CONSULTA PÚBLICA AO PROJETO DE REGULAMENTO QUE CONFIGURA A INSTRUÇÃO TÉCNICA RELATIVA À COMUNICAÇÃO E INFORMAÇÃO PARA DAR CUMPRIMENTO AO ESTABELECIDO NO DECRETO-LEI N.º 65/2021

Introdução

No presente documento detalham-se os comentários e preocupações dos associados da APRITEL ao projeto de regulamento que configura instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes ("Instruções Técnicas").

Os operadores de serviços de comunicações eletrónicas conferem primordial relevância à segurança e integridade das suas redes e serviços de comunicações eletrónicas, os quais são fatores determinantes para a confiança dos utilizadores e do mercado em geral nos seus serviços.

Com vista a assegurar este objetivo, os associados da APRITEL têm interesse e atuam proactivamente na minimização de potenciais incidentes que afetem a segurança e integridade das suas redes e serviços, seguindo e adotando as melhores práticas e que estão devidamente alinhadas com os objetivos previstos no Quadro Nacional de Referência de Cibersegurança ("QNRCS").

Adicionalmente, o setor é objeto de um forte enquadramento regulatório, com destaque para o Regulamento n.º 303/2019, de 1 de abril ("Regulamento de Segurança da ANACOM") que veio reforçar o elevado nível de segurança e integridade da redes e serviços de comunicações eletrónicas.

Tendo presente este enquadramento, a APRITEL vem demonstrar a disponibilidade dos seus associados para cooperar em todas as ações que visam garantir a definição e implementação de medidas para garantir a segurança e integridade do ciberespaço. Para este propósito, a experiência dos operadores de redes e serviços de comunicações eletrónicas é certamente uma mais-valia, nomeadamente para a definição de medidas que considerem os procedimentos já implementados, sem comprometer o combate às ameaças que colocam em causa a segurança do ciberespaço.

De facto, a APRITEL entende que as Instruções Técnicas surgem como instrumento essencial para a implementação das regras definidas, pelo que estas devem ser o mais possível orientadas à gestão dos riscos reais e alinhadas com os procedimentos já implementados. As Instruções Técnicas devem ainda evitar a imposição de uma carga administrativa que seja excessiva e desvie o foco da redução dos riscos e mitigação das ameaças.

Neste seguimento, a APRITEL apresenta nos comentários específicos alguns pedidos de esclarecimentos e sugestões fundamentadas de revisão das propostas apresentadas no Projeto de regulamento que configura instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos,

relatório anual e notificação de incidentes ("Projeto de Regulamento" ou "Instruções Técnicas"). Os pontos que suscitam estes comentários referem-se ao Projeto de Instrução Técnica relativa ao inventário de ativos, ao processo de notificação de incidentes e aos prazos associados às obrigações impostas.

Comentários específicos

Sobre o inventário de ativos

O artigo 4.º das Instruções Técnicas estabelece as regras para a elaboração do inventário de ativos, com indicação de que a informação deve ser baseada nas medidas técnicas "ID.GA - Gestão de Ativos", do "QNRCS", elaborado pelo Centro Nacional de Cibersegurança ("CNCS"). Mais concretamente, no mínimo devem ser incluídas as medidas técnicas "ID.GA-1 - Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados" e "ID.GA-2 - As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas".

Estas regras devem ser aplicadas por todas as entidades e serviços abrangidos pela Lei n.º 46/2018, de 13 de agosto para a elaboração dos seus inventários de ativos, incluindo pelos operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

Ora, no caso particular dos prestadores de serviços digitais, e especificamente os que oferecem serviços de computação em nuvem, como é o caso dos operadores de comunicações eletrónicas associados da APRITEL, os termos e regras propostos para a elaboração de um inventário de ativos são de muito difícil implementação, assim como são contrários a uma orientação plena à eficácia e eficiência operacionais ao serviço da segurança das redes e serviços.

Desde logo pelas características dinâmicas associadas à prestação destes serviços digitais, o que leva a que alguns destes elementos sejam alterados com alguma frequência e, em consequência disso, à desatualização da informação partilhada com o CNCS. É exemplo desta realidade a lista de servidores físicos associados aos serviços de computação em nuvem ("cloud"), que pode ter que ser redimensionada para fazer face a necessidades pontuais do serviço. O mesmo acontece com as aplicações, onde é possível recorrer a aumentos do poder computacional por períodos de tempo relativamente curtos, na ordem de horas ou mesmo de minutos.

Adicionalmente, os operadores de serviços de comunicações eletrónicas efetuam uma gestão operacional integrada, incluindo ao nível da gestão de vulnerabilidades e implementação de medidas de segurança, de todos os serviços disponibilizados nos seus portfólios de ofertas. Portanto, seria legítimo que todos os serviços os serviços de comunicações eletrónicas e serviços digitais fossem sujeitos a obrigações e requisitos de segurança equivalentes.

Assim sendo, tendo presente que de entre as obrigações estabelecidas pelo Regulamento de Segurança da ANACOM está a realização de um inventário de ativos, a proposta da APRITEL passa, para o caso dos prestadores de serviços digitais que são simultaneamente operadores de serviços de comunicações eletrónicas, por utilizar o mesmo processo e requisitos de elaboração do inventário de ativos previstos no referido Regulamento da ANACOM.

Para este efeito, conforme constante do anexo, a APRITEL apresenta um exemplo prático de como seria efetuado este inventário de ativos para os operadores de serviços digitais.

Esta proposta de aplicação de requisitos equivalentes encontra acolhimento no Decreto-Lei 65/2021, de 30 de julho em que está previsto que o CNCS proceda, em articulação com as entidades reguladoras e de supervisão setoriais, a uma avaliação de equivalência entre os requisitos constantes de legislação setorial que sejam considerados equivalentes aos consagrados neste decreto-lei. [1]

Finalmente, no que respeita aos ativos a serem considerados neste processo de inventário, em linha com a definição de ativo proposta no artigo 4.º[2], estes devem estar limitados aos sistemas, recursos e elementos físicos e lógicos ligados à prestação dos serviços em causa. A APRITEL entende que estes ativos devem estar ainda limitados aos que são geridos e detidos pelos prestadores, assim como aos que estão associados aos serviços diretamente controlados e desenhados pelos prestadores de serviços digitais. Por fim, devem ser excluídos do âmbito deste inventário os ativos que já constem do inventário que os prestadores de redes e serviços de comunicações eletrónicas já estão obrigados a manter no âmbito do Regulamento de Segurança da ANACOM.

Sobre o processo de notificação de incidentes

Conforme estabelecido pelo n.º 2 do artigoº 11.º do Decreto-Lei n.º 65/2021, de 30 de julho, as entidades devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.

No caso específico dos prestadores de serviços digitais, o n.º 4 do artigo 3.º estabelece que a estes aplicam-se o disposto no Regulamento de Execução (UE) 2018/151 da Comissão de 30 de janeiro de 2018, em matéria de requisitos de segurança e de notificação de incidentes.

A respeito do âmbito de notificação a ser efetuado pelos prestadores de serviços digitais, a APRITEL entende que este deve estar limitado aos serviços que são diretamente controlados e geridos por estes prestadores, sobre os quais detêm acesso a informação necessária para

[1] Tendo presente que o ciberespaço é uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade, o presente decreto-lei reconhece a necessidade de articular as disposições legais aqui consagradas com a aplicação de normativos complementares setoriais. Para este efeito, o Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, nos casos em que se considere necessário e em articulação com as entidades reguladoras e de supervisão setoriais, procede a uma avaliação de equivalência, conferindo, assim, segurança jurídica aos requisitos constantes de legislação setorial que sejam considerados equivalentes aos consagrados no presente decreto-lei.

[2] Ativo: todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerandos essenciais, que suportam, direta ou indiretamente, um ou mais serviços.

avaliar o impacto de um incidente. Neste sentido, devem estar excluídos todos os serviços que impliquem a intervenção de outras entidades na prestação das ofertas aos utilizadores finais. Por exemplo, os incidentes que afetem o acesso a serviços que sejam objeto de revenda não devem ser notificados pelos prestadores que efetuam esta revenda, mas antes pelas entidades responsáveis pela gestão destas ofertas.

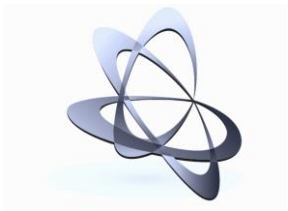
A APRITEL regista com alguma preocupação a opção prevista no n.º 1 do artigo 6.º das Instruções Técnicas, que passa pela notificação mediante o preenchimento de um formulário através do sítio na Internet do CNCS.

A este propósito, a APRITEL entende que o processo de notificações de incidentes ao CNCS deve prever a possibilidade de recurso a sistemas que permitam que este ocorra mediante integração automática, tal como já está previsto no processo de notificações enviadas ao abrigo do Regulamento de Segurança da ANACOM. Esta hipótese é particularmente relevante numa fase inicial dos incidentes, em que os esforços devem estar canalizados para a mitigação e resolução das ocorrências. Mais ainda, esta hipótese mitiga a intervenção manual, sem comprometer o cumprimento dos prazos estabelecidos. Por fim, permite que as empresas do sector das comunicações eletrónicas mantenham os processos e sistemas de notificação já desenvolvidos e em operação.

Atendendo a que o artigo 1.º das Instruções Técnicas prevê a possibilidade de envio e tratamento de informação através de um endereço de correio eletrónico,[3] a APRITEL considera que este deve ser o meio primordial para envio das notificações, devendo para tal serem preenchidos os mesmos campos que os previstos na notificação por via de formulário. Adicionalmente, a APRITEL sugere a criação de uma API[4] que permita garantir a automatização deste processo de notificação, sendo que para o efeito manifesta a sua disponibilidade para estar envolvida e acompanhar este projeto. Com efeito, para a APRITEL, a utilização do formulário para notificações de incidentes deve ocorrer apenas na ausência de outros processos de notificação. A este respeito, a APRITEL não pode deixar de demonstrar a sua preocupação quanto ao facto de o acesso ao formulário poder ser feito sem o recurso a qualquer processo de autentificação ou outros mecanismos que limitem os riscos de serem efetuadas notificações indevidas, utilizações abusivas e fraudulentas, assim como potenciem riscos de fuga de informação.

Para os casos de notificação por esta via, a APRITEL considera essencial que sejam desenvolvidos mecanismos de autentificação para o envio destas notificações que, no mínimo, permitam assegurar que estas são efetuadas por colaboradores devidamente credenciados pelos prestadores sujeitos a estas obrigações.

[3] sri@cncs.gov.pt
[4] Application Programming Interface



Por fim, em caso de falha destes meios de notificação, sugere-se que o CNCS disponibilize um contacto telefónico para este fim, o qual, por razões de confidencialidade, deverá apenas ser comunicado aos responsáveis de segurança das empresas.

Sobre os prazos para cumprimento das obrigações

O Projeto de Regulamento foi submetido a consulta pública com a publicação do Aviso na 2.ª série do Diário da República de 17 de novembro de 2021[5]. A partir desta data, a consulta pública decorre por um prazo de 30 dias úteis[6], ou seja, até dia 31 de dezembro de 2021.

Neste sentido, é legítimo considerar que uma decisão final quanto às Instruções Técnicas não deve ser conhecida antes da primeira metade do mês de janeiro de 2022.

A publicação das Instruções Técnicas tem um impacto decisivo na elaboração do inventário de ativos, uma vez que o n.º 2, do artigo 6.º (Inventário de ativos) do Decreto-Lei n.º 65/2021, de 30 de julho remete para este documento a concretização dos elementos a constarem neste inventário.

Contudo, o n.º 1, do artigo 22.º (Disposições Transitórias) deste Decreto-Lei estabelece que o primeiro relatório anual deve ser entregue até 31 de janeiro de 2022, acompanhado pela versão inicial do inventário de ativos.

A este respeito cumpre salientar que os operadores de serviços de comunicações eletrónicas têm procedimentos de inventariação de ativos, que seguem as melhores práticas da indústria e garantem o cumprimento das normas de referência, entre as quais a ISO/IEC 27001.Sucede que os esforços e a complexidade associados à elaboração de um inventário de ativos e a não (expectável) publicação de uma decisão final, com a definição dos campos a serem incluídos, com suficiente antecipação, tornam manifestamente impossível a conclusão deste processo para envio da informação no final de janeiro de 2022. Neste sentido, a APRITEL considera essencial que seja efetuada a devida derrogação das Disposições Transitórias do Decreto-Lei n.º 65/2021, de 30 de julho. Concretamente, deve ser contemplado um prazo suficientemente alargado após a publicação do Regulamento – que configura instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes – para o cumprimento da obrigação de elaboração e envio do primeiro inventário de ativos. Caso seja aceite a proposta da APRITEL para o inventário de ativos dos prestadores de serviços digitais que são simultaneamente prestadores de serviços de comunicações eletrónicas, antecipa-se ser possível concluir este processo num prazo não superior a 60 dias úteis. No

[5] https://dre.pt/dre/detalhe/aviso/21606-2021-174476379
[6] https://www.cncs.gov.pt/pt/regulacao/consultas-publicas/a-decorrer/

entanto, a manter-se o cumprimento integral dos campos indicados na proposta apresentada nas Instruções Técnicas, o processo de realização do inventário não deve ser concluído num prazo inferior a 6 meses. Por fim, caso se mantenha a obrigação de envio a 31 de janeiro de 2022, a APRITEL entende que cumprimento desta obrigação só poderá ser conseguido mediante envio de uma versão simplificada deste inventário, limitada ao identificador público (*public identifier*) e os serviços associados a cada um dos ativos ligados à prestação dos serviços.

Quanto ao Relatório anual, embora os elementos exigidos à sua elaboração estejam desde já concretizados no artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho salienta-se que as obrigações e regras definidas entram em vigor apenas em novembro e dezembro de 2021.

A este propósito, a APRITEL questiona a pertinência na elaboração de um relatório com a periodicidade anual, com especial foco em dados detalhados de incidentes, quando não está concluído ainda o inventário de ativos que serve de referência à notificação dos incidentes e o período a que respeitam as regras definidas pelo Decreto-Lei n.º 65/2021, de 30 de julho é bastante mais limitado. Assim sendo, a APRITEL sugere que o envio do primeiro relatório anual seja efetuado apenas em 2023, respeitando um período em que as regras do Decreto-Lei n.º 65/2021, de 30 de julho já estão em vigor há pelo menos um ano, e existe uma plena definição sobre as Instruções Técnicas emitidas pelo CNCS.

Por fim, quanto à indicação do ponto de contacto permanente e do responsável de segurança, nos termos previstos pelos artigos 4.º e 5.º do Projeto de Regulamento, as mesmas deveriam ser efetuadas, nos termos da lei, 90 dias após a entrada em vigor do Decreto-Lei n.º 65/2021, de 30 de julho, ou seja, até ao passado dia 6 de dezembro de 2021. Dado que os artigos 2.º e 3.º das Instruções Técnicas estabelecem que esta comunicação deve ser enviada por correio eletrónico, mediante preenchimento e junção de um formulário, solicita-se a confirmação de que as entidades sujeitas a estas obrigações devem proceder ao reenvio dos elementos já notificados ao CNCS.

ANEXO

Exemplo de inventário de ativos em alinhamento com o Regulamento de Segurança da ANACOM

	Exemplo 1
a) Identificador único	ID1
b) Identificador público	DTD HTML 1.01//PT
c) Designação	Infraestrutura de Cloud
d) Classificação, ao abrigo do disposto no artigo 8.º	C
e) As coordenadas geográficas da sua localização	X ; Y
f) A identificação das entidades detentoras ou gestoras dos locais	Operador A
g) Caracterização:	
i. Funcionalidades e serviços suportados	Infraestrutura de suporte aos serviços de Cloud (inclui servidores, storage, comunicações e segurança)
ii. Fundamentação da classificação, ao abrigo do disposto no artigo 8.º, incluindo uma descrição do impacto potencial de uma perturbação do seu funcionamento	< 30.000 clientes. Redundância de serviços garantida por ativos do mesmo tipo noutra localização
iii. Identificação como ponto de falha única	N
iv. Fornecimentos de terceiros críticos para o seu funcionamento, incluindo serviços de gestão, de operação, de segurança e de energia	Energia; AVAC; Segurança; Contrato suporte
v. Autonomia em caso de falha de fornecimento de energia	Com grupo gerador (combustível para mais de 7 dias)
vi. No caso de interligação, indicação do tipo (interligação internacional, interligação entre as Regiões Autónomas, interligação entre o Continente e uma Região Autónoma ou interligação entre ilhas na Região Autónoma dos Açores ou na Região Autónoma da Madeira) e identificação das empresas interligadas	N/A
h) Medidas, controlos e registos de segurança adotados, incluindo as medidas de redundância, robustez e resiliência no caso de ativo identificado como ponto de falha única ao abrigo do disposto na subalínea iii) da alínea anterior	Ver sistema de gestão de risco

i) Registo das violações de segurança ou perdas de integridade com impacto significativo ocorridas	Ver sistema de ticketing
j) Registo das alterações efetuadas, incluindo os resultados dos testes de integração e de sistema realizados e os planos de restauro dos ativos	Ver sistema de ticketing