VIEIRA DE ALMEIDA

COMUNICAÇÕES, PROTEÇÃO DE DADOS & TECNOLOGIA

DIRETIVA RELATIVA A MEDIDAS DESTINADAS A ASSEGURAR UM ELEVADO NÍVEL COMUM DE CIBERSEGURANÇA EM TODA A UNIÃO ("NIS2")

VdA EXPERTISE

Janeiro 2023

Diretiva relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança em toda a União ("NIS2")

No passado dia 27 de dezembro, foi publicada a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança na União (a "NIS2").

A tão esperada Diretiva reflete a preocupação e foco crescente do legislador (e mercado) europeu com a cibersegurança, atendendo aos desafios, riscos e oportunidades cada vez mais associados a esta matéria.

A NIS2 estabelece parâmetros de gestão dos riscos de cibersegurança em diversos sectores da economia e implicará a adoção de vários procedimentos, políticas e mecanismos de compliance internos, bem como obrigações perante as autoridades e os clientes/utilizadores.

A NIS2 entra em vigor a 16 de janeiro de 2023 e os Estados-Membros têm 21 meses após essa data para transpor a Diretiva para o ordenamento jurídico nacional - os diferentes *stakeholders* deverão, durante este período, adaptar as suas metodologias, políticas e sistemas de gestão interna e externa de ciber-risco, para fazer face à Diretiva.

Sem prejuízo de poder consultar informação adicional sobre o contexto da NIS 2 através do VdA Cybersecurity Series I (disponível aqui), em termos gerais, esta Diretiva estabelece várias obrigações para um universo alargado de sectores e serviços, face à atual Diretiva NIS.

Abordamos de seguida alguns dos principais aspetos da NIS2.

A quem se aplica?

A Diretiva NIS2 tem um âmbito de aplicação alargado face à Diretiva NIS original, aplicando-se a todas as entidades:

(i) **que prestem os seus serviços ou realizem as suas atividades na UE**; e (ii) cuja atividade as qualifique como uma **entidade "essencial" ou "importante"**, conforme a lista nos anexos I e II e abrangendo os seguintes sectores:

- Bancário
- Energia
- Saúde
- Infraestruturas financeiras
- Infraestruturas digitais
- Transportes
- Fornecimento e distribuição de água potável
- Serviços postais e dos correios
- Prestadores de redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público
- Gestão de serviços TIC
- Indústria transformadora
- Espaço
- Gestão de águas residuais e resíduos
- Serviços Digitais (e.g. plataformas de serviços de redes sociais e prestadores de serviços de centro de processamento de dados)
- Alimentar
- Produção, fabrico e distribuição de produtos químicos
- Administração Pública
- Investigação

Ao contrário da anterior Diretiva, **a sujeição às obrigações da NIS2 é automática**, não dependendo de identificação pelo Centro Nacional de Cibersegurança.

Não estão sujeitas à NIS2 (i) Micro e pequenas empresas (com algumas exceções); e (ii) Entidades nas áreas da segurança nacional, segurança pública, defesa ou cumprimento da lei (se os Estados-Membros assim determinarem)

Quais as implicações da NIS2?

As entidades qualificadas na NIS2 como "essenciais" ou "importantes" estão sujeitas a requisitos de gestão dos riscos de cibersegurança – internamente e perante as autoridades e os utilizadores/ clientes.

A implementação das obrigações resultantes da NIS2 dependerá da exposição ao risco, importância e dimensão de cada entidade e deverá ser alvo de uma análise personalizada, tendo em conta o respetivo âmbito de atuação, risco técnico e operacional e vulnerabilidades detetadas.

Entre as obrigações e responsabilidades impostas pela Diretiva NIS2, são de destacar as seguintes:

Medidas de Gestão dos riscos de cibersegurança

As entidades devem aprovar medidas técnicas, operacionais e organizativas adequadas para gestão dos riscos de cibersegurança existentes.

Entre outros aspetos, estas medidas de gestão de risco devem abranger pelo menos políticas de análise de risco, tratamento de incidentes, continuidade de atividades, procedimentos de avaliação da eficácia das medidas de gestão dos riscos e segurança dos recursos humanos e políticas seguidas nesta matéria, bem como soluções técnicas, como criptografia e cifragem.

As medidas a adotar por cada entidade dependerão, em larga medida, da respetiva qualificação ao abrigo da NIS2 como entidades "essenciais" ou "importantes" – classificação a densificar por cada Estado-Membro, que criará uma lista das entidades enquadradas em cada categoria.

Registo

As seguintes entidades deverão ser inscritas num registo mantido pela ENISA (Agência da UE para a Cibersegurança):

(i) prestadores de serviços de DNS,

(ii) nomes de TLD;

(iii) prestadores de serviços de registo de nomes de domínio;

(iv) prestadores de serviços de computação em nuvem;

(v) prestadores de serviços de *data centre;*

(vi) fornecedores de redes de distribuição de conteúdos;

(vii) prestadores de serviços geridos;

(viii) prestadores de serviços de segurança geridos;

(ix) prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais.

Ecossistema alargado de regulação

A NIS2 prevê uma rede ampla de autoridades com poderes de supervisão, bem como grupos de cooperação estratégica e intercâmbio de informação entre Estados-Membros:

(i) Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe), para apoiar a gestão coordenada de incidentes e crises de cibersegurança em grande escala e assegurar intercâmbio de informações entre Estados-Membros e instituições da UE.

(ii) Rede de CSIRT (equipas de resposta a incidentes de segurança ou *Computer Security Incident Response Team*) nacionais, que deverão ser notificadas em caso de incidentes com impacto significativo na atividade de entidades essenciais e importantes.

(iii) Poderes da ENISA, no sentido de manter um registo europeu de vulnerabilidades, com contributos voluntários de entidades essenciais e importantes (e seus fornecedores), bem como de entidades não abrangidas pela NIS2.

(iv) Obrigações de colaboração com autoridades de proteção de dados (em caso de incidentes e violações da NIS2 com impacto no Regulamento Geral sobre a Proteção de Dados e respetiva legislação de execução) e tribunais nacionais.

Notificação de incidentes a autoridades e utilizadores

Em caso de ocorrência de um incidente de cibersegurança significativo (conforme definido na NIS2), as entidades devem notificar os **destinatários dos seus serviços**, sem demora injustificada, se os incidentes puderem afetar negativamente a prestação desses serviços.

Deverão também notificar **a CSIRT** (ou outra autoridade competente), de forma faseada: (i) notificação inicial dentro de 24 horas após tomar conhecimento do incidente; (ii) notificação de *follow-up*, nas 72 horas seguintes; (iii) relatório final, no máximo 1 mês após a notificação de *follow-up*.

Partilha de informação

A NIS2 fomenta o intercâmbio entre as entidades sujeitas a este regime e através de acordos específicos, de informações pertinentes sobre cibersegurança, com vista a detetar e dar resposta a incidentes, ou atenuar o seu impacto.

Medidas de Supervisão

As medidas de supervisão aplicáveis variam, consoante estejam em causa entidades "essenciais" ou "importantes":

(i) as entidades *essenciais* estão sujeitas a um regime de supervisão *ex ante* (que pode incluir, por exemplo, a realização de inspeções, auditorias, verificações de segurança e pedidos de informações, acesso a dados e provas da aplicação de políticas de cibersegurança);

(ii) as entidades "*importantes* estão sujeitas a um regime de supervisão *ex post*, ao abrigo do qual as autoridades competentes poderão intervir, quando disponham de provas ou indícios de que essa entidade não cumpre as suas obrigações em matéria de segurança e notificação de incidentes.

Incumprimento: Sanções e Coimas

Em caso de incumprimento, as autoridades poderão impor/solicitar a aplicação de **coimas**: as entidades essenciais poderão ser sujeitas a coimas até 10 000 000 EUR, ou 2 % do volume de negócios anual a nível mundial, enquanto as entidades importantes podem ser sujeitas a coimas até 7 000 000 EUR, ou 1,4 % do volume de negócios anual, a nível mundial.

As autoridades poderão também, entre outros, (i) emitir advertências, (ii) ordenar que as entidades incumpridoras informem as pessoas/empresas a que prestam serviços e que sejam potencialmente afetadas por uma ciber-ameaça significativa, (iii) designar um supervisor do cumprimento legal, ou (iv) ordenar que as entidades em causa tornem públicas as suas infrações à NIS2.

Caso, relativamente a entidades essenciais, estas medidas se revelem ineficazes, as autoridades poderão suspender ou ordenar a suspensão temporária de uma certificação/autorização relativa aos serviços ou atividades em causa, ou solicitar a **proibição temporária de exercício de poderes de gestão** pelas pessoas singulares com estas responsabilidades, a nível de diretor executivo ou representante legal.

Próximos passos: como preparar as organizações para a NIS2?

Enquadramento	• Confirmar a curto prazo se a organização está abrangida pela Diretiva NIS2 e, em caso afirmativo, determinar se será qualificada como entidade essencial ou importante • Contemplar, nos respetivos planos de negócio, os custos necessariamente associados ao cumprimento das obrigações impostas pela Diretiva
Revisão/Criação de processos, políticas e procedimentos	• Analisar, de uma perspetiva jurídica, técnica, financeira e de governance, as obrigações impostas pela Diretiva e identificar os ajustes necessários às suas políticas e procedimentos • Verificar se são também aplicáveis outras obrigações legais ou regulatórias (incluindo no processo de harmonização e transposição) e incorporar as mesmas nas suas estratégias de compliance NIS2
Identificação da cadeia de risco	As organizações devem mapear os riscos de cibersegurança associados aos seus serviços e produtos em toda a cadeia de produção e fornecimento de serviços e produtos – incluindo os riscos associados às metodologias internas de prevenção e mitigação de ciber-risco, possível acesso a redes e sistemas por/de terceiros e intervenção de fornecedores e prestadores de serviços (incluindo termos contratuais e políticas aplicáveis)
Estratégia global de compliance	As organizações deverão também assegurar o cumprimento de outros diplomas complementares e/ou associados à NIS2, desde logo: • Regulamento Geral de Proteção de Dados e respetivas obrigações de notificação de violações de dados pessoais (sujeitas a prazos distintos da NIS2), e de implementação de medidas de segurança • Regulamento de Resiliência Operacional Digital do Setor Financeiro (DORA), que consubstancia uma lei especial face à NIS2 • Diretiva relativa à Resiliência das Infraestruturas Críticas • *Cyber Resilience Act*, que impõe obrigações de cibersegurança e notificação de incidentes aos fabricantes, distribuidores e importadores de *hardware* e *software*
Engagement interno	• Assegurar onboarding da equipa de Gestão/administração • Distribuir responsabilidades no processo de adaptação à NIS2, assegurando cooperação entre equipas técnicas, jurídicas, operacionais e de governance • Estabelecer iniciativas de formação e sensibilização das diferentes equipas (tendo em conta calendário de implementação do programa de compliance NIS2)

Contactos

MAGDA COCCO
MPC@VDA.PT

INÊS ANTAS DE BARROS
IAB@VDA.PT

MARIA DE LURDES GONÇALVES
MLG@VDA.PT

ISABEL ORNELAS
IGO@VDA.PT

HELENA CORREIA MENDONÇA
HCM@VDA.PT