UNIÃO EUROPEIA

DIRETIVA SRI 2

(Diretiva UE 2022/2555)

Medidas Destinadas a Garantir um Elevado Nível Comum de Cibersegurança na União

Resumo em Português Europeu para CISOs e Responsáveis de Conformidade

Referência do Documento

Campo	Valor
Designação Oficial	Diretiva (UE) 2022/2555
Data de Adoção	14 de dezembro de 2022
Data de Publicação	27 de dezembro de 2022 (JO L 333/80)
Entrada em Vigor	16 de janeiro de 2023
Prazo de Transposição Nacional	17 de outubro de 2024
Instrumento Revogado	Diretiva (UE) 2016/1148 (SRI 1)

> Este documento é um resumo não oficial da Diretiva SRI 2 da UE de 14 de dezembro de 2022; não constitui uma tradução com valor vinculativo. Para efeitos de interpretação vinculativa, consulte o texto oficial publicado no JO L 333/80, 27.12.2022.

Índice

1. Resumo Executivo

A **Diretiva SRI 2** (Diretiva UE 2022/2555), adotada pelo Parlamento Europeu e pelo Conselho em 14 de dezembro de 2022, é a diretiva de base geral da UE em matéria de cibersegurança. Revoga e substitui a anterior Diretiva SRI 1 (2016/1148) com efeitos a partir de 18 de outubro de 2024.

As avaliações concluíram que, embora a SRI 1 tivesse contribuído para elevar o nível de ciber-resiliência em toda a União, revelou-se insuficiente para fazer face às ameaças de cibersegurança atuais e futuras. A SRI 2 alarga substancialmente o âmbito de aplicação, introduz critérios uniformes, reforça as obrigações em matéria de gestão de riscos e de notificação de incidentes, e prevê disposições de execução com maior efeito dissuasor.

Os Cinco Pilares da Diretiva

1. **Âmbito alargado**: mais setores e empresas sujeitos a regulamentação.
2. **Gestão de riscos mais rigorosa**: 10 medidas mínimas técnicas e organizativas tornadas obrigatórias ao abrigo do Artigo 21.o.
3. **Notificação de incidentes rápida e faseada**: alerta rápido em 24 horas, notificação de incidente em 72 horas, relatório final em 1 mês.
4. **Responsabilidade do órgão de direção**: a direção de topo pode ser pessoalmente responsabilizada.
5. **Sanções dissuasoras**: coimas administrativas até 2% do volume de negócios anual global ou 10 milhões de EUR.

2. Objetivos e Base Jurídica

A base jurídica da diretiva é o **artigo 114.o do Tratado sobre o Funcionamento da União Europeia (TFUE)**, que permite a adoção de medidas de aproximação das regras nacionais com vista a estabelecer e assegurar o funcionamento do mercado interno.

Os principais objetivos da diretiva são:

- Eliminar as profundas divergências entre os Estados-Membros e estabelecer regras mínimas comuns em matéria de cibersegurança;
- Estabelecer mecanismos eficazes de cooperação transfronteiriça e partilha de informações;
- Atualizar a lista de setores e atividades sujeitos a obrigações de cibersegurança, de modo a refletir o panorama atual das ameaças;
- Prever vias de recurso e mecanismos de execução que garantam a implementação efetiva das obrigações;
- Reforçar as capacidades de ciber-resiliência dos operadores de infraestruturas críticas e dos prestadores de serviços digitais.

A diretiva aplica-se sem prejuízo e em conformidade com o direito da UE em matéria de proteção de dados pessoais (RGPD, Regulamento UE 2016/679) e de privacidade nas comunicações eletrónicas (Diretiva 2002/58/CE).

3. Da SRI 1 à SRI 2: Por que razão foi necessária uma nova regulamentação?

A SRI 1, que entrou em vigor em 2016, foi a primeira regulamentação horizontal da UE em matéria de cibersegurança. O processo de avaliação revelou diferenças graves na aplicação entre os Estados-Membros, com a delimitação do âmbito deixada em larga medida ao critério de cada Estado-Membro, fragmentando assim o mercado interno.

Lacunas Identificadas na SRI 1

Domínio	Situação na SRI 1	Solução na SRI 2
Delimitação do âmbito	Deixada ao critério dos Estados-Membros; variação significativa na prática.	Regra uniforme de limitação com base na dimensão da empresa em toda a UE (médias e grandes empresas).
Lista de setores	Número limitado de setores; parte significativa da economia digital excluída.	Cobertura setorial muito mais alargada; infraestruturas digitais, administração pública, espaço, etc. incluídos.
Notificação de incidentes	Fase única; prazos e conteúdo variavam entre os Estados-Membros.	Notificação multifásica: alerta rápido em 24h + notificação em 72h + relatório final em 1 mês.
Gestão de riscos	Linguagem genérica; medidas mínimas específicas pouco claras.	O Artigo 21.o enumera 10 categorias de medidas mínimas obrigatórias.
Sanções	Aplicadas a níveis muito diferentes entre os Estados-Membros.	Coimas máximas harmonizadas a nível da UE (10 M EUR / 2% do volume de negócios).
Responsabilidade da direção de topo	Não claramente definida.	Órgão de direção pessoalmente responsável pelo cumprimento; formação obrigatória.

A SRI 2 não é uma atualização da SRI 1; é uma substituição concebida para criar um **quadro de cibersegurança único, harmonizado e executável** em toda a União.

4. Âmbito de Aplicação e Exclusões

A diretiva abrange principalmente as entidades que operam em setores do **Anexo I (alta criticidade)** ou do **Anexo II (outra criticidade)** dentro da UE e que satisfazem a definição de, pelo menos, média empresa. Nos termos do artigo 2.o do Anexo da Recomendação 2003/361/CE da Comissão, uma média empresa é aquela que emprega menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de EUR (ou cujo balanço total anual não excede 43 milhões de EUR). A SRI 2 abrange as entidades que atingem ou excedem o limiar das médias empresas: o piso prático para entidades no âmbito de aplicação é de 50 trabalhadores ou 10 milhões de EUR de volume de negócios (o limite superior das "pequenas empresas" ao abrigo da mesma Recomendação).

Entidades Abrangidas Independentemente da Dimensão

- Prestadores de redes públicas de comunicações eletrónicas e prestadores de serviços de comunicações eletrónicas acessíveis ao público;
- Prestadores de serviços de confiança (ao abrigo do Regulamento eIDAS UE 910/2014);
- Registos de nomes de domínio de topo (TLD) e prestadores de serviços de DNS;
- Entidades que sejam o único prestador de um serviço num Estado-Membro ou cuja perturbação possa afetar significativamente a segurança pública, a saúde ou a ordem pública;
- Todas as entidades da administração pública central (definidas a nível nacional por cada Estado-Membro).

Áreas Excluídas do Âmbito de Aplicação

As entidades públicas cujas atividades sejam predominantemente exercidas nos domínios da **segurança nacional, da segurança pública, da defesa ou da aplicação da lei** (prevenção, investigação, deteção e repressão de infrações penais) estão excluídas do âmbito de aplicação da diretiva. As missões diplomáticas e consulares dos Estados-Membros em países terceiros e os serviços de confiança utilizados em sistemas fechados estão igualmente excluídos.

5. Definições Fundamentais

Alguns conceitos básicos devem ser claramente compreendidos para uma correta interpretação da diretiva.

Termo	Definição
Sistema de rede e informação	Redes de comunicações eletrónicas, qualquer dispositivo ou grupo de dispositivos que trata dados digitais, e todos os dados digitais tratados para efeitos da sua exploração, utilização, proteção e manutenção.
Cibersegurança	Todas as atividades necessárias para proteger os sistemas de rede e informação, os utilizadores e outras pessoas de ciberameaças.
Incidente	Um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes.
Incidente significativo	Um incidente que tenha causado ou seja suscetível de causar graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa, ou que tenha afetado ou seja suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.
Ciberameaça	Qualquer circunstância, evento ou ação potencial que possa danificar, perturbar ou de outra forma afetar negativamente os sistemas de rede e informação.
Ciberameaça significativa	Uma ciberameaça que, com base nas suas características técnicas, possa ser considerada suscetível de ter um impacto grave nos sistemas de rede e informação de uma entidade, nos seus utilizadores, ou noutras pessoas, causando danos materiais ou imateriais consideráveis.
Vulnerabilidade	Um ponto fraco, uma suscetibilidade ou uma falha de um produto ou serviço de TIC passível de ser explorada por uma ciberameaça.
Quase incidente	Um evento que poderia ter posto em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados, ou de serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes, mas que foi possível evitar com êxito ou não se materializou.
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática (do inglês, Computer Security Incident Response Team), a equipa técnica responsável pelo tratamento de incidentes.
ENISA	Agência da União Europeia para a Cibersegurança, desempenha um papel central de consultoria e apoio na aplicação da diretiva.

6. Categorias de Entidades: Entidades Essenciais e Importantes

A diretiva divide todas as entidades abrangidas em duas categorias principais. Esta distinção determina como se aplicam as obrigações e o regime de supervisão e execução.

Critério	Entidades Essenciais	Entidades Importantes
Setor	Anexo I, setores de alta criticidade	Anexo II, outros setores críticos (e médias empresas do Anexo I)
Dimensão	Grandes empresas (250 ou mais trabalhadores ou volume de negócios superior a 50 milhões de EUR)	Médias empresas (50 a 249 trabalhadores)
Regime de supervisão	Supervisão ex ante e ex post	Apenas ex post, com base em indícios ou reclamação
Coima administrativa máxima	10 milhões de EUR ou 2% do volume de negócios anual global (aplica-se o valor mais elevado)	7 milhões de EUR ou 1,4% do volume de negócios anual global (aplica-se o valor mais elevado)
Sanções à direção de topo	Pode ser aplicada proibição temporária de exercício de funções de gestão	Não se aplica proibição temporária de exercício de funções de gestão

> **Nota importante:** Se uma entidade tiver sido identificada como "operador de serviços essenciais" ao abrigo da SRI 1, o Estado-Membro pode decidir que essa entidade é diretamente uma entidade essencial ao abrigo da SRI 2. Além disso, todas as entidades identificadas como "entidades críticas" ao abrigo da Diretiva 2022/2557 (REC) são automaticamente consideradas entidades essenciais ao abrigo da SRI 2.

7. Setores Abrangidos (Anexo I e Anexo II)

Anexo I, Setores de Alta Criticidade

As grandes empresas nestes setores são entidades essenciais; as médias empresas são entidades importantes.

Setor	Subsetor / Tipo de Entidade
Energia	Eletricidade (produção, transporte, distribuição, fornecimento); aquecimento e arrefecimento urbano; petróleo (oleodutos, produção, armazenagem, transporte); gás natural; produção, armazenagem e transporte de hidrogénio
Transportes	Aéreo (companhias aéreas, aeroportos, controlo de tráfego aéreo); ferroviário (gestores de infraestrutura, operadores ferroviários); aquático (operadores marítimos e de vias navegáveis interiores); rodoviário (sistemas de transporte inteligentes, operadores rodoviários)
Banca	Instituições de crédito ao abrigo do Regulamento (UE) 575/2013
Infraestruturas dos mercados financeiros	Plataformas de negociação (bolsas) e contrapartes centrais (CCP)
Saúde	Prestadores de cuidados de saúde; laboratórios de referência da UE; entidades que realizam I&D de medicamentos; fabricantes de produtos farmacêuticos; fabricantes de dispositivos médicos considerados críticos em emergências de saúde pública (nos termos do Regulamento (UE) 2022/123)
Água potável	Fornecedores e distribuidores de água para consumo humano
Águas residuais	Entidades que recolhem, eliminam ou tratam águas residuais urbanas, domésticas ou industriais
Infraestruturas digitais	Pontos de troca de tráfego (IXP); prestadores de serviços de DNS (excluindo DNS raiz); registos de nomes de TLD; prestadores de serviços de computação em nuvem; prestadores de serviços de centro de dados; prestadores de redes de distribuição de conteúdos (CDN); prestadores de serviços de confiança; prestadores de redes ou serviços públicos de comunicações eletrónicas
Gestão de serviços de TIC (B2B)	Prestadores de serviços geridos (MSP); prestadores de serviços de segurança geridos (MSSP)
Administração pública	Entidades da administração pública central e regional, tal como definidas pelos Estados-Membros
Espaço	Operadores de infraestruturas terrestres operadas por Estados-Membros ou pelo setor privado

Anexo II, Outros Setores Críticos

Setor	Subsetor / Tipo de Entidade
Serviços postais e de correio	Prestadores de serviços postais (incluindo serviços de correio)
Gestão de resíduos	Entidades que prestam serviços de recolha, reciclagem e eliminação de resíduos
Produtos químicos	Entidades envolvidas na produção, transformação e distribuição de produtos químicos
Alimentação	Grandes empresas envolvidas na produção, transformação e distribuição grossista de géneros alimentícios
Indústria transformadora	Dispositivos médicos/dispositivos médicos para diagnóstico in vitro; produtos informáticos, eletrónicos e óticos; equipamentos elétricos; máquinas e equipamentos n.e.c.; veículos automóveis, reboques e semi-reboques; fabrico de outro equipamento de transporte
Prestadores digitais	Mercados em linha; motores de pesquisa em linha; plataformas de serviços de redes sociais
Investigação	Organismos de investigação que realizam investigação com fins comerciais

8. Obrigações dos Estados-Membros

A diretiva impõe obrigações tanto aos Estados-Membros como às entidades do setor privado. Cada Estado-Membro deve tomar as seguintes medidas:

Estratégia nacional de cibersegurança. Adotar uma estratégia nacional de cibersegurança com objetivos estratégicos claros, prioridades e um quadro de governação. A estratégia aborda temas como a segurança da cadeia de abastecimento, o ransomware, o apoio às PME, o código aberto e a ciberdefesa ativa.

Autoridade(s) competente(s). Designar ou criar uma ou mais autoridades competentes para assegurar a aplicação e a supervisão da diretiva.

Ponto de Contacto Único (PCU). Designar um ponto de contacto único responsável pela coordenação transfronteiriça a nível da UE.

CSIRT. Criar ou designar uma ou mais CSIRT responsáveis pelo tratamento de incidentes, monitorização proativa, divulgação coordenada de vulnerabilidades e cooperação nacional e internacional.

Lista de entidades. Manter, atualizar regularmente e transmitir à Comissão uma lista de entidades essenciais e importantes e de entidades que prestam serviços de registo de nomes de domínio.

Divulgação coordenada de vulnerabilidades. Designar uma CSIRT como coordenadora; promover segurança jurídica para os investigadores de vulnerabilidades.

Assistência mútua. Prestar assistência mútua a outros Estados-Membros no âmbito da supervisão e da execução transfronteiriças.

Apoio às PME. Disponibilizar orientações, ferramentas gratuitas e um ponto de contacto nacional ou regional para pequenas e microempresas.

9. Medidas de Gestão dos Riscos de Cibersegurança (Artigo 21.o)

A disposição técnica mais importante da diretiva é o Artigo 21.o. Enumera as medidas técnicas, operacionais e organizativas mínimas que as entidades essenciais e importantes devem implementar. A abordagem baseia-se numa perspetiva que **abrange todos os riscos**; são abrangidos não apenas os ciberataques, mas também ameaças como danos físicos, catástrofes naturais, falha de equipamentos e erro humano.

Artigo 21.o, Dez Medidas Mínimas

N.o	Medida	Descrição
1	Políticas de análise dos riscos e de segurança dos sistemas de informação	Análise de todos os riscos e elaboração por escrito de políticas gerais de segurança da informação.
2	Tratamento de incidentes	Processos de prevenção, deteção, resposta e recuperação de incidentes.
3	Continuidade das atividades	Gestão de cópias de segurança, recuperação de desastres e gestão de crises.
4	Segurança da cadeia de abastecimento	Incluindo as práticas de segurança dos fornecedores; disposições de cibersegurança nos contratos com fornecedores diretos.
5	Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação	Segurança ao longo do ciclo de vida, incluindo o tratamento e a divulgação de vulnerabilidades.
6	Avaliação da eficácia das medidas	Avaliação regular da eficácia das medidas de gestão dos riscos de cibersegurança.
7	Práticas básicas de ciber-higiene e formação em cibersegurança	Práticas de ciber-higiene e formação de sensibilização para os trabalhadores.
8	Criptografia e cifragem	Políticas de utilização de criptografia e, se for caso disso, de cifragem ponta a ponta.
9	Segurança dos recursos humanos, controlo do acesso e gestão de ativos	Verificações de segurança de pessoal, autorização e inventário de ativos.
10	Autenticação multifatores e comunicações seguras	Autenticação multifatores quando adequado, autenticação contínua, comunicações seguras de voz, vídeo e texto, e sistemas seguros de comunicações de emergência.

Estas medidas são aplicadas com base no **princípio da proporcionalidade**, tendo em conta o grau de exposição ao risco da entidade, a sua dimensão, a importância setorial e

10. Obrigações de Notificação de Incidentes (Artigo 23.o)

A inovação operacional mais relevante da diretiva é o regime de notificação de incidentes por fases. As entidades essenciais ou importantes devem notificar **incidentes significativos**, definidos como aqueles que causam graves perturbações operacionais, perdas financeiras ou impacto substancial noutras pessoas, à CSIRT ou à autoridade competente nos seguintes prazos.

Fase	Prazo	Conteúdo
Alerta rápido	No prazo de 24 horas após ter tomado conhecimento do incidente	Suspeita de que o incidente foi causado por um ato ilícito ou malicioso; possibilidade de impacto transfronteiriço; informação básica que permita a tomada de conhecimento pela CSIRT.
Notificação de incidente	No prazo de 72 horas após ter tomado conhecimento do incidente	Atualização do alerta rápido; gravidade, impacto e, se disponíveis, indicadores de exposição a riscos (IoC).
Relatório intercalar/final	O mais tardar 1 mês após a notificação de incidente	Descrição pormenorizada do incidente, da sua gravidade e impacto; tipo de ameaça explorada; medidas de atenuação aplicadas e previstas; impacto transfronteiriço, se aplicável.
Relatório de situação	Se o incidente estiver ainda em curso na data de entrega do relatório final	Relatório de situação sobre o estado atual do incidente; relatório final 1 mês após a resolução do incidente.

Notificação aos destinatários dos serviços: Quando seja provável a ocorrência de uma ciberameaça significativa, as entidades devem notificar, sem demora injustificada e gratuitamente, os destinatários dos seus serviços sobre as possíveis medidas de atenuação e, se for caso disso, sobre a própria ameaça, em linguagem clara e compreensível.

Quase Incidentes e Notificação Voluntária

Para além dos incidentes, as entidades **podem notificar voluntariamente quase incidentes e ciberameaças significativas** à CSIRT ou à autoridade competente. As entidades não abrangidas pelo âmbito de aplicação da diretiva também podem notificar voluntariamente. A notificação voluntária não impõe obrigações adicionais ao notificador.

> **Impacto prático:** O alerta rápido de 24 horas obriga as entidades a dispor de um plano de resposta a incidentes de cibersegurança e de um fluxo de comunicação prontos a ser ativados imediatamente após a deteção do incidente. Cumprir este prazo através de processos manuais e fragmentados é extremamente difícil.

11. Segurança da Cadeia de Abastecimento

A maioria dos grandes ciberataques dos últimos anos atingiu as organizações visadas através de fornecedores e prestadores de software, e não por ataque direto à própria organização. A diretiva coloca, por isso, o risco da cadeia de abastecimento no centro das obrigações de gestão de riscos.

- As entidades devem avaliar a **qualidade, as práticas de segurança e os processos de desenvolvimento seguro** dos produtos e serviços dos seus fornecedores e prestadores de serviços.
- **Os requisitos de cibersegurança devem ser incluídos nos contratos** com os fornecedores diretos.
- Deve ser exercida especial diligência na seleção de **prestadores de serviços de segurança geridos (MSSP)**; estes prestadores são alvos de elevado valor para os atacantes.
- O Grupo de Cooperação, em conjunto com a Comissão e a ENISA, realiza **avaliações coordenadas dos riscos de segurança** para cadeias de abastecimento críticas (tal como foi feito para as redes 5G).
- **Fatores de risco de natureza não técnica** também integram o âmbito da avaliação, incluindo a potencial influência indevida de países terceiros sobre os fornecedores, vulnerabilidades ocultas/backdoors e dependência dos prestadores.

12. Responsabilidade do Órgão de Direção

A diretiva garante que a cibersegurança deixa de ser um tema confinado aos departamentos técnicos e passa para a **área de responsabilidade direta da direção de topo**. Nos termos do Artigo 20.o, os órgãos de direção das entidades essenciais e importantes:

- São responsáveis pela **aprovação das medidas de gestão dos riscos** previstas no Artigo 21.o e pela supervisão da sua aplicação;
- Podem ser **pessoalmente responsabilizados** pela violação dessas obrigações;
- Devem frequentar regularmente ações de formação em cibersegurança para adquirir conhecimentos e competências suficientes;
- Devem incentivar ações de formação semelhantes para os seus trabalhadores.

> **Importante:** Nas entidades essenciais, a autoridade competente pode solicitar a aplicação de **proibições temporárias de exercício de funções de gestão** à direção de topo (ao nível de diretor executivo ou representante legal). Trata-se de uma medida de último recurso, aplicável apenas após o esgotamento de todas as outras opções de execução.

13. Estruturas de Cooperação a Nível da UE

A diretiva regula ou reforça várias estruturas que asseguram uma cooperação eficaz entre os Estados-Membros:

Estrutura	Função
Grupo de Cooperação	Apoia a cooperação a nível estratégico; elabora programas de trabalho bienais; publica documentos de orientação; realiza avaliações coordenadas de riscos para cadeias de abastecimento críticas.
Rede de CSIRT	Cooperação a nível operacional; partilha de informações sobre incidentes; assistência mútua; resposta conjunta.
UE-CyCLONe	Rede Europeia de Organizações de Coordenação de Cibercrises; faz a ligação entre os níveis técnico e político em incidentes e crises de grande escala; elabora análises de impacto.
ENISA	Cria e mantém a base de dados europeia de vulnerabilidades; presta apoio técnico; elabora orientações; acompanha as políticas de ciber-higiene dos Estados-Membros.
Mecanismo IPCR	Mecanismos de Resposta Política Integrada a Crises da UE (Decisão de Execução do Conselho 2018/1993), gestão de crises de grande escala a nível da União.
Coordenador CVD EU-CSIRT	Uma CSIRT em cada Estado-Membro é designada coordenadora para gerir a divulgação coordenada de vulnerabilidades de âmbito transfronteiriço.

Cooperação com países terceiros: A UE pode celebrar acordos internacionais com países terceiros ou organizações internacionais ao abrigo do artigo 218.o do TFUE. Esses acordos podem, salvaguardando os interesses da União e a proteção de dados, permitir a tais partes participar nas atividades do Grupo de Cooperação, da Rede de CSIRT ou da UE-CyCLONe.

14. Supervisão e Execução

A diretiva prevê diferentes regimes de supervisão para as duas categorias de entidades. As **entidades essenciais** estão sujeitas a supervisão ex ante e ex post, enquanto as **entidades importantes** são supervisionadas apenas ex post, com base em indícios ou reclamação.

Poderes de Supervisão das Autoridades Competentes

- Realizar inspeções no local e supervisão à distância;
- Solicitar auditorias de segurança específicas (podendo os custos ser suportados pela entidade);
- Ordenar análises de segurança;
- Solicitar documentação do cumprimento das medidas de gestão dos riscos;
- Solicitar informações sobre atos suspeitos de violação da diretiva;
- Solicitar informações que exijam acesso a dados pessoais e dados de tráfego quando necessário.

Medidas de Execução Aplicáveis

- Emitir advertências e instruções vinculativas;
- Ordenar a aplicação de medidas específicas ou a correção de vulnerabilidades num prazo determinado;
- Ordenar uma auditoria independente para verificar as medidas de gestão dos riscos;
- Ordenar às entidades que informem os destinatários dos serviços sobre a natureza da violação;
- Emitir declarações públicas (divulgando o nome da entidade e a natureza da violação);
- Para entidades essenciais (último recurso): suspensão temporária de certificações ou autorizações e proibição temporária de exercício de funções de gestão à direção de topo;
- Aplicar ou solicitar a aplicação de coimas administrativas.

15. Coimas Administrativas

A diretiva estabelece **limiares máximos harmonizados a nível da UE** para as coimas administrativas aplicadas pelos Estados-Membros. Estes limiares estão indexados ao volume de negócios global da entidade, à semelhança do RGPD.

Tipo de Entidade	Montante Máximo (aplica-se o valor mais elevado)
Entidades essenciais	10 000 000 EUR ou 2% do volume de negócios anual global
Entidades importantes	7 000 000 EUR ou 1,4% do volume de negócios anual global

Fatores na Determinação das Coimas

- Natureza, gravidade e duração da infração;
- Danos materiais ou imateriais causados;
- Caráter intencional ou negligente da infração;
- Medidas tomadas para prevenir ou atenuar os danos;
- Grau de responsabilidade e infrações anteriores;
- Grau de cooperação com a autoridade competente;
- Outros fatores agravantes ou atenuantes.

As coimas devem ser **proporcionadas** e devem ser respeitados os direitos fundamentais, como o direito de defesa, a presunção de inocência e o direito a uma tutela jurisdicional efetiva na sua aplicação. Os Estados-Membros podem igualmente prever sanções penais para as infrações ao direito nacional; porém, nenhuma pessoa pode ser punida duas vezes pelo mesmo ato, em conformidade com o princípio do **ne bis in idem**.

16. Calendário de Aplicação e Transição

Data	Evento
14 de dezembro de 2022	Adoção da diretiva pelo Parlamento Europeu e pelo Conselho
27 de dezembro de 2022	Publicação no Jornal Oficial da UE (JO L 333/80)
16 de janeiro de 2023	Entrada em vigor da diretiva (20 dias após a publicação)
17 de outubro de 2024	Prazo para os Estados-Membros transporem a diretiva para o direito nacional
18 de outubro de 2024	Início da aplicação da diretiva
18 de outubro de 2024	Revogação da Diretiva (UE) 2016/1148 (SRI 1)
17 de abril de 2025	Prazo para os Estados-Membros transmitir à Comissão a lista de entidades essenciais e importantes
A partir de 17 de outubro de 2027	Revisão periódica da aplicação da diretiva pela Comissão (de 36 em 36 meses)

> **Importante:** A SRI 2 é uma diretiva; não se aplica diretamente. Cada Estado-Membro deve transpor a diretiva para o seu direito nacional. Por conseguinte, as obrigações e sanções concretas aplicáveis a uma entidade dependem do ato nacional de transposição adotado pelo Estado-Membro em que opera.

17. Implicações para Empresas Não Pertencentes à UE

Embora a SRI 2 seja uma diretiva da UE, tem implicações substanciais para as empresas não pertencentes à UE, em especial aquelas que servem o mercado da UE ou que fornecem entidades críticas sediadas na UE:

Empresas Não Pertencentes à UE Diretamente Afetadas

- **Prestadores de serviços de DNS, prestadores de serviços de computação em nuvem, operadores de centros de dados, prestadores de CDN, prestadores de serviços geridos e de serviços de segurança geridos, mercados em linha, motores de pesquisa e plataformas de redes sociais** não pertencentes à UE que ofereçam serviços na UE devem designar um representante na UE e cumprir as obrigações da diretiva;
- As empresas não pertencentes à UE com filiais ou sucursais na UE podem ficar sujeitas à diretiva através dessas unidades;
- Os fornecedores não pertencentes à UE que prestem produtos ou serviços a entidades essenciais ou importantes da UE ficarão sujeitos a **requisitos contratuais de segurança da cadeia de abastecimento** impostos pelos seus clientes (Artigo 21.o, n.o 2, alínea d));
- Os MSP/MSSP não pertencentes à UE que sirvam infraestruturas digitais ou entidades financeiras da UE podem ficar diretamente abrangidos pelo âmbito de aplicação.

Efeitos Indiretos

- As avaliações dos riscos da cadeia de abastecimento realizadas por clientes da UE obrigam os fornecedores não pertencentes à UE a elevar os seus padrões de cibersegurança;
- As normas introduzidas pela diretiva (ISO/IEC 27001, orientações da ENISA, etc.) estão a tornar-se **pontos de referência de facto** no mercado global;
- As jurisdições não pertencentes à UE recorrem cada vez mais à SRI 2 como referência no desenvolvimento da sua própria legislação em matéria de cibersegurança.

18. Roteiro Prático de Conformidade (10 Passos)

O roteiro de 10 passos que se segue constitui um guia prático tanto para as empresas que operam dentro da UE como para aquelas que pretendem alinhar-se voluntariamente com as normas da SRI 2.

Passo	Atividade
1. Delimitação do âmbito	Determinar se a empresa se enquadra nos setores do Anexo I ou do Anexo II, satisfaz os critérios de dimensão e identificar a sua categoria (essencial/importante).
2. Análise de lacunas	Avaliar o sistema de gestão de segurança da informação existente face às 10 categorias de medidas do Artigo 21.o; mapear as lacunas.
3. Estrutura de governação	Estabelecer responsabilidades, linhas de reporte e processos de aprovação ao nível do conselho de administração / direção de topo; criar um programa regular de formação.
4. Política e documentação	Preparar ou atualizar a política de segurança da informação, a política de gestão de riscos, a política de resposta a incidentes, a política de utilização aceitável e outros documentos.
5. Avaliação de riscos	Realizar o inventário de ativos, a análise de ameaças e a avaliação de riscos com abordagem que abranja todos os riscos; estabelecer critérios de aceitação do risco.
6. Implementação de controlos técnicos	Implementar autenticação multifatores, cifragem, segmentação de redes, arquitetura zero-trust, gestão de registos, SIEM, EDR/XDR, cópias de segurança e soluções de recuperação de desastres.
7. Capacidade de resposta a incidentes	Documentar o plano de resposta a incidentes; atribuir funções e responsabilidades; estabelecer o fluxo de comunicação do alerta rápido de 24 horas; realizar exercícios de simulação.
8. Gestão da cadeia de abastecimento	Inventariar fornecedores; classificá-los por nível de risco; incluir disposições de cibersegurança nos modelos de contrato; realizar auditorias periódicas.
9. Formação e sensibilização	Realizar formação anual de ciber-higiene para todos os trabalhadores; proporcionar formação especializada ao órgão de direção; realizar simulações de phishing.
10. Melhoria contínua	Realizar auditorias internas e externas; acompanhar KPIs; aprender com cada incidente; atualizar a avaliação de riscos anualmente; prosseguir a certificação (ISO/IEC 27001, certificação de cibersegurança da UE).

19. Conclusão e Avaliação

A Diretiva SRI 2 eleva substancialmente o nível de base de cibersegurança da União Europeia. Não se limita a impor requisitos técnicos; faz também da cibersegurança uma **parte integrante da estrutura de governação e das operações comerciais das empresas**.

Pontos Fortes da Diretiva

- **Alcance alargado**: aproximadamente 18 setores e mais de 100 000 entidades abrangidas nos 27 Estados-Membros da UE;
- **Harmonização**: condições de concorrência equitativas no mercado interno através de critérios uniformes e de um regime de execução comum em toda a UE;
- **Foco na governação**: ao responsabilizar a direção de topo, garante que a cibersegurança permeia todas as camadas da empresa;
- **Ênfase na cadeia de abastecimento**: responde à realidade de que a maioria dos ataques modernos ocorre através da cadeia de abastecimento;
- **Estruturas de cooperação**: coordenação a vários níveis à escala da UE através do Grupo de Cooperação, da Rede de CSIRT e da UE-CyCLONe.

Críticas e Desafios

- Atrasos e divergências na transposição pelos Estados-Membros; na prática, a aplicação uniforme nos 27 Estados-Membros da UE é irregular;
- Sobretudo para as médias empresas, o custo de conformidade e o encerramento da lacuna de capacidade técnica constituem um desafio sério;
- A aplicação do prazo do alerta rápido de 24 horas antes de atingida a maturidade suficiente pode conduzir a fluxos de notificação superficiais ou incorretos;
- As áreas de sobreposição com regulamentações setoriais (DORA, setor financeiro; eIDAS, serviços de confiança; regulamentações setoriais da aviação, etc.) podem criar complexidade para as entidades.

Avaliação Global

A SRI 2 reencadra a cibersegurança, passando de uma preocupação técnica para uma questão de **continuidade das atividades, governação empresarial e confiança dos clientes**. Para as entidades que operam ou interagem com a UE, a conformidade é simultaneamente uma obrigação legal e um meio de reforçar a resiliência operacional.

Para as empresas não pertencentes à UE, a SRI 2 está a estabelecer um novo **padrão de facto** para o acesso ao mercado da UE e a elevar as expectativas de cibersegurança a nível global. A conformidade antecipada facilita o cumprimento das obrigações contratuais e melhora a ciber-resiliência global.

> **Nota final:** Este documento resume as principais disposições da diretiva para leitores de língua portuguesa. Para os requisitos de conformidade específicos da sua organização, consulte o texto oficial (JO L 333/80, 27.12.2022), o ato nacional de transposição do seu Estado-Membro e as regulamentações setoriais específicas; recorra a aconselhamento jurídico e de cibersegurança especializado sempre que adequado.

Fontes

- Diretiva (UE) 2022/2555, número CELEX EUR-Lex 32022L2555
- Jornal Oficial da UE L 333/80, 27 de dezembro de 2022
- ENISA, Agência da União Europeia para a Cibersegurança (www.enisa.europa.eu)
- Portal de Estratégia Digital da Comissão Europeia (digital-strategy.ec.europa.eu)

Mais sobre a SRI 2 com a Rediacc

Este resumo mapeia a estrutura e as obrigações da diretiva. Os guias complementares em rediacc.com traduzem essas obrigações em decisões operacionais e de aquisição concretas.

Três guias complementares

- **Artigo 21.o, n.o 2, alínea d) e alojamento próprio.** Por que razão o registo de TIC de terceiros diminui quando o plano de dados nunca sai da sua infraestrutura. Para CISOs e responsáveis de aquisições a renegociar DPA em 2026.
- **Eficácia contínua sem encenação.** Os Artigos 21.o, n.os 2, alíneas e) e f), e 23.o lidos em conjunto. O fork em tempo constante que torna os exercícios semanais realistas, e o calendário de notificação do Artigo 23.o que não pode ser cumprido sem artefactos de qualidade forense. Para responsáveis de SRE e operações.
- **O custo estrutural da conformidade com a SRI 2.** O conjunto de cinco ferramentas que as entidades essenciais do mercado intermédio estão silenciosamente a montar, o que um plano de controlo alojado localmente colapsa, e as rubricas que ficam sempre do seu lado. Para CFO e compradores em ciclo de renovação.

Onde encontrá-los

Os três guias, juntamente com este resumo em PDF, estão disponíveis em:

rediacc.com/resources/nis2-directive-summary

A Rediacc OÜ é uma plataforma de infraestrutura de alojamento próprio registada na Estónia (Código de registo 17363830, IVA EE102920091). O produto não substitui um programa de segurança; é uma camada de ferramentas que elimina o risco do fornecedor no plano de dados que as ferramentas tradicionais de cópia de segurança, DR e dados de teste não conseguem eliminar. Nível Community gratuito e níveis pagos a partir de 349 USD/mês.

> Este documento e os seus guias complementares são material educativo. As decisões de conformidade específicas da sua organização requerem aconselhamento jurídico e referência ao ato nacional de transposição da sua jurisdição.