Contributos para o 2º Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações electrónicas

A. INTRODUÇÃO

A APDSI teve a oportunidade de apresentar à ANACOM um conjunto de contributos aquando da consulta pública de setembro de 2016, que dava início ao procedimento para a elaboração de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas.

Por razões de circunstância não foi possível à APDSI enviar a sua contribuição aquando da consulta pública relativa ao 1º Projeto de Regulamento.

Na sequência da consulta pública recentemente publicada pela ANACOM, a APDSI vem partilhar um conjunto de comentários sobre o 2º Projeto de Regulamento.

Importa clarificar que, em coerência com a nossa anterior contribuição, os comentários que se apresentam não se dirigem a questões técnicas e operacionais, referindo-se a temas de gestão e de governação que consideramos de importância para a segurança de infraestruturas e de serviços críticos.

O Objeto do Regulamento está claramente definido no seu Artigo 1º.

Em resumo:

a) "As medidas técnicas de execução e os requisitos adicionais a cumprir pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações electrónicas acessíveis ao público em matéria de segurança e integridade, ..."

b) "As circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes com impacto significativo no funcionamento das redes e serviços ..."

c) "As condições em que as empresas ... devem divulgar ao público as violações de segurança ou as perdas de integridade das redes com impacto significativo no funcionamento das redes e serviços..."

d) "As obrigações de realização de auditorias à segurança das redes e serviços e de envio do respetivo relatório ..., bem como os requisitos a que devem obedecer as auditorias ..."

É assim natural que algumas das questões que havíamos referido na nossa contribuição inicial não são consideradas (pelo menos de forma direta) pelo Regulamento.

B. COMENTÁRIOS

Tendo em atenção o que referimos atrás relativamente ao Objeto do Regulamento, pensamos que este 2º projeto está muito bem feito e cobre globalmente as questões que referimos na nossa contribuição inicial.

Por simplicidade, apresentamos os comentários seguindo a sequência com que nos referimos anteriormente aos vários temas.

POLÍTICA DE SEGURANÇA

Tópico	Comentário
Existência de uma política de segurança de alto nível que envolva a segurança e continuidade de serviços das comunicações e dos serviços prestados ao público ou a terceiros.	Questão coberta pelo projeto de regulamento. Com o Art.º 17º está-se a confirmar que a empresa tem Política de Segurança.
Esta política deve ser promovida e assumida ao mais alto nível da instituição.	Tendo em conta o Objeto do Regulamento é natural que não haja referência explícita a este aspeto.
A política de segurança deve ser do conhecimento de todos os colaboradores, com o pressuposto de estes orientarem as suas ações e trabalhos de acordo com este conhecimento prévio.	O Art.º 17º refere somente os "...colaboradores-chave..." os quais deverão terem bom conhecimento sobre a política de segurança da empresa. Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto relativamente aos restantes colaboradores da empresa.
Para além da política de segurança global e de topo, devem existir políticas de segurança sectoriais mais detalhadas e profundas para processos de negócio ou ativos, especialmente os mais críticos.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
A(s) política(s) de segurança deverá(ão) ser monitorizada(s), no seu cumprimento, revista(s) e avaliada(s) de forma regular e extraordinariamente na sequência de incidentes ou falhas de segurança.	Para além da responsabilidade da empresa relativamente a esta monitoragem e avaliação, a ANACOM disporá de indicadores que lhe permitem atuar, em caso de necessidade, quando e como entender adequado.
Todas as violações ou comprometimentos ilícitos da política de segurança devem ser registados e os "infratores" responsabilizados pelas suas falhas.	As ações relativas a esta questão cabem à empresa.

GESTÃO DE TOPO DA ORGANIZAÇÃO

Tópico	Comentário
É importante que a gestão de topo da organização integre nas suas capacidades boa sensibilidade para as questões de segurança, de risco e de continuidade de negócio,	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
bem como é fundamental que seja identificado e nomeado a nível de topo um responsável pela segurança da informação (CISO)	O Regulamento exige que a empresa informe a ANACOM sobre este responsável.

GESTÃO DE RISCO

Tópico	Comentário
A organização deve assegurar uma lista de ativos que compõem a sua organização e que são abrangidos pela política de segurança, para que com base nesses ativos possa avaliar e estudar o risco que pode envolver cada um.	O projeto de Regulamento cobre estas questões.
Desta forma a organização deve efetuar continuamente uma avaliação de risco, mantendo uma lista dos principais riscos para a segurança e continuidade das comunicações e serviços, devidamente correlacionados com os diversos ativos da organização.	Idem.
Rever a avaliação de riscos após alterações/mudanças ou posteriormente a incidentes de segurança.	Idem.
Assegurar que todos os colaboradores têm conhecimento dos riscos e sabem como atuar relativamente aos mesmos no sentido da sua mitigação.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.

RECURSOS HUMANOS

Tópico	Comentário
A seleção e recrutamento dos elementos que venham a compor as equipas, colaboradores e funções na área de segurança, bem como outras áreas críticas, deverá ser criteriosa, não só a nível de conhecimentos, de capacidade e de experiência profissional, podendo em último caso recorrer-se a registos judiciais.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
É fundamental existir uma política/procedimento para recrutamento, definindo claramente os critérios de avaliação de competência, conhecimentos e experiência.	Idem.

Devem ser atribuídos de forma inequívoca as funções e responsabilidades aos colaboradores das áreas de segurança.	O Regulamento endereça estas preocupações através da exigência de indicação explícita destes responsáveis.
As funções e responsabilidade devem ser de conhecimento público permitindo ações rápidas e eficazes, face a um qualquer incidente ou falha de segurança.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
Aquando do recrutamento de todos os colaboradores é fundamental que estes conheçam e se comprometam formalmente com a política de segurança da organização (contrato de trabalho ou termo de responsabilidade). Os colaboradores devem conhecer claramente quais as suas obrigações e quais as suas responsabilidades no incumprimento da mesma	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.

RELACIONAMENTO COM TERCEIROS (CONTRATAÇÃO)

Tópico	Comentário
No relacionamento com outras organizações, nomeadamente em contratação, devem ser incluídos requisitos de segurança. Promove-se a existência de uma política de segurança para relacionamento com terceiras-partes.	Embora não haja referência específica no Regulamento a esta questão, pressupõe-se que estas preocupações são respondidas através das exigências relativamente à Política de Segurança.

FORMAÇÃO / SENSIBILIZAÇÃO / TREINO

Tópico	Comentário
Para uma política de segurança ser cumprida e seguida por todos os colaboradores, importa que sejam efetuadas ações formativas e de sensibilização relativamente à política e as questões de segurança, nomeadamente sobre o seu impacto sobre a organização e postos de trabalho.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
Estas sessões servirão para melhorar e atualizar os conhecimentos de todos os colaboradores nas diversas componentes da segurança da informação.	Idem
Ao mesmo tempo relembrar os colaboradores sobre quais as responsabilidades de cada uma face a um não cumprimento da política de segurança, bem como quais as ações daí resultantes.	Idem
Devem ser efectuados testes regulares as infraestruturas e sistemas, quer no sentido de	Questão endereçada pelo Regulamento.

avaliar as capacidades técnicas na eventualidade de contingência quer no sentido de treinar as equipas e elementos para uma eventualidade real.	
Devem ser definidos exercícios periódicos dedicados às várias componentes da organização, envolvendo sempre que possível terceiras-partes para tornar os exercícios mais reais. Todas as lições tiradas desses exercícios e treinos servirão para a organização consolidar a sua política de segurança, procedimentos e adaptações tecnológicas.	Idem.

SEGURANÇA FÍSICA

Tópico	Comentário
Assegurar a segurança física, das instalações e impedir que pessoal não autorizado ou credenciado possa aceder às instalações da organização. Promova-se para isso sistemas de controlo de acessos, mecanismos de monitorização ou vídeo vigilância, etc., assegurando a existência de pessoal qualificado que controle entradas e saídas, bem como assegure a monitoração de acessos e dos espaços.	Cabe à empresa.
Sejam definidas políticas especificas para o acesso às instalações ou a áreas sensíveis ou mais críticas.	Idem.
Definam-se políticas para as condições ambientais das áreas críticas e não críticas, nomeadamente energia, arrefecimento ou aquecimento, refrigeração, etc.	Idem.
Para as áreas críticas de negócio, seja assegurado que energia, água e combustíveis são equacionados no sentido de prevenir um qualquer comprometimento e que, sejam assegurados todos os serviços críticos mesmo sem abastecimento públicos destes bens.	Idem.

CONTROLO DE ACESSOS AOS SISTEMAS DE INFORMAÇÃO

Tópico	Comentário
Assegurar que todos os colaboradores ou utilizadores dos sistemas da organização dispõem de mecanismos de acesso sem o qual não poderão aceder a qualquer sistema da	Cabe à empresa. Questão normalmente incluída em planos de segurança.

organização. A organização deve escolher os mecanismos que melhor se adaptem ao seu funcionamento, no entanto a opção por autenticação forte ou duplo fator são recomendáveis.	
Registo de todos os acessos a sistemas, sendo que esses registos devem ser mantidos por um período mínimo aceitável, período esse que deve estar refletido na correspondente política.	Idem.
Definição de política de segurança que contemple os acessos e perfis de cada tipo de utilizador, impedindo assim acessos ilegítimos aos sistemas e informações.	Idem.
Deverá ainda a organização prover os seus sistemas e utilizadores de mecanismos de segurança de dados, nomeadamente através que garantam a integridade, confidencialidade e autenticidade.	Idem.

SEGURANÇA DOS SISTEMAS

Tópico	Comentário
As redes e comunicações da organização devem estar sujeitas a mecanismos e controlos apertados de segregação e controlo, sejam eles *firewalls* ou outros, mas que impeçam ou autorizem de acordo com a situação. Estes mecanismos de autorização ou validação devem proteger igualmente aplicações e serviços de rede.	Aspetos cobertos pela política e planos de segurança da empresa. O Regulamento exige a comunicação de informação sobre a política e planos de segurança.
A organização deve prover os seus sistemas de mecanismos de proteção contra código malicioso, vírus, etc.	Idem.
Deve ser definida política de segurança para os ativos e sistemas impedindo acesso ilegítimo ou protegendo-os de vulnerabilidades.	Idem.

CONTROLO DE OPERAÇÕES

Tópico	Comentário
As operações diárias e de exploração devem ser sujeitas a mecanismos de controlo, validação e monitorização.	Aspetos cobertos pela política e planos de segurança da empresa.

Devem ser definidos claramente as responsabilidades e funções para operação com sistemas críticos da organização.	Questão coberta com as exigências relativas ao Plano de Segurança.
Deve existir uma política de segurança e de procedimentos na operação destes sistemas. Deve igualmente existir uma política de mudanças ou alterações efetuadas sobre os sistemas críticos, fomentando a criação de grupos de validação de todas as alterações ou mudanças que afetem os sistemas.	Idem.
Deve a organização manter atualizada uma lista de ativos correlacionado com os serviços prestados pela mesma.	Idem.

INCIDENTES

Tópico	Comentário
As organizações devem dotar-se tecnologicamente de sistemas de deteção de incidentes, ou sistemas de monitorização de incidentes. Devem ainda recorrer a fontes de informação públicas sobre incidentes ocorridos no mundo ou até mesmo em Portugal, antecipando assim um possível evento na sua organização.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este aspeto.
Devem ser definidos em documento próprio quais os procedimentos a seguir em caso de incidente ou falha de segurança. Os colaboradores devem conhecer e saber quem contactar em caso de ter conhecimento de um incidente de segurança.	Idem.
As equipas de gestão de incidentes devem estar aptas e preparadas para lidar e atuar face a incidentes de segurança.	O Regulamento endereça esta questão.
Deve regularmente a organização efetuar a avaliação de incidentes que tenham afetado a própria instituição ou outros incidentes tenham afetado organizações congéneres, por forma antecipar e prevenir o risco.	O Regulamento exige a comunicação de informação sobre incidentes.
Deve a organização rever com frequência os procedimentos face a um incidente adaptando-se à evolução.	
Recomenda-se a promoção de ação de formação e treino com base em incidentes por forma a capacitar as equipas com resultado objetivo numa mitigação ou acção mais célere.	Cabe à empresa.

As equipas de gestão de incidentes devem ter capacidade e conhecimentos para avaliar o impacto dos incidentes, investigar os incidentes e tomar as acções devidas para os mitigar.	O regulamento endereça esta questão.
Todos os incidentes devem ser sujeitos a relatório, bem como deve ser consolidada uma base de conhecimento face a incidentes futuros.	Idem.
Devem as equipas ter capacidade para correlacionar incidentes com incidentes passados ocorridos na organização ou não.	Idem.
Deve existir um procedimento/política para a comunicação interna e externa de incidentes, assegurando assim que os decisores tenham conhecimento do mesmo, bem como as instituições públicas que por forca de lei devem ter conhecimento dos incidentes ocorridos.	Idem

CONTINUIDADE DE NEGÓCIO

Tópico	Comentário
Devem ser definidos planos de contingência para atuação em caso de constrangimento ou impacto na infraestrutura ou negócio.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este tópico.
Deve ser mantido um plano de continuidade de negócio que possa em situação de contingência manter operáveis os sistemas críticos ou assegurar que nenhum serviço ou sistema é comprometido, perdendo-se a integridade da informação neles constante.	Questão coberta com as exigências relativas ao Plano de Segurança.
É fundamental existir uma política de atuação em situação de contingência, onde esteja claro quem define essa contingência e a necessidade de ativar o plano. O plano de contingência deve ser revisto com frequência de acordo com a alterações de negócio e sempre que possível testado, provando assim a exequibilidade do mesmo.	Idem.

MONITORIZAÇÃO / AUDITORIA / TESTES

Tópico	Comentário
Implementar sistemas de monitorização e de registo dos sistemas críticos. Deve definir-se uma política de logs que permitam uma monitoração posterior dos sistemas.	Tendo em conta o Objeto do Regulamento é natural que não haja referência específica a este tópico.

Os logs devem ser recolhidos de forma fiável dos sistemas, podendo em certos casos e de acordo com a criticidade dos mesmo serem assinados eletronicamente, garantindo a validade dos mesmos.	
Definir procedimentos que garantam que os sistemas críticos são submetidos a verificações de segurança e testes de segurança regularmente, com especial enfoque nos novos sistemas colocados em exploração.	Idem.
Todos os novos sistemas ou serviços devem ser testados e avaliados antes de se colocados em produção e ligados a outros sistemas já existentes, em especial os sistemas mais críticos. Será adequado a organização dispor de um ambiente de testes específico completamente segredado de ambientes "reais".	Idem.
Assegurar que todo o qualquer processo de monitorização, respeita claramente os direitos à privacidade, devendo a organização adequar os seus sistemas e procedimentos de forma a, tornando útil a observação e estudo dos resultados das monitorizações e auditorias, assegure a privacidade de dados pessoais.	Idem.

CONFORMIDADE

Tópico	Comentário
Todos os sistemas, processos e serviços da organização devem obedecer e respeitar as leis vigentes do pais, neste caso é por demais importante que o respeito pela Lei de Proteção de Dados Pessoais e pela privacidade devam ser respeitados. Para além disso, a aprovação recente do Regulamento Europeu de Proteção de Dados, obriga a que a organização dedique de forma responsável uma monitorização e observação constante de todos os seus sistemas e processos no sentido de assegurar a legalidade das suas ações.	O Regulamento endereça bem as questões de conformidade.