GRCForce

Lista de verificação para auditoria de contratos de fornecedores ao abrigo da NIS2 e do DORA

15 de junho de 2026

grcforce.com/pt/#contact

Practical governance, risk and compliance guidance for European organisations.

Publicado em 15 de junho de 2026 | GRCForce

Utilize esta lista para verificar se os contratos com fornecedores críticos sustentam uma verdadeira resiliência operacional, e não apenas a conclusão do processo de compras.

Destina-se a organizações que analisam relações materiais com terceiros de TIC, cloud, SaaS, serviços geridos e outros fornecedores abrangidos pela NIS2 e/ou pelo DORA.

Como utilizar esta lista

Para cada cláusula ou pergunta, assinale uma das seguintes opções:

- Implementada e adequada
- Parcialmente coberta
- Em falta
- Necessita de revisão jurídica

Um contrato não precisa de ter uma redação perfeita no primeiro dia. Precisa, no entanto, de atribuir claramente a responsabilidade pelas lacunas e de incluir uma decisão sobre a aceitabilidade do risco.

12 cláusulas e perguntas contratuais a analisar

1. Direito de auditoria

O contrato confere à sua organização um direito prático de obter evidências de auditoria, analisar relatórios de controlo e solicitar medidas de seguimento quando sejam identificadas lacunas significativas?

Porque é importante: se não conseguir testar ou analisar de forma credível os controlos do fornecedor, estará a depender de confiança em vez de garantia verificável.

2. Obrigações de segurança

As obrigações mínimas de segurança do fornecedor estão claramente definidas, incluindo proteção de sistemas, controlo de acessos, gestão de vulnerabilidades, registo de atividade, cópias de segurança, recuperação e gestão segura de alterações?

Porque é importante: referências vagas a «segurança segundo as normas do setor» são normalmente demasiado fracas quando ocorre um incidente.

3. Prazo de notificação de incidentes

O contrato define a rapidez com que o fornecedor deve notificá-lo de um incidente de segurança, interrupção do serviço, violação de dados ou falha material de controlo?

Porque é importante: expressões como «sem demora injustificada» são frequentemente demasiado vagas para serviços críticos. São necessários prazos operacionalmente úteis.

4. Controlo de acessos e identidades

O contrato define como é gerido o acesso privilegiado, como as contas são revistas e como o acesso é revogado quando uma pessoa sai da organização ou quando o serviço termina?

Porque é importante: muitos incidentes em fornecedores começam com acessos administrativos fracos e uma gestão deficiente de identidades.

5. Transparência sobre localização e tratamento de dados

Consegue identificar onde os seus dados são tratados, armazenados, salvaguardados e acedidos, incluindo a utilização de subcontratantes ou equipas de suporte localizadas noutros países?

Porque é importante: a resiliência e a exposição regulamentar são mais difíceis de gerir quando o tratamento de dados é opaco.

6. Controlo de subcontratantes

O fornecedor necessita da sua aprovação, ou pelo menos de o notificar previamente, antes de nomear subcontratantes materiais que possam afetar a prestação do serviço, a segurança ou a conformidade?

Porque é importante: o risco de quarta parte surge frequentemente através de dependências ocultas que nunca foram avaliadas.

7. Continuidade de negócio e recuperação de desastres

O contrato exige que o fornecedor mantenha e teste medidas de continuidade de negócio e recuperação de desastres adequadas à criticidade do serviço?

Porque é importante: a resiliência não é uma declaração. Requer objetivos de recuperação, procedimentos testados e evidências.

8. Níveis de serviço associados à criticidade

Os níveis de serviço, tempos de recuperação, compromissos de suporte e vias de escalamento estão alinhados com a importância real do serviço para o negócio?

Porque é importante: muitos contratos são redigidos como se o serviço fosse rotineiro, mesmo quando suporta um processo crítico.

9. Devolução, extração e eliminação de dados

O contrato explica como os seus dados serão devolvidos, em que formato, dentro de que prazo, a que custo e como os dados residuais serão eliminados no momento da saída?

Porque é importante: se as condições de saída não forem claras, poderá ficar operacionalmente bloqueado.

10. Cláusulas de alteração de controlo e de alteração material

O contrato protege-o caso o fornecedor seja adquirido, altere substancialmente o modelo de serviço, desloque operações ou mude subcontratantes essenciais?

Porque é importante: o risco do fornecedor pode mudar de um dia para o outro sem qualquer alteração da sua parte.

11. Obrigações de evidência e reporte

O fornecedor tem de fornecer regularmente evidências como relatórios de auditoria, resultados de testes, certificações, atualizações de risco ou declarações sobre os controlos?

Porque é importante: uma diligência devida realizada uma única vez não é suficiente para relações críticas.

12. Apoio à saída e assistência na transição

O contrato exige que o fornecedor apoie a transição para outro prestador ou para um serviço interno, incluindo cooperação, documentação e assistência técnica?

Porque é importante: a resiliência inclui a capacidade de abandonar uma relação sem uma perturbação grave.

Sinais de alerta que exigem atenção imediata

- Ausência de direito de auditoria, ou redação que deixa a auditoria inteiramente ao critério do fornecedor
- Ausência de um prazo claro de notificação de incidentes
- Ausência de uma cláusula sobre alterações de subcontratantes
- Ausência de um compromisso de recuperação testado para serviços críticos
- Ausência de condições práticas para extração ou eliminação de dados
- Ausência de obrigações de apoio à saída
- Ausência de obrigação de fornecer evidências de garantia atualizadas
- Ausência de proteção em caso de alteração de controlo

Guia rápido de pontuação

- 10 a 12 elementos implementados e adequados: base contratual sólida
- 7 a 9 elementos implementados: base viável, mas com lacunas prioritárias a analisar
- 4 a 6 elementos implementados: risco contratual elevado
- 0 a 3 elementos implementados: o contrato deve ser considerado de elevada prioridade para remediação

Casos de utilização sugeridos

Esta lista é adequada para:

- Revisões de integração de fornecedores
- Revisões de renovação contratual
- Avaliações de terceiros de TIC ao abrigo do DORA
- Revisões do risco de fornecedores ao abrigo da NIS2
- Workshops de alinhamento entre compras e jurídico
- Reporte ao conselho de administração ou à direção sobre resiliência de terceiros

Fontes oficiais de referência

Fontes da União Europeia

- Texto oficial da Diretiva NIS2 no EUR-Lex: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Texto oficial do Regulamento DORA no EUR-Lex: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Página da Comissão Europeia sobre atos de execução e atos delegados do DORA: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en
- Página da ESMA sobre o DORA: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- Página da Comissão Europeia sobre a implementação da NIS2 na Bélgica: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Fontes belgas

- Portal de informação NIS2 do Centre for Cybersecurity Belgium: https://belgium-nis2.be/en/

- Site principal do Centre for Cybersecurity Belgium: https://ccb.belgium.be/en
- Ponto de contacto CERT.be através da página da Comissão Europeia sobre a implementação na Bélgica: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Bloco breve para publicações ou barras laterais de artigos

Fontes oficiais úteis para trabalhar com a NIS2 ou o DORA:

- Texto oficial da NIS2: Diretiva (UE) 2022/2555 no EUR-Lex
- Texto oficial do DORA: Regulamento (UE) 2022/2554 no EUR-Lex
- Visão geral e atualizações do DORA: ESMA
- Implementação da NIS2 e pontos de contacto na Bélgica: página de Estratégia Digital da Comissão Europeia
- Informação prática sobre a NIS2 na Bélgica: Centre for Cybersecurity Belgium

Apoio para uma análise prática

Contacte a GRCForce para analisar onde a redação dos contratos de fornecedores, a governação e a resiliência operacional não estão alinhadas: https://grcforce.com/pt/#contact

Esta lista fornece orientação prática e não substitui aconselhamento jurídico. A redação contratual e a interpretação regulamentar devem ser encaminhadas para a revisão jurídica adequada.