Jornadas Computação Científica 2021

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto-Lei n.º 65/2021

de 30 de julho

Sumário: Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Carlos Friaças

2021/10/21

INTRODUÇÃO

- Os artigos do Decreto-Lei não são integralmente reproduzidos nos slides seguintes

- Âmbito de aplicação: Artigo 2º
  - Estabelecido por remissão para a Lei 46/2018 (Regime Jurídico da Segurança do Ciberespaço)

CONTACTO PERMANENTE

- Disponibilidade 24/7
- Informação Operacional e Técnica

Artigo 4.º

Ponto de contacto permanente

1 — As entidades devem indicar, pelo menos, um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS, nomeadamente:

a) A articulação intersetorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;

b) A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;

c) A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;

d) A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;

e) A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;

f) A receção das instruções técnicas emitidas ao abrigo do disposto no n.º 5 do artigo 7.º do Regime Jurídico da Segurança do Ciberespaço e no artigo 18.º;

g) A operacionalização dos procedimentos fixados no âmbito dos planos de segurança previstos no artigo 7.º

2 — As entidades devem assegurar a função de ponto de contacto permanente com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação do CNCS.

RESPONSÁVEL DE SEGURANÇA

- Tem que estar de posse de muita informação local
- Muita responsabilidade
- O ponto 4 sugere que não deverá haver hiato entre responsáveis nomeados

Artigo 5.º

Responsável de segurança

1 — As entidades devem designar um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do presente decreto-lei.

2 — As entidades devem indicar ao CNCS, no prazo de 20 dias úteis a contar do início da respetiva atividade, a pessoa designada para as funções de responsável de segurança.

3 — As entidades que tenham iniciado atividade antes da data de entrada em vigor do presente decreto-lei devem efetuar a comunicação prevista no número anterior no prazo de 20 dias úteis, a contar do prazo previsto no n.º 2 do artigo 23.º

4 — As entidades devem comunicar imediatamente ao CNCS a substituição do responsável de segurança.

INVENTÁRIO DE ATIVOS

- Assinado pelo Responsável de Segurança
- Informação relativa a cada ativo, definida pelo CNCS
- Enviado anualmente ao CNCS

Artigo 6.º

Inventário de ativos

1 — As entidades devem elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços, devendo o mesmo ser assinado pelo responsável de segurança.

2 — No inventário de ativos deve constar, para cada ativo, a informação definida em instruções técnicas emitidas pelo CNCS.

3 — As entidades devem comunicar ao CNCS a lista dos ativos constantes do inventário, com a informação que venha a ser determinada nos termos do número anterior, com a seguinte periodicidade:

a) Na sua versão inicial, no prazo de 20 dias úteis a contar da data de início de atividade;

b) Numa versão atualizada, anualmente, a ser entregue em conjunto com o relatório anual a que se refere o artigo 8.º

PLANO DE SEGURANÇA

- Política de Segurança
- Medidas (Requisitos e notificação de incidentes)
- Identificação das 2 pessoas (ou uma, se for a mesma)

Artigo 7.º

Plano de segurança

1 — As entidades devem elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, que contenha:

a) A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;
b) A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;
c) A identificação do responsável de segurança;
d) A identificação do ponto de contacto permanente.

2 — Para efeitos do cumprimento do disposto no número anterior, os operadores de infraestruturas críticas podem utilizar o plano previsto no artigo 10.º do Decreto-Lei n.º 62/2011, de 9 de maio, desde que o mesmo inclua medidas relativas à segurança das redes e da informação.

RELATÓRIO ANUAL

- Atividades, Estatísticas, Análise
- Até ao final de Janeiro de cada ano
- CNCS pode definir o formato (esperemos que ajude…)
- E mais…

Artigo 8.º

Relatório anual

1 — As entidades devem elaborar um relatório anual que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:

a) Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação;
b) Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;
c) Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:

i) Número de utilizadores afetados pela perturbação do serviço;
ii) Duração dos incidentes;
iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;

d) Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;
e) Problemas identificados e medidas implementadas na sequência dos incidentes;
f) Qualquer outra informação relevante.

2 — As entidades devem remeter o relatório anual ao CNCS, devidamente assinado pelo responsável de segurança, nos seguintes termos:

a) Relativamente ao primeiro relatório anual:

i) Até ao último dia útil do mês de janeiro do ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no primeiro semestre;
ii) Até ao último dia útil do mês de janeiro do segundo ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no segundo semestre;

b) Relativamente aos relatórios subsequentes anuais, até ao último dia útil do mês de janeiro do ano civil seguinte aos quais os mesmos se reportam.

3 — Para efeitos do disposto na subalínea *ii*) da alínea *a*) do número anterior, o relatório anual deve abranger todo o período entre a data de início de atividade e o final do ano civil anterior.
4 — Para efeitos do disposto no presente artigo, o CNCS pode definir o formato em que a informação deve ser apresentada.

ANÁLISE DE RISCO ANUAL

- Limita de alguma forma a tipologia de ameaças, embora não excluindo outros tipos
- O CNCS pode emitir instruções para harmonizar a matriz

Artigo 10.º

Análise dos riscos e implementação dos requisitos de segurança

1 — As entidades da Administração Pública e os operadores de infraestruturas críticas, bem como os operadores de serviços essenciais, devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, no caso dos operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais, nos seguintes termos:

a) Análise dos riscos de âmbito global, com a seguinte periodicidade:

i) Pelo menos uma vez por ano;
ii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que implique uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS;

b) Análise dos riscos de âmbito parcial, com a seguinte periodicidade:

i) Durante o planeamento e preparação da introdução de uma alteração ao ativo ou ativos, em relação ao ativo ou ativos envolvidos;
ii) Após a ocorrência de um incidente com impacto relevante ou outra situação extraordinária, em relação aos ativos afetados;
iii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que impliquem uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS.

2 — As entidades devem documentar a preparação, a execução e a apresentação dos resultados da análise dos riscos.
3 — A análise do risco deve abranger para cada ativo:

a) A identificação das ameaças, internas ou externas, intencionais ou não intencionais, incluindo, nomeadamente:

i) Falha de sistema;
ii) Fenómeno natural;
iii) Erro humano;
iv) Ataque malicioso;
v) Falha no fornecimento de bens ou serviços por terceiro;

b) A caracterização do impacto e da probabilidade da ocorrência das ameaças identificadas na alínea anterior.

NOTIFICAÇÕES

- Impacto relevante ou substancial – remissão para o Regime Jurídico da Segurança do Ciberespaço
- «Todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação…»

Artigo 11.º

Obrigações de notificação

1 — A Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais notificam o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço.

2 — As entidades devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.

3 — A Administração Pública e os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais devem, perante qualquer incidente detetado ou a estes comunicado pelos seus clientes, utilizadores ou outras entidades, atender aos parâmetros previstos, respetivamente, no n.º 4 do artigo 15.º, no n.º 4 do artigo 17.º e no n.º 4 do artigo 19.º do Regime Jurídico da Segurança do Ciberespaço, bem como aos constantes dos nor-

ACOMPANHAMENTO FIM-A-FIM

- Notificações iniciais, de fim de impacto e finais (rescaldo)
- Se forem solucionados em menos de 2h: apenas a notificação final

Artigo 12.º

Tipos de notificações

1 — Por cada incidente que deva ser objeto de notificação ao abrigo do disposto no artigo anterior, as entidades devem submeter ao CNCS:

a) Uma notificação inicial, nos termos do artigo seguinte;
b) Uma notificação de fim de impacto relevante ou substancial, nos termos do artigo 14.º;
c) Uma notificação final, nos termos do artigo 15.º

2 — Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final com todos os campos de informação devidamente preenchidos, ficando dispensadas do envio das restantes notificações.

TAXONOMIA

- 5 causas raiz
- 9 efeitos produzidos
- Muito mais simples que a Taxonomia da RNCSIRT

Artigo 16.º

Taxonomia de incidentes e de efeitos

1 — Para efeitos do disposto nos artigos 13.º a 15.º, os incidentes podem ter as seguintes categorias de causas raiz:

a) Falha de sistema;
b) Fenómeno natural;

c) Erro humano;
d) Ataque malicioso;
e) Falha no fornecimento de bens ou serviços por terceiro.

2 — Para os efeitos do disposto nos artigos 13.º a 15.º, os incidentes podem ter os seguintes efeitos produzidos:

a) Infeção por *malware*;
b) Disponibilidade;
c) Recolha de informação;
d) Intrusão;
e) Tentativa de intrusão;
f) Segurança da informação;
g) Fraude;
h) Conteúdo abusivo;
i) Outro.

SANÇÕES

- O nº1 remete para a Lei 46/2018
- O nº2 é apenas relativo ao processo de certificação
- Não definir contacto/responsável, e não entregar relatórios aparenta não ser sancionável
  - Será um lapso?

Artigo 21.º

Regime sancionatório

1 — Às infrações ao disposto no presente decreto-lei é aplicável o regime sancionatório previsto no Regime Jurídico da Segurança do Ciberespaço aprovado pela Lei n.º 46/2018, de 13 de agosto.

2 — Constitui contraordenação punível com coima de € 1000,00 a € 3740,98, no caso de pessoa singular, ou de € 5000,00 a € 44 891,81, no caso de pessoa coletiva, a prática das seguintes infrações:

a) A utilização de marca de certificação da cibersegurança inválida, caducada ou revogada;

b) A utilização de expressão ou grafismo que expressa ou tacitamente sugira a certificação da cibersegurança de produto, serviço ou processo que não seja certificado;

c) A omissão dolosa de informação ou a prestação de falsa informação que seja relevante para o processo de certificação da cibersegurança que se encontre em curso, nos termos definidos em cada esquema de certificação.

3 — Sem prejuízo das competências atribuídas a outras entidades em razão da matéria, às contraordenações previstas no número anterior aplica-se o disposto nos artigos 21.º e 25.º a 28.º do Regime Jurídico da Segurança do Ciberespaço.

CONTACTO/RESPONSÁVEL «IN-HOUSE»

- Exige capacidade de reacção rápida
- Exige conhecimento da realidade da organização
- Confiança organizacional é mais importante que o «know-how» de segurança
- Noção de «histórico» importante para a análise de risco
- Auxilia a conformidade com a AUP RCTS

EM QUE PODEMOS AJUDAR?

- Experiência de anos em coordenação de incidentes
- Formação/Ajuda aos Contactos/Responsáveis seleccionados
- Apoio nos Relatórios Anuais
  - Partilha de templates, dados, experiências

EM QUE PODEMOS AJUDAR?

- Coordenação de incidentes, no papel de «Internet Service Provider»
  - Missão do RCTS CERT: coordenação de incidentes para toda a RCTS
  - Fornecendo dados adicionais, se existirem
  - Caso seja da vontade de cada membro, em cada caso

- Em qualquer situação de crise de segurança, assim seja requisitado o nosso auxílio

DISCUSSÃO