REGULAMENTO DE EXECUÇÃO (UE) 2018/151 DA COMISSÃO

de 30 de janeiro de 2018

que estabelece normas de execução da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como à especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União ([1]), nomeadamente o artigo 16.º, n.º 8,

Considerando o seguinte:

(1) Em conformidade com a Diretiva (UE) 2016/1148, os prestadores de serviços digitais são livres de tomar as medidas técnicas e organizativas que considerem adequadas e proporcionadas para gerir os riscos de segurança que se coloquem às suas redes e aos seus sistemas de informação, desde que essas medidas garantam um nível adequado de segurança e tenham em conta os elementos previstos nessa diretiva.

(2) Na identificação das medidas técnicas e organizativas adequadas e proporcionadas, os prestadores de serviços digitais devem abordar a questão da segurança da informação de modo sistematizado, com base em análises de risco.

(3) A fim de garantir a segurança dos sistemas e das instalações, os prestadores de serviços digitais devem aplicar procedimentos de avaliação e de análise, os quais devem incidir na gestão sistematizada das redes e dos sistemas de informação, na segurança física e ambiental, na segurança dos fornecimentos e no controlo dos acessos.

(4) Ao realizarem uma análise de riscos no âmbito da gestão sistematizada das redes e dos sistemas de informação, os prestadores de serviços digitais devem ser incentivados a identificar riscos específicos e a quantificar a importância dos mesmos, por exemplo identificando ameaças a ativos críticos e o modo como estas podem afetar as atividades e determinando a maneira de melhor as atenuar com base nas capacidades atuais e nos recursos necessários.

(5) As estratégias de recursos humanos podem abranger a gestão de competências, incluindo aspetos ligados ao desenvolvimento de competências relacionadas com a segurança e à sensibilização. Ao decidir sobre um conjunto adequado de estratégias de segurança operacional, os prestadores de serviços digitais devem ser incentivados a ter em conta aspetos de gestão da mudança, de gestão de vulnerabilidades, de formalização de práticas operacionais e administrativas e de cartografia dos sistemas.

(6) As estratégias de arquitetura da segurança podem compreender, nomeadamente, a segregação de redes e sistemas, bem como medidas específicas de segurança para operações críticas, como operações de administração. A segregação de redes e sistemas pode permitir que o prestador de serviços digitais distinga elementos como fluxos de dados e recursos informáticos pertencentes a um cliente, grupo de clientes, a ele próprio ou a terceiros.

(7) As medidas tomadas em termos de segurança física e ambiental devem garantir a proteção das redes e dos sistemas de informação da organização contra danos causados por incidentes como roubo, incêndio, inundação e outros efeitos meteorológicos e cortes de corrente ou de telecomunicações.

(8) A segurança de fornecimentos como energia elétrica, combustível ou agentes de arrefecimento pode abranger a segurança da cadeia logística, a qual compreende, nomeadamente, a segurança dos terceiros contratantes e subcontratantes e da gestão de uns e outros. Entende-se por rastreabilidade dos fornecimentos críticos a capacidade do prestador de serviços digitais de identificar e registar fontes de fornecimentos desse tipo.

(9) Os utilizadores de serviços digitais devem compreender as pessoas singulares ou coletivas que são clientes ou subscritores de mercados em linha ou de serviços de computação em nuvem, ou que visitam sítios Web de motores de busca em linha para efetuar pesquisas por palavras-chave.

([1]) JO L 194 de 19.7.2016, p. 1.

(10) No contexto da determinação da importância do impacto de um incidente, os casos referidos no presente regulamento devem ser considerados uma lista não-exaustiva de incidentes com impacto substancial. Importa extrair ensinamentos da execução do presente regulamento e do trabalho do Grupo de Cooperação, no tocante à recolha de informações sobre boas práticas respeitantes a riscos e incidentes, bem como à discussão das formas de comunicação das notificações de incidentes, como referido no artigo 11.º, n.º 3, alíneas i) e m), da Diretiva (UE) 2016/1148. Daí poderão resultar orientações gerais sobre limiares quantitativos de parâmetros de notificação para desencadeamento da obrigação de notificação que incumbe aos prestadores de serviços digitais nos termos do artigo 16.º, n.º 3, da Diretiva (UE) 2016/1148. Caso se justifique, a Comissão poderá também ponderar a revisão dos limiares atualmente estabelecidos no regulamento.

(11) Para possibilitar que as autoridades competentes sejam informadas de novos riscos potenciais, os prestadores de serviços digitais devem ser incentivados a relatarem voluntariamente todos os incidentes cujas características não eram do seu conhecimento, tais como novas ocorrências, novos vetores de ataque ou novos autores de ameaças, novas vulnerabilidades e novos perigos.

(12) A aplicabilidade do presente regulamento deve ter início no dia seguinte ao termo do prazo de transposição da Diretiva (UE) 2016/1148.

(13) As medidas previstas no presente regulamento são conformes com o parecer do Comité de Segurança das Redes e dos Sistemas de Informação referido no artigo 22.º da Diretiva (UE) 2016/1148,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento especifica pormenorizadamente os elementos a ter em conta pelos prestadores de serviços digitais na identificação e adoção de medidas destinadas a garantir o nível de segurança das redes e dos sistemas de informação que esses prestadores proporcionam no contexto da oferta de serviços referidos no anexo III da Diretiva (UE) 2016/1148 e especifica pormenorizadamente os parâmetros a ter em conta para determinar se o impacto de um incidente na prestação desses serviços é substancial.

Artigo 2.º

Elementos de segurança

1. A segurança dos sistemas e das instalações referida no artigo 16.º, n.º 1, alínea a), da Diretiva (UE) 2016/1148 é a segurança das redes e dos sistemas de informação e do ambiente físico de umas e outros, dela fazendo parte os seguintes elementos:

a) A gestão sistematizada das redes e dos sistemas de informação, isto é, a cartografia dos sistemas de informação e o estabelecimento de um conjunto de estratégias adequadas de gestão da segurança da informação, incluindo análises de risco, recursos humanos, segurança operacional, arquitetura de segurança, segurança dos dados, gestão do sistema no ciclo de vida e, se for caso disso, encriptação e a gestão desta;

b) A segurança física e ambiental, isto é, a disponibilidade de um conjunto de medidas de proteção da segurança das redes e dos sistemas de informação dos prestadores de serviços digitais contra danos, por meio de uma abordagem global dos riscos que cubra todos os perigos, por exemplo cortes do sistema, erros humanos, ações dolosas e fenómenos naturais;

c) A segurança dos fornecimentos, isto é, o estabelecimento e a manutenção de estratégias adequadas para garantir a acessibilidade aos fornecimentos críticos para a prestação dos serviços e, se for caso disso, a rastreabilidade desses fornecimentos;

d) O controlo do acesso às redes e aos sistemas de informação, isto é, a disponibilidade de um conjunto de medidas destinadas a garantir que o acesso físico e lógico às redes e aos sistemas de informação, incluindo a segurança administrativa das redes e desses sistemas, é autorizado e restringido com base em requisitos comerciais e de segurança.

2. As medidas tomadas pelos prestadores de serviços digitais relativamente ao tratamento dos incidentes referido no artigo 16.º, n.º 1, alínea b), da Diretiva (UE) 2016/1148 devem compreender:

a) Processos e procedimentos de deteção mantidos e ensaiados para garantir uma perceção atempada e adequada de ocorrências anómalas;

b) Processos e estratégias de comunicação de incidentes e de identificação de fragilidades e vulnerabilidades nos sistemas de informação do prestador;

c) Reações conformes com procedimentos estabelecidos e comunicação dos resultados das medidas tomadas;

d) Avaliação da gravidade do incidente, documentando os conhecimentos extraídos da análise do incidente e das informações pertinentes recolhidas que possam servir de provas e de apoio a um processo de aperfeiçoamento contínuo.

3. A gestão da continuidade das atividades referida no artigo 16.º, n.º 1, alínea c), da Diretiva (UE) 2016/1148 é a capacidade de uma organização de, após um incidente perturbador, manter ou, se for caso disso, restabelecer a prestação de serviços a níveis aceitáveis predefinidos. Deve incluir:

a) O estabelecimento e a utilização de planos de contingência baseados numa análise de impacto nas atividades, destinados a assegurar a continuidade dos serviços fornecidos pelo prestador de serviços digitais, a avaliar e ensaiar periodicamente, por exemplo por meio de exercícios;

b) Capacidades de recuperação de desastres, a avaliar e ensaiar periodicamente, por exemplo por meio de exercícios.

4. O acompanhamento, a auditoria e os testes realizados referidos no artigo 16.º, n.º 1, alínea d), da Diretiva (UE) 2016/1148 devem compreender o estabelecimento e a manutenção de estratégias nos seguintes domínios:

a) A realização de uma sequência planeada de observações ou medições, para avaliar se as redes e os sistemas de informação estão a funcionar como pretendido;

b) Inspeções e verificações destinadas a avaliar se uma norma ou um conjunto de orientações está a ser seguido, se os registos são exatos e se os objetivos de eficiência e eficácia estão a ser atingidos;

c) Um processo destinado a evidenciar falhas nos mecanismos de segurança das redes e dos sistemas de informação, que protege os dados e mantém a funcionalidade pretendida. Este processo deve incluir os processos técnicos e o pessoal que participam no fluxo operacional.

5. As normas internacionais referidas no artigo 16.º, n.º 1, alínea e), da Diretiva (UE) 2016/1148 são normas aprovadas por um organismo internacional de normalização, como referido no artigo 2.º, n.º 1, alínea a), do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([1]). Em conformidade com o artigo 19.º da Diretiva (UE) 2016/1148, podem igualmente ser utilizadas normas e especificações europeias ou internacionalmente aceites, assim como normas nacionais, aplicáveis à segurança das redes e dos sistemas de informação.

6. Os prestadores de serviços digitais devem assegurar que dispõem de documentação adequada que permita à autoridade competente verificar a conformidade com os elementos de segurança estabelecidos nos n.ºs 1, 2, 3, 4 e 5.

Artigo 3.º

Parâmetros a ter em conta para determinar se o impacto de um incidente é substancial

1. O prestador de serviços digitais deve estar em condições de estimar, relativamente ao número de utilizadores afetados pelo incidente, nomeadamente de utilizadores que dependem do serviço para prestarem os seus próprios serviços, referido no artigo 16.º, n.º 4, alínea a), da Diretiva (UE) 2016/1148:

a) O número de pessoas singulares e de pessoas coletivas com as quais foi celebrado um contrato de prestação do serviço que foram afetadas; ou

b) O número de utilizadores que utilizaram o serviço que foram afetados, com base, designadamente, em dados de tráfego anteriores.

2. A «duração do incidente» referida no artigo 16.º, n.º 4, alínea b), é o período compreendido entre a perturbação da correta prestação do serviço, em termos de disponibilidade, autenticidade, integridade e confidencialidade, e o momento do restabelecimento do serviço.

3. Relativamente à distribuição geográfica, no que se refere à zona afetada pelo incidente, referida no artigo 16.º, n.º 4, alínea c), da Diretiva (UE) 2016/1148, o prestador de serviços digitais deve estar em condições de identificar se o incidente afeta a prestação dos seus serviços em Estados-Membros específicos.

4. Deve medir-se o nível de gravidade da perturbação do funcionamento do serviço referido no artigo 16.º, n.º 4, alínea d), da Diretiva (UE) 2016/1148 relativamente a uma ou mais das seguintes características afetadas pelo incidente: disponibilidade, autenticidade, integridade, confidencialidade dos dados ou dos serviços conexos.

([1]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

5. O prestador de serviços digitais deve estar em condições de concluir, relativamente à extensão do impacto nas atividades económicas e societais referida no artigo 16.º, n.º 4, alínea e), da Diretiva (UE) 2016/1148, com base em indicações como a natureza das suas relações contratuais com o cliente ou, se for caso disso, o número potencial de utilizadores afetados, se o incidente causou perdas materiais ou não-materiais significativas aos utilizadores, nomeadamente em termos de saúde, proteção ou danos patrimoniais.

6. Para efeitos dos n.ºs 1, 2, 3, 4 e 5, não pode ser exigido aos prestadores de serviços digitais que recolham informações adicionais às quais não tenham acesso.

Artigo 4.º

Incidentes com impacto substancial

1. Considera-se que um incidente tem impacto substancial caso se verifique alguma das seguintes situações:

a) O serviço prestado pelo prestador de serviços digitais esteve indisponível durante mais de 5 000 000 horas-utilizador, designando o termo «hora-utilizador» um utilizador afetado na União durante 60 minutos;

b) Resultou do incidente uma perda de integridade, autenticidade ou confidencialidade dos dados armazenados, transmitidos ou tratados ou dos serviços conexos oferecidos ou acessíveis através de redes e de sistemas de informação do prestador de serviços digitais, tendo sido afetados mais de 100 000 utilizadores da União;

c) O incidente gerou um risco de segurança pública, proteção pública ou morte;

d) O incidente provocou danos materiais superiores a 1 000 000 EUR a, pelo menos, um utilizador na União.

2. A Comissão pode rever os limiares estabelecidos no n.º 1, com base nas boas práticas recolhidas pelo Grupo de Cooperação no exercício das tarefas deste nos termos do artigo 11.º, n.º 3, da Diretiva (UE) 2016/1148 e nas discussões previstas na alínea m) desse número.

Artigo 5.º

Entrada em vigor

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

2. A aplicabilidade do presente regulamento inicia-se a 10 de maio de 2018.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 30 de janeiro de 2018.

Pela Comissão

O Presidente

Jean-Claude JUNCKER