Transposição da Diretiva NIS 2: Regime Jurídico da Cibersegurança

Guia Prático

Transformative Legal Experts

PLMJ

Índice

Foi publicado, no dia 4 de dezembro, o Decreto-Lei n.º 125/2025, de 4 de dezembro que estabelece o novo regime jurídico da cibersegurança ("**Regime Jurídico da Cibersegurança**" ou "**RJC**"), após a sua aprovação em Conselho de Ministros e subsequente promulgação pelo Presidente da República.

O diploma transpõe a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União ("**Diretiva NIS 2**"), reforçando a capacidade nacional de prevenção e resposta a ciberameaças.

O Regime Jurídico da Cibersegurança – há muito aguardado – vem clarificar as obrigações de cada entidade abrangida, podendo agora ter início os respetivos processos de implementação e/ou melhoria dos seus sistemas de gestão de segurança da informação, no cumprimento das obrigações decorrentes da transposição.

Este guia explicativo pretende dar a conhecer as alterações e informações mais relevantes do novo Regime Jurídico da Cibersegurança.

1. O que é a Diretiva NIS 2?

A Diretiva (UE) 2016/1148, de 6 de julho de 2016 ("**Diretiva NIS**"), foi o primeiro ato legislativo horizontal da UE a abordar os novos desafios da cibersegurança e constituiu um ponto de viragem em termos de resiliência e cooperação da União em matéria de cibersegurança, uma vez que, até então, não existia uma estratégia única para a promoção da cibersegurança, cabendo a cada empresa definir como implementar essa estratégia.

A implementação da Diretiva NIS em Portugal foi feita através da transposição pela Lei n.º 46/2018, de 13 de agosto, ("**Regime Jurídico da Segurança do Ciberespaço**") e complementada pelo Decreto-Lei n.º 65/2021 e pelo Regulamento n.º 183/2022 (Instrução Técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes).

▲ VOLTAR AO INÍCIO

Contudo, a evolução do panorama de ameaças e a necessidade de reforço da atividade preventiva das empresas, mas também da cooperação entre os Estados-Membros em matéria de cibersegurança, exigiu a publicação de uma versão melhorada e adaptada ao cenário atual da antiga Diretiva NIS, surgindo, assim, a Diretiva NIS2.

Num cenário de aumento significativo de ameaças digitais, a Diretiva NIS 2 (Diretiva (UE) 2022/2555) estabelece um quadro jurídico europeu para a cibersegurança, visando aumentar a resiliência das infraestruturas críticas e essenciais contra ciberameaças. Em Portugal, a transposição desta diretiva:

- Reflete o aumento da sofisticação das ciberameaças, que se tornam cada vez mais frequentes e complexas;
- Reforça a segurança nacional, protegendo setores estratégicos e críticos; e
- Harmoniza medidas a nível europeu, garantindo uniformidade e colaboração entre os Estados-Membros.

A Diretiva amplia a lista de entidades abrangidas e introduz requisitos mais rigorosos para prevenir e mitigar incidentes de cibersegurança.

2. Quais são os objetivos do RJC e que mudanças vem trazer?

O antigo Regime Jurídico de Segurança do Ciberespaço era aplicável a operadores de serviços essenciais, operadores de infraestruturas críticas, a prestadores de serviços digitais e à Administração Pública e tinha como principais objetivos a adoção de medidas de segurança adequadas para a gestão dos riscos aos seus sistemas de rede e de informação, a definição de critérios e prazos claros de notificação de incidentes significativos de cibersegurança às respetivas autoridades nacionais e a promoção do intercâmbio de informações e a cooperação entre os Estados Membros da UE e entre os setores público e privado.

Apesar de terem denominadores comuns, o novo Regime Jurídico da Cibersegurança traz algumas novidades e um rigor mais acentuado para as entidades envolvidas, face ao seu antecessor.

Nesse sentido, do Regime Jurídico da Cibersegurança, destacam-se as seguintes mudanças:

- O alargamento do âmbito de aplicação subjetivo, tanto para novos setores de atividade, como para os setores existentes no regime jurídico anterior[1].
- O papel do Centro Nacional de Cibersegurança ("CNCS") na regulação e fiscalização.
- A distinção das obrigações e fiscalização com base na dimensão da entidade, no negócio e no nível de exposição ao risco.

A clarificação de um conjunto de medidas de segurança da informação mínimas a adotar pelas entidades abrangidas, sem prejuízo de as entidades poderem optar por um regime mais rigoroso.

O enquadramento legal proposto é também orientado pelo princípio da proporcionalidade, equilibrando os custos de implementação e de manutenção dos sistemas de informação com o nível de risco associado ao setor, entidade ou tipo de negócio. Apesar de todas as entidades estarem sujeitas à implementação das mesmas medidas de segurança da informação e de gestão dos riscos de cibersegurança, à responsabilização da gestão de topo e à notificação de incidentes de cibersegurança, as diferenças mais visíveis deste princípio da proporcionalidade são, desde logo, na supervisão pelo CNCS: as entidades essenciais serão sujeitas a supervisão *ex ante* e *ex post* (antes ou depois de um incidente significativo), enquanto as entidades importantes apenas estarão sujeitas a supervisão *ex post*; em relação a auditorias, as entidades essenciais serão sujeitas

1 Cfr. Artigo 3º.

a auditorias regulares, específicas e *ad-hoc*, enquanto as entidades importantes apenas a auditorias específicas. Adicionalmente, as coimas decorrentes das contraordenações estabelecidas no Decreto-Lei variam consoante sejam aplicadas a entidades essenciais ou importantes, uma vez que as entidades importantes, para além de um nível de exposição ao risco reduzido face às entidades essenciais, têm, regra geral, uma dimensão e volume de negócios mais reduzido, pelo que a proporcionalidade do valor das coimas reflete também uma preocupação do legislador em assegurar que o presente Regime Jurídico da Cibersegurança não promove o estrangulamento económico do tecido empresarial de pequena e média dimensão.

Além disso, fomenta a partilha de informações e a cooperação entre entidades públicas e privadas, promovendo uma resposta coordenada a incidentes de cibersegurança, visando fortalecer a resiliência do tecido empresarial em Portugal.

3. Que entidades estão abrangidas?

O RJC divide as entidades abrangidas em quatro categorias principais:

ENTIDADES ESSENCIAIS

Correspondem às entidades referidas no Anexo I do Decreto-Lei (setores críticos) que não sejam uma PME[2], ou às entidades referidas no Artigo 6.º n.º 1:

- Prestadores de serviços de confiança qualificados e registo de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio;
- Médias empresas que ofereçam redes públicas de comunicações eletrónicas ou serviços de comunicações eletrónicas acessíveis ao público;
- Entidades da Administração Pública que tenham como atribuições a prestação de serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação, ou aquelas que apresentem um grau particularmente elevado de integração digital na prestação dos seus serviços, e ainda a entidade pública responsável pela área da avaliação educativa;
- Entidades identificadas como críticas nos termos do disposto na Diretiva (EU) 2022/2557, do Parlamento Europeu e o Conselho, de 14 de dezembro de 2022);
- Qualquer entidade constante dos Anexos I ou II do Decreto-Lei que seja qualificada como entidade essencial com base no respetivo grau de exposição da entidade aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico, quer porque:

a) A entidade em causa seja o único prestador de um serviço que é essencial para a manutenção de atividades sociais ou económicas críticas (tais como as identificadas nos Anexos I e II);

b) Uma perturbação do serviço por si prestado possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública;

c) Uma perturbação do serviço por si prestado possa gerar riscos sistémicos consideráveis, incluindo perturbações com um impacto transfronteiriço; ou

d) A entidade seja crítica devido à sua importância específica, a nível nacional ou regional, para o setor ou tipo de serviço em causa, ou para outros setores interdependentes.

2 De acordo com o art. 2.º do Anexo III, a categoria das PME é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros o cujo balanço total anual não excede 43 milhões de euros.

Exemplo de setores críticos são energia, transportes (rodoviário, ferroviário, aéreo e marítimo), saúde, água (água potável e águas residuais), infraestruturas digitais, infraestruturas do mercado financeiro, instituições de crédito, gestão de TIC e Espaço (cfr. Anexo I).

ENTIDADES IMPORTANTES

Corresponde a uma categoria residual de entidades referidas no Anexo I que não sejam consideradas entidades essenciais.

Outros setores críticos (cfr. Anexo II) incluem serviços postais, produção e distribuição de produtos químicos, gestão de resíduos, indústria alimentar (produção e distribuição), indústria transformadora (no qual se inclui a produção de equipamentos médicos, de equipamentos informáticos, de equipamento elétrico, de máquinas, de produção automóvel e de outros equipamentos de transporte), prestadores de serviços digitais e organismos de investigação.

Exemplo dos setores críticos são energia, transportes, saúde, água, infraestruturas digitais, infraestruturas financeiras, gestão de TIC e Espaço.

ENTIDADES PÚBLICAS RELEVANTES

Divididas em Grupo A[3] e Grupo B[4], incluem organismos da administração pública com impacto na prestação de serviços essenciais.

As entidades públicas relevantes estão sujeitas a medidas de supervisão proporcionais ao seu grupo, com obrigações específicas a definir por regulamento do CNCS[5].

ENTIDADES INDEPENDENTEMENTE DA NATUREZA OU DIMENSÃO

Cumpre referir que o diploma exclui do seu âmbito pequenas e microempresas, exceto quando:

- A entidade em causa seja:

a) fornecedor de redes públicas de comunicações eletrónicas ou prestador de serviços de comunicações eletrónicas acessíveis ao público;

b) prestador de serviços de confiança; ou

c) registo de nomes de domínio de topo, prestador de serviços de registo de nomes de domínio, prestador de serviços de sistemas de nomes de domínio.

- A entidade em causa seja o único prestador de um serviço que é essencial para a manutenção de atividades sociais ou económicas críticas;

- Uma perturbação do serviço por si prestado possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública;

3 Cfr. Artigo 7.º n.º 2, entidades do Grupo A constituem por exemplo os serviços de administração direta e indireta do Estado, com 250 trabalhadores ou mais no seu quadro de pessoal.
4 Cfr. Artigo 7.º n.º 3, entidades do Grupo B constituem por exemplo os serviços de administração direta ou indireta do Estado, com entre 75 a 249 trabalhadores no seu quadro de pessoal.
5 Artigo 33.º.

- Uma perturbação do serviço por si prestado possa gerar riscos sistémicos consideráveis, especialmente para os setores relativamente aos quais tal perturbação possa ter um impacto transfronteiriço;

- A entidade seja crítica devido à sua importância específica, a nível nacional ou regional, para o setor ou tipo de serviço em causa, ou para outros setores interdependentes[6];

- Sejam identificadas como entidades críticas nos termos do disposto na Diretiva (EU) 2022/2557, do Parlamento Europeu e o Conselho, de 14 de dezembro de 2022[7]; ou

- Instituições de ensino superior[8].

4. Qual a diferença entre as obrigações de *qualificação* e de *registo*?

A qualificação e o registo, embora complementares, têm funções distintas devendo ambos ser submetidos pelas entidades a quem o RJC se aplique, através de uma plataforma eletrónica do CNCS que será criada para o efeito.

A *qualificação*[9] é a comunicação das entidades abrangidas da sua existência e enquadramento no âmbito do Regime. Este procedimento deve ter lugar **no prazo de 30 dias após o início da atividade, ou, para entidades já em funcionamento na data da entrada em vigor do Regime, no prazo de 60 dias após disponibilização da referida plataforma** e permite ao CNCS confirmar se a entidade em causa está abrangida pelo RJC e em que categoria se enquadra, definido assim a que obrigações está a entidade em causa sujeita. Estas qualificações são revistas pelo menos de dois em dois anos ou sempre que haja alterações relevantes.

O processo de qualificação deve ser fundamentado pelo CNCS, e as entidades sujeitas a qualificação têm direito a audiência prévia. Uma vez concluído o processo de qualificação de uma entidade, o CNCS tem um prazo máximo de 30 dias para notificar a entidade.

O CNCS pode ainda requalificar a entidade se verificar que a realidade não corresponde ao declarado – havendo sempre obrigação de fundamentar a decisão e direito a audiência prévia.

6 Artigo 3.º, n.º 2.
7 Artigo 3.º, n.º 5.
8 Artigo 3.º, n.º 6.
9 Artigo 8.º.

▲ VOLTAR AO INÍCIO

Em caso de concurso em mais do que um tipo de qualificação, aplica-se o regime mais exigente para gerir os riscos que se colocam à segurança das redes e sistemas de informação[10].

O incumprimento dos prazos de qualificação, a omissão de elementos obrigatórios ou a prestação de informação inexata podem conduzir a advertências, a instruções vinculativas (incluindo ordens para a adoção de medidas preventivas ou corretivas e para a correção de infrações), à realização de auditorias e à aplicação de coimas. Acresce que a falta de qualificação não é condição necessária à aplicação do RJC – i.e. o facto de não ter havido processo de qualificação não afasta as obrigações aplicáveis em função do enquadramento da entidade em causa ao abrigo do RJC.

Concluída a qualificação, inicia-se a obrigação permanente de *registo* e de atualização tempestiva dos dados, que serve de base à comunicação de incidentes e à atuação de supervisão[11].

As entidades devem indicar os elementos que permitam a sua identificação completa, incluindo nome, número de identificação fiscal, endereço e dados de contacto atualizados, bem como informação sobre responsáveis designados (incluindo o Responsável pela Cibersegurança), o ponto de contacto permanente e os setores de atividade e a Estado(s)-Membro(s) da UE onde prestam os serviços. Este registo serve de base para a comunicação de incidentes, facilita a fiscalização por parte do CNCS e permite uma resposta mais célere em caso de necessidade. Assim, enquanto a qualificação é um passo inicial e pontual, o registo representa uma obrigação permanente de atualização e transparência perante o CNCS.

Além disso, os prestadores de serviços específicos - incluindo os que oferecem serviços de computação em nuvem, centros de dados, serviços geridos, mercados em linha e plataformas de redes sociais - são obrigados a registar informações adicionais. Nestes casos, as entidades devem fornecer o endereço do seu estabelecimento principal na UE ou, se não estiverem estabelecidas na UE, os dados do seu representante designado. Devem também fornecer informações de contacto, uma lista dos Estados-Membros da UE onde operam e os seus intervalos de endereços IP.

É importante notar que quaisquer alterações a estas informações registadas devem ser comunicadas no prazo de 30 dias úteis, exceto no caso dos prestadores de serviços acima mencionados, para os quais o período de atualização é de três meses.

O incumprimento dos prazos de qualificação, a omissão de elementos obrigatórios ou a prestação de informação inexata podem conduzir a advertências, a instruções vinculativas, à realização de auditorias e à aplicação de coimas.

10 Artigo 9.º.
11 Artigo 35.º.

5. Quais as medidas de cibersegurança exigidas?

As medidas variam de acordo com a categoria da entidade, sendo sobretudo direcionadas a entidades essenciais e importantes[12], incluindo:

- Identificação e mitigação de riscos de cibersegurança relevantes;
- Segurança da cadeia de abastecimento, através da avaliação e gestão dos riscos associados a fornecedores e prestadores de serviços diretos da entidade;
- Políticas e procedimentos de segurança de informação, em particular relacionados com a formação em cibersegurança, a gestão de cópias de segurança, a gestão de acessos e de ativos relevantes, o tratamento de incidentes e a continuidade das atividades em caso de incidente;
- Designação de responsáveis, incluindo um responsável interno pela cibersegurança e um ponto de contacto único permanente que colabora diretamente com o CNCS[13];
- Planos de contingência e recuperação, de modo a garantir a continuidade operacional;
- Certificação de cibersegurança conforme definidas pelo CNCS (cfr. artigo 34.º).

As medidas de cibersegurança aplicadas a entidades públicas relevantes serão aprovadas por regulamento do CNCS, conforme o disposto no artigo 33.º do RJC.

O CNCS definirá, através de regulamento específico a aprovar pelo CNCS, as medidas mínimas e específicas de cibersegurança e os níveis de cumprimento a adotar pelas entidades essenciais e pelas entidades importantes. Além disso, as mesmas entidades essenciais e importantes devem avaliar e gerir o "risco residual", devendo adotar as medidas adequadas e proporcionais para responder a esses riscos residuais.

6. Quais são as obrigações da gestão de topo das entidades?

Contrariamente ao Regime Jurídico de Segurança do Ciberespaço – o regime que transpôs a Diretiva agora revogada -, o RJC densifica as responsabilidades, funções e obrigações tanto dos órgãos de gestão, direção e administração[14], como do Responsável pela Cibersegurança[15], evitando discrepâncias de responsabilidades entre os vários intervenientes e trazendo igualmente uma segurança jurídica no papel destas figuras de destaque das entidades abrangidas. Esta clarificação é particularmente relevante na medida em que o Regime inova em relação ao seu regime antecessor ao prever a responsabilização dos órgãos de gestão, direção e administração por ações ou omissões, com dolo ou culpa grave, pelas infrações previstas neste novo regime.

Os órgãos de gestão, direção e administração das entidades essenciais e importantes desempenham um papel central na implementação e supervisão das políticas de cibersegurança, assumindo responsabilidades específicas previstas no enquadramento legal em vigor. As principais obrigações destes órgãos incluem a aprovação e supervisão das medidas de gestão dos riscos de cibersegurança e a garantia de que são realizadas, de forma regular, as ações de formação e sensibilização de cibersegurança.

12 Artigo 27.º.
13 Artigos 31.º e 32.º.
14 Artigo 25.º, n.º 1.
15 Artigo 31.º, n.º 2.

As funções e responsabilidades destes órgãos de gestão, direção e administração não poderão ser delegadas, exceto noutro titular destes órgãos.

Quanto ao Responsável pela Segurança (que poderá ser algum titular de órgão de gestão, direção ou administração, ou alguém que lhes responda de forma direta), este acumula as seguintes funções:

- Propor a aplicação de determinadas medidas de gestão dos riscos de cibersegurança;
- Prestar informações e suporte aos restantes órgãos de gestão de topo na manutenção e no cumprimento das medidas de gestão dos riscos de cibersegurança propostas e implementadas na entidade;
- Contribuir para a promoção de uma cultura de cibersegurança, juntamente com os restantes órgãos, nomeadamente através de ações de formação e sensibilização de cibersegurança;
- Assegurar a gestão dos riscos residuais de cibersegurança;
- Garantir o cumprimento com as obrigações de envio do relatório anual ao CNCS; e
- Coordenar as ações do ponto de contacto permanente em tudo o que sejam funções deste último.

No caso de entidades essenciais e importantes que pertencem ao mesmo grupo empresarial, é possível designar um representante em cada empresa para atuar como interlocutor em matéria de cibersegurança, sob a supervisão de um Responsável de Segurança que seja comum ao grupo.

7. Como funciona a notificação de incidentes?

As entidades devem avaliar os incidentes com base em parâmetros específicos[16] que incluem:

- O número de utilizadores afetados pela perturbação do serviço,
- A duração do incidente, e
- A gravidade da perturbação das operações do serviço.

A notificação de incidentes divide-se em três fases principais[17]:

16 Artigo 40.º.
17 Secção II, Artigos 40.º e seguintes.

NOTIFICAÇÃO INICIAL E ATUALIZAÇÃO

Deve ser enviada ao CNCS no prazo máximo de 24 horas após a deteção de um incidente significativo e deve incluir informação preliminar sobre o impacto e as medidas adotadas.

Quando se justifique, e caso o incidente ainda não tenha perdido o impacto significativo, a entidade deverá enviar ao CNCS, no prazo máximo de 72 horas após a verificação do incidente significativo, uma atualização das informações do incidente.

NOTIFICAÇÃO DO FIM DO IMPACTO SIGNIFICATIVO

Deve ser feita até 24 horas após a verificação do fim do impacto significativo, indicando a descrição da situação de impacto, as medidas adotadas para resolver o incidente e a atualização das informações transmitidas na notificação inicial.

RELATÓRIO FINAL E INTERCALAR

Deve ser enviado ao CNCS no prazo máximo e 30 dias úteis desde a notificação de fim de impacto significativo e deve detalhar as causas, impactos, ações corretivas e medidas preventivas adotadas.

Adicionalmente, o CNCS pode solicitar informação ao público em casos de incidentes com impacto significativo, para aumentar a transparência e proteger os utilizadores.

O Regime Jurídico da Cibersegurança estipula ainda que as entidades devem cumprir os limiares e critérios técnicos definidos pelo CNCS, embora estes ainda não tenham sido publicados. O atual Quadro Nacional de Cibersegurança exige que as organizações definam níveis de impacto para a gestão do risco, considerando fatores como a classificação dos ativos de informação, as violações de segurança, o impacto financeiro, a interrupção de planos e os danos à reputação.

A notificação de incidentes deve ser feita através de uma plataforma eletrónica criada pelo CNCS. Estão a ser consideradas atualizações à plataforma para permitir um mecanismo de comunicação coordenado, destinado a agilizar a comunicação entre o CNCS, as autoridades setoriais de cibersegurança e outros organismos designados, como o Ministério Público e a Comissão Nacional de Proteção de Dados. No entanto, esta plataforma coordenada está ainda pendente da formalização de um protocolo interagências.

8. Qual o papel do CNCS e da sua coordenação com outras entidades?

O CNCS é a autoridade nacional de cibersegurança e dispõe de um conjunto de competências, entre as quais:

- Coordenação das respostas a incidentes nacionais e internacionais;
- Supervisão do cumprimento das obrigações de cibersegurança;
- Ponto de contacto único para a UE no contexto da Diretiva NIS 2; e
- Elaboração de regulamentos técnicos, incluindo o Quadro Nacional de Referência para a Cibersegurança.

O CNCS terá um papel ampliado, incluindo a supervisão da implementação da Estratégia Nacional de Cibersegurança, a coordenação de respostas a incidentes de grande escala e a garantia de conformidade com o Quadro de Referência Nacional de Cibersegurança.

9. Como funcionam as Equipas de Resposta?

O diploma prevê a designação do "CERT.PT", integrado no CNCS, como a equipa nacional de resposta a incidentes de cibersegurança, dotada de autonomia técnica e operacional[18]. Esta autonomia permite-lhe atuar diretamente em situações críticas, sem depender de outras entidades para decisões técnicas, garantindo rapidez e eficácia na mitigação de ameaças[19].

Algumas das competências do CERT.PT incluem:

- Assegurar a intervenção imediata perante incidentes de cibersegurança, coordenando ações para conter e mitigar os impactos;
- Monitorizar continuamente o panorama nacional de ciberameaças, vulnerabilidades e incidentes, prestando apoio técnico às entidades essenciais, importantes e públicas relevantes, incluindo monitorização em tempo real quando solicitado;
- Ativar mecanismos de alerta rápido e divulgar informações críticas sobre ameaças e incidentes às entidades afetadas, autoridades competentes e outras partes interessadas, garantindo rapidez e clareza, inclusive em tempo real;
- Apoiar diretamente as entidades afetadas, propondo ao CNCS instruções e medidas concretas para conter, mitigar e resolver incidentes, definindo prazos adequados para implementação;
- Em cenários de risco grave e comprovado, recomendar à autoridade competente a adoção imediata de medidas executivas, caso a entidade não atue voluntariamente;
- Recolher e preservar dados forenses, realizar análises dinâmicas de riscos e incidentes e desenvolver conhecimento situacional para reforçar a cibersegurança nacional;
- Efetuar, a pedido, análises detalhadas das redes e sistemas das entidades para identificar vulnerabilidades com impacto significativo; e
- Implementar mecanismos que permitam troca segura de dados entre entidades essenciais, importantes e públicas relevantes, bem como outras partes interessadas.

18 Artigos 19.º, n.º 3, e 22.º.
19 Artigo 22.º.

▲ VOLTAR AO INÍCIO

Para além do CERT.PT, existem equipas setoriais e especiais, nomeadamente para setores regulados como o setor bancário, financeiro, dos seguros e das comunicações, garantindo uma resposta ágil e especializada em cada área. Estas equipas asseguram uma resposta especializada e adaptada às especificidades de cada área, mas sempre em articulação com o CERT.PT. Assim, quando ocorre um incidente que afeta um setor regulado, a equipa setorial assume a intervenção direta, enquanto o CERT.PT coordena e apoia, garantindo que a resposta se insere na estratégia nacional.

A dinâmica entre equipas é de cooperação e partilha de informação, com o CNCS a coordenar a resposta nacional e a garantir a interoperabilidade com equipas congéneres europeias.

O CNCS coordena a resposta nacional garante a interoperabilidade com equipas congéneres europeias

Em situações de crise de grande escala, como ataques que comprometam infraestruturas críticas ou serviços essenciais com expressão transfronteiriça, é ativado um gabinete de crise composto por representantes das principais entidades de segurança e defesa, assegurando uma resposta coordenada e eficaz. Este gabinete garante uma resposta coordenada e eficaz, integrando esforços técnicos e estratégicos para restaurar a normalidade e proteger os interesses nacionais.

Na prática, o CERT.PT atua em contextos que vão desde incidentes isolados (*e.g.*, ataques de ransomware a organismos públicos), até cenários complexos que exigem articulação internacional (*e.g.*, ataque de DDoS contra infraestruturas de mercados financeiros). A função do CERT.PT não se limita à reação - envolve também prevenção, monitorização e aconselhamento técnico sempre que se mostre necessário para a resposta adequada a um incidente de cibersegurança.

10. De que forma será garantida a conformidade entre os diferentes setores?

O quadro institucional reforça o papel do CNCS enquanto autoridade nacional responsável pela supervisão e fiscalização das entidades abrangidas, bem como a sua articulação com as autoridades de supervisão setoriais e especiais para setores económicos específicos, que atuam em articulação com o CNCS.

Adicionalmente, o quadro institucional da segurança do ciberespaço é composto pelo Conselho Superior de Segurança do Ciberespaço ("CSSC"), na qualidade de órgão consultivo do Primeiro-Ministro em matéria de segurança do ciberespaço, sendo da sua competência, entre outras atividades, assegurar a coordenação estratégica de cibersegurança, responder a solicitações do Primeiro-Ministro e propor a realização de avaliações de segurança pela Comissão de Avaliação de Segurança do Ciberespaço, a qual forma parte do quadro institucional previsto neste Regime.

O RJC estabelece, como autoridades nacionais sectoriais de cibersegurança:

- O Gabinete Nacional de Segurança (GNS); e
- A Autoridade Nacional de Comunicações (ANACOM).

Já as autoridades nacionais especiais de cibersegurança, no que respeita à matéria da resiliência operacional digital do setor financeiro, são:

- A Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF);
- A Comissão do Mercado de Valores Mobiliários (CMVM);
- O Banco de Portugal (BdP).

Integram também o quadro institucional da segurança do ciberespaço:

- O Secretário-Geral do Sistema de Segurança Interna (enquanto autoridade nacional de gestão de crises e incidentes de cibersegurança em grande escala);
- A Polícia Judiciária;
- O Serviço de Informações de Segurança;
- O Serviço de Informações Estratégicas de Defesa; e
- O Comando de Operações de Ciberdefesa.

No âmbito operacional, destaca-se ainda o CERT.PT, a equipa nacional de resposta a incidentes de cibersegurança integrada no CNCS (v. questão 13).

O CNCS e as autoridades de supervisão setoriais e especiais deverão monitorizar o cumprimento do RJC e assegurar que as entidades abrangidas estão em conformidade com o regime, garantindo que as entidades cumpram os requisitos regulamentares e padrões de gestão de riscos. A atuação destas autoridades não se limita à fiscalização. Inclui também a aplicação de medidas corretivas e sancionatórias, como inspeções, auditorias e ordens vinculativas, sempre com o objetivo de assegurar que as entidades cumprem os padrões definidos pelo regime em questão.

A coordenação com a CNPD (Comissão Nacional de Proteção de Dados) assume especial relevância quando ocorrem incidentes significativos que envolvam dados pessoais, ou quando o CNCS ou as autoridades nacionais setoriais e especiais de cibersegurança considerem, no decurso de uma ação de supervisão ou da imposição de medida de execução, com um grau razoável de certeza, que determinadas infrações (e.g., relacionadas com as medidas de cibersegurança implementadas, gestão de riscos ou a notificação de incidentes) possam resultar na violação de dados pessoais[20].

No caso de incidentes significativos que envolvam a violação de dados pessoais, o CNCS ou as autoridades nacionais sectoriais e especiais estão obrigados a comunicar à CNPD a verificação dessa violação[21].

Adicionalmente, o Regime prevê uma dinâmica de cooperação e de interoperabilidade entre as várias autoridades envolvidas no respetivo cumprimento, que se reflete na transversalidade dos fluxos de informação entre as autoridades de supervisão, bem como no acesso, pelo CNCS, às bases de dados e registos nacionais relevantes.

11. Quais são os principais instrumentos do Regime?

Os instrumentos previstos no Regime Jurídico da Cibersegurança têm como objetivo criar uma arquitetura integrada para reforçar a cibersegurança nacional, garantindo a prevenção, deteção e resposta eficaz a incidentes. Os principais instrumentos incluem:

- **Estratégia Nacional de Segurança do Ciberespaço (artigo 12.º):** constitui o instrumento orientador da política nacional de cibersegurança. Esta estratégia define as prioridades nacionais e os objetivos estratégicos que devem nortear a atuação do Estado e das entidades públicas e privadas na proteção do ciberespaço. A Estratégia deverá ser revista periodicamente para acautelar e adequar-se à evolução do panorama de ameaças nacional e à evolução das tecnologias;

20 Artigo 23.º n.º 1 a) e 79.º.
21 Artigo 40.º n.º 5.

- **Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança em Grande Escala (artigo 13.º):** define procedimentos para a gestão coordenada de incidentes que ultrapassem a capacidade de resposta nacional e que tenham impacto em, pelo menos, dois Estados Membros da União Europeia, e inclui a comunicação, coordenação e mitigação, assegurando a articulação com as autoridades europeias e a ativação de mecanismos de cooperação internacional. O referido plano será aprovado no prazo de 6 meses após a entrada em vigor do presente Regime[22];

- **Quadro Nacional de Referência para a Cibersegurança (artigo 14.º):** O Quadro de Referência Nacional de Cibersegurança compila várias normas, boas práticas e orientações técnicas que devem ser seguidas pelas entidades abrangidas pelo regime. Este instrumento serve como referência para a implementação e manutenção de medidas eficazes de segurança da informação, alinhadas com padrões internacionais e com as exigências da Diretiva NIS2, com vista à harmonização de práticas, redução de vulnerabilidades e promoção de uma abordagem consistente à gestão de riscos;

- A par destes instrumentos, o RJC articula-se com a **Estratégia Nacional de Ciberdefesa** (Artigo 11.º, alínea d)) e com o **Conceito Estratégico de Defesa Nacional** (Artigo 11.º, alínea e)), que estabelecem as linhas gerais para a proteção do espaço cibernético no contexto da defesa nacional. Estes documentos complementam a abordagem civil da cibersegurança com uma perspetiva de defesa, assegurando que as capacidades militares e civis estão alinhadas para responder a ameaças híbridas e ataques que possam comprometer a soberania ou a segurança do Estado.

Os instrumentos do RJC constituem pilares fundamentais e ferramentas essenciais não apenas na manutenção do cumprimento do regime pelas entidades abrangidas, mas também do ponto de vista da segurança nacional, ao prever uma abordagem integrada e coordenada, particularmente em caso de incidentes significativos.

12. Quais medidas de fiscalização e supervisão estão previstas?

Tal como referido no Ponto 2 acima, em particular relativamente às alterações do RJC e o princípio da proporcionalidade, a atuação do CNCS será distinta dependendo da respetiva classificação:

- **Entidades essenciais[23]:** fiscalização proativa, incluindo inspeção no local e supervisão remota, auditorias de segurança, regulares ou direcionadas, e auditorias *ad hoc*; e

- **Entidades importantes e públicas relevantes[24]:** supervisão *ex post*, promovida por denúncia ou suspeita de incumprimento da lei através de indícios ou provas nesse sentido), sendo as medidas previstas de fiscalização as mesmas que para as entidades essenciais, e auditorias *ad hoc*.

22 Artigo 85.º.
23 Artigo 54.º.
24 Artigo 55.º.

Caso a autoridade nacional de supervisão verifique que uma entidade não está a cumprir as obrigações decorrentes do RJC, pode adotar medidas, entre as quais:

- Advertências sobre as infrações detetadas ou instruções para a correção das mesmas;
- Instruções vinculativas para a adoção de determinadas medidas preventivas ou corretivas de um incidente;
- Ordens ou instruções para a correção de infrações;
- Ordens para a comunicação às pessoas singulares ou coletivas a quem prestam serviços, do potencial impacto de um incidente;
- Designação, por tempo limitado, de um supervisor responsável pela monitorização do cumprimento com as obrigações de gestão de riscos de cibersegurança; e
- Aplicação de coimas.

O CNCS pode, igualmente, ordenar ou instruir a entidade para a implementação de medidas de neutralização de ciberataques, como por exemplo o bloqueio ou redireccionamento em caso de utilização abusiva de nomes de domínio ou endereços de protocolo IP[25].

> O CNCS pode ordenar ou instruir a entidade para a implementação de medidas de neutralização de ciberataques.

13. Quais são as contraordenações e coimas previstas por incumprimento do Regime Jurídico da Cibersegurança?

O regime sancionatório[26] inclui contraordenações, escalonadas em função da gravidade da infração e da qualificação das entidades que incumpriram o regime jurídico de cibersegurança. As coimas podem ser divididas em:

MUITO GRAVES

É o caso, por exemplo, do incumprimento das medidas de cibersegurança ou do dever de notificação de incidente.

- **Coimas para entidades essenciais:** Até 10 milhões de euros ou 2% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado. Até 200 mil euros, se praticadas por pessoa singular.
- **Coimas para entidades importantes:** Até 7 milhões de euros ou num montante máximo não inferior a 1,4% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado. Até 200 mil euros, se praticadas por pessoa singular,
- **Coimas para entidades públicas:** Até 4 milhões de euros, no caso das entidades públicas integradas no Grupo A, e até 350 mil euros, no caso de entidades públicas integradas no Grupo B. Se praticadas por pessoa singular, até 16 mil euros.

25 Artigo 57.º.
26 Capítulo VII.

GRAVES

É o caso, por exemplo, de incumprimento dos deveres previsto no artigo 8.º ou do dever de registo na plataforma do CNCS.

- **Coimas para entidades essenciais:** Até 5 milhões de euros ou 1% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado. Até 125 mil euros se praticadas por pessoa singular;
- **Coimas para entidades importantes:** Até 3.5 milhões de euros ou num montante máximo não inferior a 0,7% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado. Até 125 mil euros se praticadas por pessoa singular; e
- **Coimas para entidades públicas:** Até 2.5 milhões de euros, no caso das entidades públicas integradas no Grupo A, e até 225 mil euros, no caso de entidades públicas integradas no Grupo B. Até 10 mil euros se praticadas por pessoa singular.

CONTRAORDENAÇÕES LEVES

É o caso, por exemplo, da utilização indevida de marcas de certificação de cibersegurança inválidas, caducadas ou revogadas. A aplicação da contraordenação leve é uniforme, independentemente da classificação da entidade e pode ir até 45 mil euros, se praticada por pessoa coletiva, ou até 3 750 euros, se praticada por pessoa singular

O RJC prevê ainda a punição, a título de negligência, das obrigações que consubstanciem contraordenações muito graves e graves, bem como da utilização de marca de certificação de cibersegurança inválida, caducada ou revogada, e da utilização de expressão ou grafismo que sugira a certificação de produto, serviço ou processo que não seja certificado. Neste caso, os limites mínimos e máximos das coimas são reduzidos a metade.

O produto das coimas será distribuído, revertendo 60% para o Estado e 40% para o CNCS ou para a autoridade nacional setorial de cibersegurança, dependendo da entidade que tenha instaurado e instruído o processo[27].

Os critérios para a aplicação de coimas incluem:

- Gravidade da infração;
- A culpa do agente;
- A situação económica do agente; e
- O benefício económico que o agente retirou da prática da contraordenação.

14. Para quando a entrada em vigor e qual o período transitório?

O novo regime entra em vigor 120 dias após a publicação.

Durante 12 meses a contar da data de entrada em vigor do Decreto-Lei, as entidades podem solicitar dispensa de coimas, desde que demonstrem estar em processo de adaptação ao novo quadro legal[28].

O CNCS está atualmente a trabalhar na disponibilização de regulamentos que densifiquem as obrigações previstas, de formulários e da plataforma eletrónica para realização da qualificação, do registo e da notificação de incidentes. A produção de efeitos das medidas e obrigações das quais dependam os referidos regulamentos ocorrerá 24 meses após a disponibilização dos mesmos[29].

27 Artigo 73.º.
28 Artigo 65.º.
29 Artigo 10.º, n.º 2, do Decreto-Lei.

15. O que esperar do novo Regime Jurídico da Cibersegurança?

Espera-se que o Regime Jurídico da Cibersegurança reforce uma cultura de cibersegurança mais transversal entre os vários setores do tecido empresarial, não apenas numa perspetiva preventiva de cibersegurança, mas também numa lógica reativa a incidentes de segurança da informação.

Prevê-se igualmente que o impacto deste regime não se cinja apenas às entidades abrangidas, mas que seja também estendido à cadeia de abastecimento destas, por via da obrigação de assegurar que os prestadores de serviços não acarretam um risco de cibersegurança acrescido para estas entidades. Quando confrontados com processos rigorosos de análise prévia do risco da cadeia de abastecimento e com obrigações contratuais mais exigentes, os prestadores de serviço ver-se-ão forçados a adotar, também eles, medidas de segurança mínimas e adequadas para assegurar a competitividade no mercado em que se inserem.

Adicionalmente, o regime terá um impacto diferenciado consoante o setor e a dimensão das empresas abrangidas: para as entidades que já estavam abrangidas pelo anterior Regime Jurídico de Segurança do Ciberespaço, e que demonstravam a maturidade e resiliência adequadas aos riscos do seu setor, não se prevê que o rigor do RJC venha impactar a cultura organizacional já implementada e promovida; no caso das entidades que passam, agora, a estar abrangidas por este regime, em particular para as empresas de pequena e média dimensão, o RJC obrigará a um investimento planeado e estruturado para a sua implementação.

Em todo o caso, as empresas devem começar por delinear uma estratégia faseada de verificação e, se necessário, de implementação do Regime Jurídico da Cibersegurança, que passará por:

- Identificar os riscos a que podem estar sujeitas, bem como definir ou rever os procedimentos de gestão de risco;
- Identificar e classificar os ativos, em particular os ativos críticos para a prestação do serviço ou, caso já estejam identificados, rever a sua classificação com base na revisão dos riscos de cibersegurança;
- Desenvolver ou rever políticas e procedimentos internos relacionados com a segurança da informação, por forma a assegurar o total cumprimento com o regime;
- Rever os procedimentos de análise da cadeia de abastecimento ou, se for caso disso, identificar os prestadores de serviços que possam acoplar riscos acrescidos à empresa e desenvolver um plano de análise prévia e de revisão contratual;
- Assegurar que os órgãos de gestão, direção e administração estão conscientes dos seus papéis para a promoção da cultura em cibersegurança;
- Desenvolver ou rever o plano de sensibilização e de formação para a cibersegurança, para toda a organização e, se aplicável, a entidades terceiras.

Com a aprovação deste regime, podemos esperar um quadro regulatório robusto que potencia uma vantagem competitiva para as organizações que se antecipam e investem na sua resiliência digital, bem como uma economia mais segura e resiliente que garante a confiança no uso das tecnologias. Preparar-se para este novo regime é, mais do que nunca, uma oportunidade estratégica para liderar com segurança no universo digital.

▲ VOLTAR AO INÍCIO

Sobre a PLMJ

→ Quem somos

Sobre a área de Tecnologia, Media e Telecomunicações

→ O que fazemos

> "PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us."
>
> CLIENT REFERENCE FROM CHAMBERS AND PARTNERS

KEY CONTACTS

Pedro Lomba

Sócio

(+351) 213 197 412
pedro.lomba@plmj.pt

Pedro foi membro do Grupo de Trabalho designado pelo Governo português para a preparação de anteprojeto em transposição da Diretiva NIS 2, em matéria de cibersegurança.

Marta Salgado Areias

Associada Sénior

(+351) 210 103 741
marta.salgadoareias@plmj.pt

Marta tem prestado assessoria em cibersegurança, com enfoque em *governance* e gestão de riscos. Possui, ainda, ampla experiência na negociação de contratos de tecnologia, bem como na condução de auditorias e projetos de implementação que exigem enquadramento regulatório.

Inês Cabugueira

Associada

(+351) 213 197 462
ines.cabugueira@plmj.pt

Inês tem vindo a prestar assessoria a clientes na interseção entre cibersegurança e proteção de dados, e detém a certificação ITIL4 Foundation orientada para a gestão de serviços de TI.

Mafalda de Brito Fernandes

Associada

(+351) 213 197 300*
mafalda.britofernandes@plmj.pt

Mafalda tem experiência como consultora na área da cibersegurança e gestão de risco e detém certificações como ISO/IEC 27001, ISO/IEC 27701 E ITIL4 Foundation.

▲ VOLTAR AO INÍCIO

Deze,mbro 2025

PLMJ COLAB ANGOLA — MOÇAMBIQUE — PORTUGAL

www.plmj.com