ANACOM

Segundo Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas - Consulta Pública

(AVISO da ANACOM n.º 11948/2018, publicado a 22.08.2018)

Contributos da EDP Distribuição – Energia, SA

Outubro 2018

Índice

1. Introdução 1

2. Comentários Gerais 2

3. Comentários Específicos 3

Anexo 1 - Anterior contributo na sequência do Aviso da ANACOM em 5 de agosto de 2016 7

Anexo 2 - Anterior contributo na sequência do Aviso da ANACOM em 10 de Janeiro de 2017 9

1. Introdução

As redes e serviços de Comunicações Eletrónicas desempenham um papel vital para a sociedade e para a atividade económica em geral, fruto do seu contributo essencial na persecução da transformação e inovação dos processos de negócio e nos comportamentos sociais, constituindo um recurso essencial ao seu funcionamento, o que coloca novos desafios aos operadores, nomeadamente na perspetiva da acrescida garantia de continuidade de serviço, acessibilidade, desempenho, disponibilidade e segurança dos serviços.

É nesta perspetiva que reconhecemos a pertinência da iniciativa regulamentar lançada pela ANACOM[1], que recolhe enquadramento na normalização existente e boas práticas que vão sendo provadas e adotadas transversalmente pelos diversos setores da economia, no sentido de promover de forma sistemática a integridade e segurança das infraestruturas e dos serviços prestados, adotando uma abordagem holística e sistematizada aos respetivos sistemas tecnológicos, incluindo o fator humano.

Consideramos igualmente de grande relevância o envolvimento da ERSE neste processo atendendo à elevada interdependência dos serviços essenciais de Energia e Comunicações Eletrónicas.

No setor da Energia, a EDP Distribuição também desenvolve um serviço de elevado valor crítico para a economia e sociedade em Geral, ocupando com as comunicações eletrónicas uma posição cimeira no impacto potencial na economia e na sociedade em caso de disrupção.

Pelo exposto, a EDP Distribuição reconhece nesta iniciativa uma resposta apropriada às diretivas 2009/140/CE (Segurança e Integridade) e 2016/1148 (NIS), revendo-se nas suas orientações e recomendações no sentido do desenvolvimento de ações consonantes com a normalização existente e incremento de cooperação entre operadores que prestam serviços essenciais e interdependentes.

O ajuste das organizações a estas práticas regulamentares é fundamental para assegurar uma resposta capaz aos crescentes desafios do mundo digital e assegurar um elevado e homogéneo nível de segurança das redes e sistemas de informação.

Reconhecemos que a presente redação reflete contributos e sugestões que partilhámos em sede da primeira consulta, o que traduz a N/ ver um adequado alinhamento com as principais recomendações e práticas internacionais.

Após este capítulo introdutório, apresentamos nos capítulos seguintes os comentários gerais e os contributos da EDP Distribuição sobre o procedimento de elaboração de um Regulamento relativo à segurança e integridade das redes e serviços de comunicações eletrónicas.

[1] Aviso n.º 11948/2018, publicado a 22.08.2018

2. Comentários Gerais

Conforme oportunamente manifestado, a EDP Distribuição considera que o trabalho desenvolvido pela ENISA em conjugação com os reguladores nacionais, com enfoque na identificação de medidas e respetiva operacionalização harmonizada para provisão do artigo 13ª da Diretiva 2002/21/EC na redação da Diretiva 2009/140/EC, materializada no Guia "*Technical Guideline for Minimum Security Measures*", constitui uma base de requisitos adequada ao suporte do futuro regulamento.

Deste Guia, consideramos ser de destacar a sua abordagem holística, nomeadamente através dos domínios definidos e respetivas ações: Governo e Gestão de Risco, Segurança no âmbito dos Recursos Humanos, Segurança de Sistemas e Instalações, Gestão de Operações, Gestão de Incidentes, Gestão de Continuidade de Negócio, Monitorização, auditoria e teste.

Nesta perspetiva, reconhecemos na presente proposta de redação do Regulamento práticas mais sustentáveis, transversais e com melhores condições de transparência e comparabilidade.

Consideramos que o documento pode beneficiar de uma clarificação sobre a taxionomia "Segurança" e "Integridade", semelhante ao promovido no Guia ENISA "Technical Guideline on Security Measures, V2.0 de Outubro de 2014", que a partir dos requisitos de "Segurança" e de "Integridade" introduzidos pelo artigo 13ª da Diretiva 2009/140/EC, clarifica o entendimento "Integridade" como resiliência e continuidade (conforme literatura de segurança de informação).

Nesta conformidade, a ENISA explicita ainda que o conjunto de medidas preconizadas endereça simultaneamente os objetivos de "Segurança" e "Integridade", clarificando que no documento se utiliza a terminologia "segurança" e "continuidade", ou somente "Segurança", dado que na literatura técnica o conceito de segurança já incorpora a necessidade de continuidade.

3. Comentários Específicos

Apresentam-se seguidamente os comentários aos artigos do regulamento:

Artigo 2º - Âmbito

A utilização de serviços de comunicações eletrónicas por parte de empresas operadoras de serviços essenciais e de outros utilizadores empresarias é, maioritariamente, regida por contratos que, na medida do possível, contemplam as condições de serviço específicas e adequadas, incluindo as características do serviço a prestar, aspetos construtivos particulares, níveis de desempenho, disponibilidade e objetivos associados aos processos e tempos operacionais a considerar no âmbito do seu restauro e controlo de segurança.

Neste sentido, sugerimos que a redação do nº 4 deste artigo, em extensão à sua alínea c), também contemple as obrigações emergentes de contratos cuja abrangência é complementar à do serviço universal.

Artigo 6º - Obrigações das empresas

Pela objetividade que julgamos poder proporcionar ao regulamento e seus efeitos, incluindo no entendimento de outros artigos, sugerimos que a redação da alínea b) do número 2 seja alterada no sentido de estabelecer a obrigação de "adoção" das especificações e recomendações enunciadas, bem como do seu cumprimento.

Complementarmente, considera-se que seria importante referir a família de normas ISO 27000, conferindo maior abrangência e prevendo a sua aplicabilidade na construção e ciclo de vida de um sistema de gestão de risco.

Artigo 7º - Medidas técnicas de execução e requisitos adicionais

A adoção do sistema ISO27000, conforme proposta de clarificação enunciada no artigo 6º, irá contribuir para a estrutura e sistematização da ação a desenvolver pelas empresas na persecução do dever referido no número 1 deste artigo, e mais ainda na interpretação dos níveis de sofisticação do Anexo, em particular no cumprimento do número 2 do Anexo "Governação e gestão dos riscos"

Pela sua estruturação e maturidade, esta norma reforçará a consistência dos sistemas de Governo, salvaguardando uma análise de riscos necessariamente holística.

Como exemplo, o efeito e risco da elevada interdependência dos serviços essenciais de energia e de comunicações eletrónicas, por aplicação da norma e das recomendações da ENISA, será obrigatoriamente endereçado, nomeadamente por via da ISO27002/9.2.2 Supporting utilities e ENISA "Technical Guidelines for the implementation of minimum

security measures dor Digital Service Providers – Security of supporting utilities", devendo impor níveis de autonomia energética em função dos regulamentos e garantias de abastecimento de energia que estão em vigor e dos riscos de interrupção que lhes estão associados.

Artigo 8º - Classificação de Ativos

Ao conferir o enquadramento dos serviços prestados à EDP Distribuição (alínea f) do nº 2 do artigo 21º), entendemos que a totalidade dos ativos envolvidos no suporte dos serviços serão considerados do tipo A, incluindo as estações base afetas ao serviço móvel terrestre que suportam os atuais serviços de dados do tipo M2M e que estão afetos à gestão e automação da Rede de Distribuição de Energia Elétrica.

A EDP Distribuição propõe a clarificação da redação das disposições regulamentares em que a classificação dos ativos seja relevante, em linha com o entendimento exposto no parágrafo anterior.

Artigo 15º - Ponto de Contacto Permanente

Para além da função de Ponto de Contacto Permanente com a ANACOM, sugere-se que sejam estabelecidas regras sobre a comunicação e estabelecimento dos necessários protocolos com Clientes que, pela dimensão ou criticidade, devem merecer um acesso agilizado, nomeadamente aqueles que são responsáveis por serviços essenciais.

A comunicação e sua prontidão possuem neste regulamento uma abrangência de natureza complementar à abordada no "Relatório dos Incêndios Florestais", como seja e a título de exemplo, a pronta comunicação da deteção de incidentes de segurança, mesmo que estes não se cheguem a repercutir na integridade e continuidade dos serviços prestados.

Artigo 21º - Circunstâncias

Em relação ao projeto de regulamento e atendendo ao previsto na Diretiva NIS que define operadores de serviços essenciais, figura aplicável à EDP Distribuição, atendendo que estes incorporam comunicações eletrónicas como parte dos respetivos processos críticos, entendemos que o dever de comunicação/notificação de violações de segurança ou perdas de integridade da rede deverá ser alargado àqueles Clientes/operadores.

Considerando a dependência dos serviços críticos de empresas/clientes especiais das redes e serviços de comunicações eletrónicas, reforçamos a necessidade de adequação do dever de notificação em caso de violação de segurança ou perda de integridade, permitindo ao cliente uma rápida resposta no sentido de controlar ou mitigar o impacto do incidente.

O formato e o prazo de comunicação deverão responder às orientações emanadas na diretiva NIS, promovendo nomeadamente a cooperação e ação coordenada no âmbito dos incidentes de segurança.

A utilização de serviços de comunicações eletrónicas por parte de empresas operadoras de serviços essenciais é, maioritariamente, regida por contratos que, na medida do possível, contemplam as condições de serviço específicas e adequadas, incluindo as características do serviço, níveis de desempenho, disponibilidade e processos e tempos operacionais a considerar no âmbito do seu restauro.

Julgamos, portanto, essencial integrar a quebra dos níveis de serviço ou de outras condições essenciais à definição do serviço, conforme estabelecidos em contrato (acordadas), na definição de eventos de "impacto significativo" ou quebra de segurança ou continuidade dos serviços.

Passando a integrar a métrica objetiva que é apresentada, definida em função do impacto no parque de serviços de utilização geral ("assinantes"), conferindo suporte aos compromissos acordados para satisfação de utilizadores com requisitos específicos no suporte da sua atividade nuclear, essencial ou outra.

Também pela definição de "incidente de Segurança", conforme h) do Artigo 3º e recomendações aplicáveis, este pode causar ou ter o potencial de vir a causar impacto nos serviços.

Neste sentido, o presente artigo beneficiará de uma redação que inclua a obrigação de comunicar, prontamente, qualquer incidente de segurança mesmo que este não se tenha repercutido em perturbação grave, com impacto significativo na continuidade desse funcionamento, condição indispensável a uma ação preventiva de todas as partes envolvidas, incluindo pelos utilizadores dos serviços, no sentido de minimizar o risco de impacto até à total reposição das condições de segurança.

Esta abrangência é de especial interesse às entidades que operam outros serviços essenciais f) do nº 2, nomeadamente na ação preventiva e coordenada a incidentes de segurança que ocorram nas empresas, não se devendo aplicar a condição de impacto efetivo e de duração mínima.

Artigo 23º - Condições

Este artigo considera o dever de informação dirigido ao público em geral e condicionado a uma condição quantitativa de impacte. Conforme comentário ao artigo 21º, consideramos importante enquadrar incidentes de segurança, mesmo que de afetação individual de clientes ou clientes operadores de serviços essenciais, com ou sem impacte na continuidade do serviço. Este enquadramento poderá ser feito em secção própria de "Obrigações de informação a Operadores de Serviços Essenciais" tal como disposto no Artigo 21º, Ponto 5 f).

Considera-se igualmente que através do Ponto de Contacto Permanente (Artigo 21º) deverá ser assegurada a pronta comunicação de incidentes de segurança ou de falha de integridade dos Serviços.

Considera-se que a atual redação do artigo 13º não assegura a comunicação pronta, ou logo que possível, e que considere a abrangência comentada no artigo 21º.

Nesta conformidade, a necessidade que os utilizadores críticos têm de ser informados a tempo, mais se aproxima do previsto no nº4 do artigo 22º, acautelando as correções sugeridas em relação à não obrigatoriedade de se verificar impacto.

Pela sua natureza, esta informação poderá ser classificada como de circulação e divulgação reservada, cabendo à ANACOM a decisão de a divulgar publicamente (exemplo: quebra de sigilo das comunicações afetas à condução de serviços essenciais, mesmo que sem impacto efetivo na continuidade do serviço).

Anexo 1 - Anterior contributo na sequência do Aviso da ANACOM em 5 de agosto de 2016

Seguidamente apresenta-se uma transcrição dos contributos enviados pela EDP Distribuição à ANACOM em setembro passado, no âmbito do procedimento de elaboração deste Regulamento (Aviso de 5 de agosto).

"**3.1** ***A aprovação de medidas técnicas de execução no âmbito das obrigações das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público em matéria de segurança e integridade, ao abrigo do disposto no n.º 1 do artigo 54.º-C da Lei das Comunicações Eletrónicas;***

Conforme anteriormente exposto, consideramos adequada a definição das condições mínimas elaborada pela ENISA, que julgamos ser de incorporar integralmente no regulamento, com as seguintes sugestões complementares:

- Incluir uma "*Threat List*" para suporte à avaliação de risco dos operadores
    - Proposta: *ENISA Threat Taxonomy* 2016, que pode ser adaptado à realidade dos operadores (*sector specific*) https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information
- Partilha de informação entre os vários operadores nacionais e internacionais – *Information Sharing and Cooperation*, incluindo nessa partilha os Clientes que prestam serviços essenciais, nomeadamente para efeitos do cumprimento das obrigações que lhes estão cometidas pela Diretiva NIS;
- Reforçar, pela sua importância, a necessidade dos operadores estabelecerem um modelo de governo que permita uma gestão e *ownership* de risco adequada;
- Implementar mecanismos de proteção de dados pessoais sobre a informação veiculada através das redes e serviços, incluindo os dados armazenados e processados pelo operador; uma vez que a privacidade dos clientes é um tema de extrema importância, incluindo o controlo de acesso na ótica do *as-needed-basis* e técnicas de anonimização de informação;
- A seleção de controlos a implementar deve considerar as seguintes áreas:
    - Segurança de Rede
    - Proteção contra *Malware*
    - Configuração Segura de Sistemas e Equipamentos
    - Armazenamento Externo
    - Teletrabalho Seguro
    - Gestão de Utilizadores
    - Gestão Segura das Operações
    - Monitorização e Auditoria
    - Gestão de Incidentes
    - Continuidade de Negócio

3.2 A fixação de requisitos adicionais em matéria de segurança e integridade às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, ao abrigo do disposto no artigo 54.º-D da Lei das Comunicações Eletrónicas;

Atendendo à elevada interdependência dos serviços essenciais de Energia e Comunicações Eletrónicas consideramos que no respeitante ao exposto em *Security of supplies (SD3.2)-power failures*, será de estabelecer uma autonomia de funcionamento dos serviços de comunicações adequada e que tenha em conta a continuidade de serviço que as redes elétricas podem assegurar. Consideramos que a fixação destes requisitos deverá ser estabelecida pela ANACOM em articulação com a ERSE.

3.3 A aprovação das medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes, ao abrigo do disposto no n.º 2 do artigo 54.º-C da Lei das Comunicações Eletrónicas;

Em relação ao regulamento em vigor e atendendo ao previsto na Diretiva NIS que define operadores de serviços essenciais, figura aplicável à EDP Distribuição, atendendo que estes incorporam comunicações eletrónicas como parte dos respetivos processos críticos, julgamos que o dever de comunicação/notificação de violações de segurança ou perdas de integridade da rede deverá no futuro ser alargado àqueles operadores, distinguindo-as dos conceitos de Público em Geral e de Assinante.

O formato e o prazo de comunicação deverão responder às orientações emanadas nesta diretiva, promovendo a cooperação e ação coordenada no âmbito dos incidentes de segurança, onde se exige a criação de CSIRT.

3.4 A fixação das condições em que a ANACOM considera existir um interesse público na divulgação ao público, por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços, ao abrigo do disposto na alínea b) do artigo 54.º-E da Lei das Comunicações Eletrónicas;

Em linha com o anterior comentário.

3.5 A determinação às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público da realização de auditorias à segurança das suas redes e serviços e do envio do respetivo relatório, incluindo a fixação dos requisitos a que devem obedecer as auditorias e as entidades auditorias, ao abrigo do disposto nos n.ºs 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas.

As auditorias previstas devem estar de acordo com o sistema ISO27001, nomeadamente quanto ao seu âmbito, periodicidade, procedimentos e normas de referência, bem como quanto aos requisitos aplicáveis às entidades auditoras."

Anexo 2 - Anterior contributo na sequência do Aviso da ANACOM em 10 de Janeiro de 2017

Seguidamente apresenta-se uma transcrição dos contributos enviados pela EDP Distribuição à ANACOM em Janeiro de 2017, no âmbito do Projeto de Regulamento relativo à Segurança e Integridade das Redes e Serviços (Aviso de 10 de Janeiro de 2017).

Comentários Gerais

A EDP Distribuição considera que o trabalho desenvolvido pela ENISA em conjugação com os reguladores nacionais, com enfoque na identificação de medidas e respetiva operacionalização harmonizada para provisão do artigo 13ª da Diretiva 2002/21/EC na redação da Diretiva 2009/140/EC, materializada no documento "*Technical Guideline for Minimum Security Measures*", constitui uma especificação base adequada de referência para o presente regulamento.

Deste Guia, tomamos boa nota da sua abordagem holística, nomeadamente através dos domínios definidos e respetivas ações: governo e gestão de risco, segurança no âmbito dos recursos humanos, segurança de sistemas e instalações, gestão de operações, gestão de incidentes, gestão de continuidade de negócio, monitorização e auditoria e testes.

A análise do presente projeto de Regulamento permitiu identificar um conjunto de clarificações e sugestões que julgamos contribuir para a sua melhor abrangência e estímulo à cooperação e articulação entre as empresas e os seus clientes, nomeadamente aqueles que recorrem a serviços no âmbito da operação de serviços e atividades considerados essenciais para a economia e sociedade (referenciados nas alíneas 6 d) i) e 6 d) ii) do Artigo 24º).

Nesta conformidade, passamos a expor os seguintes comentários e sugestões de ordem geral:

Âmbito de aplicação do Regulamento

Tratando-se, na sua génese, de conferir uma orientação no sentido do estabelecimento de um sistema de gestão de risco das redes e de informação, consideramos pertinente reforçar a necessidade das empresas adotarem uma politica de segurança de informação e de um sistema de gestão de risco, nomeadamente com a adoção de norma com aceitação internacional, facilitando a uniformização de sistemas e a adoção de práticas de reporte e de auditoria aceites

internacionalmente. As referências e normas a adotar poderiam ser estabelecidas nos mesmos termos do Artigo 30.º, relativo a normas de referência para realização de Auditorias.

A definição do âmbito de aplicação do Regulamento deve, em nossa opinião, refletir de forma mais clara o vetor de segurança, nomeadamente definindo incidente como um evento que pode originar uma quebra de segurança ou a perda de integridade na operação das redes e serviços. Considerando-se quebra de segurança a violação das propriedades de confidencialidade, integridade e disponibilidade de ativos tecnológicos ou de informação.

Desta forma, por definição, a declaração, identificação e notificação de um "incidente" não deverá estar limitada ao impacto em termos de duração e volume de assinantes ou acessos afetados, tal como está descrito nos artigos 24.º e 25.º.

O modelo pode também beneficiar de uma melhor clarificação da figura e contexto conferido aos clientes de serviços de comunicações eletrónicas que integram tais serviços no âmbito de operações e serviços essenciais de que são responsáveis.

Como exemplo, no que concerne à EDP Distribuição, e atendendo à elevada interdependência dos serviços essenciais de distribuição de eletricidade e de comunicações eletrónicas, consideramos de elevada importância que o Regulamento estabeleça um enquadramento que que favoreça a cooperação e a partilha de informação, refletindo-o nos mecanismos de comunicação, promovendo o alinhamento dos contactos permanentes para a comunicação de incidentes e acompanhamento das medidas de mitigação e de correção.

Proteção de dados de clientes e controlo de privacidade

Numa ótica de segurança e integridade, a definição de ativos deve ser sistematizada, considerando na classificação proposta todos aqueles cuja exploração, violação ou falha possam ter um impacto negativo na segurança ou na continuidade do funcionamento das redes.

Assim, aquela definição deve também incluir ativos de informação das empresas, bem como relevar dados/informação referente a configurações, localizações, palavras de acesso e outros, referentes às soluções e serviços de clientes, incluindo-os no sistema de gestão de risco.

Um acesso indevido ou que atinja a integridade e confidencialidade desta informação, podendo não originar um impacto nos serviços, deve ser considerado como incidente e despoletar a necessária coordenação com o cliente para a ativação de medidas de controlo e de mitigação.

De modo a prevenir estas situações, deve assegurar-se a implementação de mecanismos de proteção de dados, nomeadamente pessoais, sobre a informação veiculada através das redes e serviços, incluindo os dados armazenados e processados pelo operador, o controlo de acesso na

ótica do *as-needed-basis* e técnicas de anonimização de informação.

Por conseguinte, incidentes afetando o ativo "informação" devem ser igualmente reportados aos clientes e sujeitos aos procedimentos do sistema de gestão de risco e posterior acompanhamento das medidas implementadas.

Comentários específicos

Apresentam-se seguidamente os comentários da EDP Distribuição, procurando traduzir os comentários gerais nos artigos do projeto de Regulamento constantes no Aviso n.º 459/2017, publicado pela ANACOM a 10.01.2017.

Artigo 1º - Objeto

Sugere-se que seja incluída uma referência sobre a adoção de Sistema de Governo e Gestão de Risco, por adoção de norma internacional, sugerindo aquelas que são identificadas pela ANACOM onde se incluirá a 27000 que tem vindo a ser adotada na Europa.

Artigo 3º - Definições

Sugere-se que seja incluída a definição de entidades operadoras de serviços essenciais que recorrem a serviços de comunicações eletrónicas disponibilizado pelas empresas.

Artigo 4º - Cooperação e partilha de informação

Na redação atual a referência a cooperação e partilha de informação é exclusiva ao setor das telecomunicações. No entanto, esta abordagem deveria ser aberta a outros setores, nomeadamente aos operadores de serviços essenciais e que também configuram a preocupação referida em b) dependência/interdependência, como é o caso da energia elétrica.

Artigo 5º - Obrigações das empresas

Em consonância com os números 2 e 3 deste artigo, sugere-se que seja explicitada a orientação para a adoção de uma politica de segurança de informação e de um Sistema de Governo e Gestão de Risco.

Artigo 7º - Classificação de ativos

Sugere-se que a classificação de ativos considere o ativo "informação", nomeadamente a

interna à empresa e a informação relativa à configuração e acesso aos serviços dos Clientes, como fator de integridade dos serviços prestados aos Clientes, com o consequente enquadramento no Sistema de Governo e Gestão de Risco.

Artigo 9º - Gestão dos riscos

Conforme recomendação ENISA, as empresas deveriam adotar um sistema de Governo e Gestão de Risco, de preferência internacional, no âmbito do qual é efetuada análise dos riscos, gestão e *ownership* de Risco adequadas.

Artigo 21º - Ponto de Contacto Permanente

Sugere-se que sejam estabelecidas regras sobre a comunicação e estabelecimento dos necessários protocolos com Clientes que pela dimensão ou criticidade devem merecer um acesso agilizado, nomeadamente aqueles que são responsáveis por serviços essenciais.

Artigo 24º - Circunstâncias

- Em relação ao projeto de regulamento e atendendo ao previsto na Diretiva NIS que define operadores de serviços essenciais, figura aplicável à EDP Distribuição, atendendo que estes incorporam comunicações eletrónicas como parte dos respetivos processos críticos, entendemos que o dever de comunicação/notificação de violações de segurança ou perdas de integridade da rede deverá no futuro ser alargado àqueles Clientes/operadores, distinguindo-os dos conceitos de público em geral e de assinante.
- No que se refere ao n.º 2 deste artigo, a condição de notificação obrigatória de causa de perturbação grave deve ser complementada com uma definição de maior abrangência (ver ponto 8), que inclua incidentes detetados no domínio dos ativos cadastrados sem que obrigatoriamente tenha havido perturbação na continuidade dos serviços, como por exemplo, a perda de confidencialidade de informação de rede de cliente. Mais se informa que esta classificação de empresas/clientes especiais está mencionada na alínea 6 d) i) e 6 d) ii) deste artigo.
- Considerando a dependência dos serviços críticos de empresas/clientes especiais das redes e serviços de comunicações eletrónicas, reforçamos a necessidade de adequação do dever de notificação em caso de violação de segurança ou perda de integridade, permitindo ao cliente uma rápida resposta no sentido de controlar ou mitigar o impacto do incidente.
- No que concerne à EDP Distribuição, e atendendo à elevada interdependência dos serviços essenciais de energia e comunicações eletrónicas, consideramos de grande importância o estabelecimento de uma autonomia de funcionamento dos serviços de comunicações adequada e que tenha em conta a continuidade de serviço que as redes elétricas devem assegurar. Consideramos que a fixação destes requisitos deveria ser estabelecida pela ANACOM em articulação com a ERSE.

- O formato e o prazo de comunicação deverão responder às orientações emanadas duma determinada norma, promovendo a cooperação e ação coordenada no âmbito dos incidentes de segurança, onde se exige a criação de CSIRT.
- Um incidente de segurança pode ser dirigido a serviço/cliente em particular, eventualmente detetado sem que tenha ocorrido disrupção do serviço. Os incidentes com ou sem impacte disruptivo deveriam ser comunicados aos clientes de forma a garantir coordenação das necessárias ações subsequentes para garantia da segurança e integridade dos Serviços.
- Quebras de segurança podem afetar o nível de risco sem que se concretize disrupção grave/alargada, pelo que o Sistema de Governo e Gestão deveria enquadrá-los para efeitos de controlo em sede de auditoria, com notificação ao(s) utilizadore(s) dos serviços afetados ou que foram alvo de ação.

Artigo 26º - Condições

- Este artigo considera o dever de informação dirigido ao público em geral e condicionado a uma condição quantitativa de impacte. Consideramos importante enquadrar incidentes de segurança, mesmo que de afetação individual de clientes ou clientes operadores de serviços essenciais, com ou sem impacte na continuidade do serviço.
- Neste projeto de Regulamento, um ataque à rede de cliente pode ser “mascarado” como incidente técnico por não atingir as métricas globais apresentadas como limiares para falha de Integridade (a ENISA recomenda a comunicações de Incidentes sem critério de impacto verificado), situação que entendemos não ser desejável.
- Através do Ponto de Contacto Permanente (Artigo 21º) deverá assegurar-se a pronta comunicação de incidentes de segurança ou de falha de integridade dos Serviços.