Comentários da OPTIMUS – Comunicações, S.A à consulta sobre a notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações electrónicas e respectiva divulgação pública

I. Introdução

O presente documento visa apresentar os contributos da OPTIMUS – Comunicações, S.A (OPTIMUS) ao sentido provável de decisão do ICP – ANACOM sobre a notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações electrónicas e respectiva divulgação pública (SPD).

As propostas agora alvo de comentários pretendem: i) definir as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes, em conformidade com o disposto no nº2 do artigo 54º C da Lei nº 5/2004, de 10 de Fevereiro de acordo com a redacção que lhe foi conferida pela Lei nº 51/2011, de 13 de Setembro (LCE); e ii) especificar os incidentes de segurança que, no interesse do público, devam ser publicamente divulgados pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações electrónicas acessíveis ao público nos termos previstos na alínea b) do artigo 54.º-E da LCE.

Conforme destacado no SPD, as matérias associadas à segurança e integridade das redes e serviços têm merecido particular atenção por parte do ICP-ANACOM, com a promoção de Workshops e Estudos, assim como através do acompanhamento dos desenvolvimentos a nível internacional, com particular destaque para a actividade desenvolvida pela Agência Europeia para a Segurança das Redes e da Informação (ENISA), na sequência da importância atribuída a estas matérias ao nível das instituições comunitárias.

Esta posição quanto à extrema relevância da segurança e a integridade das redes é partilhada pela OPTIMUS, em particular, e pelos operadores, em geral. Por isso mesmo, e no caso da OPTIMUS foram implementados diversos procedimentos internos de garantia e prevenção de incidentes de segurança, nomeadamente, relacionados com a interrupção de serviço.

A prioridade da segurança e integridade é consubstanciada em diversas vertentes, incluindo a existência de serviços com arquitecturas de rede resilientes, de processos de gestão de incidentes/crise, o desenvolvimento de Planos de Contingência de rede, a existência de uma área dedicada à Gestão de Risco

que dinamiza e supervisiona iniciativas de continuidade e segurança e ainda a existência de Auditorias Internas a processos e sistemas da rede comunicações.

Os operadores de comunicações electrónicas assumem-se como os primeiros interessados na minimização de incidentes que afectem a segurança ou integridade das suas redes e, como referido, estão atentos e adoptam proactivamente as melhores práticas no sentido de alcançar aquele objectivo.

Assim sendo, a OPTIMUS considera positiva e de grande utilidade a discussão alargada e aberta das propostas concretas do regulador neste domínio com os operadores, de modo a incorporar a experiência adquirida com a implementação dos procedimentos definidos internamente neste domínio. É com base neste enquadramento que se apresentam de seguida um conjunto de comentários gerais e específicos às propostas apresentadas.

II. Comentários gerais

Tal como já aludido, os operadores de comunicações em geral consideram de primordial importância a salvaguarda da integridade e seguranças das suas redes.

Deste modo, há abertura e interesse na adopção de medidas adicionais que visem reduzir a ocorrência de incidentes que afectem a integridade e continuidade da prestação dos serviços de comunicações, o que, de acordo com o entendimento da OPTIMUS, constituirá o objectivo do ICP - ANACOM com o processo agora em curso. Importa, todavia, realçar a necessidade de as medidas regulatórias que venham a ser definidas não serem absolutamente disruptivas face à prática da indústria.

Adicionalmente é imprescindível que essas medidas sejam claras, devidamente fundamentadas face aos objectivos pretendidos e que o papel a desempenhar por todos os intervenientes esteja explícito. Sendo que este último ponto releva, como se verá mais adiante, para a definição concreta dos procedimentos de notificação a definir.

Ora, constata-se que das propostas apresentadas não decorre qual o tipo de intervenção que o ICP-ANACOM irá ter no âmbito dos incidentes relativos a violações de segurança ou perdas de integridade, designadamente na sua resolução.

Em concreto, os documentos colocados em consulta não esclarecem se o regulador pretende ter um papel interventivo na resolução dos incidentes reportados ou se o papel a desempenhar pelo ICP-ANACOM será restrito à recolha da informação, análise e consequentemente notificação dos incidentes relevantes à ENISA e articulação, se necessária, com outros congéneres europeus, em linha com aquela que foi a opção adoptada pelo regulador britânico (OFCOM)[1].

A clarificação do nível da intervenção que o regulador pretende assumir durante um incidente tem a maior relevância na definição dos parâmetros, prazos e demais obrigações de notificação a impor aos prestadores de serviços de comunicações electrónicas. Por exemplo, caso o regulador não tenha uma intervenção activa na resolução do incidente, não se justifica a imposição de obrigações tão exigentes para os prazos de notificação. Bastará obter a informação *a posteriori*, inclusive após a resolução do incidente. Note-se que a recepção da informação após a resolução do incidente também não coloca em causa o exercício das competências da ANACOM respeitantes ao acompanhamento e supervisão do mercado.

Em conformidade com o artigo 5º da LCE, as determinações da ANACOM sobre esta matéria deverão ser razoáveis, fundamentadas e proporcionais face aos objectivos que visam atingir. Acontece que perante a informação disponibilizada, na opinião da OPTIMUS, as (exigentes) obrigações de notificação propostas não preenchem aqueles requisitos.

De facto, a serem adoptados os parâmetros constantes do presente SPD, nomeadamente quanto aos patamares mínimos de clientes/acessos e duração expectável, o ICP-ANACOM poderia receber uma quantidade elevada de notificações dos operadores que decorrem naturalmente das incidências da actividade de gestão de uma rede que está sujeita a falhas de equipamentos e serviços, mas que não são verdadeiramente significativas do ponto de vista nacional, nem para o público. Para além disso, recepção de um elevado número de notificações seria contraproducente para o regulador porquanto dispersaria a atenção dos eventuais incidentes efectivamente relevante e, em simultâneo, imporia um ónus desproporcional e sem fundamento para os operadores.

O âmbito dos serviços e os parâmetros a considerar para notificação deverão reflectir circunstâncias de falha que são realmente fundamentais e críticas e que afectem a segurança nacional ou representem situações de emergência.

[1] Ofcom guidance on security requirements in the revised Communications Act 2003, Implementing the revised EU Framework, 11 de Maio de 2011, p. 18.

Por fim, salienta-se que o ICP – ANACOM na avaliação da proporcionalidade e razoabilidade das medidas a impor não poderá deixar de ponderar os custos de implementação e de operação. As obrigações que venham a ser definidas não podem implicar a realização de investimentos avultados, nem um acréscimo considerável dos custos administrativos para os operadores, sem que sejam claros os seus benefícios para o mercado, em geral, e para os utilizadores, em particular. Este aspecto é particularmente relevante no actual contexto macroeconómico e financeiro caracterizado pela queda da actividade económica e dificuldades de acesso a financiamento.

III. Comentários específicos

Conceito de Incidentes e âmbito dos serviços a notificar

a) Conceito de incidentes

A redacção da decisão final deverá especificar explicitamente que apenas serão alvo de notificação as violações de segurança ou perdes de integridade que impliquem a interrupção da prestação de serviços de comunicações electrónicas, isto é, incidentes que afectem a continuidade/disponibilidade do serviço. Este entendimento está em linha com o conceito de incidentes e violações de segurança vertido nas Technical Guidelines da ENISA (ponto 4.1): Scope of incident reporting: "*Network and Information security incidents having a significant impact on the continuity of supply of electronic communications networks or services*" e com a definição adoptada pela OFCOM para o efeito "*we consider an "incident" to be an information or network security event which has a significant impact on the continuity of the communications network and services*".

Esta clarificação é particularmente relevante porquanto no documento em consulta é referido o reporte de incidentes que provoquem "perturbação grave no funcionamento". Ora, no limite, esta situação poderia ser interpretada como uma exigência de notificação de incidentes relacionados com *LoS (Level of Service)* e *QoS (Quality of Service)*, o que, de acordo com o entendimento da OPTIMUS, não corresponde ao pretendido neste âmbito. Os níveis de qualidade de serviço são aferidos, designadamente pelo regulador, através de outros mecanismos.

Para além disso, a obrigação da notificação de incidentes que afectem temporariamente a qualidade de serviço ou parcialmente o nível de serviço não deverá ser considerado neste âmbito, sob pena de ser

introduzida complexidade e subjectividade na avaliação dos incidentes, indo para além dos objectivos pretendidos com o processo de notificações que está agora a ser definido, ou seja, a aferição se um serviço está interrompido ou não e quando tal interrupção tenha um impacto significativo.

b) Âmbito dos serviços associados

A deliberação do regulador deverá também explicitar o âmbito dos serviços cuja interrupção exige notificação, sendo que a OPTIMUS considera que esse âmbito deverá ser alinhado com o definido no documento da ENISA relativo aos procedimentos de notificação *Technical Guideline on Reporting Incidents*. Em concreto, os serviços de voz abrangidos devem ser os relativos aos serviços básicos de telefonia por acesso fixo ou móvel. Os serviços de dados abrangidos devem ser os serviços primários relativos a Internet e, SMS, sendo que os serviços secundários que correm sobre estes deverão ser excluídos dos processos de notificação.

Os serviços cuja interrupção exija a notificação deverão ser significativos e relevantes do ponto de vista dos objectivos da sua utilização. Por exemplo, mensagens multimédia (MMS), serviço de *voice mail*, serviços de subscrição de alertas/músicas/jogos, serviços de portais multimédia, serviços de TV por IP no telemóvel, serviços de dados empresariais desenvolvidos à medida para determinados clientes, não se consideram relevantes para efeitos de notificação neste âmbito.

No que respeita ao serviço de *e-mail*, a proporção deste serviço fornecido directamente pelos operadores de comunicações pode ser considerada residual face ao que é actualmente suportado maioritariamente "na nuvem" (por exemplo através de serviços como Gmail, Facebook, etc), pelo que não é relevante considerá-lo no âmbito dos serviços a notificar. Acresce que a possibilidade de utilizar este serviço já estará abrangida no âmbito do serviço de acesso à Internet.

Também os serviços de televisão deverão ser excluídos de notificação, uma vez que não se enquadram no espírito e objectivos do presente processo de decisão, sendo que este serviço não foi considerado como relevante pela ENISA.

Mais adiante neste documento será apresentada uma proposta concreta de tabela com os agrupamentos de serviços que devem estar no âmbito das notificações e os seus patamares mínimos que, no entender da Optimus, justificam as notificações à ANACOM e ao público.

A. Notificações ao ICP – ANACOM

Circunstâncias

a) Interpretação dos patamares

A interpretação da tabela apresentada com os patamares de reporte não é clara, carecendo de explicitação a forma de aplicação dos critérios aí incluídos. Por exemplo, não é claro se os critérios são cumulativos e/ou como deverão ser conjugados. Considerando um exemplo concreto: um incidente que tenha duração de 20 minutos e afecte 400.000 assinantes/acessos deve ser considerado para efeitos de notificação?

A Optimus está firmemente convencida que a verificação dos patamares é cumulativa, ou seja, apenas a verificação dos patamares mínimos dos diferentes critérios relevantes exigem notificação. Salienta-se que foi esta a opção seguida pela OFCOM[2]. No entanto, face à relevância deste aspecto ta interpretação deve ser inequívoca na redacção da decisão final.

b) Adequação dos patamares

Na definição dos patamares de notificação deverá ser considerado o impacto dos incidentes tendo também em conta a experiência e expectativas dos clientes. Não se antecipam motivos para definir critérios de notificação ao regulador ou de divulgação ao público, que não estejam alinhados com a prática do mercado, com a experiência dos utilizadores e com os requisitos de resiliência adicionais eventualmente contratados.

Por exemplo, revela-se injustificado considerar como relevante um incidente que afecte o serviço durante 2 horas se os clientes empresariais tiverem contratado e aceite um nível de interrupções de serviço até 4 horas. Naturalmente que isto não prejudica todo o empenho dos operadores em minimizar as interrupções de serviço independentemente dos níveis de interrupção que tenham acordado com os seus clientes. Por isso mesmo, reitera-se, que os operadores implementam internamente processos de gestão de incidentes e tomam decisões de investimento em resiliência da infraestrutura e plataformas de rede que estão alinhadas com esse objectivo.

[2] *These thresholds consider both the duration of the outage and the number of end customers affected. If both the number and duration thresholds are exceeded, or are expected to be exceeded, during the outage, then it should be reported to Ofcom* - Ofcom guidance on security requirements in the revised Communications Act 2003, Implementing the revised EU Framework, 11 de Maio de 2011, p. 21

De qualquer modo, a OPTIMUS considera injustificada a notificação de incidentes cujo impacto tenha uma duração inferior a 4 horas, na medida em que tais interrupções não se consideram significativas nem do ponto de vista da nacional, nem europeu.

Para além disso, a detecção de um incidente cuja duração seja de 15, 30 ou mesmo 60 minutos levanta algumas questões quanto à sua possível operacionalidade/exequibilidade. Pois, alguns daqueles incidentes poderão não ser sequer detectáveis actualmente. O que significa que a imposição de níveis tão exigentes em termos de duração dos incidentes iria exigir da parte dos operadores um esforço adicional na alocação de recursos e adaptação de procedimentos, sem que sejam claras as mais-valias associadas à notificação de incidentes com durações tão reduzidas.

A OPTIMUS entende ainda que a conjugação entre as variáveis assinantes/acessos ou área geográfica para avaliar a dimensão do impacto torna o processo demasiado exaustivo e complexo, sem que se antecipe valor acrescentado nesse processo.

Assim, sugere-se que, para além do patamar relativo à duração, seja apenas considerada a variável "assinantes/acessos". Esta sugestão ganha maior acuidade se for tido em conta que presentemente não estão implementadas ferramentas que permitam calcular a área geográfica (em km^2) afectada por este tipo de incidentes, nem se prevê que estejam disponíveis a curto/médio prazo. De referir que este critério não foi tido em consideração pela OFCOM na definição dos critérios de notificação, sendo apenas considerados para o efeito o tipo de serviços, a duração do incidente e número de clientes afectados [3].

Ainda no que que respeita à variável assinantes/acessos importa desde já salientar que existem situações em que, por restrições técnicas, não é possível determinar o número de assinantes/acessos impactados por uma falha de serviço, sendo necessário o recurso a estimativas. Por exemplo, no caso de um incidente tornar o acesso móvel indisponível, não é possível determinar quantos clientes foram realmente afectados durante o período de interrupção do serviço. Esta determinação é feita apenas por estimativa com base em dados históricos de utilização do serviço.

No caso de um incidente tornar o acesso fixo indisponível, só é possível estimar o universo de acessos que o nó de rede afectado serve, no entanto não é garantido que os clientes estivessem a usar o serviço ou tivessem tentado usá-lo durante o período de falha.

[3] Ofcom guidance on security requirements in the revised Communications Act 2003, Implementing the revised EU Framework, 11 de Maio de 2011, p. 21 "Reporting thresholds for different types of networks and outages"

De registar ainda que se o incidente acontecer ao nível das plataformas *core* da rede, a avaliação do número de utilizadores afectados requer uma análise morosa e exaustiva, pelo que não é compatível com a notificação ao regulador no prazo de minutos ou escassas horas. Refira-se que em algumas situações anteriores foi necessário cerca de 1 dia útil para apuramento dos clientes afectados.

No seguimento do exposto, a Optimus apresenta nas conclusões deste documento uma tabela que sumaria os critérios de notificação – relação entre a duração da interrupção e o número de assinantes/acessos afectados – que considera razoáveis e proporcionais.

c) Chamadas de emergência

Em relação às situações com impacto no acesso ao número único de emergência (112), a definição proposta pelo ICP-ANACOM: "*que afectem a entrega… quer directa quer indirectamente* " é demasiado ampla. Numa interpretação literal, todas as falhas no serviço fixo com o mínimo de 15 minutos numa área teriam que ser notificadas, pois sempre que existir uma falha de acesso ao serviço as potenciais chamadas para o 112, tal como as restantes, deixarão de ser concretizadas.

No caso das redes móveis se a rede de um operador estiver indisponível as chamadas param as 112 serão encaminhadas pela rede de outro operador móvel. Esta funcionalidade é disponibilizada automaticamente nas redes e nos terminais móveis dos utilizadores. Por isso mesmo, considera-se que os serviços móveis deverão ser excluídos do âmbito destas.

Face ao exposto, a Optimus é de opinião que na decisão final deverá ser explicitado que apenas deverão ser considerados para efeitos de notificação ao regulador os incidentes que interrompam a entrega directa de chamadas a um ou mais PSAP, destinadas ao número 112 e originadas na rede fixa, quando a duração expectável do incidente seja igual ou superior a 1 hora.

d) Incidentes com impacto acumulado

A notificação de incidentes com impacto acumulado, nos termos propostos pelo regulador, revela-se inexequível, uma vez que não existem processos, nem sistemas capazes de registar e verificar os incidentes de forma a analisar as suas causas/efeitos e determinar se contribuíram para o mesmo tipo de incidente, nem efectuar a consolidação desses resultados para obter o efeito acumulado.

Acresce que, em tese, poderão estar em causa incidentes com uma duração de minutos, que cumulativamente poderiam atingir os níveis mínimos de duração definidos pelo regulador, implicando a notificação de um incidente que isoladamente não teria impacto relevante. Por exemplo, a falha acumulada de diferentes estações base (BTS) ao longo de um mês até poderia atingir o patamar mínimo de notificação, mas implicaria uma notificação sobre a falha do serviço de voz móvel relativa a incidentes isolados que não têm qualquer significado.

Não se encontrando relevância para a notificação deste tipo de incidentes solicita-se a sua eliminação do âmbito das notificações.

e) **Incidentes que afectem mais do que uma empresa**

Como ponto prévio, de referir que a interpretação da Optimus é que a "empresa" se refere a operador de comunicações e, consequentemente, o que se pretende cobrir neste ponto são incidentes que tenham impacto em mais do que um operador e, de forma acumulada, atinjam os patamares mínimos de notificação.

A concretização deste critério de notificação implicaria a partilha de informação constante entre operadores quanto aos incidentes registados individualmente para averiguar se a causa afectava mais do que uma empresa e apurar se o impacto acumulado preencheria os requisitos de notificação. Na prática, a imposição deste critério de notificação implicaria a existência de um processo e sistema/aplicação central com capacidade para constantemente receber informação dos operadores e efectuar essa análise. Tal mecanismo não só se mostra complexo, como implicaria a afectação de recursos para operação, gestão e manutenção do mesmo que não se afiguram proporcionais. Ademais, semelhante procedimento levanta questões de confidencialidade porquanto está em causa a partilha de informação sensível.

Finalmente importa referir que a adopção de tal critério de notificação não foi definida pela OFCOM, nem existe orientação forte da ENISA neste sentido, pelo que se sugere a sua eliminação.

f) **Incidentes que se registem em datas especiais**

A execução dos requisitos associados às datas especiais implica um conhecimento prévio dos operadores de um calendário oficial com as datas, eventos, duração, locais e clientes críticos a monitorizar. A ser

implementado este critério deve caber ao regulador o ónus de enviar a todos operadores, com a devida antecedência face à data especial todos os elementos indicados.

Mais, a aplicação deste critério exige alterações pontuais aos processos que o torna de difícil execução. De facto, obrigaria a que nessas datas especiais as tabelas internas para avaliação e notificação de incidentes fossem temporariamente alteradas pelos operadores, o que é complexo do ponto de vista de implementação e acarreta custos operacionais acrescidos.

Pelos motivos apresentados, solicita-se que este critério não seja incluído no âmbito das notificações.

g) Regiões Autónomas

A ENISA nas suas *Technical Guidelines* estipula que incidentes que afectem determinadas regiões como ilhas ou áreas remotas podem ser consideradas de forma particular, mas sem que para tal seja proposto um patamar mínimo de impacto.

O ICP-ANACOM propõe que todos os incidentes de segurança que tenham uma duração superior a 30 minutos sejam considerados para efeitos de notificação. Assim, a ser interpretado *latu sensu* este critério poderia resultar na notificação de uma falha de 30 minutos numa estação base (BTS) móvel ou num distribuidor de acessos cobre (DSLAM) da rede fixa que afecte um número de clientes bastante reduzido (que poderia em termos extremos ser inferior a duas dezenas de clientes).

Face ao exposto, pese embora pelas características particulares das regiões autónomas se entenda a aplicação de critérios distintos, sugere-se a ponderação e reavaliação dos mesmos, tendo em conta a sua adequação e proporcionalidade.

h) Clientes governamentais e entidades relevantes em termos de serviços à sociedade e aos cidadãos

No se refere aos critérios definidos para as entidades governamentais, teria antes de mais que ser definida uma lista oficial de entidades governamentais e regionais a serem consideradas para este efeito. A necessidade de ser definida uma lista aplicar-se-ia também às "outras entidades relevantes em termos de serviços à sociedade e aos cidadãos". Quanto a estas entidades, a sua definição levanta algumas questões, uma vez que genericamente poderiam ser incluídas neste âmbito instituições públicas e privadas de solidariedade.

Acresce que existem alguns obstáculos técnico-operacionais à implementação dessas listas. Por exemplo, obrigaria os operadores a manter em paralelo uma lista interna desses clientes, com os respectivos serviços e localizações. Sucede que os operadores não possuem, hoje em dia, as ferramentas mais adequadas para esse propósito específico. Ainda mais relevante, situações em que não é tecnicamente possível efectuar monitorização e detecção de falhas em clientes concretos/individuais em determinadas componentes de rede.

Ainda a este respeito, a OPTIMUS questiona a relevância do exemplo apresentado relativo ao SIRESP (Sistema Integrado de Redes de Emergência e Segurança de Portugal), já que na sua essência este consiste num sistema que deve ser independente dos operadores comerciais de comunicações, de modo a assegurar o funcionamento de uma rede de emergência autónoma de suporte a forças de segurança, serviços de emergência e outras entidades.

Neste sentido, a falha dos serviços dos operadores não deve impactar o SIRESP, cuja missão, conforme indicado, é precisamente suportar as comunicações críticas dessas entidades relevantes para a sociedade (http://www.siresp.com/utilizadores.html).

Finalmente importa ainda acautelar questões legais quanto ao tratamento diferenciado dos vários utilizadores, dado que, como é do conhecimento do regulador actualmente recai sobre os operadores a obrigação de não discriminação dos clientes finais.

Face ao exposto, a Optimus entende que as ocorrências restritas a clientes específicos não deverão ser incluídas no âmbito das notificações.

Formato e procedimentos

Em complemento às circunstâncias que definem a validade de uma ocorrência para efeitos de notificação, o ICP-ANACOM apresenta um conjunto de propostas relativas ao formato e procedimentos associados ao reporte dos incidentes a serem reportados. Para tal o regulador propõe a notificação dos incidentes por via de correio electrónico (*e-mail*), a necessidade de cooperação entre operadores e a submissão de uma notificação inicial, uma notificação intercalar de seguimento, e, se necessário, uma notificação final.

A OPTIMUS entende que os termos propostos pelo ICP-ANACOM para formato e procedimento de notificação carecem de revisão e ajustamento, tendo como base os já enunciados critérios de adequação e razoabilidade face aos objectivos que subjazem ao presente SPD.

a) Notificação por *e-mail*

Note-se que se o serviço afectado for o serviço de Internet ou de correio electrónico, poderá não ser possível efectuar a notificação até que o serviço esteja recuperado. Assim, deverão ser indicados meios e contactos alternativos. Adicionalmente, os meios de notificação deverão recorrer a mecanismos de autenticação, integridade e não repúdio, como por exemplo a certificação digital. O regulador deverá também garantir que o conteúdo das notificações é salvaguardado.

b) Cooperação entre operadores

A OPTIMUS entende como válido o princípio da cooperação entre operadores, sobretudo na fase de resolução de um incidente que afecte vários operadores. Todavia, os aspectos relativos à detecção, avaliação e notificação não são exequíveis em termos operacionais e levantam questões de partilha de informação confidencial, em linha com referido no ponto II. i)

Presentemente regista-se a existência de cooperação entre operadores quando um incidente requer a intervenção conjunta. No entanto, caso se verifiquem incidentes com a mesma causa externa, por exemplo um incêndio florestal ou problemas de transmissão provocados por um fornecedor de fibra comum, não é prática habitual o contacto e partilha de informações entre operadores.

De referir ainda que nos casos onde se verifique a dependência na prestação de serviços entre operadores, por exemplo no acesso indirecto fixo, caso ocorra um incidente na rede do detentor da infra-estrutura, não é possível ao operador de acesso indirecto intervir directamente na sua resolução, nem identificar as causas específicas associadas ao incidente.

Atendendo ao exposto propõe-se a reavaliação desta obrigação, podendo a cooperação entre operadores em matéria de segurança ser conseguida através de outros meios que não impliquem necessariamente a coordenação no âmbito das notificações de incidentes.

c) Identificação das causas

A respeito da identificação das causas associadas, deve ser tido em consideração que quando a interrupção do serviço tem como causa a falha no fornecimento de serviços por uma entidade externa (por exemplo o fornecedor de energia eléctrica ou outro operador), nem sempre é possível obter a curto/médio prazo a informação das causas e do tempo estimado de resolução. Podem ainda existir alguns tipos de incidentes cujas causas nem sempre são determináveis, devido à arquitectura tecnológica de rede implementada, incapacidade de algumas plataformas manterem registos, etc.

d) Dados estatísticos

O ICP-ANACOM refere na proposta que os dados a incluir nas notificações relativamente ao impacto nos utilizadores deverão, sempre que possível, ser consonantes com os dados estatísticos disponibilizados trimestralmente ao ICP-ANACOM. A Optimus solicita esclarecimentos sobre as situações concretas que determinaram a referência neste âmbito às estatísticas remetidas trimestralmente.

e) Notificações

No caso da **notificação inicial**:

- O prazo de 2 horas para notificação é manifestamente insuficiente, pelas razões de impraticabilidade operacional já referidas;
- Considera-se que a notificação deverá ser feita num prazo superior a 4 horas úteis, contabilizadas a partir da detecção do incidente. Importa ressalvar que este prazo de 4 horas úteis será exequível apenas se o âmbito dos serviços a notificar estiver claramente delimitado e as durações de falha estiverem alinhadas com a proposta da OPTIMUS quanto aos patamares de notificação;
- Importa referir que existem processos de comunicação internos ao operador para gestão de incidentes/crise, com intervenção necessária de várias áreas da organização e diferentes níveis hierárquicos, que necessitam no mínimo de 2 horas para começarem a ser executados, de modo a que posteriormente possam ser emitidas notificações para entidades externas ao operador. Este é mais um aspecto que milita a favor da notificação num prazo superior a 4 horas úteis;
- Acresce que o nível de prontidão em períodos de noite, fins-de-semana e feriados dos elementos da empresa com capacidade para decidir e executar os processos de comunicação e gestão de crise necessários à notificação (que não os elementos técnicos de prevenção) não pode ser o mesmo

que é exigível durante o período diurno em dias úteis. Este facto também levanta questões de cumprimento da legislação laboral.

No que respeita à **notificação final**:

- Sugere-se que a "notificação final" seja designada de "Relatório de Incidente"
- Note-se que a notificação deste relatório de incidente deve ter associado um prazo mais alargado, dado que, conforme referido, para certos incidentes o prazo de 10 dias úteis é insuficiente para avaliação e identificação de todos os parâmetros de reporte. Esta situação é sobretudo pertinente quando existem dependências de informações a serem obtidas junto de terceiros (por exemplo fornecedores) ou em situações em que as causas se revelem de difícil precisão;
- Relativamente ao conteúdo, note-se que tendo em conta a extensão de informação solicitada, caso os critérios referidos no pontos alusivos às circunstâncias de reporte não forem alterados de modo a tornar o âmbito dos serviços perfeitamente delimitados, bem como as durações e o número de assinantes/acessos menos exigentes, então os operadores vão ter de canalizar de forma permanente os seus esforços e recursos para a elaboração de relatórios de incidente, desviando o *focus* do fundamental que é assegurar a manutenção da rede e dos serviços aos clientes.

No que respeita à notificação **intercalar**:

- A OPTIMUS entende que não se justifica que esta notificação intercalar seja obrigatória. A necessidade de envio deverá ser alvo de avaliação por parte do operador em função das características do incidente, nomeadamente, da sua duração. Adicionalmente, a relevância da notificação intercalar também dependerá da intervenção que o ICP – ANACOM pretende ter durante a resolução de incidentes. A OPTIMUS entende que a notificação intercalar poderá acontecer, por exemplo, quando o operador considerar relevante actualizar a informação transmitida anteriormente ou para informar sobre a resolução do incidente. Nas situações em que a notificação inicial é enviada depois da resolução do incidente, naturalmente, não faz sentido a existência da notificação intercalar;
- A este respeito refira-se também a opção do regulador britânico de não incluir uma notificação intercalar, compreendendo unicamente o envio de uma notificação inicial e, se a duração e impacto do incidente justificarem o reporte à ENISA, o envio um relatório final [4];

[4] *In some cases, Ofcom will request a follow up report in relation to a particular incident, to better understand the nature of the incident. This may be because we consider the incident to be reportable to ENISA in our annual summary report and we therefore require sufficient additional information to complete the required fields in this report. Where*

- O prazo para envio da notificação intercalar opcional deverá ser até ao final do dia útil seguinte ao dia em que o incidente ficou resolvido, em linha com o indicado no SPD.

B. Notificações ao Público

a) Condições de divulgação

Como ponto prévio, de salientar que os operadores já possuem processos de comunicação reactiva para esclarecer os clientes quando estes contactam os operadores por chamada telefónica ou por *email* com questões sobre falha de serviços. Este tipo de processos tem a vantagem de passar apenas a informação precisa e necessária aos clientes afectados e não a todos os clientes ou ao público em geral, para além de ser adaptada ao serviço prestado a cada cliente.

A definição das situações concretas que justificam uma comunicação proactiva deve caber, caso a caso, ao ICP-ANACOM, sendo de destacar que esta foi a opção adoptada pelo regulador britânico. Esta divulgação deverá ter em consideração a relação entre os riscos e benefícios associados, não podendo deixar de ser considerado neste âmbito que a divulgação generalizada e sistemática de incidentes poderá criar "alarmismo" desnecessário nos clientes e no público em geral e poderá contribuir, injustificadamente para a descredibilização do sector. Por exemplo, clientes podem ser notificados sobre situações que afectam serviços que nem sequer usam ou que usam muito pontualmente.

Para além disso, em alguns tipos de incidentes poder-se-á estar a revelar informação ao público sobre falhas de rede ou vulnerabilidades provocadas pelo incidente cuja divulgação acarreta mais riscos do que benefícios. A indicação do prazo expectável de resolução poderá também potenciar situações de abuso por clientes. Ademais, este procedimento poderá incitar a uma grande quantidade de clientes a tentar verificar constantemente se a rede/serviço está disponível, contribuindo para uma sobrecarga da rede e maior demora na reposição do serviço para os clientes que realmente necessitem de os utilizar naquele momento.

---

possible, we will request additional information only after the incident has been resolved and analysed, to avoid impact on management of the incident and to improve the quality of data available - Ofcom guidance on security requirements in the revised Communications Act 2003, Implementing the revised EU Framework, 11 de Maio de 2011, p. 32

Neste sentido, a OPTIMUS considera desajustada e infundamentada a opção do regulador em definir critérios/patamares de notificação ao público que sejam equivalentes aos usados nas notificações ao regulador. A OPTIMUS que a divulgação ao público se justifica apenas nos casos onde a interrupção e o número de clientes afectados tenham um impacto relevante em termos nacionais.

Adicionalmente, sempre que se registem incidentes que atinjam os patamares mínimos para notificação, os operadores devem acompanhar a notificação ao regulador com a indicação dos riscos inerentes à divulgação pública deste incidente. Com base nos dados da notificação enviados pelo operador, deverá ser da responsabilidade do regulador a decisão da divulgação de, face aos riscos e benefícios da situação em concreto, se justifica a sua divulgação ao público.

De salientar que se apresenta nas conclusões deste documento uma tabela que sumariam os critérios de notificação – relação entre a duração da interrupção e o número de assinantes/acessos afectados – que a Optimus considera razoáveis e proporcionais.

b) Prazos de divulgação

A divulgação ao público no prazo de 1 hora apresenta-se como irrealista do ponto de vista do tempo necessário à execução dos processos internos de gestão e comunicação de incidentes/crise e de canalização de esforços para a sua resolução. Também do ponto de vista dos utilizadores, tendo em conta a experiência dos operadores, a notificação no prazo de 1 hora se mostra desnecessariamente exigente.

Atendendo aos prazos sugeridos para notificação ao regulador, e num sentido de uniformização e simplificação dos procedimentos, sugere-se que o prazo de divulgação ao público seja de 4 horas úteis, contabilizadas a partir da detecção do incidente e após aprovação do regulador e a devida comunicação ao operador.

c) Meios de divulgação

No que respeita à forma de divulgação, a obrigatoriedade por parte dos operadores da publicação dos incidentes na página electrónica, especialmente a manutenção de um histórico de 6 meses de incidentes, deve ser eliminada, pois pode ser contraproducente face aos riscos de interpretações danosas, aproveitamentos sensacionalistas pela comunicação social ou ainda aproveitamento malicioso por terceiros para exploração de potenciais vulnerabilidades das redes de comunicações electrónicas.

d) Conteúdo da informação

No que respeita ao conteúdo das notificações ao público, a informação a disponibilizar deve ser "esclarecedora para o público e tão precisa quanto possível" face às circunstâncias específicas do incidente. Por exemplo, a informação a disponibilizar deverá ser esclarecedora, mas deverá ter o grau de detalhe adequado em função de uma análise custo/benéfico a realizar em cada situação. Com efeito, a divulgação de informação não poderá implicar um aumento dos riscos, sem que existam objectivamente benefícios para os utilizadores.

Prazo de implementação

O prazo definido pelo ICP-ANACOM no seu sentido provável de decisão, 30 dias, é manifestamente insuficiente, estando em causa a implementação de procedimentos complexos e onerosos de adaptação face aos actualmente implementados pelos operadores para detecção e reporte de incidentes de segurança.

Sugere-se que, no mínimo, seja definido um prazo de 6 meses para implementação dos procedimentos após a divulgação da decisão final.

IV. Conclusão

A OPTIMUS entende que o SPD deverá ser alvo de ajustamentos em conformidade com os princípios da razoabilidade, fundamentação e proporcionalidade, nomeadamente no que respeita à concretização e adequação dos critérios que definem a relevância de um incidente para efeitos de notificação. Ademais, a OPTIMUS entende como primordial a definição clara e inequívoca do âmbito e serviços a serem abrangidos por esta notificação, sendo sugerido que este seja restrito aos serviços percebidos como críticos para o mercado e utilizadores finais.

No que se refere à decisão de divulgação ao público, a OPTIMUS entende que a mesma deverá ser caber ao ICP-ANACOM, com base em critérios menos exigentes que os definidos para efeitos de notificação ao regulador, e com base numa análise casuísticas que tenha em conta os riscos e benefícios inerentes à divulgação de cada situação em particular.

No seguimento de tudo quanto se expôs, a Optimus propõe na tabela seguinte os patamares, que em justificam a notificação de incidentes:

	Notificação ao ICP-ANACOM		Divulgação ao Público	
Prazo da Notificação Inicial ▶	4 horas úteis		4 horas úteis*	
Serviços ▼	**duração ≥**	**PASP ≥**	**duração ≥**	**PASP ≥**
112 (Fixo)	1	1	4	1
Serviços ▼	**duração ≥**	**clientes ≥**	**duração ≥**	**clientes ≥**
Voz Fixo	1	450.000		
	2	300.000		
	4	150.000		
	6	60.000		
	8	30.000	8	150.000
Voz Móvel; SMS	1	2.250.000		
	2	1.500.000		
	4	750.000		
	6	300.000		
	8	150.000	8	750.000
Internet (Móvel; Fixo)	1	2.700.000		
	2	1.800.000		
	4	900.000		
	6	360.000		
	8	180.000	8	900.000

Legenda:
Duração - duração expectável mínima do incidente em horas (de acordo com a escala da ENISA)
Clientes - número mínimo de assinantes/acessos afectados
PASP - Ponto de Atendimento de Segurança Pública (Centro de Atendimento do 112)
* Divulgação ao público efectuada só após aprovação/decisão da ANACOM
- Incidentes que se enquadrem neste patamar NÃO devem ser notificados
- Incidentes que se enquadrem neste patamar devem ser notificados

Interpretação da tabela:
1º- Identificar o tipo de serviço
2º- Percorrer, linha a linha, os patamares aplicáveis ao tipo de serviço
3º- Se pelo menos uma linha for verdadeira em ambos os critérios (duração + clientes ou PASP), fixar essa linha
4º- Se a linha estiver assinalada a vermelho, então o incidente deve ser objecto de notificação

Por fim, o prazo de implementação de verá ser alargado tendo em que está em causa a implementação de procedimentos novos, para os quais se prevê a necessidade de desenvolvimento de plataformas e sistemas, adaptação de procedimentos, formação e sensibilização de recursos humanos a necessidade de investimentos significativos.