Comissão Europeia

CONJUNTO DE INSTRUMENTOS DA UE PARA A CIBERSEGURANÇA DAS REDES 5G

UM CONJUNTO DE MEDIDAS SÓLIDAS E ABRANGENTES PARA UMA ESTRATÉGIA COORDENADA AO NÍVEL DA UE QUE GARANTA A SEGURANÇA DAS REDES 5G

Março de 2021
#Cybersecurity

5G: uma nova tecnologia

Depois de as tecnologias 3G e 4G terem permitido, respetivamente, o acesso móvel à Internet e as ligações de banda larga móvel, espera-se que a tecnologia 5G se torne a infraestrutura de conectividade que abrirá caminho a novos produtos e serviços, afetando todos os setores da sociedade. Os benefícios incluirão:

SAÚDE EM LINHA

- Vigilância da saúde à distância, registos dos pacientes e diagnóstico inteligente
- Utilização de robôs para ajudar os cirurgiões e melhorar os resultados médicos

REDES DE ENERGIA INTELIGENTES

- Linhas elétricas de elevada eficiência e menos interrupções de serviço em menor escala
- Implantação mais fácil e com menor impacto ambiental

FÁBRICAS DO FUTURO

- Melhor controlo de processos internos sensíveis ao fator tempo
- Controlo à distância de maquinaria de armazenagem

MEIOS AUDIOVISUAIS E ENTRETENI-MENTO

- Experiência de visualização amplificada, como a realidade virtual
- Aplicações de banda larga ultrarrápida, como a transmissão de vídeo em contínuo

MOBILIDADE

- Viabilização da mobilidade conectada e automatizada com o objetivo de zero acidentes
- Viabilização da conectividade em todos os modos de transporte

A Europa é a região mais avançada na realização de ensaios 5G em grande escala nas indústrias verticais (que, até ao final de 2020, beneficiavam de um investimento de quase mil milhões de euros), incluindo para os corredores de transporte 5G. Até ao final de 2020, estavam disponíveis serviços 5G em 500 cidades europeias.

Cibersegurança das redes 5G: uma condição prévia indispensável

As redes 5G serão a futura espinha dorsal das nossas economias e sociedades cada vez mais digitalizadas. Estão em causa milhares de milhões de objetos e sistemas conectados, nomeadamente os utilizados em setores críticos como a energia, os transportes, a banca e a saúde, bem como em sistemas de controlo industriais que transmitem informações sensíveis e servem de base a sistemas de segurança. É, por isso, essencial garantir a cibersegurança e a resiliência das redes 5G.

Ao mesmo tempo, as redes 5G oferecem mais potenciais pontos de entrada a eventuais atacantes, devido, nomeadamente, a uma arquitetura menos centralizada, à capacidade computacional inteligente de proximidade, à necessidade de um maior número de antenas e à sua maior dependência do *software*.

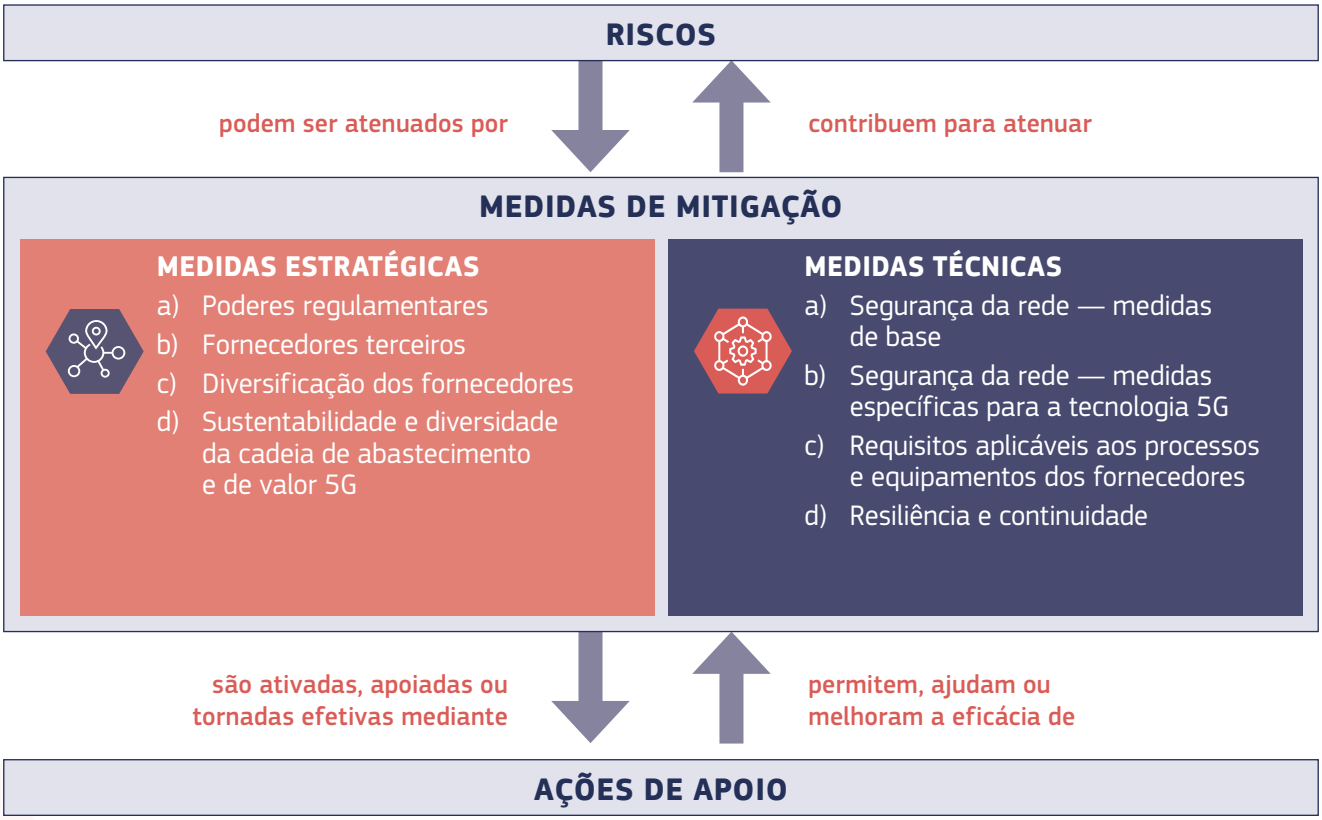
Avaliação de riscos da UE: cenários de risco

A avaliação coordenada dos riscos de segurança das redes 5G ao nível da UE identifica nove riscos principais, agrupados em cinco cenários de risco.

I — Cenários de risco relacionados com medidas de segurança insuficientes	R1 — Má configuração das redes R2 — Falta de controlos de acesso
II — Cenários de risco relacionados com a cadeia de abastecimento 5G	R3 — Fraca qualidade dos produtos R4 — Dependência de um único fornecedor em determinadas redes ou falta de diversidade a nível nacional
III — Cenários de risco relacionados com o *modus operandi* dos principais perpetradores	R5 — Interferência de Estados através da cadeia de abastecimento 5G R6 — Exploração de redes 5G pela criminalidade organizada ou por organizações criminosas que visem os utilizadores finais
IV — Cenários de risco relacionados com interdependências entre as redes 5G e outros sistemas críticos	R7 — Perturbação significativa de infraestruturas ou serviços críticos R8 — Falha generalizada das redes devido à interrupção do fornecimento de eletricidade ou de outros sistemas de apoio
V — Cenários de risco relacionados com dispositivos dos utilizadores finais	R9 — Exploração da IdC (Internet das coisas), de telemóveis ou de dispositivos inteligentes

Conjunto de instrumentos da UE para a cibersegurança das redes 5G

Tendo por base a avaliação coordenada dos riscos de segurança das redes 5G ao nível da UE, o conjunto de instrumentos estabelece uma série de medidas de segurança que visam atenuar os riscos de forma eficaz e garantir a implantação de redes 5G seguras em toda a Europa. Estabelece também **planos de atenuação** pormenorizados para cada um dos riscos identificados e recomenda uma série de **medidas estratégicas e técnicas essenciais** a adotar por todos os Estados-Membros e/ou pela Comissão.



Conclusões sobre o conjunto de instrumentos da UE: principais medidas

Os **Estados-Membros** devem dispor de medidas e de poderes para atenuar os riscos. Devem, designadamente:

- reforçar os **requisitos de segurança** para os **operadores de redes móveis**;
- avaliar o perfil de risco dos fornecedores; aplicar **restrições adequadas aos fornecedores considerados de alto risco**, incluindo exclusões necessárias, no respeitante aos ativos essenciais;
- assegurar que cada operador disponha de uma **estratégia de diversificação de fornecedores** adequada para **evitar** ou **limitar** qualquer **dependência significativa** de um único fornecedor e evitar a dependência de fornecedores considerados de alto risco.

A **Comissão Europeia**, juntamente com os Estados-Membros, deve tomar medidas para:

- manter uma **cadeia de abastecimento 5G diversificada** e **sustentável**, a fim de evitar a dependência a longo prazo, devendo para tal:
  - utilizar plenamente os instrumentos e as ferramentas da UE existentes (análise de investimentos diretos estrangeiros, instrumentos de defesa comercial, regras de concorrência);
  - reforçar as capacidades da UE nas tecnologias 5G e pós-5G, recorrendo a programas e financiamentos adequados da UE;
- facilitar a coordenação entre os Estados-Membros no que diz respeito à **normalização**, a fim de alcançar objetivos de segurança específicos, e desenvolver **sistemas de certificação** pertinentes ao nível da UE.

Importa ainda alargar o mandato do **grupo de cooperação Segurança das Redes e da Informação nesta vertente de trabalho**, para que este apoie, monitorize e avalie a aplicação do conjunto de instrumentos.

Planos de atenuação dos riscos — exemplos de medidas do conjunto de instrumentos

O conjunto de instrumentos identifica planos de atenuação dos riscos para cada uma das nove áreas de risco identificadas no relatório sobre a avaliação coordenada dos riscos ao nível da UE. Estes planos consistem em possíveis combinações de medidas, baseadas na sua eficácia.

O conjunto de instrumentos fornece orientações sobre critérios objetivos, incluindo fatores de risco técnicos e não técnicos, para avaliar o perfil de risco dos fornecedores, ou seja, o risco de interferência por parte de um país terceiro; capacidade de assegurar o fornecimento e práticas de cibersegurança.

SM03	**Avaliar o perfil de risco dos fornecedores e aplicar restrições aos fornecedores considerados de alto risco, incluindo exclusões necessárias para atenuar eficazmente os riscos, no que respeita a ativos essenciais**	Estabelecer um quadro com critérios claros, tendo em conta os fatores de risco identificados no ponto 2.37 da avaliação coordenada dos riscos ao nível da UE e adicionando informações específicas por país (por exemplo, avaliação de ameaças dos serviços de segurança nacionais, etc.), para que as autoridades nacionais competentes e os operadores de redes móveis (ORM): — efetuem avaliações rigorosas dos perfis de risco de todos os fornecedores pertinentes a nível nacional e/ou ao nível da UE (por exemplo, juntamente com outros Estados-Membros ou outros operadores de redes móveis); — com base na avaliação do perfil de risco, apliquem restrições, incluindo exclusões necessárias para atenuar eficazmente os riscos, no que respeita a ativos essenciais definidos como críticos ou sensíveis no relatório sobre a avaliação coordenada dos riscos ao nível da UE (por exemplo, funções de rede principal, de gestão e orquestração da rede e de rede de acesso); — tomem medidas para assegurar que os operadores de redes móveis têm em vigor controlos e processos adequados para gerir potenciais riscos residuais, tais como auditorias e avaliações regulares dos riscos da cadeia de abastecimento, gestão sólida dos riscos e/ou requisitos específicos para os fornecedores com base nos seus perfis de risco.

O conjunto de instrumentos fornece orientações sobre o grau de sensibilidade de elementos e funções da rede.

TM03	**Assegurar controlos de acesso rigorosos**	Assegurar que os operadores de redes móveis aplicam medidas técnicas adequadas, flexíveis e passíveis de verificação com vista a garantir: — a aplicação de controlos de acesso rigorosos às redes; — a aplicação do princípio do menor privilégio, garantindo que vários direitos na rede (por exemplo, direitos de acesso entre funções de rede, direitos de administradores da rede, configuração de virtualização) são minimizados; — a aplicação do princípio da separação de funções; — a existência de procedimentos que assegurem que estas regras estão sempre em vigor e evoluem com a rede. No estabelecimento das políticas de controlo de acesso, deverá haver um especial cuidado em garantir que o acesso remoto por terceiros, em especial fornecedores considerados de alto risco, é minimizado e/ou evitado sempre que possível. Quando o acesso remoto seja necessário, por exemplo, para dar resposta a cortes de serviço, os operadores de redes móveis devem aplicar procedimentos adequados de autenticação, autorização, registo e auditoria que permitam obter uma perspetiva clara do acesso aos dados e das alterações de configuração ou de rede.

Calendário da política da UE em matéria de cibersegurança das redes 5G

22 de março de 2019
Conclusões do **Conselho Europeu.**

26 de março de 2019
A **Comissão Europeia** publicou uma **recomendação** instando os Estados-Membros a tomarem medidas concretas para avaliar os riscos de cibersegurança das redes 5G e reforçar as medidas de atenuação dos riscos.

9 de outubro de 2019
Os Estados-Membros concluíram a avaliação coordenada dos riscos de segurança das redes 5G ao nível da UE.

21 de novembro de 2019
A Agência da UE para a Cibersegurança publicou um exaustivo relatório sobre ameaças relacionadas com as redes 5G.

29 de janeiro de 2020
Publicação do conjunto de medidas de atenuação pelos Estados-Membros. Comunicação da Comissão sobre a aplicação do conjunto de instrumentos da UE [COM(2020) 50 final, de 29 de janeiro de 2020].

Julho de 2020
Relatório intercalar sobre a aplicação do conjunto de instrumentos.

Outubro de 2020
O **Conselho Europeu** exortou a União e os seus Estados-Membros «a fazerem pleno uso do conjunto de instrumentos para a cibersegurança das redes 5G» e a «aplicarem as restrições necessárias aos fornecedores de alto risco no que respeita a ativos essenciais».

Dezembro de 2020
Nova estratégia de cibersegurança da UE e **Relatório** sobre o impacto da Recomendação da Comissão sobre a cibersegurança das redes 5G.

Até junho de 2021
A Comissão insta os Estados-Membros a **concluírem a aplicação das principais medidas do conjunto de instrumentos**.

Próximas etapas (no âmbito da estratégia de cibersegurança da UE para a década digital)

- Concluir a aplicação das principais medidas do conjunto de instrumentos até ao segundo trimestre de 2021.
- Garantir que os riscos identificados foram atenuados de forma adequada e coordenada, em especial no que diz respeito ao objetivo de minimizar a exposição a fornecedores de alto risco e de evitar a dependência desses fornecedores a nível nacional e ao nível da UE.
- Prosseguir e aprofundar a coordenação ao nível da UE, colocando a ênfase nos objetivos principais:

1. Assegurar abordagens nacionais convergentes em matéria de atenuação dos riscos em toda a UE

2. Apoiar um intercâmbio de conhecimentos permanente e o reforço de capacidades

3. Promover a resiliência das cadeias de abastecimento e outros objetivos estratégicos da UE no domínio da segurança

Luxemburgo: Serviço das Publicações da União Europeia, 2021

Serviço das Publicações da União Europeia

Print ISBN 978-92-76-37752-8 doi:10.2759/424246 KK-02-21-626-PT-C
PDF ISBN 978-92-76-37732-0 doi:10.2759/212439 KK-02-21-626-PT-N

2021-05-25