From:
To: Departamento de Regulação Supervisão e Certificação
Subject: Consulta Pública - Aviso 21606/2021
Date: 24 de novembro de 2021 17:10:24
Attachments: image001.jpg
image002.png
image003.png
image004.jpg

Exmo senho subdiretor-geral do Gabinete Nacional de Segurança,

Após leitura da proposta de regulamento com as instruções técnicas relativas à comunicação e informação, constante no aviso n.º 21606/2021, e estando o mesmo em consulta pública, humildemente envio aquilo que possa ser útil de considerações sobre os mesmo.

Artigo 1

No n.º 2 é deixada a hipótese de encriptar a informação a enviar, não seria mais prudente que esta fosse obrigatoriamente encriptada?

Observação: A criação de formulários online que permitisse o envio "direto" de informação em https, não permitiria um grau de segurança e uniformização maior que o envio de emails não formatados? Neste aspeto, seria talvez importante, e caso tais formulários ainda não se encontrem criados, poder deixar em regulamento a sua possibilidade, nem que como alternativa:

1 - O envio de informação ao CNCS no âmbito dos artigos 4.º, 5.º, 6.º e 8.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, deve ser realizado com recurso às áreas próprias em linha disponibilizados no portal do CNCS, podendo em caso de indisponibilidade dos mesmos, ser realizada por envio para o correio eletrónico sri@cncs.gov.pt.

2 — No caso das entidades enviarem a informação via correio eletrónico como estabelecido no número anterior, esta deve ser protegida por método criptográfico, podendo ser utilizada a chave pública de PGP, associada ao endereço de correio eletrónico referido no número anterior, publicada no sítio na Internet do CNCS.

Artigo 2

3 – Esta comunicação deve ser realizada mediante o estabelecido no n.1 e n.º 2 do artigo 1.º do presente regulamento, sendo que no caso do envio segundo o n.º 2 do artigo 1.º, deverá ser adicionado depois de preenchido o anexo I constante no presente regulamento, e disponível também no portal da Internet do CNCS.

Artigo 3

3 – Esta comunicação deve ser realizada mediante o estabelecido no n.1 e n.º 2 do artigo 1.º do presente regulamento, sendo que no caso do envio segundo o n.º 2 do artigo 1.º, deverá ser adicionado depois de preenchido o anexo II constante no presente regulamento, e disponível também no portal da Internet do CNCS.

Artigo 4

Recomposição estipulado no n.º 1 e correção de erro:

1 — Para os efeitos do disposto na presente instrução, entende-se por «Ativo» todo o sistema de informação e comunicação, equipamento ou outro recurso físico ou lógico **considerado** essencial, no suporte direto ou indireto a um ou mais serviços.

Recomposição estipulado no n.º 3 retirando a redundância de lista de ativos:

3 — Para efeitos do n.º 3 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, as entidades devem comunicar ao CNCS, com base no inventário de ativos a que se refere o n.º 1 do artigo 6.º do referido normativo, **e** para todos os ativos direta ou indiretamente acessíveis publicamente através da Internet, a seguinte informação:

4 — A lista resultante do número anterior deve ser remetida da forma estipulada no n.1 e n.º 2 do artigo 1.º do presente regulamento, sendo que no caso do envio segundo o n.º 2 do artigo 1.º, deverá ser adicionado depois de preenchido o anexo III constante no presente regulamento, e disponível também no portal da Internet do CNCS.

Artigo 5

NOTA: Se fosse disponibilizado um modelo XML, ou um outro qualquer modelo pré formatado de metadados, seria mais simples a uniformização e até compilação de dados por parte do CNCS.

2 – O relatório deve ser remetido da forma estipulada no n.1 e n.º 2 do artigo 1.º do presente regulamento, sendo que no caso do envio segundo o n.º 2 do artigo 1.º, deverá ser adicionado depois de preenchido o anexo IV constante no presente regulamento, e disponível também no portal da Internet do CNCS.

Artigo 6

2 - Nos casos em que a entidade em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, não **tiver** temporariamente capacidade operacional para assegurar a notificação no sítio na Internet do Centro Nacional de Cibersegurança, ou nos casos em que o mesmo esteja indisponível, a notificação poderá ser efetuada, a título excecional, através:

a) De correio eletrónico, devidamente encriptado com a chave PGP disponível em…, remetido para o seguinte endereço: cert@cert.pt;

Retirava o 3, pois julgo que o tipo de informação a notificar deva ser alvo de proteção criptográfica.

Ficam no entanto algumas outras dúvidas que seria importante de alguma forma esclarecer, e dizem respeito por exemplo à possibilidade do ponto de contato, ou até mesmo o responsável de segurança ser um elemento externo à entidade, da mesma forma que por exemplo no caso do RGPD e da Lei 58/2019 sobre proteção de dados pessoais, é estabelecido na lei que o Encarregado de Proteção de dados possa ser um elemento externo com contrato de prestação de serviços (até porque esta figura tem mais um carater consultivo e de sensibilização), o que não acontece nesta legislação nem regulamentação até ao momento. Considerando eu que o responsável de segurança, e devido às necessárias competências terá de se rum elemento decisor na determinação de medidas de segurança e Cibersegurança, seria importante esclarecer a possibilidade de subcontratar serviços externos, e as garantias necessárias, nessa possibilidade.

Note-se que nesta vossa proposta no artigo 2 e artigo 3, é solicitada o nome da entidade, mas em nenhum ponto é solicitado nome de entidade terceira que possa prestar o serviço, pelo que pode levar também a deduzir a não possibilidade de externalizar o serviço.

Esperando poder ter sido útil,

Com os melhores cumprimentos,