

Cibersegurança **industrial**

— GUIA SOBRE NIS2 —



Sabias que em outubro irá entrar em vigor uma nova diretiva NIS2?

Que seja o teu propósito de 2024 começar já a aplicá-la, porque, uma vez transposta, começará a ser implementada no dia seguinte.

Partilhamos contigo alguns princípios básicos da diretiva para te dar alguma orientação e contexto.





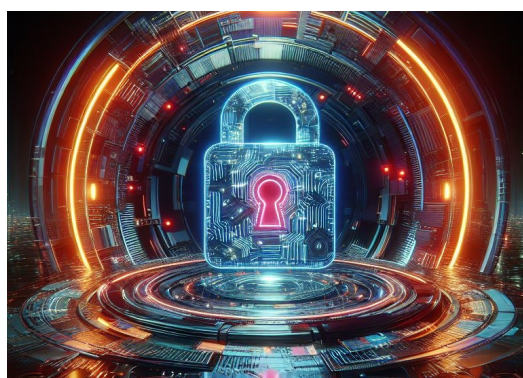
01

A nova diretiva NIS2 de cibersegurança: Infrações e impacto para os diretores das empresas

A nova diretiva NIS2 reforça a cibersegurança

Uma nova diretiva de cibersegurança prevê sanções para transgressões e impactará os cargos de liderança.

Em janeiro de 2023 foi promulgada uma nova diretiva NIS (sigla para segurança de sistemas de redes e de informação: Network and Information Systems) através do Regulamento ((UE) 2022/2555), denominada por NIS2 destinada a assegurar um elevado nível comum de cibersegurança em toda a União, revogando a diretiva anterior, NIS ((UE) 2016/1148). A data máxima para que seja transposta para o ordenamento jurídico português é 17 de outubro de 2024.



O prazo máximo para a implementação da diretiva está marcado para dia 17 de outubro, vindo a mesma reforçar os requisitos anteriores da NIS1, de forma a melhorar a resposta ao aumento de ameaças que tem pairado sob os sistemas de redes e de informação, dos quais a nossa sociedade está cada vez mais dependente. Além disso, na nova diretiva estarão também incluídas **ações contra as infrações**, e as autoridades competentes estarão habilitadas a levar a cabo ações de **suspensão de certificações e serviços**, podendo ainda **proibir temporariamente uma pessoa física de exercer funções de direção geral ou representação legal**. Logo, sublinha-se a urgência de agir preventivamente e antecipar a implementação desta diretiva, visto que as consequências se sobrepõem às da anterior normativa.



NIS2 amplia o seu alcance

O âmbito de aplicação pode afetar os ambientes industriais OT e a dispositivos IoT.

Um dos aspetos em que a NIS2 se diferencia da NIS1 é o seu âmbito de aplicação. Embora a NIS1 estivesse basicamente reservada para entidades formalmente designadas como fornecedores de serviços essenciais dentro de diferentes setores críticos, a NIS2 expande o leque e vai aplicar-se a médias e grandes empresas de setores críticos e a outras entidades que, independentemente da sua proporção, cumpram com certas características como, por exemplo:

- Prestem serviços específicos (tais como os prestadores de serviços de confiança ou de DNS),
- Que sejam o único fornecedor a prestar um serviço essencial num estado-membro,
- Que sejam uma entidade crítica formalmente designada.

Dentro dos setores de aplicação, podemos encontrar alguns que incluem tecnologias de operação (o que comumente chamamos de OT, do inglês "Operation Technologies", em contraste com os sistemas de informação ou corporativos, denominados IT, do inglês "Information Technologies"). Ainda dentro dos setores de aplicação, incluem-se também os dispositivos IoT, não menos importantes, e que também estariam no âmbito ao qual se dirigem os requisitos de proteção desta diretiva..





02

NIS2 amplia o seu alcance

Setores afetados

| Setores de alta criticidade | | Outros setores críticos | |
|---|---|---|---|
|  | Energia |  | Serviços postais e de correio |
|  | Transporte |  | Gestão de resíduos |
|  | Banca |  | Fabrico, produção e distribuição de substâncias e misturas químicas |
|  | Infraestruturas dos mercados financeiros |  | Produção, transformação e distribuição de alimentos |
|  | Setor da saúde |  | Fabrico |
|  | Água potável |  | Fornecedores de serviços digitais |
|  | Águas residuais |  | Investigação |
|  | Infraestrutura digital | | |
|  | Gestão de serviços de TIC (de empresa para empresa) | | |
|  | Entidades da Administração Pública, excluindo o poder judicial, os parlamentos e os bancos centrais | | |
|  | Espaço | | |



Setores de alta criticidade

| Setor | Subsetor | Tipo de entidade |
|--|--|--|
|  1. Energia | a) Electricidade | Empresas elétricas, conforme definido no artigo 2, número 57, da Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho, que realizam a função de "fornecimento", conforme definido no artigo 2, número 12, dessa Diretiva |
| | | Gestores da rede de distribuição, conforme definido no artigo 2, número 29, da Diretiva (UE) 2019/944 |
| | | Gestores da rede de transporte, conforme definido no artigo 2, número 35, da Diretiva (UE) 2019/944 |
| | | Produtores, conforme definido no artigo 2, número 38, da Diretiva (UE) 2019/944 |
| | | Operadores designados para o mercado elétrico, conforme definido no artigo 2, número 8, do Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho |
| | | Participantes no mercado da eletricidade, conforme definido no artigo 2, número 25, do Regulamento (UE) 2019/943 que prestam serviços de agregação, resposta da demanda ou armazenamento de energia, conforme definido no artigo 2, números 18, 20 e 59, da Diretiva (UE) 2019/944 |
| | b) Sistemas urbanos de aquecimento e de arrefecimento | Operadores de um ponto de recarga que são responsáveis pela gestão e exploração de um ponto de recarga, que prestam um serviço de recarga ao utilizador final também em nome e por conta de um fornecedor de serviços de mobilidade |
| | | Operadores de sistemas urbanos de aquecimento ou de arrefecimento, conforme definidos no artigo 2, número 19, da Diretiva (UE) 2018/2001 do Parlamento Europeu e do Conselho |
| | c) Crude | Operadores de oleodutos de transporte de crude |
| | | Operadores de produção de crude, instalações de refinação e tratamento, armazenamento e transporte |
| | | Entidades centrais de armazenamento, conforme definido no artigo 2, letra f), da Diretiva 2009/119/CE do Conselho |
| | d) Gás | Empresas fornecedoras de gás, conforme definido no artigo 2, número 8, da Diretiva 2009/73/CE do Parlamento Europeu e do Conselho |
| | | Gestores da rede de distribuição, conforme definido no artigo 2, número 6, da Diretiva 2009/73/CE |
| | | Gestores da rede de transporte, conforme definido no artigo 2, número 4, da Diretiva (UE) 2009/73/CE |
| | | Gestores de armazenamentos, conforme definido no artigo 2, número 10, da Diretiva 2009/73/CE |
| Gestores da rede de GNL, conforme definido no artigo 2, número 12, da Diretiva 2009/73/CE | | |
| Companhias de gás natural, conforme definido no artigo 2, número 1, da Diretiva 2009/73/CE | | |
| Operadores de instalações de refinação e tratamento de gás natural | | |
| e) Hidrogénio | Operadores de produção, armazenamento e transporte de hidrogénio | |

CIBERSEGURANÇA INDUSTRIAL

| Setor | Subsetor | Tipo de entidade |
|---|----------------------------------|---|
|  2. Transporte | a) Transporte aéreo | Companhias aéreas, conforme definido no artigo 3, número 4, do Regulamento (CE) n.º 300/2008 utilizadas para fins comerciais |
| | | Entidades gestoras de aeroportos, conforme definido no artigo 2, número 2, da Diretiva 2009/12/CE do Parlamento Europeu e do Conselho; aeroportos, conforme definidos no artigo 2, número 1, dessa Diretiva, em particular os aeroportos da rede básica listados no anexo II, secção 2, do Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho; e entidades que exploram instalações anexas dentro dos recintos dos aeroportos |
| | | Operadores de controlo da gestão do tráfego que prestam serviços de controlo do trânsito aéreo, conforme definido no artigo 2, número 1, do Regulamento (CE) n.º 549/2004 do Parlamento Europeu e do Conselho |
| | b) Transporte por ferrocarril | Administradores de infraestruturas, conforme definido no artigo 3, número 2, da Diretiva 2012/34/UE do Parlamento Europeu e do Conselho |
| | | Empresas ferroviárias, conforme definido no artigo 3, número 1, da Diretiva 2012/34/UE, incluindo os exploradores de instalações de serviço, conforme definido no artigo 3, número 12 dessa Diretiva |
| | c) Transporte marítimo e fluvial | Empresas de transporte marítimo, fluvial e de cabotagem, tanto de passageiros quanto de mercadorias, conforme definido para o transporte marítimo no anexo I do Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, sem incluir os navios particulares explorados por essas empresas |
| | | Organismos gestores dos portos, conforme definido no artigo 3, número 1, da Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, incluindo suas instalações portuárias, conforme definido no artigo 2, número 11, do Regulamento (CE) n.º 725/2004, e entidades que operam obras e equipamentos localizados nos portos |
| | | Operadores de serviços de tráfego de navios (STB), conforme definido no artigo 3, letra o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho |
| | d) Transporte por estrada | Autoridades rodoviárias, tal como definidas no artigo 2, ponto 12, do Regulamento Delegado (UE) 2015/962 da Comissão responsáveis pelo controlo da gestão do tráfego, excluindo as entidades públicas para as quais a gestão do tráfego ou a exploração de sistemas de transporte inteligentes seja uma parte não essencial da sua atividade geral |
| | | Operadores de sistemas de transporte inteligentes, tal como definidos no artigo 4, ponto 1, da Diretiva 2010/40/UE do Parlamento Europeu e do Conselho |
|  3. Banca | | Entidades de crédito, tal como se definem no artigo 4, número 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho |
|  4. Infraestruturas dos mercados financeiros | | Gestores de centros de negociação, tal como se definem no artigo 4, número 24, da Diretiva 2014/65/UE do Parlamento Europeu e do Conselho |
|  5. Setor sanitário | | Prestadores de assistência sanitária, tal como se definem no artigo 3, letra g), da Diretiva 2011/24/UE do Parlamento Europeu e do Conselho |
| | | Laboratórios de referência da UE, tal como se definem no artigo 15, do Regulamento (UE) .../... do Parlamento Europeu e do Conselho |
| | | Entidades que realizam atividades de investigação e desenvolvimento de medicamentos, tal como se definem no artigo 1, número 2, da Diretiva 2001/83/CE do Parlamento Europeu e do Conselho |
| | | Entidades que fabricam produtos farmacêuticos de base e especialidades farmacêuticas a que se refere a secção C, divisão 21, da NACE Rev. 2 |
|  6. Água potável | | Entidades que fabricam produtos sanitários considerados essenciais em situações de emergência de saúde pública ("lista de produtos sanitários essenciais durante a emergência de saúde pública") no sentido do artigo 22 do Regulamento (UE) 2022/123 do Parlamento Europeu e do Conselho |
| | | Fornecedores e distribuidores de águas destinadas ao consumo humano, tal como se definem no artigo 2, número 1, letra a), da Diretiva (UE) 2020/2184 do Parlamento Europeu e do Conselho, excluindo os distribuidores para os quais a distribuição de águas destinadas ao consumo humano seja uma parte não essencial da sua atividade geral de distribuição de outros bens e produtos básicos |

CIBERSEGURANÇA INDUSTRIAL

| Setor | Subsetor | Tipo de entidade |
|---|----------|--|
|  7. Águas residuais | | Empresas dedicadas à recolha, eliminação ou tratamento de águas residuais urbanas, domésticas ou industriais, tal como se definem no artigo 2, números 1 a 3, da Diretiva 91/271/CEE do Conselho, excluídas as empresas para as quais a recolha, eliminação ou tratamento de águas residuais urbanas, domésticas ou industriais seja uma parte não essencial da sua atividade geral |
|  8. Infraestrutura digital | | <p>Fornecedores de pontos de intercâmbio de internet</p> <p>Fornecedores de serviços de DNS, excluídos os operadores de servidores raiz</p> <p>Registos de nomes de domínio de primeiro nível</p> <p>Fornecedores de serviços de computação em nuvem</p> <p>Fornecedores de serviços de centro de dados</p> <p>Fornecedores de redes de distribuição de conteúdos</p> <p>Prestadores de serviços de confiança</p> <p>Fornecedores de redes públicas de comunicações eletrónicas</p> <p>Fornecedores de serviços de comunicações eletrónicas disponíveis para o público</p> |
|  9. Gestão de serviços de TIC (de empresa a empresa) | | <p>Fornecedores de serviços geridos</p> <p>Fornecedores de serviços de segurança geridos</p> |
|  10. Entidades da Administração pública, com exclusão do poder judicial, os parlamentos e os bancos centrais | | <p>Entidades da Administração pública central, tal como se definem no Estado membro de acordo com as disposições do Direito nacional</p> <p>Entidades da Administração pública a nível regional, segundo a sua definição no Estado membro de acordo com as disposições do Direito nacional</p> |
|  11. Espaço | | Operadores de infraestruturas terrestres, cuja propriedade, gestão e exploração recaem sobre os Estados membros ou entidades privadas, que apoiam a prestação de serviços espaciais, exceto os provedores de redes públicas de comunicações eletrónicas |

Outros setores críticos

| Sector | Subsector | Tipo de entidad |
|--|--|---|
|  1. Serviços postais e de mensageria | | Fornecedores de serviços postais, tal como definidos no artigo 2, número 1 bis, da Diretiva 97/67/CE, incluindo provedores de serviços de mensageria |
|  2. Gestão de resíduos | | Empresas que realizam a gestão de resíduos, tal como definidas no artigo 3, número 9, da Diretiva 2008/98/CE do Parlamento Europeu e do Conselho, exceto aquelas para as quais a gestão de resíduos não é a sua principal atividade económica |
|  3. Fabricação, produção e distribuição de substâncias e misturas químicas | | Empresas que realizam a fabricação de substâncias e a distribuição de substâncias ou misturas, tal como definidas no artigo 3, números 9 e 14, do Regulamento (CE) n.º 1907/2006 do Parlamento Europeu e do Conselho e empresas que realizam a produção de artigos, tal como definidas no artigo 3, número 3, desse Regulamento, a partir de substâncias e misturas |
|  4. Produção, transformação e distribuição de alimentos | | Empresas alimentares, tal como definidas no artigo 3, número 2, do Regulamento (CE) n.º 178/2002 do Parlamento Europeu e do Conselho, que se dedicam à distribuição por grosso e à produção e transformação industriais |
|  5. Fabricação | a) Fabricação de produtos sanitários e produtos sanitários para diagnóstico in vitro | Entidades que fabricam os produtos sanitários, tal como definidos no artigo 2, número 1, do Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, e entidades que fabricam os produtos sanitários para diagnóstico in vitro, tal como definidos no artigo 2, número 2, do Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, exceto as entidades que fabricam produtos sanitários a que se refere o anexo I, ponto 5, quinto traço, da presente Diretiva |
| | b) Fabricação de produtos informáticos, eletrónicos e ópticos | Empresas que realizam qualquer das atividades económicas referidas na seção C, divisão 26, da NACE Rev. 2 |
| | c) Fabricação de material elétrico | Empresas que realizam qualquer das atividades económicas referidas na seção C, divisão 27, da NACE Rev. 2 |
| | d) Fabricação de maquinaria e equipamento n.c.o.p. | Empresas que realizam qualquer das atividades económicas referidas na seção C, divisão 28, da NACE Rev. 2 |
| | e) Fabricação de veículos de motor, reboques e semirreboques | Empresas que realizam qualquer das atividades económicas referidas na seção C, divisão 29, da NACE Rev. 2 |
| | f) Fabricação de outro material de transporte | Empresas que realizam qualquer das atividades económicas referidas na seção C, divisão 30, da NACE Rev. 2 |
|  6. Fornecedores de serviços digitais | | Fornecedores de mercados online |
| | | Fornecedores de motores de busca online |
| | | Fornecedores de plataformas de serviços de redes sociais |
|  7. Investigação | | Organismos de investigação |



03

Requisitos de segurança: Para além das medidas puramente técnicas

Requisitos de segurança: Para além das medidas puramente técnicas

Os requisitos de carácter técnico-organizativo são os recolhidos no artigo 21 da diretiva, a saber:



As políticas de segurança dos sistemas de informação e análise de riscos;



A gestão de incidentes;



A continuidade das atividades, como a gestão de cópias de segurança e a recuperação em caso de catástrofe, e a gestão de crises;



A segurança da cadeia de fornecimento, incluindo os aspetos de segurança relativos às relações entre cada entidade e os seus fornecedores ou prestadores de serviços diretos;



A segurança na aquisição, o desenvolvimento e a manutenção de sistemas de redes e de informação, incluindo a gestão e divulgação das vulnerabilidades;



As políticas e os procedimentos para avaliar a eficácia das medidas para a gestão de riscos de cibersegurança;



As práticas básicas de ciberhigiene e formação em cibersegurança;



As políticas e procedimentos relativos à utilização de criptografia e, se aplicável, de cifragem;



A segurança dos recursos humanos, as políticas de controlo de acesso e a gestão de ativos;



O uso de soluções de autenticação multifatorial ou de autenticação contínua, comunicações de voz, vídeo e texto seguras e sistemas seguros de comunicações de emergência na entidade, quando apropriado.



04

Adotar uma abordagem eficaz

Cibersegurança industrial e NIS2

Adotando uma abordagem eficaz.

Em 2023, a União Europeia lançou uma nova regulamentação conhecida como NIS 2, que tem como objetivo reforçar a cibersegurança em setores críticos e serviços digitais essenciais. Esta diretiva, que sucede à anterior NIS, introduz um conjunto de requisitos técnico-organizacionais destinados a proteger os ambientes de tecnologia operacional (OT) e Internet das coisas (IoT).

Uma das principais **dificuldades que as organizações enfrentam** com a implementação da NIS 2 é a necessidade de adaptar os requisitos técnico-organizacionais à **heterogeneidade de elementos presentes nos ambientes IT/OT/IoT**. Isto implica compreender as particularidades de cada um destes ambientes e integrá-los de maneira coerente e eficaz no quadro regulatório estabelecido pela diretiva.





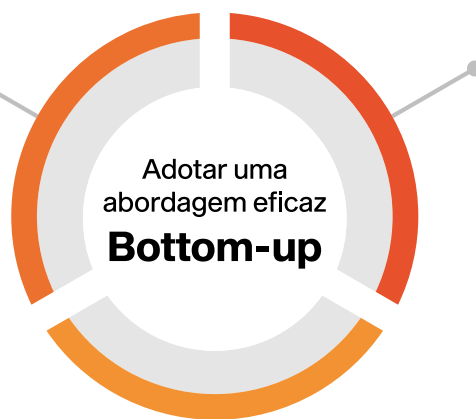
CIBERSEGURANÇA INDUSTRIAL

Por outro lado, é crucial considerar **outras normas ou padrões de cibersegurança que possam ser aplicáveis à organização**, com o objetivo de evitar a duplicação de esforços na implementação e manutenção de medidas de segurança.

Evitar a duplicação de esforços na implementação é o segredo para uma abordagem eficaz

NIS2
Medidas em
ambiente OT/ IoT

NIS2
Medidas em
ambiente IT



Outra normativa

Perante este cenário complexo, surge a necessidade de adotar uma **abordagem bottom-up e de melhoria contínua na implementação da NIS 2**. Esta abordagem implica começar a partir da análise detalhada dos riscos e vulnerabilidades específicos de cada ambiente, para depois desenvolver e implementar medidas de segurança adequadas. Além disso, promove a revisão e atualização periódica destas medidas em resposta às mudanças no panorama de ameaças cibernéticas e à evolução dos ambientes tecnológicos.

Bottom-up | Desenvolvimento e aplicação



Ao adotar esta abordagem, as organizações podem garantir uma maior eficácia e sustentabilidade na sua estratégia de cibersegurança, bem como uma melhor preparação para enfrentar os desafios do futuro digital.

Se a NIS2 te afeta ou poderá prejudicar-te no futuro, conta com a **BABEL**

Na BABEL podemos ajudar os nossos clientes a criar ferramentas para tirar partido dos diferentes aspetos comuns na legislação, regulamentação e padrões vigentes, avançando para um modelo global mais eficaz e com um impacto positivo na qualidade e resiliência dos nossos serviços digitais, essenciais para facilitar o negócio e ganhar competitividade no mercado.



www.babelgroup.com

