

Após a consulta pública em maio deste ano, foi publicada na semana passada a Circular nº 638, de 3 de agosto de 2021, que dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

A nova regra tem por objetivo minimizar as vulnerabilidades dos sistemas utilizados pelas entidades supervisionadas e garantir maior segurança aos segurados, tomadores e beneficiários, bem como ao sistema financeiro de modo geral.

O texto final da Circular não trouxe alterações substanciais face à minuta submetida a consulta pública, mantendo sua essência.

Algumas importantes obrigações foram criadas para conferir maior rigor técnico às imposições da regulamentação:

- i. possuir política de segurança cibernética;
- ii. possuir e manter atualizados processos, procedimentos e controles para identificar e reduzir vulnerabilidades de forma proativa, bem como detectar, responder e se recuperar de incidentes;
- iii. comunicar à SUSEP, no prazo máximo de 5 (cinco) dias úteis a partir do conhecimento do evento, a ocorrência de incidentes relevantes, detalhando a extensão do dano causado e, se for o caso, as ações em curso para regularização completa da situação e os respectivos responsáveis e prazos;
- iv. informar a SUSEP, em até 30 (trinta) dias após a formalização dos contratos, sobre a terceirização de serviços de processamento e armazenamento de dados; e
- v. exigir que os prestadores de serviços de processamento e armazenamento de dados observem as disposições legais e regulamentares em vigor e, entre outras exigências, possuam processos, procedimentos e controles de segurança cibernética não inferiores aos que a própria supervisionada adota para processamento e armazenamento de dados de mesmo grau de sensibilidade, podendo ser observados controles mitigatórios.

A Circular entra em vigor em 1º de setembro de 2021, devendo as supervisionadas se adequarem nos seguintes prazos: (i) até 30 de junho de 2022 para S1 ou S2 e (ii) até 1º de setembro de 2022 para S3 ou S4.

Clique [aqui](#) para acessar a íntegra da Circular.

Susep publishes regulation on cyber security compliance requirements for supervised entities

After a public consultation earlier this year, Superintendence of Private Insurance (“SUSEP”) published Circular No. 638, of 3 August 2021, establishes that supervised entities must comply with cyber security requirements.

For purpose of this regulation, supervised entities are insurance companies, open private pension entities (EAPC), capitalization companies and local reinsurers.

The rule proposes to minimise vulnerabilities of systems used by supervised entities and ensure safety for insureds, policyholders, beneficiaries, and the wider financial system.

Supervised entities are required to have a cyber security policy, ensure they have appropriate controls in place to identify and reduce any system vulnerabilities and inform the regulator within 5 days of any cyber incidents.

Supervised entities are required to inform SUSEP of outsourcing of any data processing or data storage solutions. Furthermore, service providers must comply with the regulation.

The rule becomes enforceable on 1 September 2021. Supervised entities in segments S1 and S2 must adhere to the regulation by 30 June 2022 and those under S3 and S4 by 1 September 2022.

Click [here](#) to access the new Circular.

Fonte: Campos Mello Advogados, em 12.08.2021