CNPD
Comissão Nacional
de Proteção de Dados

DIRETRIZ/2023/1

Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais

1. Os ataques a sistemas de informação que têm ocorrido em número crescente, em especial no ano de 2022, alguns dos quais de grande dimensão e complexidade, afetaram, na sua grande maioria, dados pessoais.

2. Verifica-se que os principais vetores de ataque têm sido a exploração das vulnerabilidades das infraestruturas, a falta de formação dos utilizadores para detetarem campanhas de *phishing*[1] que permitem depois a distribuição de *malware*[2], com especial relevância para os ataques de *ransomware*[3], a ausência de consciencialização dos responsáveis pelos tratamentos quanto aos riscos para os direitos dos titulares dos dados que a falta de investimento em mecanismos de segurança acarreta.

3. Na verdade, na maior parte dos ataques a que se assistiu, as consequências para os direitos dos titulares dos dados poderiam ter sido senão evitadas, pelo menos substancialmente reduzidas.

4. Assim, a Comissão Nacional de Proteção de Dados (doravante CNPD), enquanto autoridade de controlo nacional, na prossecução da atribuição definida na alínea *d)* do n.º 1 do artigo 57.º do Regulamento Geral sobre a Proteção de Dados (RGPD)[4], em conjugação com o artigo 3.º da Lei n.º 58/2019, de 8 de agosto, entende oportuno sensibilizar os responsáveis pelos tratamentos e os subcontratantes para as suas obrigações no domínio da segurança dos tratamentos de dados pessoais.

5. Alerta-se para o facto de as medidas de segurança do tratamento de dados pessoais que em seguida se elencam não terem caráter exaustivo e serem forçosamente dinâmicas, pela sua direta dependência do desenvolvimento tecnológico, estando, por isso, sujeitas a atualização sempre que se revelar necessário.

---

[1] *Phishing* é um tipo de ataque que tem como objetivo capturar informação sensível de uma vítima, tentando enganá-la de modo que esta forneça informação sensível, seja por clicar em anexos ou *links* maliciosos no correio eletrónico, seja por partilhar dados em páginas fraudulentas.

[2] *Malware* refere-se a qualquer tipo de programa ou código malicioso criado para invadir, danificar ou incapacitar computadores e outros dispositivos, sistemas ou redes, ou até para roubar, encriptar ou apagar dados.

[3] *Ransomware* é um tipo específico de *malware* que encripta os ficheiros armazenados em servidores ou computadores, tornando-os inacessíveis, e exigindo um pagamento para a sua desencriptação. Alguns tipos de *ransomware* também extraem dados dos computadores afetados, enviando-os para os atacantes.

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

I. Sobre notificação de violação de dados

6. Uma violação de dados pessoais é «uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento», conforme definição constante do artigo 4.º, alínea 12*)*, do RGPD.

7. O RGPD introduz a obrigação de que seja notificada a violação de dados pessoais à autoridade de controlo nacional competente, no caso a CNPD, sempre que possível, até 72 horas, após ter tido conhecimento da mesma, nas situações em que a violação seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (Cf. artigo 33.º, n.º 1, do RGPD).

8. Quanto a este prazo sempre se refere que, mesmo que inicialmente o responsável pelo tratamento não esteja na posse de todas as informações necessárias, deve notificar a autoridade de controlo sem demora, informando que posteriormente fornecerá o resultado da investigação. E sublinha-se que o prazo é contínuo, não se suspendendo aos sábados, domingos e feriados.

9. De todo o modo, a informação necessária para notificar a autoridade de controlo pode ser fornecida por fases, como explicita o n.º 4 do artigo 33.º do RGPD.

10. Mesmo que o responsável pelo tratamento considere que não é exigível a notificação à CNPD, está obrigado a documentar quaisquer violações de dados, nos termos do n.º 5 do artigo 33.º do RGPD.

11. O responsável pelo tratamento está ainda obrigado a dar conhecimento aos titulares dos dados da ocorrência de uma violação de dados, se reunidos os requisitos legais e nas condições descritas no artigo 34.º do RGPD, ou seja, «quando a violação de dados for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares», e logo que seja razoavelmente possível. O principal objetivo dessa notificação é prestar informações específicas acerca das medidas que devem tomar para se protegerem das consequências negativas da violação dos seus dados pessoais.

12. Sendo certo que, desde 2018, cabe, em primeira linha, ao responsável pelo tratamento de dados pessoais assegurar o respeito pelos direitos e interesses dos titulares dos dados sobre ele recaindo o dever de verificar, antes de realizar um tratamento – bem como o dever de demonstrar –, se cumpre todas as regras de proteção de dados e se os concretos tratamentos de dados que realiza estão em conformidade com os princípios elencados no n.º 1 do artigo 5.º do RGPD.

13. No quadro de uma evolução profunda da tecnologia e de uma economia e sociedade cada vez mais digitais, a realização desse objetivo depende de os responsáveis pelo tratamento adaptarem os seus modelos de

negócio ou de gestão pública e os respetivos meios técnicos e organizativos para assegurar o efetivo cumprimento da lei e a devida proteção dos dados pessoais e da esfera de interesses, direitos e liberdades dos titulares dos mesmos.

14. Essa adaptação não deve ser meramente superficial e formal (burocrática), devendo os responsáveis pelo tratamento acompanhar as alterações de um tempo que é, em si mesmo, disruptivo, através da regular avaliação substantiva e profunda das operações de tratamento e do impacto que as tecnologias implicam no funcionamento das suas organizações e, no caso dos dados pessoais, dos riscos para os direitos e liberdades das pessoas singulares.

15. O recurso à subcontratação não altera o facto de o responsável pelo tratamento deter a responsabilidade global pela proteção dos dados pessoais. Os subcontratantes atuam apenas por conta do responsável, mediante as suas instruções (cf. artigo 4.º). No que diz respeito ao tratamento de dados pessoais, impõe o RGPD que a sua atuação resulte estritamente do que lhes for prescrito pelo responsável pelo tratamento (cf. artigo 28.º, n.º 3, alínea a*)*, do RGPD). Isto sem prejuízo de, caso o responsável pelo tratamento dê instruções que violem o RGPD ou outras disposições do direito da União ou dos Estados-Membros, o subcontratante dever informar imediatamente o responsável pelo tratamento de tal facto (cf. artigo 28.º, n.º 3, alínea h*)*, segundo parágrafo, do RGPD).

16. Com efeito, independentemente das propostas feitas pelos subcontratantes, a decisão última sobre as operações de tratamento de dados compete ao responsável pelo tratamento, que não pode eximir-se de desempenhar o seu papel e de cumprir as suas obrigações legais, eventualmente diferindo para subcontratantes responsabilidades que são apenas suas.

17. O responsável pelo tratamento deve ter em prática uma política interna que lhe permita detetar e gerir incidentes de segurança com impacto na proteção de dados pessoais e, quando o tratamento de dados for realizado por subcontratantes, ter mecanismos de controlo eficazes quanto à atuação dos subcontratantes, assegurando que aqueles não prejudicam o cumprimento das obrigações que recaem sobre o responsável neste domínio.

18. Neste contexto, e no exercício das suas atribuições e competências[5], a CNPD define, de forma sucinta, orientações para que os responsáveis pelo tratamento, e os subcontratantes (com as devidas adaptações), possam, através da adoção de medidas técnicas e organizativas adequadas, garantir a segurança adequada

[5] Cf. alíneas b*)* e d*)* do n.º 1 do artigo 57.º e alínea b) do n.º 1 do artigo 58.º do RGPD e artigos 3.º e 6.º da Lei n.º 58/2019, de 8 de agosto.

dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

II. Medidas técnicas e organizativas a adotar pelo responsável pelo tratamento e pelo subcontratante

19. Em conformidade com as exigências previstas no artigo 32.º, n.ºs 1 e 2, do RGPD, incumbe ao responsável pelo tratamento avaliar e aplicar as medidas técnicas e organizativas necessárias para conferir ao tratamento dos dados pessoais um nível de segurança adequado ao risco, incluindo a capacidade para garantir a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento.

20. Nesse sentido, e consoante o que for adequado às características e sensibilidade de cada tratamento de dados pessoais efetuado e às especificidades da concreta organização, devem ser consideradas as seguintes medidas de segurança:

A. Organizativas

a. Definir e exercitar regularmente o plano de resposta a incidentes e recuperação do desastre, prevendo os mecanismos necessários para garantir a segurança da informação e a resiliência dos sistemas e serviços, bem como assegurar que a disponibilidade dos dados é restabelecida atempadamente após um incidente;

b. Classificar a informação de acordo com o nível de confidencialidade e sensibilidade e adotar as medidas organizativas e técnicas adequadas à classificação;

c. Documentar as políticas de segurança;

d. Adotar procedimentos de análise para a monitorização dos fluxos de tráfego na rede;

e. Definir políticas de gestão de palavras-passe seguras, impondo requisitos para o tamanho, a composição, o armazenamento e a frequência com que uma palavra-passe precisa de ser alterada;

f. Criar uma política de gestão de ciclo de vida dos utilizadores, para garantir que cada trabalhador tem acesso apenas aos dados necessários para executar as suas funções e rever com frequência as permissões dos vários perfis de utilizadores, se possível, bem como a desativação/revogação de perfis inativos

g. Adotar alarmística que permita identificar situações de acesso, tentativas ou utilização indevida;

h. Definir, numa fase inicial, as melhores práticas de segurança de informação a adotar, quer em fase de desenvolvimento de *software*, quer em fase de testes de aceitação, considerando em particular:

os princípios de proteção de dados desde a conceção e por defeito, análises de risco do tratamento e do ciclo de vida dos dados, métodos de pseudonimização e anonimização dos dados –mesmo quando o sistema é desenvolvido e mantido por subcontratante(s);

i. Realizar auditorias de segurança de TI[6] e avaliações de vulnerabilidade (testes de penetração) sistemáticos, para que os utilizadores possam ter conhecimento das próprias fragilidades e para que as organizações consigam monitorizar os alvos mais frágeis e invistam em formação com conteúdo específico e direcionado, de acordo com as vulnerabilidades detetadas;

j. Verificar se as medidas de segurança definidas estão em prática, garantindo que são eficazes e atualizando-as regularmente, especialmente quando o processamento ou as circunstâncias se alteram, incluindo as que são implementadas pelos subcontratantes nos tratamentos de dados;

k. Documentar e corrigir as vulnerabilidades de segurança detetadas sem demora;

l. Tomar as medidas necessárias para garantir o pleno cumprimento do artigo 33.º do RGPD, em particular no que diz respeito ao desenvolvimento de uma política interna para lidar e documentar eventuais violações de dados pessoais;

m. Fomentar junto dos colaboradores uma cultura de privacidade e segurança da informação, para que cada colaborador esteja capacitado para reconhecer potenciais ameaças e agir em conformidade, e como forma de reduzir a ocorrência e o impacto do erro humano;

n. Dar a conhecer aos trabalhadores o dever de confidencialidade a que estão sujeitos pelo facto de tratarem dados pessoais;

o. Avaliar periodicamente as medidas de segurança, técnicas e organizativas, internas e proceder à sua atualização e revisão sempre que necessário.

B. Técnicas

i. Autenticação

a. Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, alterando-as com frequência;

b. Equacionar, designadamente face à sensibilidade da informação, aos privilégios dos utilizadores ou à forma de acesso (*v.g.* remota), a aplicação de autenticação multifator;

[6] Tecnologias de informação.

ii. Infraestrutura e sistemas

a. Garantir que os sistemas operativos de servidores e terminais se encontram atualizados, bem como todas as aplicações (por exemplo, *browser* e *plugins*);

b. Manter atualizado o *firmware* dos equipamentos de rede;

c. Desenhar e organizar os sistemas e a infraestrutura por forma a segmentar ou isolar os sistemas e as redes de dados para prevenir a propagação de *malware* dentro da organização e para sistemas externos;

d. Robustecer a segurança dos postos de trabalho e servidores, nomeadamente:

   i. bloquear o acesso a sítios que sejam suscetíveis de constituir um risco para a segurança;

   ii. bloquear os redireccionamentos suspeitos através de motores de busca;

   iii. bloquear de imediato os ficheiros e aplicações infetadas com *malware*[2];

   iv. realizar inspeção periódica do estado e utilização dos recursos do sistema;

   v. monitorizar a utilização do *software* instalado;

   vi. ativar e conservar os registos de auditoria (*log*);

   vii. validar os acessos por *IP* aos servidores que estão expostos ao público;

   viii. alterar o porto configurado por omissão para o protocolo de acessos remotos (*RDP*).

iii. Ferramenta de correio eletrónico

a. Definir de forma clara e inequívoca políticas e procedimentos internos sobre o específico envio de mensagens de correio eletrónico contendo dados pessoais, que introduzam as verificações adicionais necessárias, no sentido de:

   i. garantir a inserção dos endereços de correio eletrónico dos destinatários no campo *'Bcc*:', nos casos de múltiplos destinatários;

   ii. prevenir erros na introdução manual de endereços de correio eletrónico;

   iii. assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendem comunicar;

b. Equacionar a criação de listas de distribuição ou grupos de contacto, com o objetivo de prevenir a divulgação dos endereços dos destinatários em operações de envio massivo de mensagens de correio eletrónico;

c. Equacionar a criação de regras com o objetivo de adiar/atrasar a entrega de mensagens de correio eletrónico contendo dados pessoais, mantendo-as na 'Caixa de Saída' por um tempo determinado, permitindo verificações de conformidade, após clique em 'Enviar';

d. Encriptar com código, ao qual só o destinatário tenha acesso, os emails e/ou anexos enviados que contenham dados pessoais;

e. Confirmar com o destinatário, antes de envio de e-mail contendo dados pessoais, o endereço de e-mail preferencial para contacto;

f. Realizar ações de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico de acordo com os procedimentos definidos, sensibilizando-os para os erros mais comuns, potencialmente suscetíveis de originar violações de dados pessoais e incentivando-os à dupla verificação;

g. Reforçar o sistema de alerta da ferramenta de alarmística utilizada pela entidade, para assegurar visibilidade imediata sobre a criação por utilizadores de regras de encaminhamento automático de e-mails para contas externas;

h. Reforçar o sistema com ferramentas *antiphishing* e *antispam*, que permitam bloquear ligações e/ou anexos com código malicioso;

i. Adotar controlos de segurança que permitam classificar e proteger as mensagens de correio eletrónico sensíveis.

iv. Proteção contra *malware*

a. Utilizar encriptação segura especialmente no caso de credenciais de acesso, de dados especiais[7], de dados de natureza altamente pessoal[8] ou de dados financeiros;

b. Criar um sistema de cópias de segurança (*backup*) atualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa;

7 Os dados pessoais elencados no n.º 1 do artigo 9.º do RGPD.

8 Grosso modo, os dados pessoais relacionados com condenações penais e infrações (cf. artigo 10.º do RGPD) ou com dimensões da vida privada e familiar.

c. Reforçar o sistema com ferramentas *antimalware* que inclua a capacidade de o verificar e detetar, bem como o bloqueio em tempo real de ameaças do tipo *ransomware*.

v. Utilização de equipamentos em ambiente externo

a. Armazenar dados em sistemas internos, protegidos com medidas de segurança apropriadas, e acessíveis remotamente através mecanismos de acesso seguro (VPN);

b. Permitir acessos apenas por VPN;

c. Bloquear as contas após várias tentativas inválidas de *login*;

d. Ativar a autenticação multifator para os utilizadores dos equipamentos;

e. Aplicar cifragem dos dados no sistema operativo;

f. Sempre que for aplicável, ativar a funcionalidade de "*remote wipe*" e "*find my device*";

g. Efetuar cópias de segurança automáticas das pastas de trabalho, quando o equipamento se encontra ligado à rede da entidade;

h. Definir regras claras e adequadas para a utilização de equipamentos em ambiente externo.

vi. Armazenamento de documentos em papel que contenham dados pessoais

a. Utilizar papel e impressão que seja durável;

b. Conservar documentação em local com controlo de humidade e temperatura;

c. Armazenar, devidamente organizados, os documentos que contêm dados pessoais sensíveis em local fechado, resistente ao fogo e inundação;

d. Controlar os acessos, com registo das respetivas data e hora, de quem acede e do(s) específico(s) documento(s) acedido(s).

e. Destruir os documentos através de equipamento específico que garanta a destruição "segura";

vii. Transporte de informação que integre dados pessoais

a. Adotar medidas para impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;

b. Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB).

III. Conclusão

21. Os responsáveis pelo tratamento e os subcontratantes são incentivados a definir antecipadamente e a colocar em prática planos de prevenção, para que possam proteger os seus sistemas e infraestrutura e ter mecanismos prontos a detetar uma violação de dados pessoais e mitigar rapidamente os efeitos negativos sobre os direitos dos respetivos titulares. Esse plano de resposta a incidentes deve incluir uma avaliação do risco para estas pessoas singulares, que permita ao responsável pelo tratamento concluir se deve notificar a violação de dados, quer à autoridade de controlo, quer aos titulares dos dados afetados.

22. A informação necessária para notificar a autoridade de controlo pode ser fornecida por fases, mas isso não exclui a obrigação de o responsável pelo tratamento agir em tempo útil para dar resposta à violação de dados pessoais.

23. Assim, ao abrigo do artigo 57.º, n.º 1, alínea d*)*, do RGPD, a CNPD recomenda ao responsável pelo tratamento, bem como ao subcontratante (com as devidas adaptações), que adote medidas de segurança elencadas na presente diretriz, consoante o que for adequado às características e sensibilidade dos tratamentos de dados pessoais efetuados e às especificidades da sua organização, com vista a dar cumprimento às obrigações previstas no artigo 32.º, n.ºs 1 e 2, do RGPD, quanto à segurança do tratamento de dados pessoais.

Aprovada na reunião da CNPD de 10 de janeiro de 2023