Regulamento Delegado (UE) 2024/1505 que determina o montante das taxas de superintendência
- RTS sobre a harmonização das condições que permitem o exercício de atividades de superintendência
- Orientações sobre cooperação e troca de informação CAs-ESA

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

- **Regulamento Delegado (UE) 2024/1773 que especifica a política de utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC**

Política deve	ter em conta a **dimensão** e o perfil de risco global da EF e a natureza, escala e **complexidade** dos seus serviços
	ser aplicada de forma coerente, pela empresa-mãe, a **todas as entidades financeiras do grupo**
	estabelecer mecanismos da sua própria **governação**
	especificar requisitos para cada fase principal do **ciclo de vida do acordo contratual**
	exigir que antes da celebração do acordo sejam **definidas as necessidades** operacionais e realizada uma **avaliação de risco**

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

- **Regulamento Delegado (UE) 2024/1773 que especifica a política de utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC**

Política deve	estabelecer um processo adequado e proporcional de seleção e avaliação de terceiros prestadores de serviços de TIC (***Due Diligence***)
	estabelecer medidas adequadas para identificar, prevenir e gerir **conflitos de interesses** reais ou potenciais decorrentes da utilização de terceiros prestadores de serviços de TIC
	estabelecer os elementos que devem constar dos **acordos contratuais** (incluindo os que constam da RTS)
	estabelecer requisitos relativos à **monitorização dos acordos** contatuais
	incluir requisitos para um **plano de saída** para cada acordo contratual

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

- **Regulamento de Execução (UE) 2024/2956 que estabelece os modelos do registo de informações**
  - O registo de informação (RoI) tem diversos propósitos, designadamente permitir que:
    - as entidades financeiras monitorizarem o seu risco em relação a terceiros prestadores de serviços de TIC,
    - as autoridades competentes supervisionem as TIC e a gestão do risco de terceiros das entidades financeiras, e
    - as ESA possam designar as CTTP que estarão sujeitas à superintendência ao nível da UE
  - O RoI devem ser mantido ao nível da entidade, subconsolidado e consolidado, obedecendo à estrutura e conteúdos estabelecidos no regulamento

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

- **Regulamento de Execução (UE) 2024/2956 que estabelece os modelos do registo de informações**
  - Considerando 7 – (…) caso uma entidade atue em nome de uma entidade financeira relativamente a todas as atividades da entidade financeira (incluindo os serviços de TIC), os terceiros prestadores de serviços de TIC diretos a essa entidade devem ser registados nos modelos pertinentes do registo de informações da entidade financeira. Nesse caso, a entidade só é registada como entidade que mantém o registo.
  - Anexo III – Lista os tipos de serviços de TIC

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

Dry run exercise

- **Principal objetivo** - ajudar as EF a preparar o RoI – melhorando a qualidade dos dados para o reporte formal que terá início a partir de 2025.

- Permitiu também testar os processos de reporte e facilitar a **preparação das autoridades competentes**, integrando-as nos canais de comunicação que serão utilizados para a comunicação oficial.

- Conclusões do exercício em: https://www.eiopa.europa.eu/publications/key-findings-2024-esas-dry-run-exercise-dora_en

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Gestão do risco devido a terceiros

Principais conclusões

- **EF são encorajadas a familiarizarem-se, tanto quanto possível, com o Regulamento de Execução e a seguirem todas as instruções neles contidas**
- Parte essencial dos requisitos está disponível ao público desde a publicação do relatório final das ESA, em janeiro de 2024
- EF são encorajadas a antecipar, tanto quanto possível, a preparação do RoI, especialmente, no que diz respeito a informações que podem não estar imediatamente disponíveis (por exemplo, os identificadores dos terceiros prestadores de serviços de TIC), para o qual pode ser necessário um esforço adicional de recolha de dados, uma vez que essas informações não foram utilizadas no exercício

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Implementação do Regulamento DORA: mandatos regulatórios e desafios para a supervisão

Principais desafios

	Autoridades Competentes	Entidades financeiras	Recursos Financeiros	Recursos Humanos
Gestão do risco associado às TIC	Desenvolvimento de metodologias de avaliação e supervisão de riscos TIC, Inspeções; Coordenação com outras autoridades competentes	Implementação de requisitos, desenvolvimento de procedimentos de controlo interno e auditoria interna	Adaptação/ implementação dos sistemas de informação (recolha e transmissão de informação, em particular - comunicação de incidentes, registo de acordos contratuais)	Formação contínua das equipas e desenvolvimento de competências internas em gestão de riscos TIC
Gestão do risco devido a terceiros prestadores de serviços de TIC	Identificação de prestadores de serviços críticos a nível nacional, Monitorização de riscos	*Due diligence* de fornecedores de TIC, gestão de contratos e SLAs, Manutenção do registo de informações sobre acordos contratuais com terceiros prestadores de serviços de TIC		
Testes de Resiliência Operacional Digital	Coordenação e certificação de testes TLPT	Realização de testes de resiliência operacional digital		
Gestão de incidentes relacionados com as TIC	Desenvolvimento de ferramenta e procedimentos de submissão e análise de incidentes por parte das entidades supervisionadas	Desenvolvimento de processos para classificação e reporte de incidentes de carácter severo relacionados com as TIC		

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Q&A

Dúvidas ou pedidos de esclarecimento

DORA@asf.com.pt