CUATRECASAS

Regulamentação da ASF em matéria de segurança e governação dasTIC

Norma Regulamentar - Segurança e governação das Tecnologias da Informação e Comunicação (TIC) e subcontratação a prestadores de serviços de computação em nuvem

Legal flash Bancário, Financeiro e Mercado de Capitais

30 de junho de 2022

Aspetos chave

- Estabelecimento de requisitos e princípios gerais em matéria de segurança e governação das TIC, incluindo cibersegurança;
- Estabelecimento de requisitos específicos em matéria de subcontratação a prestadores de serviços de computação em nuvem pelas empresas de seguros e resseguros, em base individual e ao nível do grupo.

Segurança e Governação das TIC e Subcontratação a prestadores de serviços de computação em nuvem – Norma Regulamentar da ASF n.º 6/2022-R, de 30 de junho

Foi publicada em Diário da República, a 30 de junho, a Norma Regulamentar da ASF n.º 6/2022-R, de 30 de junho, que regulamenta a Segurança e Governação das TIC e Subcontratação a prestadores de serviços de computação em nuvem ("**Norma Regulamentar da ASF n.º 6/2022-R, de 30 de junho**").

Descrevem-se, abaixo, sucintamente, as principais alterações introduzidas.

Âmbito de aplicação

A nova norma regulamentar aplica-se: (i) às empresas de seguros e resseguros com sede em Portugal; (ii) às sucursais de empresas de seguros e de resseguros de um país terceiro que exerçam a sua atividade em território português; (iii) aos grupos seguradores ou resseguradores, quando a ASF seja o supervisor do grupo; e aos subgrupos cuja empresa-mãe de seguros ou de resseguros de topo a sociedade gestora de participações no setor dos seguros de topo ou a companhia financeira mista de topo a nível nacional se encontre submetida a supervisão de grupo pela ASF.

Sistema de governação das TIC e Segurança da informação

- De acordo com a nova norma, o orgão de administração é responsável por estabelecer um **sistema eficaz para a gestão de riscos associados às TIC e à segurança**, como parte do sistema de gestão global dos riscos da empresa de seguros ou de resseguros, no âmbito do qual as empresas devem identificar e medir os riscos e avaliar os requisitos de proteção dos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, tendo em conta as vulnerabilidades conhecidas e os incidentes anteriores;

- Define-se a necessidade de existência de uma **estratégia em matéria de TIC**;

- Estabelece-se a obrigação de **auditoria periódica** aos sistemas e processos das empresas no âmbito dos riscos associados às TIC e à segurança e as responsabilidades e características da **função de segurança da informação**, que deverá ser independente e objetiva;

- As empresas de seguros e de resseguros deverão aprovar uma **política de segurança da informação** que inclua regras para a proteção da confidencialidade, integridade e disponibilidade da informação;

- Regulamenta-se o dever de criação de processos de **monitorização das atividades** que afetem a segurança da informação – impondo-se o dever de realização de revisões, avaliações e testes de segurança da informação, por forma a identificar vulnerabilidades, – assim como os seus sistemas e serviços. Por outro lado, consagra-se o dever de documentadção e implementação de **medidas de segurança** lógica e física;

- A nova norma sensibiliza também para o dever de formação neste domínio;

- Na gestão das suas operações de TIC, as empresas deverão, designadamente: (i) documentar a forma como operam; (ii) adequar a frequência das cópias de segurança à avaliação dos riscos realizada; (iii) testar os procedimentos de segurança e de recuperação regularmente; (iv) garantir que os dados são armazenados num ou mais locais; (v) implementar um processo de gestão de problemas e incidentes; e (vi) aprovar uma **política de continuidade das TIC** como parte da política global de gestão da continuidade de negócio da empresa, incluindo esta uma **análise de impacto no negócio** e respetivos **planos de resposta e recuperação**.

Subcontratação a prestadores de serviços de computação em nuvem

- Antes de celebrar qualquer acordo com prestadores de serviços de computação em nuvem, as empresas deverão, nomeadamente, avaliar se está em causa uma **função ou atividade fundamental** ou importante, e proceder a uma **avaliação de risco exaustiva**;

- Quando forem subcontratados serviços relacionados com funções fundamentais ou importantes, as empresas devem estabalecer **requisitos específicos de segurança da informação**, controlando o seu cumprimento, e dispor de uma **estratégia de saída** que garanta a possibilidade de pôr termo ao acordo, se necessário;

- Impõe-se às empresas de seguros e resseguros um **dever de acompanhamento e supervisão permanente das atividades dos seus prestadores de serviços**, com especial atenção às funções operacionais fundamentais. As empresas de seguros e resseguros deverão exercer os seus **direitos de acesso e de auditoria**, por forma a garantir que os prestadores de serviços de computação em nuvem cumprem a legislação europeia e nacional aplicável, assim como as normas de segurança adequadas em matéria de TIC;

- Regulamenta-se o dever de **informação prévia à ASF** no caso de subcontratações de funções e atividades fundamentais ou importantes a prestadores de serviços em nuvem, definindo-se um conjunto de menções que integram o conteúdo mínimo desta informação;

- Finalmente, impõe-se a obrigação de celebração destes acordos por **escrito** – e o seu conteúdo mínimo - e o dever de **manter um registo de informações** atualizado sobre tais acordos, bem como, a obrigação de disponibilização à ASF de todas as informações necessárias solicitadas, incluindo uma cópia dos mesmos.

Entrada em vigor

A Norma Regulamentar n.º 6/2022-R produz os seus efeitos a partir de 30 de julho de 2022.

Para obter informação adicional sobre o conteúdo deste documento, por favor dirija-se ao seu contacto habitual na Cuatrecasas.