SEGURANÇA DO CIBERESPAÇO REQUISITOS DE SEGURANÇA DAS REDES E SISTEMAS DE INFORMAÇÃO

O Decreto-Lei n.º 65/2021 regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança, nomeadamente, quanto à regulamentação dos **requisitos de segurança das redes e sistemas de informação** e, por outro lado, das regras para a **notificação de incidentes**, que devem ser cumpridos pela Administração Pública, operadores de infra-estruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

I - Requisitos de Segurança das Redes e Sistema de informação

A nível da **segurança das redes e dos sistemas informáticos**, as entidades devem cumprir medidas para cumprimento dos requisitos de segurança e medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam. Nestes termos, devem ser cumpridos determinados requisitos, pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais, a saber:

1. Indicar um **ponto de contacto permanente**, que assegure os fluxos de informação de nível operacional e técnico com o Centro Nacional de Cibersegurança (CNCS), com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, nomeadamente:

a. A articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos sectores;

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 actualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;

d. A partilha de informação quando estejam activados planos de emergência de protecção civil directamente 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 infra-estruturas críticas nacionais ou europeias;

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

ADVOGADOS

LÍDIA SILVESTRE
ADVOGADA

BÁRBARA DUARTE
ADVOGADA

TERESA PATRÍCIO & ASSOCIADOS
SOCIEDADE DE ADVOGADOS, SP, RL

Avenida Almirante Gago Coutinho, 96, 1700-031 Lisboa
+351 217 981 030 . info@tpalaw.pt . www.tpalaw.pt

SEGURANÇA DO CIBERESPAÇO
REQUISITOS DE SEGURANÇA DAS REDES E SISTEMAS DE INFORMAÇÃO

f. A recepção 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. Indicar um **responsável de segurança** para a gestão do conjunto das medidas adoptadas em matéria de requisitos de segurança e de notificação de incidentes;

3. Elaborar e manter actualizado um **inventário de activos** de todos os activos essenciais para a prestação dos respectivos serviços, devendo o mesmo ser assinado pelo responsável de segurança;

4. Elaborar e manter actualizado 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 adoptadas 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.

5. Elaborar um **relatório anual** que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:

a. Descrição sumária das principais actividades 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 afectados pela perturbação do serviço;
ii. Duração dos incidentes;
iii. Distribuição geográfica, no que se refere à zona afectada pelo incidente, incluindo a indicação de impacto transfronteiriço;

d. Recomendações de actividades, 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.

No âmbito destas medidas, as entidades deverão proceder a uma **análise dos riscos e implementação dos requisitos de segurança**, nos seguintes termos:

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

a. Pelo menos uma vez por ano;

b. 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:

a. Durante o planeamento e preparação da introdução de uma alteração ao activo ou activos, em relação ao activo ou activos envolvidos;

TERESA PATRÍCIO & ASSOCIADOS
SOCIEDADE DE ADVOGADOS, SP, RL
Avenida Almirante Gago Coutinho, nº 96, 1700-031 Lisboa
www.tpalaw.pt . info@tpalaw.pt . Tel: +351 217 981 030

SEGURANÇA DO CIBERESPAÇO REQUISITOS DE SEGURANÇA DAS REDES E SISTEMAS DE INFORMAÇÃO

b. Após a ocorrência de um incidente com impacto relevante ou outra situação extraordinária, em relação aos activos afectados;

c. 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.

A análise do risco deve abranger para cada activo, a identificação das ameaças, internas ou externas, intencionais ou não intencionais e a caracterização do impacto e da probabilidade da ocorrência das ameaças.

II- Notificações de incidentes

A nível das **notificações de incidentes**, as entidades devem implementar todos os meios e os procedimentos necessários à detecção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.

Devem, assim, ser tidos em consideração os seguintes requisitos de notificação de incidentes que afectem a segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas, pelos operadores de serviços essenciais e pelos prestadores de serviços digitais:

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

  a) Uma notificação inicial, enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação, devendo a entidade, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução do incidente;

  b) Uma notificação de fim de impacto relevante ou substancial, que deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial;

  c) Uma notificação final, a enviar no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar.

Às **infracções** ao disposto no presente decreto-lei é aplicável o regime sancionatório previsto no Regime Jurídico da Segurança do Ciberespaço. Constitui contra-ordenação punível com coima de € 1.000,00 a € 3.740,98, no caso de pessoa singular, ou de € 5.000,00 a € 44.891,81, no caso de pessoa colectiva, a prática das seguintes infracções:

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.

O cumprimento dos requisitos de segurança e das obrigações de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei não prejudica o cumprimento dos requisitos específicos de segurança e das obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades competentes, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Protecção Civil (ANEPC), pela Autoridade Nacional de Comunicações (ANACOM), pela Comissão Nacional de Protecção de Dados (CNPD) e por outras autoridades sectoriais, nos termos das disposições legais e regulamentares aplicáveis, nem o cumprimento de legislação da **União Europeia.**

TERESA PATRÍCIO & ASSOCIADOS
SOCIEDADE DE ADVOGADOS, SP, RL
Avenida Almirante Gago Coutinho, nº 96, 1700-031 Lisboa
www.tpalaw.pt . info@tpalaw.pt . Tel: +351 217 981 030