[redacted]

From: [redacted] <[redacted]>
Sent: 14 de março de 2017 21:00
To: regulamento.seguranca@anacom.pt
Cc: [redacted]

Subject: Posição da CT 163 relativamente ao projeto de regulamento criado pela ANACOM(2)

A quem o assunto diz respeito,

O email anteriormente enviado sobre este mesmo assunto correspondia a um documento de trabalho em desenvolvimento e foi enviado inadvertidamente. Pelo facto peço desculpas e peço-vos que considerem este email, em substituição do anterior.

Saudações,
Henrique Santos
(Presidente da CT 163)

Na sequência de um processo de reflexão no seio da CT 163 (que, como é sabido, acompanha o CS 27 do ISO/IEC JTC 1) sobre o "Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas", disponibilizado pela ANACOM e aberto a consulta pública, gostaríamos, antes de tudo, de felicitar a ANACOM pela importante iniciativa e enviar o resultado dessa reflexão que, esperamos, possa contribuir para o melhoramento do documento.

Saudações,
Henrique Santos
(Presidente da CT 163)

---

1 (Comentários gerais). Na ótica da CT e da família de normas 27k, não faz muito sentido falar de "segurança e integridade", já que na definição de Segurança da Informação, a integridade é uma das suas propriedades fundamentais (integridade aparece assim como uma redundância, sendo motivo até para uma interpretação dúbia, relativamente a outros riscos de perda de integridade, que não a física); um exemplo claro dessa confusão realça-se no Art. 2° 1.b.i) quando se refere "Violação de segurança ou perda de integridade", como se a perda de integridade não fosse um problema de segurança; lendo esta descrição coma definição apresentada no Art. 3 1.k) «Segurança das redes e serviços», a incoerência fica ainda mais evidente.

Na realidade parece que o texto foi redigido numa ótica de continuidade de negócio e de segurança física (safety) e na componente da integridade da segurança da informação não é claro se existe algo a proteger. Não sendo claro o objetivo de proteção no âmbito da segurança da informação não se percebem o que é esperado do ISO 27001 e normas conexas.

Sendo a atividade da comissão técnica nacional CT 163 – Segurança em Sistemas de Informação - um espelho da atividade da referida comissão técnica internacional e, como tal, participando na evolução e votando estas normas, faz sentido valorizar a participação de vogais das empresas do setor das comunicações, a quem se dirige este regulamento, bem como dos vogais das empresas auditoras. Assim sendo, ainda que a atividade de normalização seja voluntária, propomos que a lista de normas a publicar identifique as comissões técnicas nacionais que participam na evolução e que votam as normas da lista, nomeadamente a CT 163.

Refira-se ainda que, o procedimento proposto acima, está em linha com o consagrado nos estatutos da ANACOM (Decreto-Lei n.° 309/2001, de 7 de dezembro), nos termos do qual é atribuição desta entidade, "promover a normalização técnica, em colaboração com outras organizações, no sector das comunicações e áreas relacionadas".

2. Art 3 .1 g) A definição entra em conflito com a definição do mesmo conceito na ISO 27001;

3. Art 3 .1 i) Possível confusão com a figura prevista no SEGNAC. Uma vez que a referida legislação é aplicável seria interessante homogeneizar, talvez incluir os requisitos como obrigatórios, nem que seja a qualificação individual prevista no SEGNAC. De acordo com a missão da ANACOM de homogeneizar as normas<,

4. Art 3 .1 m) A definição de vulnerabilidades entra em conflito com o mesmo conceito, tal como definido na ISO 27001;

5. Art 5 .3 a) b) As listas deviam ter uma componente imutável e atualizações anuais.

6. Art. 7 (e Art. 24 3., nomeadamente a tabela aí localizada) A referência a valores absolutos para classificação de ativos, numa altura em que o ciberespaço está em profunda modificação parece-nos perigoso, podendo obrigar a rever o regulamento em consequência de possíveis alterações significativas do número de clientes/nós afetos (a entrada em produção do IPv6 e o desenvolvimento de conceitos como o de IopT); na nossa opinião, seria mais cauteloso usar valores relativos, por exemplo, a classe A podia corresponder a ativos que afetam 80% ou mais do número de assinantes ou acessos afetados;

7. Art 7 .3 Sendo estes os ativos/processos que se pretende gerir na perspetiva da segurança da informação, essa indicação devia estar clara no prêambulo do documento;

8. Art 9 As listas de ameaças/vulnerabilidades ou de riscos a avaliar deviam ter uma componente imutável e uma componente atualizada anualmente pela ANACOM, de acordo com a evolução do enquadramento Nacional;

9. Art 20 O Regulamento devia definir as condições de acesso a responsável pela segurança, nomeadamente qualificações em Segurança de Informação, Segurança Física, Continuidade de negócio e outras relevantes; qualificação enquanto responsável de segurança de acordo com o SEGNAC;

10. Art 28
- Não existe uma obrigação de rotação da equipa auditora, podendo a mesma entidade efetuar a auditoria para sempre. Neste caso existe potencial para conluio entre as partes. O regulamento devia identificar um período máximo de 3 anos para uma entidade auditora poder efetuar auditorias consecutivas;
- O conjunto de requisitos mínimos identificado é demasiadamente lato, o regulamento devia; o regulamento devia fixar o entendimento sobre a competência, nomeadamente certificações internacionais que qualifiquem corretamente a competência dos auditores: CISA,
CISSP, etc., a experiência mínima em anos e em que áreas e com que vínculo às empresas do género; um consultor externo numa operadora não pode ser equiparado a um quadro técnico do próprio operador;
- Existem normas especificas na série ISO 27000 sobre os requisitos de equipa auditora, tempos e metodologias de auditoria que deviam ser adotadas uma vez que refletem as melhores práticas existentes.
- A credenciação SEGNAC devia ser obrigatória

11. Artº 30º Normas de referência no contexto das auditorias, contém também alusão à publicação no "sítio institucional na Internet" da ANACOM de uma lista de normas, especificações e recomendações (ver também comentário 14., em baixo), mas aqui é mencionado o dia 30 de Junho de cada ano. Não encontramos justificação para a diferença de procedimento em relação à fixação da data da publicação da lista de normas referida neste nº2 do art. 30º face à alínea a) do nº 3 do art 5º, pelo que, parece fazer sentido aplicar a mesma data em ambas as situações, ou publicar uma só lista, na mesma data, com referência a todas as normas, especificações e recomendações abrangidas por este regulamento.
A revisão anual aqui prevista é consentânea com a dinâmica dos assuntos do âmbito deste regulamento e, bem assim, com a evolução das normas, nas suas várias versões.
Também aqui, no nº2 do art. 30, não nos parece suficiente a publicação da lista de normas, especificações e recomendações apenas no "sítio institucional da internet", podendo ser considerada a necessidade de

publicação no Diário da República.

12. Artº 31, 1.a) refere normas no âmbito da competência técnica das auditoras e seus colaboradores. A alínea a) do nº 3 do art. 35º refere as não conformidades, detetadas pelo processo de auditoria, relativamente às normas a que alude o artº 30 e, estas duas alusões, conduzem a identificar a comissão técnica ISO/IEC JTC 1 SC 27 como produtora das normas neste âmbito. A título de exemplo recente, identifica-se como estando em votação nesta comissão técnica internacional, os seguintes documentos:
- ISO/IEC DIS 27007 (Ed 2) Information technology -- Security techniques -- Guidelines for information security management systems auditing; e
- ISO/IEC DIS 27021 Information technology -- Security techniques -- Competence requirements for information security management systems professionals

13. Art 37 Não existem sanções específicas previstas no caso de incumprimento, logo não percebemos como a ANACOM pretende garantir a sua execução. Existem as sanções prevista na Lei das comunicações, mas estas não mapeiam diretamente com as exigências do presente regulamento.

14. Concordamos com o texto da alínea alínea a) do nº 3 do art. 5º que refere que a ANACOM publicará, no seu sítio institucional na Internet, uma lista das normas, especificações e recomendações europeias e internacionais existentes sobre a matéria (alínea a). Resta apenas a dúvida de a publicação no "site" da ANACOM ser um meio suficiente. Julgamos que pelo facto de se estar perante um Regulamento, essa lista deveria ser publicada em Diário da República. Segundo a perspetiva da CT 163, a lista de normas da família ISO 27k e com ela relacionadas, com relevância para as listas referidas no Art 5 .3 a) b), são:
- ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems - Overview and vocabulary
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management
- ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on information security controls
- ISO/IEC 27010:2015 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications
- ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
- ISO/IEC DIS 27021 Information technology -- Security techniques -- Competence requirements for information security management systems professionals
- ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity
ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity
- ISO/IEC 27035:2016 Information technology — Security techniques — Information security incident management
- ISO/IEC 27039:2015 — Information technology — Security techniques — Selection, deployment and operation of intrusion detection and prevention systems (IDPS)
- ISO 31000 - Risk management