Deloitte. Legal

ALERTA LEGAL

7 de novembro de 2024

ASF emite Norma Regulamentar quanto à comunicação de incidentes severos relacionados com as tecnologias de informação e comunicação

A **Norma Regulamentar n.º 9/2024-R, de 26 de setembro**, emitida pela Autoridade de Supervisão de Seguros e Fundos de Pensões ("ASF"), entrou em vigor no dia 8 de outubro de 2024, regulando a **comunicação de incidentes de caráter severo relacionados com as tecnologias de informação e comunicação** ("TIC") pelas entidades sujeitas à supervisão da ASF.

Todas estas entidades estão expostas a riscos relacionados com as TIC, encontrando-se abrangidas pelo Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro ("Regulamento DORA"), que estabelece, nos termos do artigo 19.º, a obrigação de comunicação dos incidentes de caráter severo relacionados com as TIC à autoridade competente designada, que os transmite a um organismo superior.

A quem se aplica esta Norma Regulamentar:

✓ Às **empresas de seguros e de resseguros com sede em Portugal**, incluindo as que exerçam a respetiva atividade através de sucursal ou em regime de livre prestação de serviços no território de outros Estados Membros da União Europeia;

✓ Às **sociedades gestoras de fundos de pensões autorizadas em Portugal**, incluindo as que exerçam a respetiva atividade através de sucursal ou em regime de livre prestação de serviços no território de outros Estados Membros da União Europeia; e

✓ Aos **mediadores de seguros, de resseguros e de seguros a título acessório residentes ou com sede em Portugal**, que não sejam microempresas ou pequenas ou médias empresas, com exceção dos mediadores de seguros que também sejam instituições de crédito.

O que veio esta Norma estabelecer:

Noção de incidente severo

As entidades abrangidas classificam os incidentes relacionados com as TIC como severos de acordo com os seguintes **critérios**:

a) Existência de um acesso bem-sucedido, mal-intencionado e não autorizado às redes e sistemas de informação da entidade de apoio a funções críticas ou importantes; ou

b) O incidente afeta serviços críticos da entidade e, cumulativamente, verificam-se duas ou mais das seguintes situações:

   i. O número de clientes afetados pelo incidente é superior a 10% do total de clientes

que utilizam o serviço afetado ou é superior a cem mil clientes;

ii. A duração do incidente é superior a 24 horas ou o tempo de indisponibilidade do serviço crítico é superior a duas horas;

iii. O incidente afeta a disponibilidade, autenticidade, integridade ou confidencialidade dos dados, com impacto ou potencial impacto negativo na implementação dos objetivos de negócio ou no cumprimento de exigências regulatórias;

iv. O incidente tem impacto económico, nomeadamente quando os custos e as perdas diretos e indiretos incorridos pela entidade devido ao incidente excedam ou sejam suscetíveis de exceder os cem mil euros, excluindo eventuais montantes recuperáveis;

v. O incidente tem impacto em termos de reputação. Considera-se este requisito verificado quando:

- O incidente é noticiado nos meios de comunicação social; ou
- O incidente tenha dado origem a múltiplas reclamações de diferentes clientes relativamente a serviços de contacto direto com clientes ou a relações de negócio críticas; ou
- A entidade, em resultado do incidente, não consiga dar cumprimento ou seja suscetível de não dar cumprimento a exigências regulatórias; ou
- A entidade, em resultado do incidente, seja ou possa ser suscetível a uma perda de clientes com um impacto material na sua atividade.

Na avaliação do impacto de um incidente em termos reputacionais, as entidades devem tomar em consideração o nível de visibilidade que o incidente adquiriu ou é suscetível de adquirir.

Quando não seja possível calcular com precisão o número de clientes afetados, a duração do incidente/tempo de indisponibilidade ou o impacto económico do incidente, as entidades devem ter em conta estimativas com base na informação disponível.

Comunicação destes incidentes

Sendo um incidente classificado como severo pela entidade abrangida, esta deve comunicá-lo à ASF, de forma completa e rigorosa, através da apresentação dos seguintes **elementos**, que **constam de formulários próprios disponibilizados no *site* da ASF**:

a) **Notificação Inicial** – deve ser apresentada no prazo de quatro horas desde o momento em que o incidente é classificado como severo ou, no máximo, no prazo de 24 horas desde o momento em que o incidente é detetado;

b) **Relatório Intercalar** – deve ser apresentado no prazo de 72 horas desde a submissão da notificação inicial, mesmo que o estado do incidente não tenha mudado significativamente, podendo ser apresentada uma versão atualizada do relatório intercalar caso se verifique a recuperação das respetivas atividades regulares;

c) **Relatório Final** – deve ser apresentado no prazo de um mês desde o momento da submissão do relatório intercalar ou da sua última versão atualizada.

Responsável pela comunicação

O Órgão de Administração destas entidades deve designar um **responsável pela comunicação** de incidentes de carácter severo relacionados com as TIC podendo, no entanto, ser contratado um terceiro prestador de serviços para este efeito.

A Norma esclarece também que no caso das **empresas de seguros e de resseguros com sede em Portugal e no caso das sociedades gestoras de fundos de pensões autorizadas em Portugal**, o responsável pela comunicação do incidente severo **pode ser o responsável pela função de segurança da informação**.

Notas finais

Quando um incidente afete **mais do que uma entidade ou todas as entidades do mesmo grupo**, os elementos acima referidos podem ser apresentados, de forma agregada, através de um reporte, desde que as entidades em causa se encontrem sujeitas à Norma Regulamentar n.º 9/2024-R, a origem do incidente seja a mesma e o incidente seja classificado como severo em todas as entidades.

As entidades deverão ter presente que a obrigação de comunicação à ASF ora prevista **difere da obrigação de reporte de incidentes cibernéticos** prevista nas Normas Regulamentares n.os 4/2023-R e 5/2023-R, de 11 de julho, nomeadamente quanto ao respetivo âmbito, momento da comunicação, natureza e finalidade da informação a prestar, sendo que a primeira não preclude a segunda, em caso de incidente cibernético.

Para aceder à **versão integral** da Norma Regulamentar da ASF n.º 9/2024-R, **clique aqui**.

Para mais informações sobre este tema, queira entrar em contacto com:

Miguel Cordeiro
Sócio | Bancário e Financeiro
micordeiro@deloitte.pt