



Número de notificação : 2023/0761/ES (Spain)

DECRETO REAL QUE APROVA O REGIME NACIONAL DE SEGURANÇA DAS REDES E DOS SERVIÇOS 5G

Data de receção : 29/12/2023

Fim do período de statu quo : 02/04/2024 (closed)

Message

Mensagem 001

Comunicação da Comissão - TRIS/(2023) 3739

Directiva (UE) 2015/1535

Notificação: 2023/0761/ES

Notificação de um projeto de texto de um Estado-Membro

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifikasi – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμπία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késésekét - Non fa decorrere la mora - Atidéjimal nepradedami - Atlíkšanas laikposms nesākas - Ma jiftaħx il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.PT

1. MSG 001 IND 2023 0761 ES PT 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Telecomunicações

5. DECRETO REAL QUE APROVA O REGIME NACIONAL DE SEGURANÇA DAS REDES E DOS SERVIÇOS 5G

6. Redes e serviços de comunicações eletrónicas 5G



Equipamentos de telecomunicações.

7.

8. O regulamento é composto por uma parte explicativa, um artigo único que aprova o ENS5G (Regime Nacional de Segurança 5G), duas disposições complementares e quatro disposições finais.

O ENS5G a aprovar é constituído por 33 artigos divididos em oito capítulos e três anexos.

A exposição de motivos explica as razões subjacentes à adoção do regulamento e os artigos do Decreto Real-Lei que estão a ser desenvolvidos.

O artigo único aprova o Regime Nacional de Segurança das redes e dos serviços 5G.

A primeira disposição complementar estabelece que o Governo, por decreto real, sob proposta do Ministério da Transformação Digital, na sequência de um relatório do Conselho de Segurança Nacional, deve rever o Regime Nacional de Segurança das redes e dos serviços 5G quando as circunstâncias assim o exigirem e, em todo o caso, de quatro em quatro anos.

A segunda disposição complementar estabelece que o Real Decreto-lei n.º 7/2022, de 29 de março de 2022, e o ENS5G são aplicáveis às gerações de comunicações eletrónicas posteriores à quinta geração, embora não exista regulamentação específica para estas.

A primeira disposição final relativa ao título de competência precisa que o decreto real e o regime por ele aprovado são emitidos nos termos do disposto no artigo 149.º, n.º 1, ponto 21 e no artigo 149.º, n.º 1 ponto 29, da Constituição espanhola, que conferem ao Estado, respetivamente, competência exclusiva em matéria do sistema geral de telecomunicações e em matéria de segurança pública.

A segunda disposição final declara a Lei n.º 11/2022, de 28 de junho de 2022, relativa às telecomunicações gerais, e os respetivos regulamentos de aplicação, de aplicação complementar, e estabelece que, em todas as matérias não regulamentadas na referida legislação, o Real Decreto-lei n.º 12/2018, de 7 de setembro de 2018, relativo à segurança das redes e dos sistemas de informação e a Lei n.º 8/2011, de 28 de abril de 2011, que estabelece medidas de proteção das infraestruturas críticas, bem como os respetivos regulamentos de aplicação, são de aplicação complementar.

A terceira disposição final sobre o desenvolvimento regulamentar permite ao chefe do Ministério da Transformação Digital desenvolver as disposições do presente decreto real e o regime que aprova, e alterar por despacho o conteúdo dos anexos de acordo com a evolução do progresso tecnológico, a aprovação de novas normas técnicas e sistemas de certificação para equipamentos de telecomunicações e produtos conectados, bem como o desenvolvimento de diferentes configurações e parâmetros técnicos das redes e serviços 5G e das futuras gerações de comunicações eletrónicas.

A quarta disposição final prevê que o regulamento entra em vigor no dia seguinte ao da sua publicação no «Boletín Oficial del Estado».

No que diz respeito ao conteúdo do ENS5G, que é aprovado:

O artigo 1.º estabelece que o regulamento é emitido em aplicação do Real Decreto-lei n.º 7/2022, de 29 de março de 2022, nomeadamente em aplicação do respetivo capítulo IV.

O artigo 2.º é referente aos objetivos do regulamento, que já foram analisados.

O artigo 3.º estabelece que devem ser utilizadas as definições constantes do Real Decreto-lei n.º 7/2022, de 29 de março de 2022, da Lei n.º 11/2022, de 28 de junho de 2022, relativa às telecomunicações gerais e do Código Europeu das Comunicações Eletrónicas.

O artigo 4.º estabelece que o regulamento é aplicável aos operadores 5G, aos fornecedores 5G e aos utilizadores corporativos 5G que tenham o direito de utilizar o domínio público das radiocomunicações para instalar, implantar ou operar uma rede privada 5G ou para prestar serviços 5G para fins profissionais ou para a prestação de serviços próprios.

O artigo 5.º identifica os elementos, infraestruturas e recursos mínimos que constituem uma rede de comunicações eletrónicas 5G, remetendo para o anexo I para a sua descrição pormenorizada. Estabelece igualmente os elementos críticos de uma rede 5G que, regra geral, devem estar em território nacional (incluindo eventuais exceções).

O artigo 6.º refere-se ao tratamento global da segurança em conformidade com a legislação comunitária internacional e nacional aprovada ou suscetível de ser aprovada, exigindo que as partes obrigadas efetuam, por meio de um método holístico, uma análise das vulnerabilidades, ameaças e riscos que as afetam enquanto agentes económicos e dos vários componentes, bem como uma gestão adequada e abrangente desses riscos através da utilização de técnicas e medidas adequadas para a sua atenuação ou eliminação e para alcançar o objetivo final de utilização e operação seguras das



redes e serviços 5G.

O artigo 7.º salienta que a análise e a gestão dos riscos constituem uma parte essencial do processo de segurança e devem ser uma atividade contínua e continuamente atualizada.

O artigo 8.º refere-se à monitorização permanente e à reavaliação periódica.

O artigo 9.º estabelece que a análise de riscos a nível nacional é a que consta do anexo II e foi efetuada tendo em conta vários elementos, como as informações recolhidas junto das partes obrigadas, o exame das vulnerabilidades ligadas à cadeia de distribuição das redes e serviços 5G, a avaliação do grau de dependência dos fornecedores, o risco de interrupção do abastecimento devido a circunstâncias económicas, empresariais ou comerciais que afetem os fornecedores ou a avaliação da eficácia das medidas de segurança aplicadas.

O artigo 10.º, relativo à gestão dos riscos a nível nacional, estabelece que os critérios, requisitos, condições e prazos para as partes obrigadas conceberem e aplicarem técnicas e medidas de atenuação dos riscos são os estabelecidos no anexo III.

O artigo 11.º desenvolve o disposto no artigo 14.º do Real Decreto-lei n.º 7/2022, de 29 de março de 2022, no que diz respeito ao procedimento e aos aspetos a avaliar pelo Conselho de Ministros para a classificação dos fornecedores como de alto risco e aos elementos a ter em conta ao ordenar a eventual substituição dos equipamentos, produtos e serviços fornecidos por esses fornecedores. Do mesmo modo, em conformidade com o disposto no referido real decreto-lei, é estabelecido que os fornecedores de alto risco cujos equipamentos de telecomunicações, hardware, software ou serviços auxiliares prestados sejam utilizados única e exclusivamente em redes privadas 5G ou para a prestação de serviços 5G em regime de autoprestação são classificados como fornecedores de médio risco.

O artigo 12.º, relativo à determinação dos locais onde não podem ser instalados equipamentos de fornecedores classificados como de alto risco, estabelece que o Conselho Nacional de Segurança, na sequência de um relatório do Ministério da Transformação Digital, pode determinar os locais, zonas e centros onde os equipamentos dos fornecedores classificados como de alto risco não podem ser instalados. Para a instalação, modificação ou adaptação de estações de rádio que proporcionem cobertura a esses locais, zonas e centros, os operadores 5G devem solicitar autorização ao Ministério da Transformação Digital.

O artigo 13.º obriga os operadores 5G a conceberem uma estratégia de diversificação da cadeia de distribuição e a disporem de equipamento de transmissão na rede de acesso que seja fornecido por, pelo menos, dois fornecedores diferentes. Prevê igualmente critérios a ter em conta pelo Conselho de Ministros, a fim de decidir se é possível manter um único fornecedor se o número de fornecedores for reduzido na sequência de fusões. Além disso, indica os pressupostos e o procedimento através dos quais o Ministério da Transformação Digital pode alterar a estratégia de diversificação da cadeia de distribuição de um operador 5G.

O artigo 14.º centra-se na análise de riscos a efetuar pelos operadores 5G em relação a todos os elementos, infraestruturas e recursos da rede constante do anexo I, enumera os fatores a ter em conta e obriga os operadores a recolher dos seus fornecedores as práticas e medidas de segurança adotadas nos produtos e serviços que lhes forneceram e a incluírem uma hierarquização e priorização dos riscos de acordo com determinados parâmetros também enumerados. Até 1 de outubro de 2024, os operadores 5G devem apresentar uma análise de riscos e, posteriormente, de dois em dois anos.

O artigo 15.º, relativo à análise de riscos por parte dos fornecedores 5G, exige a análise dos riscos dos equipamentos, hardware e software de telecomunicações e dos serviços complementares envolvidos no funcionamento ou operação de redes 5G ou na prestação de serviços 5G, bem como o fornecimento da referida análise ao Ministério, mediante pedido. No caso dos fornecedores classificados como de alto ou médio risco, a análise deve ser apresentada no prazo de seis meses a contar dessa classificação e, posteriormente, de dois em dois anos.

O artigo 16.º, relativo à análise de riscos por parte dos utilizadores corporativos 5G, exige que a referida análise de riscos seja fornecida ao Ministério da Transformação Digital, sempre que esses utilizadores sejam obrigados a fazê-la.

O artigo 17.º permite que o Ministério da Transformação Digital recolha junto das partes obrigadas as informações necessárias para a análise de risco e classifique como infração grave o não fornecimento dessas informações no prazo de 15 dias úteis. A informação é considerada confidencial e não pode ser utilizada para outro fim que não o cumprimento dos objetivos e obrigações estabelecidos no Real Decreto-lei n.º 7/2022, de 29 de março de 2022, no ENS5G e nas leis emitidas em cumprimento de ambas as disposições.

O artigo 18.º proclama o dever geral de todas as partes obrigadas a gerir os riscos de segurança.

O artigo 19.º centra-se na gestão da segurança por parte dos operadores 5G, enumerando as obrigações de todos os operadores (tais como adotar planos e medidas de contingência, cumprir as normas ou especificações técnicas europeias



e os sistemas de certificação, realizar uma auditoria de segurança a expensas próprias ou exigir que os seus fornecedores cumpram as normas de segurança) e obrigações adicionais para os operadores que possuem ou operam elementos críticos de uma rede pública 5G (tais como proibições de utilização de equipamentos de fornecedores de alto risco em elementos críticos da rede ou em determinados locais, zonas e centros). Os operadores 5G devem apresentar ao Ministério da Transformação Digital uma descrição das medidas técnicas e organizacionais concebidas e aplicadas para gerir e atenuar os riscos até 1 de outubro de 2024 e, posteriormente, de dois em dois anos. Além disso, os operadores 5G que possuam ou operem elementos críticos de uma rede pública 5G devem apresentar ao Ministério da Transformação Digital uma estratégia de diversificação da cadeia de distribuição até 1 de outubro de 2024 e, posteriormente, sempre que esta esteja sujeita a alterações. As informações sobre o estado de aplicação desta estratégia devem ser apresentadas até 1 de outubro de cada ano.

O artigo 20.º, relativo à gestão da segurança pelos fornecedores 5G, contém uma lista de obrigações, incluindo a realização de uma auditoria de segurança dos seus equipamentos, produtos e serviços, a prestação de informações sobre possíveis interferências por terceiros na conceção, operação e funcionamento dos seus equipamentos, produtos e serviços e a colaboração com operadores 5G e utilizadores corporativos 5G, fornecendo informações e certificando o cumprimento das normas e certificações. Os fornecedores 5G devem elaborar um relatório sobre as medidas técnicas e organizacionais concebidas e implementadas para gerir e mitigar os riscos e fornecer o referido relatório ao Ministério, mediante pedido. No caso dos fornecedores classificados como de alto ou médio risco, o relatório deve ser apresentado no prazo de seis meses a contar dessa classificação e, posteriormente, de dois em dois anos.

O artigo 21.º, relativo à gestão da segurança por parte dos utilizadores corporativos 5G, estabelece que estes não podem utilizar nos elementos críticos da rede equipamentos de telecomunicações, sistemas de transmissão, equipamentos de comutação ou encaminhamento e outros recursos que permitam o transporte de sinais, hardware, software ou serviços complementares de fornecedores que tenham sido classificados como de risco médio. Além disso, os utilizadores devem fornecer ao Ministério da Transformação Digital, mediante pedido, de dois em dois anos, uma descrição das medidas técnicas e organizacionais concebidas e implementadas para gerir e atenuar os riscos.

O artigo 22.º, relativo à gestão da segurança pelas administrações públicas, estabelece que, por razões de segurança nacional, na instalação, implantação e exploração de redes 5G, públicas ou privadas, ou na prestação de serviços 5G, acessíveis ao público ou para autoprestação, as administrações públicas não podem utilizar equipamentos, produtos e serviços fornecidos por fornecedores de alto ou médio risco.

O artigo 23.º estabelece que, no cumprimento das obrigações previstas nos artigos anteriores, as partes obrigadas devem ter em conta e aplicar o estabelecido no Real Decreto-lei n.º 7/2022, de 29 de março de 2022, no ENS5G e nas leis emitidas em cumprimento de ambas as disposições.

O artigo 17.º permite que o Ministério da Transformação Digital recolha junto das partes obrigadas as informações necessárias para gestão dos riscos e classifique como infração grave o não fornecimento dessas informações no prazo de 15 dias úteis. A informação é considerada confidencial e não pode ser utilizada para outro fim que não o cumprimento dos objetivos e obrigações estabelecidos no Real Decreto-lei n.º 7/2022, de 29 de março de 2022, no ENS5G e nas leis emitidas em cumprimento de ambas as disposições.

O artigo 25.º estabelece que todas as partes obrigadas, bem como as administrações públicas, os fabricantes, os importadores, os distribuidores e aqueles que colocam no mercado e vendem equipamentos e dispositivos terminais para ligação a uma rede 5G e para poderem prestar serviços 5G, devem cooperar e apresentar as informações necessárias para a alteração e aplicação do ENS5G.

O artigo 26.º estabelece que, por despacho do chefe do Ministério da Transformação Digital, a utilização de um equipamento, sistema, programa ou serviço específico pode ser sujeita a certificação prévia nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), ou ao abrigo de regimes de certificação e normas técnicas de certificação de equipamentos e produtos 5G que possam ser aprovados a nível europeu ou internacional.

O artigo 27.º estabelece que o regulamento é aplicável sem prejuízo do investimento estrangeiro e do direito da concorrência.

O artigo 28.º, relativo aos equipamentos terminais, prevê que o fabrico, a importação, a distribuição, a colocação no mercado e a venda de equipamentos terminais e de dispositivos para ligação a uma rede 5G e para a prestação de serviços 5G estejam subordinados ao cumprimento dos requisitos de segurança dos produtos digitais e dos requisitos



essenciais aplicáveis em matéria de cibersegurança, adotados em conformidade com a legislação da União Europeia, nomeadamente no que diz respeito à proteção dos dados pessoais, à privacidade e à proteção contra a fraude. O artigo 29.º refere-se à cooperação internacional a desenvolver pelo Ministério da Transformação Digital, nomeadamente a nível da União Europeia. O artigo 30.º refere-se à competência do Ministério da Transformação Digital para a aplicação do ENS5G. O Ministério deve coordenar-se com os outros organismos responsáveis pela cibersegurança e pelas infraestruturas críticas, a fim de assegurar uma aplicação coerente do ENS5G.

O artigo 31.º define as competências de aplicação do ENS5G que correspondem ao Ministério da Transformação Digital, incluindo, por exemplo, o desenvolvimento, a especificação e o pormenor do conteúdo do ENS5G, a realização de auditorias para verificar e controlar o cumprimento das obrigações impostas e a concessão de auxílio público.

O artigo 32.º atribui ao Ministério da Transformação Digital todos os poderes da função de inspeção.

O artigo 33.º, relativo ao regime sancionatório, remete para o disposto nos artigos 30.º e 31.º do Real Decreto-lei n.º 7/2022, de 29 de março de 2022.

O anexo I descreve os elementos, as infraestruturas e os recursos que constituem uma rede 5G.

O anexo II contém a análise de riscos a nível nacional.

O anexo III estabelece a gestão dos riscos a nível nacional.

9. As comunicações móveis de quinta geração ou 5G constituem um novo paradigma das comunicações eletrónicas com grande potencial transformador em benefício da sociedade e da economia, uma vez que abrem a possibilidade de incorporar novas funcionalidades que terão grande impacto, como a computação em rede, e permitem a criação de redes virtuais, oferecendo baixa latência e prestando serviços de elevado valor acrescentado em domínios como a medicina, os transportes e a energia.

Por conseguinte, tanto a União Europeia como a Espanha estão a promover a rápida implantação de redes 5G e a execução de projetos que demonstrem a sua utilidade para diferentes setores através da prestação de serviços 5G. As redes e serviços 5G têm vantagens de segurança comparativas em relação às gerações anteriores. No entanto, apresentam também riscos específicos decorrentes, por exemplo, da sua arquitetura de rede mais complexa, aberta e desagregada, e da sua capacidade de transportar enormes volumes de informação e de permitir a interação simultânea de múltiplas pessoas e coisas. A sua interligação com outras redes e a natureza transnacional de muitas das ameaças têm impacto na sua segurança, e a utilização generalizada previsível dessas redes para funções económicas e sociais essenciais aumentará o impacto potencial dos incidentes de segurança de que são vítimas.

Estes novos riscos de segurança específicos das comunicações móveis 5G foram abordados em termos regulamentares através do Real Decreto-lei n.º 7/2022, de 29 de março de 2022, relativo aos requisitos para garantir a segurança das redes e serviços de comunicações eletrónicas de quinta geração, que incorpora plenamente a

Recomendação (UE) 2019/534 da Comissão Europeia, de 26 de março de 2019, Cibersegurança das redes 5G, bem como as recomendações que a Comunicação da Comissão Europeia, de 29 de janeiro de 2020, Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE (COM/2020/50 final), forneceu aos Estados-Membros no que diz respeito à utilização do referido conjunto de instrumentos.

O referido Real Decreto-lei n.º 7/2022, de 29 de março de 2022, prevê o seu desenvolvimento regulamentar através do Regime Nacional de Segurança das redes e dos serviços 5G (ENS5G).

Nos termos do n.º 3 do artigo 5.º do real decreto-lei referido, o ENS5G procede a um tratamento abrangente da segurança das redes e serviços 5G, tendo em conta os contributos para o alcance de cada agente da cadeia de valor 5G, bem como os regulamentos, recomendações e normas técnicas da União Europeia, da União Internacional das Telecomunicações (UIT) e de outras organizações internacionais, a fim de garantir o objetivo final de utilização e operação seguras das redes e serviços 5G em Espanha.

Por sua vez, o artigo 20.º do real decreto-lei prevê que, a fim de assegurar o funcionamento contínuo e seguro da rede e dos serviços 5G, o ENS5G deve realizar uma análise de riscos a nível nacional sobre a segurança das redes e serviços 5G e identificar, especificar e desenvolver medidas para atenuar e gerir os riscos analisados.

Por último, nos termos do artigo 21.º do real decreto-lei, o ENS5G é aprovado pelo Governo, por decreto real, sob proposta do Ministério da Transformação Digital, na sequência de um relatório do Conselho de Segurança Nacional.

O presente regulamento aprova o ENS5G, desenvolvendo o disposto no Real Decreto-lei n.º 7/2022, de 29 de março de 2022, relativo aos requisitos para garantir a segurança das redes e serviços de comunicações eletrónicas de quinta geração.



EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

10. Referências aos textos de base:

11. Não

12.

13. Não

14. Não

15. Sim

16.

Aspectos OTC: Não

Aspectos MSF: Não

Comissão Europeia

Contacto para obter informações de carácter general Directiva (UE) 2015/1535

email: grow-dir2015-1535-central@ec.europa.eu