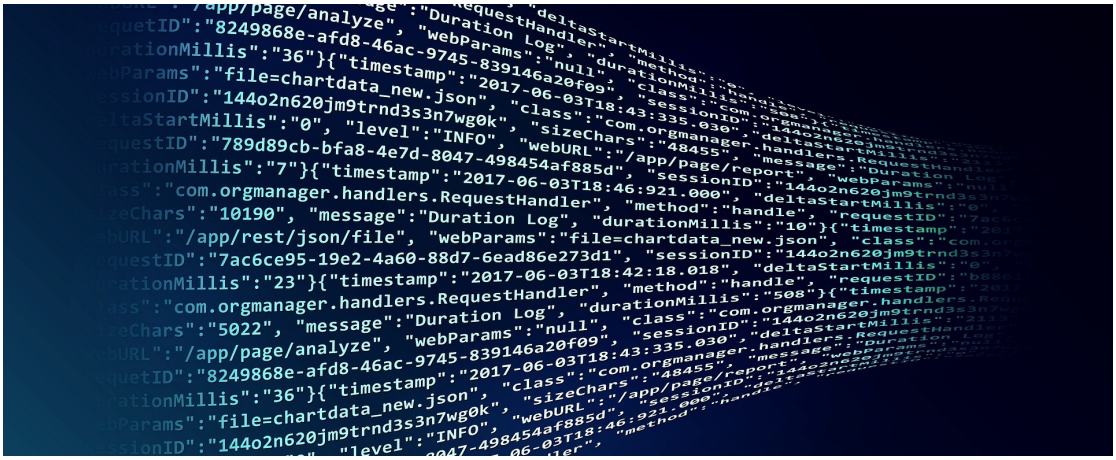
AMMOURA

INSIGHTS



O ESSENCIAL DA LEGISLAÇÃO DE CIBERSEGURANÇA

Os **ataques cibernéticos** a redes, dispositivos e infraestruturas informáticas, governamentais ou privadas, são cada vez mais comuns, em Portugal, na Europa e, também, no resto do mundo. Os objetivos desses ataques virtuais são múltiplos, incluindo o acesso a **dados pessoais** e a obtenção ilícita de fundos, sendo, por vezes, motivados por conflitos bélicos entre países.

Relativamente às **empresas**, os ataques cibernéticos podem comprometer informações comerciais, dados pessoais de colaboradores e clientes, por exemplo, e até a boa imagem ou posição relativa no mercado, potenciando eventuais prejuízos avultados e coimas, nomeadamente se tiverem sido incumpridas normais legais em matéria de **cibersegurança**.

> Regime Jurídico da Segurança do Ciberespaço

Em Portugal, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, foi publicada, em Diário da República, a Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC).

O RJSC determina variadas medidas destinadas a garantir um **elevado nível comum de segurança** das redes e dos sistemas de informação, sendo **aplicável às seguintes entidades**:

a) **Administração Pública**;

b) **Operadores de infraestruturas críticas**;

c) **Operadores de serviços essenciais** (designadamente, setores bancário, infraestruturas digitais e mercado financeiros, energia, transportes, saúde e água);

d) **Prestadores de serviços digitais** (designadamente, serviços de mercado em linha, serviços de motor de pesquisa em linha e serviços de computação em nuvem); e,

e) Outras entidades que utilizem **redes e sistemas de informação**.

Sem prejuízo, existem algumas especificidades e diferenças entre as diversas obrigações a que estão sujeitas as entidades abrangidas pelo RJSC, inclusivamente no âmbito do mais recente **Decreto-Lei n.º 65/2021, de 30 de julho**, que regulamenta o Regime Jurídico da Segurança do Ciberespaço, em matéria de requisitos de segurança e notificação de incidentes.

> Requisitos de segurança

As entidades devem cumprir as **medidas técnicas e organizativas** adequadas e proporcionais para gerir os **riscos** que se colocam à **segurança das redes e dos sistemas de informação** que utilizam, nomeadamente medidas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto.

> Responsável de segurança

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.

> Ponto de contacto permanente

As entidades devem indicar, pelo menos, um **ponto de contacto permanente**, para assegurar os fluxos de informação operacional e técnica com o Centro Nacional de Cibersegurança (CNCS).

> Inventário de ativos

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

A lista dos ativos constantes no inventário deve ser comunicada ao CNCS.

> Plano de segurança

As entidades devem elaborar e manter atualizado um **plano de segurança**, devidamente documentado e assinado pelo responsável de segurança, que, no mínimo, contenha:

a) **Política de segurança** (medidas organizativas e formação de recursos humanos);

b) Descrição das medidas adotadas em matéria de **requisitos de segurança**;

c) Descrição das medidas adotadas em matéria de **notificação de incidentes**;

d) Identificação do **responsável de segurança**;

e) Identificação do **ponto de contacto permanente**.

> **Relatório anual**

As entidades devem elaborar um **relatório anual** com os seguintes elementos, no mínimo:

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;

c) Análise agregada dos incidentes de segurança com impacto relevante ou substancial;

d) Recomendações de atividades, medidas ou práticas que promovam a melhoria da segurança das redes e dos sistemas de informação; e,

e) Problemas identificados e medidas implementadas na sequência dos incidentes.

O plano anual deve ser remetido ao CNCS.

> Análise de riscos

As entidades devem realizar uma **análise de riscos** em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam.

Na sequência de cada análise dos riscos, as entidades devem adotar as **medidas técnicas e organizativas** adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam. As medidas a adotar devem permitir o seguinte:

a) Prevenção, gestão e redução dos riscos;

b) Reforço da robustez e da resiliência dos ativos; e,

c) Resposta eficaz a incidentes, a ameaças ou a vulnerabilidades.

> Notificação de incidentes

As entidades devem notificar o CNCS da ocorrência de incidentes **com impacto relevante ou substancial**. Sendo assim, as entidades devem implementar todos os meios e procedimentos necessários à **deteção, avaliação do impacto e notificação** de incidentes.

Em regra, por cada incidente, as entidades devem submeter ao CNCS:

a) Notificação inicial;

b) Notificação de fim de impacto relevante ou substancial; e,

c) Notificação final.

Exemplificativamente, os incidentes podem ter como causas ou efeitos: (i) ataque malicioso; (ii) infeção por malware; (iii) recolha ilícita de informação; (iv) intrusão; (v) fraude, entre outros.

Quaisquer outras entidades podem, voluntariamente, notificar incidentes com impacto importante na continuidade dos serviços por si prestados.

> Centro Nacional de Cibersegurança

O CNCS exerce funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias, nos termos das suas competências legalmente previstas.

O CNCS pode emitir instruções de cibersegurança e definir o nível nacional de alerta de cibersegurança, podendo atuar em articulação com a Comissão Nacional de Proteção de Dados (CNPD) quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais.

Adicionalmente, o CNCS pode solicitar a quaisquer entidades, públicas ou privadas, toda a colaboração ou auxílio que julgue necessários para o exercício das suas atividades.

> Infrações

A violação do RJCS e regulamentação legal pode comportar a aplicação de **coimas**. Por exemplo:

Constituem **infrações muito graves**:

a) Incumprimento da obrigação de implementar requisitos de segurança;

b) Incumprimento de instruções de cibersegurança emitidas pelo CNCS.

Estas contraordenações são punidas com coima de € 5.000,00 a € 50.000,00.

Constituem **infrações graves**:

a) Incumprimento da obrigação de notificar os incidentes ocorridos ao CNCS;

b) Incumprimento da obrigação de notificar o exercício de atividade sujeita ao RJCS.

Estas contraordenações são punidas com coima de € 1.000,00 a €9.000,00.

Por fim, a prática de outras **infrações** também pode configurar contraordenação, como:

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

b) Utilização de expressão ou grafismo que sugira a certificação da cibersegurança de produto, serviço ou processo que não seja certificado.

Estas contraordenações são punidas com coima de € 1.000,00 a € 44.891,81, no máximo

Artigo redigido de acordo com a legislação vigente em 29 de novembro de 2022.