Orientações 01/2021

sobre exemplos da notificação de uma violação de dados pessoais

Adotadas em 14 de dezembro de 2021

Versão 2.0

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Histórico das versões

Versão 2.0	14.12.2021	Adoção das orientações após consulta pública
Versão 1.0	14.1.2021	Adoção das orientações para consulta pública

Índice

O COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS

Tendo em conta o artigo 70.º, n.º 1, alínea e), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado por «RGPD»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta os artigos 12.º e 22.º do seu regulamento interno,

Tendo em conta a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital – dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados»[2],

ADOTOU AS PRESENTES ORIENTAÇÕES:

1 INTRODUÇÃO

1. O RGPD introduz, em certos casos, o requisito de que seja notificada a violação de dados pessoais à autoridade de controlo nacional competente (a seguir designada por «AC») e de comunicar a violação às pessoas singulares cujos dados pessoais tenham sido afetados pela violação (artigos 33.º e 34.º).

2. Em outubro de 2017, o Grupo de Trabalho do Artigo 29.º elaborou orientações *gerais* sobre a notificação de uma violação de dados pessoais, analisando as secções pertinentes do RGPD [Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, WP250] (a seguir designadas por «Orientações WP250»)[3]. No entanto, devido à sua natureza e calendário, estas orientações não abordaram todas as questões práticas de forma suficientemente pormenorizada. Por conseguinte, surgiu a necessidade de criar orientações *práticas e casuísticas* que utilizem a experiência adquirida pelas AC desde que o RGPD está em vigor.

3. O presente documento destina-se a complementar as Orientações WP250 e reflete as experiências comuns das AC do EEE desde a entrada em vigor do RGPD. O seu objetivo é ajudar os responsáveis pelo tratamento

[1] As referências a «Estados-Membros» efetuadas ao longo do presente documento devem entender-se como referências a «Estados-Membros do EEE».

[2] COM(2020) 264 final de 24 de junho de 2020.

[3] GT29 WP250 rev.1, de 6 de fevereiro de 2018, «Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679» – aprovadas pelo CEPD, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

de dados a decidir como lidar com violações de dados e quais os fatores a ter em conta durante a avaliação dos riscos.

4. Em qualquer tentativa de resolver uma violação, o responsável pelo tratamento e o subcontratante devem primeiro ser capazes de reconhecer uma. O artigo 4.º, n.º 12, do RGPD define uma «violação de dados pessoais» como «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».

5. No seu Parecer 03/2014 relativo à notificação da violação de dados pessoais[4] e nas respetivas Orientações WP250, o GT29 explicou que as violações podem ser categorizadas de acordo com os três princípios bem conhecidos de segurança da informação que se seguem:

- «Violação da confidencialidade» – quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais,
- «Violação da integridade» – quando existe uma alteração acidental ou não autorizada dos dados pessoais,
- «Violação da disponibilidade» – quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais[5].

6. Uma violação pode potencialmente ter um leque de efeitos adversos significativos sobre as pessoas, que podem resultar em danos físicos, materiais ou imateriais. O RGPD explica que estes podem incluir a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação e a perda de confidencialidade de dados pessoais protegidos por sigilo profissional. Podem incluir igualmente qualquer outra desvantagem económica ou social significativa para essas pessoas singulares. Uma das obrigações mais importantes do responsável pelo tratamento é avaliar estes riscos para os direitos e liberdades dos titulares dos dados e aplicar medidas técnicas e organizativas adequadas para corrigi-los.

7. Por conseguinte, o RGPD exige que o responsável pelo tratamento:

- Documente quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada[6];
- Notifique a violação de dados pessoais à autoridade de controlo, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares[7];

---

[4] GT29 WP 213, 25 de março de 2014, Parecer 03/2014 relativo à notificação da violação de dados pessoais, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Ver Orientações WP250, p. 7. – Importa ter em conta que uma violação de dados pode dizer respeito a uma ou mais categorias em simultâneo ou combinadas.

[6] Artigo 33.º, n.º 5, do RGPD.

[7] Artigo 33.º, n.º 1, do RGPD.

- Comunique a violação de dados pessoais ao titular dos dados quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares[8].

8. As violações de dados são por si só um problema, mas podem também ser sintomas de um sistema de segurança dos dados vulnerável, possivelmente desatualizado, podendo também indicar deficiências do sistema a resolver. A verdade é que é sempre melhor prevenir as violações de dados preparando-se antecipadamente, uma vez que várias consequências são, por natureza, irreversíveis. Antes de um responsável pelo tratamento poder avaliar *totalmente* o risco decorrente de uma violação causada por alguma forma de ataque, é necessário identificar a causa principal do problema, a fim de determinar se as vulnerabilidades que deram origem ao incidente ainda se encontram presentes e, por conseguinte, ainda são exploráveis. Em muitos casos, o responsável pelo tratamento é capaz de identificar que o incidente é suscetível de resultar num risco, pelo que deve ser notificado. Noutros casos, a notificação não precisa de ser adiada até que o risco e o impacto em torno da violação tenham sido plenamente avaliados, uma vez que a avaliação completa dos riscos pode ocorrer paralelamente à notificação e as informações assim obtidas podem ser fornecidas por fases à AC, sem demora injustificada[9].

9. A violação deve ser notificada quando o responsável pelo tratamento considerar que é suscetível de resultar num risco para os direitos e liberdades do titular dos dados. Os responsáveis pelo tratamento devem efetuar esta avaliação no momento em que tomam conhecimento da violação. O responsável pelo tratamento não deve aguardar um exame forense pormenorizado e medidas de atenuação (precoces) antes de avaliar se a violação de dados é ou não suscetível de resultar num risco e, por conseguinte, deve ser notificada.

10. Se um responsável pelo tratamento autoavaliar o risco como improvável, mas se verificar que o risco se materializa, a AC competente pode utilizar os seus poderes de correção e decidir aplicar sanções.

11. Todos os responsáveis pelo tratamento e subcontratantes devem dispor de planos e procedimentos para o tratamento de eventuais violações de dados. As organizações devem dispor de hierarquias claras e de pessoas responsáveis por determinados aspetos do processo de recuperação.

12. A formação e a sensibilização para questões de proteção de dados destinadas ao pessoal do responsável pelo tratamento e do subcontratante, centradas na gestão das violações de dados pessoais (identificação de um incidente de violação de dados pessoais e outras medidas a tomar, etc.), são também essenciais para os responsáveis pelo tratamento e os subcontratantes. Esta formação deve ser repetida regularmente, em função do tipo de atividade de tratamento e da dimensão do responsável pelo tratamento, abordando as tendências mais recentes e os alertas decorrentes de ciberataques ou outros incidentes de segurança.

13. O princípio da responsabilização e o conceito de proteção de dados desde a conceção poderiam incorporar uma análise que seria incluída no *Handbook on Handling Personal Data Breach* (Manual sobre o Tratamento da Violação de Dados Pessoais) do responsável pelo tratamento e do subcontratante, que visa estabelecer factos para cada elemento do tratamento em cada uma das fases importantes da operação. Esse manual preparado antecipadamente proporcionaria uma fonte de informação muito mais rápida para permitir que os responsáveis pelo tratamento de dados e os subcontratantes atenuassem os riscos e cumprissem as obrigações sem demora injustificada, de modo a assegurar que, em caso de violação de dados pessoais, as

[8] Artigo 34.º, n.º 1, do RGPD.

[9] Artigo 33.º, n.º 4, do RGPD.

pessoas na organização saibam o que fazer e o incidente seja tratado de forma provavelmente mais célere do que se não existissem medidas de atenuação ou um plano.

14. Embora os casos a seguir apresentados sejam fictícios, baseiam-se em casos típicos retirados da experiência coletiva da AC em matéria de notificação de violações de dados. As análises propostas dizem explicitamente respeito aos casos apresentados, mas com o objetivo de prestar assistência aos responsáveis pelo tratamento de dados na avaliação das suas próprias violações de dados. Qualquer alteração das circunstâncias dos casos a seguir descritos pode resultar em níveis de risco diferentes ou mais significativos, exigindo assim medidas diferentes ou acrescidas. As presentes orientações estruturam os casos de acordo com determinadas categorias de violações (por exemplo, ataques de *software* de sequestro). Cada caso exige determinadas medidas de atenuação quando se trata de uma determinada categoria de violações. Estas medidas não são necessariamente repetidas em cada caso de análise pertencente à mesma categoria de violações. Para os casos pertencentes à mesma categoria, apenas são indicadas as diferenças. Por conseguinte, o leitor deve ler todos os casos relevantes para a categoria da violação em causa, a fim de identificar e distinguir todas as medidas corretas a tomar.

15. A documentação interna de uma violação é uma obrigação independente dos riscos inerentes à violação e deve ser realizada em todos os casos. Os casos a seguir apresentados tentam esclarecer se é necessário ou não notificar a violação à AC e comunicá-la aos titulares dos dados afetados.

2 *SOFTWARE* DE SEQUESTRO

16. Uma causa frequente para uma notificação de uma violação de dados é um ataque de *software* de sequestro sofrido pelo responsável pelo tratamento. Nestes casos, um código malicioso cifra os dados pessoais e, subsequentemente, o atacante exige ao responsável pelo tratamento um resgate em troca do código de decifração. Este tipo de ataque pode geralmente ser classificado como uma violação da disponibilidade, mas, muitas vezes, também pode ocorrer uma violação da confidencialidade.

2.1 CASO n.º 01: *software* de sequestro com uma cópia de segurança adequada e sem exfiltração

Os sistemas informáticos de uma pequena empresa transformadora foram expostos a um ataque de *software* de sequestro e os dados armazenados nesses sistemas foram cifrados. O responsável pelo tratamento utilizou a cifragem em repouso, pelo que todos os dados acedidos pelo *software* de sequestro foram armazenados sob forma cifrada utilizando um algoritmo de cifragem de ponta. A chave de decifração não foi comprometida no ataque, ou seja, o atacante não pôde aceder à mesma nem a utilizar indiretamente. Consequentemente, o atacante apenas teve acesso a dados pessoais cifrados. Em especial, nem o sistema de correio eletrónico da empresa nem os sistemas de clientes utilizados para aceder à mesma foram afetados. A empresa utiliza os conhecimentos especializados de uma empresa externa de cibersegurança para investigar o incidente. Estão disponíveis registos de todos os fluxos de dados que saem da empresa (incluindo correio eletrónico de saída). Após análise dos registos e dos dados recolhidos pelos sistemas de deteção que a empresa implantou, um inquérito interno apoiado pela empresa externa de cibersegurança determinou *com certeza* que o atacante apenas cifrou dados, sem os exfiltrar. Os registos não mostram qualquer fluxo de dados de saída no período do ataque. Os dados pessoais afetados pela violação dizem respeito a clientes e trabalhadores da empresa, algumas dezenas de pessoas no total. Havia uma cópia de segurança disponível, tendo os dados sido restaurados algumas horas após o ataque. A violação não teve quaisquer consequências para o funcionamento quotidiano do responsável pelo tratamento. Não houve atrasos nos pagamentos dos trabalhadores nem no tratamento dos pedidos dos clientes.

17. Neste caso, foram obtidos os seguintes elementos a partir da definição de «violação de dados pessoais»: uma violação da segurança levou à alteração ilegal e ao acesso não autorizado aos dados pessoais armazenados.

2.1.1 CASO n.º 01 – Medidas prévias e avaliação dos riscos

18. Tal como acontece com todos os riscos colocados por intervenientes externos, a probabilidade de um ataque de *software* de sequestro ser bem-sucedido pode ser drasticamente reduzida através do reforço da segurança do ambiente de controlo de dados. É possível evitar a maioria destas violações garantindo a adoção de medidas de segurança adequadas a nível organizacional, físico e tecnológico. Exemplos de tais medidas são a gestão adequada das atualizações corretivas e a utilização de um sistema de deteção anti-*malware* adequado. A existência de uma cópia de segurança adequada e separada ajudará a atenuar as consequências de um ataque bem-sucedido, caso este ocorra. Além disso, um programa de educação, formação e sensibilização em matéria de segurança dos trabalhadores (SETA) ajudará a prevenir e a reconhecer este tipo de ataques. (A secção 2.5 contém uma lista de medidas aconselháveis). Entre as medidas apresentadas, uma gestão adequada das atualizações corretivas que assegure que os sistemas estão atualizados e que todas as vulnerabilidades conhecidas dos sistemas implantados são corrigidas é uma das medidas mais importantes, uma vez que a maioria dos ataques de *software* de sequestro exploram vulnerabilidades bem conhecidas.

19. Ao avaliar os riscos, o responsável pelo tratamento deve investigar a violação e identificar o tipo de código malicioso para compreender as possíveis consequências do ataque. Entre esses riscos a considerar figura o risco de os dados serem exfiltrados sem deixar vestígios nos registos dos sistemas.

20. Neste exemplo, o atacante teve acesso a dados pessoais e a confidencialidade do texto cifrado que contém dados pessoais sob forma cifrada ficou comprometida. No entanto, quaisquer dados que possam ter sido exfiltrados não podem ser lidos ou utilizados pelo atacante, pelo menos por enquanto. A técnica de cifragem utilizada pelo responsável pelo tratamento está em conformidade com o estado da técnica. A chave de decifração não foi comprometida e, presumivelmente, também não pôde ser determinada por outros meios. Por conseguinte, os riscos de confidencialidade para os direitos e liberdades das pessoas singulares são reduzidos a um progresso criptanalítico mínimo que torne os dados cifrados inteligíveis no futuro.

21. O responsável pelo tratamento deve ter em conta o risco para as pessoas resultantes de uma violação[10]. Neste caso, afigura-se que os riscos para os direitos e liberdades dos titulares dos dados resultam da falta de disponibilidade dos dados pessoais e a confidencialidade dos dados pessoais não é comprometida[11].

---

[10] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver as «Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679», WP 248 rev.01, do Grupo de Trabalho do Artigo 29.º – aprovadas pelo CEPD, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Tecnicamente, a cifragem dos dados implicará o «acesso» aos dados originais e, no caso de *software* de sequestro, o apagamento do original – os dados têm de ser acedidos através de um código de *software* de sequestro para os encriptar e remover os dados originais. Um atacante pode fazer uma cópia do original antes de apagar, mas os dados pessoais nem sempre serão extraídos. À medida que o inquérito do responsável pelo tratamento progride, podem

Neste exemplo, os efeitos adversos da violação foram atenuados muito pouco tempo após a ocorrência da violação. A existência de uma cópia de segurança adequada[12] torna os efeitos da violação menos graves e, neste caso, o responsável pelo tratamento pôde utilizá-la efetivamente.

22. Quanto à gravidade das consequências para os titulares dos dados, só foi possível identificar consequências menores, uma vez que os dados afetados foram restaurados em poucas horas, a violação não teve quaisquer consequências para o funcionamento quotidiano do responsável pelo tratamento e não teve qualquer efeito significativo sobre os titulares dos dados (por exemplo, pagamentos de trabalhadores ou tratamento de pedidos de clientes).

2.1.2 CASO n.º 01 – Atenuação e obrigações

23. Sem uma cópia de segurança, existem poucas medidas à disposição do responsável pelo tratamento para reparar a perda de dados pessoais, devendo os dados ser novamente recolhidos. No entanto, neste caso específico, a reposição de todos os sistemas comprometidos para um estado limpo, que se sabe estar livre de códigos maliciosos, e que permita corrigir as vulnerabilidades e restaurar os dados afetados pouco tempo após o ataque, permitiria atenuar eficazmente os impactos do ataque. Sem uma cópia de segurança, os dados perdem-se e a gravidade pode aumentar porque os riscos ou impactos para as pessoas também aumentam.

24. Um restauro eficaz e atempado dos dados a partir de uma cópia de segurança de fácil acesso é uma variável fundamental na análise da violação. A fixação de um prazo adequado para restaurar os dados comprometidos depende das circunstâncias únicas da violação em causa. O RGPD determina que uma violação de dados pessoais deve ser notificada sem demora injustificada e, sempre que possível, no prazo máximo de 72 horas. Por conseguinte, pode determinar-se que, em qualquer um dos casos, não é aconselhável exceder o prazo de 72 horas, mas quando se trata de casos de alto risco, mesmo o cumprimento deste prazo pode ser considerado insatisfatório.

25. Neste caso, na sequência de uma avaliação de impacto pormenorizada e de um plano de resposta a incidentes, o responsável pelo tratamento considerou que a violação não era suscetível de implicar um risco para os direitos e liberdades das pessoas singulares e, como tal, não era necessário comunicar a violação aos titulares dos dados, nem a notificar à AC. No entanto, à semelhança do que acontece com todas as violações de dados, estas devem ser documentadas em conformidade com o artigo 33.º, n.º 5. Pode igualmente ser necessário (ou, mais tarde, exigido pela AC) que a organização atualize e corrija as suas medidas e procedimentos organizativos e técnicos em matéria de segurança dos dados pessoais e de redução dos riscos. No âmbito desta atualização e redução, a organização deve investigar exaustivamente a violação e identificar as causas e os métodos utilizados pelo atacante, a fim de evitar quaisquer situações semelhantes no futuro.

---

surgir novas informações para alterar esta avaliação. O acesso que resulte na destruição, perda e alteração ilícita, divulgação não autorizada dos dados pessoais ou num risco de segurança para um titular dos dados, mesmo sem interpretação dos dados, pode ser tão grave como o acesso com interpretação dos dados pessoais.

[12] Os procedimentos de cópia de segurança devem ser estruturados, coerentes e reprodutíveis. Exemplos de procedimentos de cópia de segurança incluem o método 3-2-1 e o método «grandfather-father-son». É importante testar sempre qualquer método para aferir a eficácia da cobertura e caso seja necessário restaurar os dados. Os testes devem também ser repetidos a intervalos regulares e, em especial, quando ocorram alterações na operação de tratamento ou nas suas circunstâncias, a fim de garantir a integridade do sistema.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

2.2 CASO n.º 02: *software* de sequestro sem uma cópia de segurança adequada

Um dos computadores utilizados por uma empresa agrícola foi exposto a um ataque de *software* de sequestro e os seus dados foram cifrados pelo atacante. A empresa está a utilizar os conhecimentos especializados de uma empresa externa de cibersegurança para controlar a sua rede. Estão disponíveis registos de todos os fluxos de dados que saem da empresa (incluindo correio eletrónico de saída). Após análise dos registos e dos dados que os outros sistemas de deteção recolheram, o inquérito interno, com o auxílio da empresa de cibersegurança, determinou que o atacante apenas cifrou os dados, sem os exfiltrar. Os registos não mostram qualquer fluxo de dados de saída no período do ataque. Os dados pessoais afetados pela violação dizem respeito a clientes e trabalhadores da empresa, algumas dezenas de pessoas no total. Não foram afetadas categorias especiais de dados. Não existia uma cópia de segurança em formato eletrónico. A maior parte dos dados foi restaurado a partir de cópias de segurança em papel. O restauro dos dados demorou cinco dias úteis e provocou ligeiros atrasos na entrega de encomendas aos clientes.

2.2.1 CASO n.º 02 – Medidas prévias e avaliação dos riscos

26. O responsável pelo tratamento dos dados devia ter adotado as mesmas medidas prévias que foram mencionadas na parte 2.1 e na secção 2.9. A principal diferença em relação ao caso anterior é a falta de uma cópia de segurança eletrónica e a falta de cifragem em repouso, o que cria diferenças críticas nas etapas que se seguem.

27. Ao avaliar os riscos, o responsável pelo tratamento deve investigar o método de infiltração e identificar o tipo de código malicioso para compreender as possíveis consequências do ataque. Neste exemplo, o *software* de sequestro cifrou os dados pessoais sem os exfiltrar. Como tal, afigura-se que os riscos para os direitos e liberdades dos titulares dos dados resultam da falta de disponibilidade dos dados pessoais e a confidencialidade dos dados pessoais não é comprometida. Para determinar o risco, é essencial proceder a uma análise minuciosa dos registos das barreiras de segurança (*firewalls*) e das suas implicações. O responsável pelo tratamento deve apresentar, mediante pedido, as conclusões factuais dessas investigações.

28. O responsável pelo tratamento dos dados deve ter em mente que, se o ataque for mais sofisticado, o *malware* tem a funcionalidade de editar ficheiros de registo e remover o rastreio. Assim – uma vez que os registos não são transmitidos ou reproduzidos para um servidor de registo central – mesmo após um inquérito minucioso que tenha determinado que os dados pessoais não foram exfiltrados pelo atacante, o responsável pelo tratamento não pode declarar que a ausência de uma entrada de registo prova a ausência de exfiltração, pelo que a probabilidade de violação da confidencialidade não pode ser totalmente rejeitada.

29. O responsável pelo tratamento deve avaliar os riscos desta violação[13] se o atacante tiver acedido aos dados. Durante a avaliação dos riscos, o responsável pelo tratamento deve também ter em conta a natureza, a sensibilidade, o volume e o contexto dos dados pessoais afetados pela violação. Neste caso, não são afetadas

[13] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

categorias especiais de dados pessoais e a quantidade de dados violados e o número de titulares de dados afetados são reduzidos.

30. A recolha de informações precisas sobre o acesso não autorizado é fundamental para determinar o nível de risco e prevenir um ataque novo ou continuado. Se os dados tivessem sido copiados da base de dados, tal teria constituído obviamente um fator de maior risco. Em caso de incerteza quanto às especificidades do acesso ilegítimo, deve ser considerado o pior cenário e o risco deve ser avaliado em conformidade.

31. A ausência de uma base de dados de cópia de segurança pode ser considerada um fator de maior risco, dependendo da gravidade das consequências para os titulares dos dados resultantes da falta de disponibilidade dos dados.

2.2.2 CASO n.º 02 – Atenuação e obrigações

32. Sem uma cópia de segurança, restam poucas medidas que o responsável pelo tratamento possa tomar para reparar a perda de dados pessoais, e os dados têm de ser novamente recolhidos, a menos que esteja disponível outra fonte (por exemplo, mensagens de confirmação de encomendas). Sem uma cópia de segurança, os dados podem perder-se e a gravidade dependerá do impacto sobre as pessoas.

33. O restauro dos dados não deve revelar-se excessivamente problemático[14] se os dados ainda estiverem disponíveis em papel, mas dada a falta de uma base de dados eletrónica de segurança, considera-se necessária uma notificação à AC, uma vez que o restauro dos dados demorou algum tempo e pode causar alguns atrasos na entrega das encomendas aos clientes e pode não ser possível recuperar uma quantidade considerável de metadados (por exemplo, registos, carimbo de data/hora).

34. A comunicação da violação aos titulares dos dados pode também depender da duração da indisponibilidade dos dados pessoais e das dificuldades daí resultantes para o funcionamento do responsável pelo tratamento (por exemplo, atrasos na transferência dos pagamentos dos trabalhadores). Uma vez que estes atrasos nos pagamentos e nas entregas podem provocar perdas financeiras para as pessoas cujos dados foram comprometidos, também se pode argumentar que a violação é suscetível de resultar num elevado risco. Além disso, poderá dar-se o caso de ser obrigatório informar os titulares dos dados caso a sua contribuição seja necessária para restaurar os dados cifrados.

35. Este caso serve de exemplo para um ataque de *software* de sequestro que implica um risco para os direitos e liberdades dos titulares dos dados, mas que não implica um risco elevado. Deve ser documentado em conformidade com o artigo 33.º, n.º 5, e notificado à AC em conformidade com o artigo 33.º, n.º 1. Pode igualmente ser necessário (ou exigido pela AC) que a organização atualize e corrija as suas medidas e procedimentos organizativos e técnicos em matéria de segurança dos dados pessoais e de redução dos riscos.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	X

[14] Tal dependerá da complexidade e da estrutura dos dados pessoais. Nos cenários mais complexos, o restabelecimento da integridade dos dados, a coerência com os metadados, a garantia de relações corretas dentro das estruturas de dados e a verificação da exatidão dos dados podem exigir recursos e esforços significativos.

2.3 CASO n.º 03: *software* de sequestro com cópia de segurança e sem exfiltração num hospital

O sistema de informação de um hospital/centro de saúde foi exposto a um ataque de *software* de sequestro e uma parte significativa dos seus dados foi cifrada pelo atacante. A empresa está a utilizar os conhecimentos especializados de uma empresa externa de cibersegurança para controlar a sua rede. Estão disponíveis registos de todos os fluxos de dados que saem da empresa (incluindo correio eletrónico de saída). Após análise dos registos e dos dados que os outros sistemas de deteção recolheram, o inquérito interno, com o auxílio da empresa de cibersegurança, determinou que o atacante apenas cifrou os dados, sem os exfiltrar. Os registos não mostram qualquer fluxo de dados de saída no período do ataque. Os dados pessoais afetados pela violação dizem respeito a doentes e trabalhadores, que representam milhares de pessoas. Existiam cópias de segurança em formato eletrónico. A maioria dos dados foi restaurada, mas esta operação durou dois dias úteis e provocou grandes atrasos no tratamento dos doentes e levou ao cancelamento e adiamento de cirurgias, bem como a uma diminuição do nível de serviço devido à indisponibilidade dos sistemas.

2.3.1 CASO n.º 03 – Medidas prévias e avaliação dos riscos

36. O responsável pelo tratamento dos dados devia ter adotado as mesmas medidas prévias que foram mencionadas na parte 2.1 e na secção 2.5. A principal diferença em relação ao caso anterior é a elevada gravidade das consequências para uma grande parte dos titulares dos dados[15].

37. A quantidade de dados violados e o número de titulares de dados afetados são elevados, uma vez que, por norma, os hospitais tratam grandes volumes de dados. A indisponibilidade dos dados tem um grande impacto numa parte substancial dos titulares dos dados. Além disso, existe um risco residual de elevada gravidade para a confidencialidade dos dados dos doentes.

38. O tipo de violação, a natureza, a sensibilidade e o volume dos dados pessoais afetados pela violação são importantes. Embora existisse uma cópia de segurança dos dados e estes tenham sido restaurados ao fim de uns dias, continua a existir um risco elevado devido à gravidade das consequências para os titulares dos dados resultantes da falta de disponibilidade dos dados no momento do ataque e nos dias seguintes.

2.3.2 CASO n.º 03 – Atenuação e obrigações

39. Considera-se necessária uma notificação à AC, uma vez que estão envolvidas categorias especiais de dados pessoais e o restauro dos dados pode demorar muito tempo, resultando em grandes atrasos nos cuidados aos doentes. A comunicação da violação aos titulares dos dados é necessária devido ao impacto para os doentes, mesmo após o restauro dos dados cifrados. Embora os dados relativos a todos os doentes tratados no hospital nos últimos anos tenham sido cifrados, apenas foram afetados os doentes que tinham tratamento marcado no hospital durante o período em que o sistema informático estava indisponível. O responsável pelo tratamento deve comunicar diretamente a violação de dados a esses doentes. É possível que a comunicação direta aos outros doentes, alguns dos quais podem não estar internados no hospital há mais de 20 anos, não seja exigida devido à exceção prevista no artigo 34.º, n.º 3, alínea c). Nesse caso, é feita uma comunicação

[15] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

pública[16] ou adotada uma medida semelhante através da qual os titulares de dados são informados de forma igualmente eficaz. Neste caso, o hospital deve tornar público o ataque de *software* de sequestro e os seus efeitos.

40. Este caso serve de exemplo para um ataque de *software* de sequestro que implica um risco elevado para os direitos e liberdades dos titulares dos dados. Deve ser documentado em conformidade com o artigo 33.º, n.º 5, notificado à AC em conformidade com o artigo 33.º, n.º 1, e comunicado aos titulares dos dados de acordo com o artigo 34.º, n.º 1. A organização também precisa de atualizar e corrigir as suas medidas e procedimentos organizativos e técnicos em matéria de segurança dos dados pessoais e de redução dos riscos.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

2.4 CASO n.º 04: *software* de sequestro sem cópia de segurança e com exfiltração

O servidor de uma empresa de transportes públicos foi exposto a um ataque de *software* de sequestro e os seus dados foram cifrados pelo atacante. De acordo com as conclusões do inquérito interno, o atacante não só cifrou os dados, como também os exfiltrou. O tipo de dados violados consistia nos dados pessoais de clientes e trabalhadores, bem como de vários milhares de pessoas que utilizavam os serviços da empresa (por exemplo, a compra de bilhetes em linha). Para além dos dados de identificação básicos, os números do bilhete de identidade e os dados financeiros, como os dados do cartão de crédito, estão envolvidos na violação. Existia uma base de dados de cópia de segurança, mas que também foi cifrada pelo atacante.

2.4.1 CASO n.º 04 – Medidas prévias e avaliação dos riscos

41. O responsável pelo tratamento dos dados devia ter adotado as mesmas medidas prévias que foram mencionadas na parte 2.1 e na secção 2.5. Embora existisse uma cópia de salvaguarda, também foi afetada pelo ataque. Esta disposição, por si só, suscita questões sobre a qualidade das medidas prévias de segurança informática do responsável pelo tratamento e deve ser analisada mais aprofundadamente durante o inquérito, uma vez que, num sistema de cópia de segurança bem concebido, as várias cópias de segurança devem ser armazenadas de forma segura, sem acesso do sistema principal, sob pena de poderem ser comprometidas no mesmo ataque. Além disso, os ataques de *software* de sequestro podem passar despercebidos durante dias enquanto os dados pouco utilizados são lentamente cifrados, o que pode inutilizar várias cópias de segurança, pelo que as cópias de segurança também devem ser recolhidas periodicamente e isoladas. Tal aumentaria a probabilidade de recuperação, embora com um aumento da perda dos dados.

[16] O considerando 86 do RGPD explica que «essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação».

42. Esta violação diz respeito não só à disponibilidade dos dados, mas também à confidencialidade, uma vez que o atacante pode ter modificado e/ou copiado dados do servidor. Por conseguinte, o tipo de violação resulta num risco elevado[17].

43. A natureza, a sensibilidade e o volume dos dados pessoais aumentam ainda mais os riscos, uma vez que o número de pessoas afetadas é elevado, tal como o volume global de dados pessoais afetados. Para além dos dados de identificação básicos, os documentos de identificação e os dados financeiros, como os dados do cartão de crédito, estão envolvidos na violação. Uma violação de dados relativa a estes tipos de dados apresenta um elevado risco em si mesma e, se forem tratados em conjunto, esses dados podem ser utilizados, nomeadamente, para usurpação ou roubo da identidade.

44. Devido a deficiências na lógica do servidor ou a controlos organizacionais, os ficheiros da cópia de segurança foram afetados pelo *software* de sequestro, impedindo o restauro dos dados e aumentando o risco.

45. Esta violação de dados representa um elevado risco para os direitos e liberdades das pessoas singulares, uma vez que poderia conduzir tanto a danos materiais (por exemplo, perdas financeiras, uma vez que os dados do cartão de crédito foram afetados) como a danos imateriais (por exemplo, roubo ou usurpação da identidade, uma vez que os dados do bilhete de identidade foram afetados).

2.4.2 CASO n.º 04 – Atenuação e obrigações

46. A comunicação aos titulares dos dados é essencial para que estes possam tomar as medidas necessárias para evitar danos materiais (por exemplo, bloquear os seus cartões de crédito).

47. Para além de documentar a violação em conformidade com o artigo 33.º, n.º 5, a notificação à AC é também obrigatória neste caso (artigo 33.º, n.º 1) e o responsável pelo tratamento é igualmente obrigado a comunicar a violação aos titulares dos dados (artigo 34.º, n.º 1). Este último pode ser realizado individualmente, mas no caso das pessoas em que os dados de contacto não estão disponíveis, o responsável pelo tratamento deve fazê-lo publicamente, desde que essa comunicação não seja suscetível de provocar consequências negativas acrescidas para os titulares dos dados, por exemplo, através de uma notificação no seu sítio Web. Neste último caso, é necessária uma comunicação precisa e clara, de forma visível na página inicial do responsável pelo tratamento, com referências exatas das disposições pertinentes do RGPD. Pode igualmente ser necessário que a organização atualize e corrija as suas medidas e procedimentos organizativos e técnicos em matéria de segurança dos dados pessoais e de redução dos riscos.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

2.5 Medidas organizacionais e técnicas para prevenir/atenuar os impactos dos ataques de *software* de sequestro

48. Por norma, a ocorrência de um ataque de *software* de sequestro é um sinal de uma ou mais vulnerabilidades no sistema do responsável pelo tratamento. O mesmo se aplica nos casos de *software* de sequestro em que os dados pessoais foram cifrados, mas não foram exfiltrados. Independentemente do resultado e das consequências do ataque, nunca é de mais salientar a importância de uma avaliação abrangente do sistema

[17] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

de segurança dos dados, com especial ênfase na segurança informática. As deficiências e lacunas de segurança identificadas devem ser documentadas e corrigidas sem demora.

49. Medidas aconselháveis:

(A seguinte lista de medidas não é, de modo algum, exclusiva ou exaustiva. Pelo contrário, o objetivo é apresentar ideias de prevenção e possíveis soluções. Cada atividade de tratamento é diferente, pelo que o responsável pelo tratamento deve tomar a decisão sobre quais as medidas que melhor se adequam à situação em causa).

- Manter atualizado o *firmware*, o sistema operativo e o *software* de aplicação nos servidores, máquinas-clientes, componentes de rede ativos e quaisquer outras máquinas no mesmo LAN (incluindo dispositivos Wi-Fi). Assegurar a aplicação de medidas de segurança informática adequadas, garantir a sua eficácia e mantê-las regularmente atualizadas quando o tratamento ou as circunstâncias mudarem ou evoluírem. Tal inclui a manutenção de registos pormenorizados das atualizações corretivas aplicadas e do respetivo carimbo de data/hora.
- Conceber e organizar sistemas e infraestruturas de tratamento para segmentar ou isolar sistemas e redes de dados, a fim de evitar a propagação de *malware* na organização e para sistemas externos.
- Existência de um procedimento de cópia de segurança atualizado, seguro e testado. Os suportes para cópias de segurança a médio e longo prazo devem ser mantidos separados do armazenamento de dados operacionais e fora do alcance de terceiros, mesmo em caso de ataque bem-sucedido (por exemplo, uma cópia de segurança diária incremental e uma cópia de segurança semanal completa).
- Ter/obter um *software* anti-*malware* adequado, atualizado, eficaz e integrado.
- Dispor de um sistema de prevenção e deteção de intrusões adequado, atualizado, eficaz e integrado. Dirigir o tráfego da rede através da barreira de segurança/deteção de intrusões, mesmo no caso de trabalho no domicílio ou móvel (por exemplo, utilizando ligações VPN para mecanismos de segurança organizativos no acesso à Internet).
- Formação dos trabalhadores sobre os métodos de reconhecimento e prevenção de ataques informáticos. O responsável pelo tratamento deve fornecer meios para determinar se as mensagens de correio eletrónico e as mensagens obtidas por outros meios de comunicação são autênticas e fiáveis. Os trabalhadores devem receber formação para reconhecer quando tal ataque se concretizou, como retirar o terminal da rede e a sua obrigação de o comunicar imediatamente ao diretor de segurança.
- Salientar a necessidade de identificar o tipo de código malicioso para ver as consequências do ataque e poder encontrar as medidas adequadas para atenuar o risco. Caso um ataque de *software* de sequestro seja bem-sucedido e não exista uma cópia de segurança disponível, podem ser aplicados instrumentos como os do projeto «No more ransom» (nomoreransom.org) para obter dados. No entanto, caso exista uma cópia de segurança, é aconselhável restaurar os dados dela constantes.
- Reencaminhar ou replicar todos os registos para um servidor de registos central (incluindo eventualmente a assinatura ou a marcação temporal criptográfica das entradas de registos).
- Cifragem forte e autenticação multifatorial, em especial para o acesso administrativo a sistemas informáticos, gestão adequada de chaves e palavras-passe.
- Testes regulares de vulnerabilidade e penetração.
- Criar uma equipa de resposta a incidentes de segurança informática (CSIRT) ou equipa de resposta a emergências informáticas (CERT) dentro da organização, ou aderir a uma CSIRT/CERT coletiva. Criar um plano de resposta a incidentes, um plano de recuperação em caso de catástrofe e um plano de continuidade das atividades, e certificar-se de que estes são cuidadosamente testados.
- Ao avaliar as contramedidas – a análise de risco deve ser revista, testada e atualizada.

3 ATAQUES DE EXFILTRAÇÃO DE DADOS

50. Os ataques que exploram as vulnerabilidades em serviços oferecidos pelo responsável pelo tratamento a terceiros pela Internet, por exemplo, através de ataques de injeção (por exemplo, injeção de SQL, *path traversal*), métodos de comprometimento de sítios Web e semelhantes, podem assemelhar-se a ataques de *software* de sequestro, no sentido em que o risco é causado pela ação de um terceiro não autorizado, mas, por norma, esses ataques têm como objetivo copiar, exfiltrar e utilizar indevidamente dados para fins maliciosos. Por conseguinte, constituem sobretudo violações da confidencialidade e, possivelmente, também da integridade dos dados. Ao mesmo tempo, se o responsável pelo tratamento tiver conhecimento das características deste tipo de violações, existem muitas medidas ao dispor dos responsáveis pelo tratamento que podem reduzir substancialmente o risco de uma execução bem-sucedida de um ataque.

3.1 CASO n.º 05: exfiltração dos dados das candidaturas a emprego a partir de um sítio Web

Uma agência de emprego foi vítima de um ciberataque, que colocou um código malicioso no seu sítio Web. Este código malicioso tornou os dados pessoais apresentados através de formulários de candidatura de emprego em linha e armazenados no servidor Web acessíveis a pessoas não autorizadas. Desses formulários, 213 poderão ter sido afetados e, após a análise dos dados afetados, determinou-se que a violação não afetou categorias especiais de dados. O conjunto de ferramentas específico de *malware* instalado tinha funcionalidades que permitiam ao atacante remover qualquer historial de exfiltração, bem como monitorizar o tratamento no servidor e recolher dados pessoais. O conjunto de ferramentas foi descoberto apenas um mês após a sua instalação.

3.1.1 CASO n.º 05 – Medidas prévias e avaliação dos riscos

51. A segurança do ambiente do responsável pelo tratamento dos dados é extremamente importante, uma vez que é possível evitar a maioria destas violações assegurando que todos os sistemas são constantemente atualizados, que os dados sensíveis são cifrados e que as aplicações são desenvolvidas de acordo com normas de segurança elevadas, como a autenticação forte e as medidas contra a força bruta, os ataques e o «escape» ou «limpeza»[18] dos dados introduzidos pelos utilizadores, etc. São igualmente necessárias auditorias periódicas de segurança informática, avaliações da vulnerabilidade e testes de penetração para detetar antecipadamente estes tipos de vulnerabilidades e corrigi-las. Neste caso específico, as ferramentas de monitorização da integridade dos ficheiros no ambiente de produção podem ter ajudado a detetar a injeção de código. (A secção 3.7 contém uma lista de medidas aconselháveis).

52. O responsável pelo tratamento deve começar sempre a investigar a violação identificando o tipo de ataque e os seus métodos, a fim de avaliar as medidas a tomar. Para o tornar rápido e eficiente, o responsável pelo tratamento dos dados deve dispor de um plano de resposta a incidentes que especifique as medidas céleres e necessárias para assumir o controlo do incidente. Neste caso específico, o tipo de violação constituía um fator de aumento do risco, uma vez que não só a confidencialidade dos dados foi restringida, como o atacante

[18] O escape ou limpeza dos dados introduzidos pelos utilizadores é uma forma de validação de dados de entrada, que garante que apenas os dados devidamente formatados são introduzidos num sistema de informação.

dispunha também dos meios para introduzir alterações no sistema, pelo que a integridade dos dados também se tornou questionável.

53. A natureza, a sensibilidade e o volume dos dados pessoais afetados pela violação devem ser avaliados para determinar em que medida a violação afetou os titulares dos dados. Embora não tenham sido afetadas categorias especiais de dados pessoais, os dados acedidos contêm informações consideráveis sobre as pessoas constantes dos formulários em linha e esses dados podem ser utilizados de diversas formas (direcionamento de publicidade não solicitada, roubo da identidade, etc.), pelo que a gravidade das consequências deverá aumentar o risco para os direitos e liberdades dos titulares dos dados[19].

3.1.2 CASO n.º 05 – Atenuação e obrigações

54. Se possível, após a resolução do problema, a base de dados deve ser comparada com a base de dados armazenada numa cópia de segurança protegida. A experiência adquirida com a violação deve ser utilizada na atualização da infraestrutura informática. O responsável pelo tratamento deve repor todos os sistemas informáticos afetados num estado limpo conhecido, corrigir a vulnerabilidade e aplicar novas medidas de segurança para evitar violações de dados semelhantes no futuro, por exemplo, controlos de integridade dos ficheiros e auditorias de segurança. Se os dados pessoais tiverem sido não só exfiltrados, mas também apagados, o responsável pelo tratamento tem de tomar medidas sistemáticas para repor os dados pessoais no estado em que se encontravam antes da violação. Pode ser necessário aplicar cópias de segurança completas, alterações incrementais e, eventualmente, repetir o tratamento desde a última cópia de segurança incremental – o que exige que o responsável pelo tratamento possa reproduzir as alterações efetuadas desde a última cópia de segurança. Tal poderá exigir que o responsável pelo tratamento disponha de um sistema concebido para conservar os ficheiros diários de entrada caso estes tenham de ser novamente tratados e exige um método sólido de armazenamento e uma política de conservação adequada.

55. Tendo em conta o que precede, uma vez que a violação é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, os titulares dos dados devem inquestionavelmente ser informados desse facto (artigo 34.º, n.º 1), o que significa, evidentemente, que a(s) AC(s) competente(s) também deve(m) estar envolvida(s) sob a forma de uma notificação de violação de dados. A documentação da violação é obrigatória nos termos do artigo 33.º, n.º 5, do RGPD e facilita a avaliação da situação.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

3.2 CASO n.º 06: exfiltração de palavra-passe colocada em *hash* de um sítio Web

Foi explorada uma vulnerabilidade de injeção de SQL para obter acesso a uma base de dados do servidor de um sítio Web de culinária. Os utilizadores apenas podiam escolher pseudónimos arbitrários como nomes de utilizador. A utilização de endereços de correio eletrónico para este efeito foi desencorajada. As palavras-passe armazenadas na base de dados foram colocadas em *hash* com um algoritmo forte e a técnica *salt* não foi comprometida. Dados afetados: palavras-passe colocadas em *hash* de 1 200 utilizadores. Por razões de segurança, o responsável pelo tratamento informou os titulares dos dados sobre a violação por correio eletrónico e pediu-lhes que alterassem as suas palavras-passe, especialmente se a mesma palavra-passe fosse utilizada para outros serviços.

[19] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

3.2.1 CASO n.º 06 – Medidas prévias e avaliação dos riscos

56. Neste caso específico, a confidencialidade dos dados está comprometida, mas as palavras-passe da base de dados foram colocadas em *hash* com um método atualizado, o que diminuiria o risco relativo à natureza, sensibilidade e volume dos dados pessoais. Este caso não representa riscos para os direitos e liberdades dos titulares dos dados.

57. Além disso, não foram comprometidos quaisquer dados de contacto dos titulares dos dados (por exemplo, endereços eletrónicos ou números de telefone), o que significa que não existe um risco significativo para os titulares dos dados de serem alvo de tentativas de fraude [por exemplo, receção de mensagens de correio eletrónico de mistificação da interface (*phishing*) ou de mensagens de texto e chamadas telefónicas fraudulentas]. Não foram envolvidas categorias especiais de dados pessoais.

58. Alguns nomes de utilizadores podem ser considerados dados pessoais, mas o objeto do sítio Web não permite conotações negativas. Embora importe salientar que a avaliação dos riscos pode mudar[20], o tipo de sítio Web e os dados acedidos podem revelar categorias especiais de dados pessoais (por exemplo, sítio Web de um partido político ou sindicato). A utilização da cifragem de ponta poderia atenuar os efeitos adversos da violação. Garantir que é permitido um número limitado de tentativas de início de sessão impedirá que os ataques brutais de início de sessão sejam bem-sucedidos, reduzindo assim em grande medida os riscos impostos pelos atacantes que já conhecem os nomes de utilizador.

3.2.2 CASO n.º 06 – Atenuação e obrigações

59. A comunicação aos titulares dos dados pode, em alguns casos, ser considerada um fator atenuante, uma vez que os titulares dos dados também estão em condições de tomar as medidas necessárias para evitar novos danos decorrentes da violação, por exemplo alterando a sua palavra-passe. Neste caso, a notificação não era obrigatória, mas em muitos casos pode ser considerada uma boa prática.

60. O responsável pelo tratamento dos dados deve corrigir a vulnerabilidade e aplicar novas medidas de segurança para evitar violações de dados semelhantes no futuro, como, por exemplo, auditorias sistemáticas de segurança no sítio Web.

61. A violação deve ser documentada em conformidade com o artigo 33.º, n.º 5, mas não é necessária qualquer notificação ou comunicação.

62. Além disso, é fortemente aconselhável comunicar aos titulares dos dados uma violação que envolva palavras-passe, mesmo quando as palavras-passe foram armazenadas utilizando um *hash* salgado (*salted*) com um algoritmo conforme ao estado da técnica. É preferível utilizar métodos de autenticação que evitem a necessidade de tratar senhas do lado do servidor. Os titulares dos dados devem poder optar por tomar as medidas adequadas relativamente às suas próprias palavras-passe.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

[20] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

3.3 CASO n.º 07: Ataque do tipo «credential stuffing» num sítio Web bancário

Um banco sofreu um ciberataque contra um dos seus sítios Web bancários em linha. O ataque tinha como objetivo enumerar todos os identificadores de utilizador possíveis através de uma palavra-passe trivial fixa. As palavras-passe são compostas por oito dígitos. Devido a uma vulnerabilidade do sítio Web, em alguns casos, as informações relativas aos titulares dos dados (nome, apelido, sexo, data e local de nascimento, código fiscal, códigos de identificação do utilizador) foram divulgadas ao atacante, mesmo que a palavra-passe utilizada não estivesse correta ou a conta bancária já não estivesse ativa. Esta situação afetou cerca de 100 000 titulares de dados. De entre estas, o atacante acedeu com êxito a cerca de 2 000 contas que estavam a utilizar a palavra-passe trivial experimentada pelo atacante. Após o incidente, o responsável pelo tratamento conseguiu identificar todas as tentativas ilegítimas de início de sessão. O responsável pelo tratamento dos dados pôde confirmar que, de acordo com os controlos antifraude, estas contas não realizaram transações durante o ataque. O banco tinha conhecimento da violação de dados porque o seu centro de operações de segurança detetou um elevado número de pedidos de início de sessão dirigidos ao sítio Web. Em resposta, o responsável pelo tratamento desativou a possibilidade de iniciar uma sessão no sítio Web, desligando-o e forçando a mudança de palavra-passe das contas comprometidas. O responsável pelo tratamento comunicou a violação apenas aos utilizadores com as contas comprometidas, ou seja, aos utilizadores cujas palavras-passe foram comprometidas ou cujos dados foram divulgados.

3.3.1 CASO n.º 07 – Medidas prévias e avaliação dos riscos

63. É importante mencionar que os responsáveis pelo tratamento de dados de natureza altamente pessoal[21] têm uma maior responsabilidade de garantir uma segurança adequada dos dados, por exemplo, dispor de um centro de operações de segurança e de outras medidas de prevenção, deteção e resposta a incidentes. O não cumprimento destas normas mais rigorosas resultará certamente em medidas mais graves durante o inquérito de uma AC.

64. A violação diz respeito a dados financeiros para além da identidade e das informações de identificação do utilizador, o que a torna particularmente grave. O número de pessoas afetadas é elevado.

65. O facto de uma violação poder ocorrer num ambiente tão sensível aponta para lacunas significativas em matéria de segurança dos dados no sistema do responsável pelo tratamento e pode ser um indicador de um momento em que a revisão e atualização das medidas afetadas é «necessária», em conformidade com o artigo 24.º, n.º 1, o artigo 25.º, n.º 1, e o artigo 32.º, n.º 1, do RGPD. Os dados violados permitem a identificação única dos titulares dos dados e contêm outras informações sobre os mesmos (incluindo o género, a data e o local de nascimento). Além disso, podem ser utilizados pelo atacante para adivinhar as palavras-passe dos clientes ou realizar uma campanha de mistificação da interface dirigida aos clientes do banco.

[21] Tais como informações dos titulares dos dados referentes a métodos de pagamento, tais como números de cartões, contas bancárias, pagamentos em linha, folhas de pagamento, extratos bancários, estudos económicos ou quaisquer outras informações que possam revelar informações económicas relativas aos titulares dos dados.

66. Por estes motivos, considerou-se que a violação de dados era suscetível de resultar num elevado risco para os direitos e liberdades de todos os titulares dos dados em causa[22]. Por conseguinte, a ocorrência de danos materiais (por exemplo, perdas financeiras) e imateriais (por exemplo, usurpação ou roubo da identidade) é um resultado possível.

3.3.2 CASO n.º 07 – Atenuação e obrigações

67. As medidas do responsável pelo tratamento mencionadas na descrição do caso são adequadas. Na sequência da violação, corrigiu igualmente a vulnerabilidade do sítio Web e tomou outras medidas para evitar futuras violações de dados semelhantes, tais como o aditamento de autenticação de dois fatores no sítio Web em causa e a transição para uma autenticação forte do cliente.

68. A documentação da violação nos termos do artigo 33.º, n.º 5, do RGPD e a notificação da violação à AC não são facultativas neste cenário. Além disso, o responsável pelo tratamento deve notificar todos os 100 000 titulares de dados (incluindo os titulares cujas contas não tenham sido comprometidas), em conformidade com o artigo 34.º do RGPD.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

3.4 Medidas organizacionais e técnicas para prevenir/atenuar os impactos dos ataques de piratas informáticos

69. Tal como no caso de ataques de *software* de sequestro, independentemente do resultado e das consequências do ataque, a reavaliação da segurança informática é obrigatória para os responsáveis pelo tratamento em casos semelhantes.

70. Medidas aconselháveis[23]:

(*A seguinte lista de medidas não é, de modo algum, exclusiva ou exaustiva*. *Pelo contrário, o objetivo é apresentar ideias de prevenção e possíveis soluções. Cada atividade de tratamento é diferente, pelo que o responsável pelo tratamento deve tomar a decisão sobre quais as medidas que melhor se adequam à situação em causa*).

- Cifragem de ponta e gestão de chaves, especialmente quando estão a ser tratadas palavras-passe, dados sensíveis ou financeiros. A *hashing* e a *salting* criptográfica de informações secretas (palavras-passe) são sempre preferíveis à cifragem das palavras-passe. A utilização de métodos de autenticação que evitem a necessidade de processar palavras-passe do lado do servidor é preferível.
- Manter o sistema atualizado (*software* e *firmware*). Assegurar a aplicação de todas as medidas de segurança informática, garantir a sua eficácia e mantê-las regularmente atualizadas quando o tratamento ou as circunstâncias mudarem ou evoluírem. A fim de poder demonstrar a conformidade com o artigo 5.º, n.º 1, alínea f), em conformidade com o artigo 5.º, n.º 2, do RGPD, o responsável pelo tratamento deve manter um registo de todas as atualizações efetuadas, que inclua a hora em que foram aplicadas.

[22] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

[23] Para o desenvolvimento seguro de aplicações Web, ver também: https://www.owasp.org/index.php/Main_Page.

- Utilização de métodos de autenticação forte, como a autenticação de dois fatores e servidores de autenticação, complementados por uma política atualizada de palavras-passe.
- As normas de desenvolvimento seguro incluem a filtragem dos dados introduzidos pelos utilizadores (utilizando a lista branca, na medida do possível), o escape dos dados introduzidos pelos utilizadores e as medidas de prevenção da força bruta (como a limitação da quantidade máxima de novas tentativas). As «barreiras de aplicação Web» podem contribuir para a utilização eficaz desta técnica.
- Existência de fortes privilégios de utilizador e de uma política de gestão do controlo de acessos.
- Utilização de barreiras de proteção adequadas, atualizadas, eficazes e integradas, deteção de intrusões e outros sistemas de defesa do perímetro.
- Auditorias sistemáticas da segurança informática e avaliações da vulnerabilidade (testes de penetração).
- Revisões e testes regulares para garantir que as cópias de segurança podem ser utilizadas para restaurar quaisquer dados cuja integridade ou disponibilidade tenha sido afetada.
- Não há ID de sessão no URL em texto simples.

4 FONTE INTERNA DE RISCO HUMANO

71. O papel do erro humano nas violações de dados pessoais tem de ser realçado, devido à sua aparência comum. Uma vez que estes tipos de violações podem ser intencionais e não intencionais, é muito difícil para os responsáveis pelo tratamento de dados identificar as vulnerabilidades e adotar medidas para as evitar. A Conferência Internacional de Comissários para a Proteção dos Dados e da Vida Privada reconheceu a importância de abordar esses fatores humanos e adotou, em outubro de 2019, a resolução para abordar o papel dos erros humanos nas violações de dados pessoais[24]. Esta resolução salienta que devem ser tomadas medidas de segurança adequadas para evitar erros humanos e fornece uma lista não exaustiva dessas salvaguardas e abordagens.

4.1 CASO n.º 08: Exfiltração de dados da empresa por um trabalhador

Durante o período de pré-aviso, o trabalhador de uma empresa copiou os dados comerciais da base de dados da empresa. O trabalhador só está autorizado a aceder aos dados para desempenhar as suas funções. Alguns meses mais tarde, após a cessação de funções, este utilizou os dados assim obtidos (dados de contacto de base) para assumir o cargo de responsável de dados de um novo tratamento de dados, a fim de contactar os clientes da empresa de modo a aliciá-los para a sua nova empresa.

4.1.1 CASO n.º 08 – Medidas prévias e avaliação dos riscos

72. Neste caso em concreto, não foram tomadas medidas prévias para impedir o trabalhador de copiar os dados de contacto dos clientes da empresa, uma vez que necessitava – e dispôs – legitimamente de acesso a esses dados para o desempenho das suas funções profissionais. Uma vez que o cumprimento da maior parte das funções profissionais relacionadas com os clientes exige algum tipo de acesso dos trabalhadores a dados pessoais, estas violações de dados podem ser as mais difíceis de evitar. As limitações ao âmbito do acesso podem limitar o trabalho que o trabalhador em causa pode realizar. Contudo, a existência de políticas de acesso bem pensadas e de um controlo constante pode ajudar a evitar essas violações.

73. Como habitualmente, durante a avaliação dos riscos, devem ser tidos em conta o tipo de violação e a natureza, sensibilidade e volume dos dados pessoais afetados. Por norma, estes tipos de violações são

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

violações da confidencialidade, uma vez que a base de dados é normalmente deixada intacta e o seu conteúdo «apenas» copiado para posterior utilização. O volume de dados afetados é geralmente baixo ou médio. Neste caso específico, não foram afetadas categorias especiais de dados pessoais, e o trabalhador só necessitava dos dados de contacto dos clientes para poder entrar em contacto com eles depois de sair da empresa. Por conseguinte, os dados em causa não são sensíveis.

74. Embora o único objetivo do ex-funcionário que copiou os dados de forma mal-intencionada possa limitar-se a obter os dados de contacto dos clientes da empresa para os seus próprios fins comerciais, o responsável pelo tratamento não está em condições de considerar que o risco para os titulares dos dados em causa é baixo, uma vez que o responsável pelo tratamento não tem qualquer tipo de garantias quanto às intenções do trabalhador. Assim, embora as consequências da violação possam limitar-se à exposição à publicidade direta não solicitada do ex-trabalhador, não pode ser excluída a possibilidade de ocorrência de outro abuso mais grave dos dados roubados, dependendo da finalidade do tratamento efetuado pelo antigo trabalhador[25].

4.1.2 CASO n.º 08 – Atenuação e obrigações

75. A atenuação dos efeitos adversos da violação no caso acima descrito é difícil. Poderá passar por uma ação judicial imediata para impedir o antigo trabalhador de continuar a utilizar abusivamente e a divulgar os dados. O passo seguinte deve ser evitar que ocorram situações semelhantes no futuro. O responsável pelo tratamento pode tentar ordenar ao ex-funcionário que deixe de utilizar os dados, mas o êxito desta ação é, na melhor das hipóteses, duvidoso. A aplicação de medidas técnicas adequadas, como a impossibilidade de copiar ou descarregar dados para dispositivos amovíveis, pode revelar-se útil.

76. Não existe uma solução única para este tipo de casos, mas uma abordagem sistemática pode ajudar a evitá-los. Por exemplo, a empresa pode ponderar – sempre que possível – retirar determinadas formas de acesso aos trabalhadores que tenham manifestado a sua intenção de sair da empresa ou implementar registos de acesso, de modo que seja possível registar e assinalar o acesso indesejado. O contrato assinado com os trabalhadores deve incluir cláusulas que proíbam tais ações.

77. Em suma, uma vez que a violação em causa não resultará num risco elevado para os direitos e liberdades das pessoas singulares, será suficiente efetuar uma notificação à AC. No entanto, informar os titulares dos dados pode também ser benéfico para o responsável pelo tratamento, uma vez que é melhor saber pela empresa que houve uma fuga de dados do que pelo ex-funcionário quando este tentar contactá-los. Nos termos do artigo 33.º, n.º 5, a documentação relativa à violação de dados é uma obrigação jurídica.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	X

[25] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

4.2 CASO n.º 09: Transmissão acidental de dados a terceiros de confiança

Um agente de seguros apercebeu-se de que – devido à má configuração de um ficheiro Excel recebido por correio eletrónico – conseguia aceder a informações relativas a duas dezenas de clientes de outro departamento. Este agente está sujeito ao sigilo profissional e foi o único destinatário da mensagem de correio eletrónico. O acordo celebrado entre o responsável pelo tratamento e o agente de seguros obriga o agente a assinalar ao responsável pelo tratamento, sem demora injustificada, uma violação de dados pessoais. Por conseguinte, o agente sinalizou imediatamente o erro ao responsável pelo tratamento, que corrigiu o ficheiro e o enviou de novo, pedindo ao agente que apagasse a mensagem anterior. De acordo com o acordo acima referido, o agente é obrigado a confirmar o apagamento numa declaração escrita, e ele assim o fez. As informações obtidas não incluem categorias especiais de dados pessoais, apenas dados de contacto e dados sobre o seguro propriamente dito (tipo de seguro, montante). Depois de analisar os dados pessoais afetados pela violação, o responsável pelo tratamento não identificou quaisquer características especiais relativas às pessoas ou ao responsável pelo tratamento que possam afetar o nível de impacto da violação.

4.2.1 CASO n.º 09 – Medidas prévias e avaliação dos riscos

78. Neste caso, a violação não resulta de um ato intencional de um trabalhador, mas sim de um erro humano involuntário causado pela falta de atenção. É possível evitar ou reduzir a ocorrência deste tipo de violação através a) da aplicação de programas de formação, educação e sensibilização que permitam aos trabalhadores compreender melhor a importância da proteção dos dados pessoais, b) da redução da troca de ficheiros através do correio eletrónico, utilizando, por exemplo, em vez disso, sistemas próprios para o tratamento de dados dos clientes, c) da dupla verificação dos ficheiros antes do envio, d) da separação entre a criação e o envio de ficheiros.

79. Esta violação de dados diz respeito apenas à confidencialidade dos dados, mantendo-se intacta a integridade e a acessibilidade dos mesmos. A violação de dados dizia respeito apenas a cerca de duas dezenas de clientes, pelo que o volume de dados afetados pode ser considerado baixo. Além disso, os dados pessoais afetados não contêm quaisquer dados sensíveis. O facto de o subcontratante ter contactado imediatamente o responsável pelo tratamento após ter tomado conhecimento da violação de dados pode ser considerado um fator de atenuação do risco. (É necessário avaliar igualmente a possibilidade de os dados terem sido enviados a outros agentes de seguros e, caso se confirme o envio, é necessário aplicar medidas adequadas.) Uma vez que foram aplicadas medidas adequadas após a violação de dados, é provável que esta não tenha qualquer impacto nos direitos e liberdades dos titulares dos dados.

80. A combinação do número reduzido de pessoas afetadas, da deteção imediata da violação e das medidas tomadas para minimizar os seus efeitos eliminam os riscos deste caso específico.

4.2.2 CASO n.º 09 – Atenuação e obrigações

81. Além disso, estão também em causa outras circunstâncias de atenuação dos riscos: o agente está sujeito ao sigilo profissional; ele próprio comunicou o problema ao responsável pelo tratamento; e apagou o ficheiro quando lhe foi pedido. A sensibilização e, eventualmente, a inclusão de medidas suplementares na verificação de documentos que envolvam dados pessoais ajudarão provavelmente a evitar casos semelhantes no futuro.

82. Para além de documentar a violação em conformidade com o artigo 33.º, n.º 5, não há necessidade de tomar mais nenhuma medida.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

4.3 Medidas organizacionais e técnicas para prevenir/atenuar os impactos das fontes internas de risco humano

83. Uma combinação das medidas a seguir mencionadas – aplicadas em função das características únicas do caso – deverá ajudar a reduzir a probabilidade de reincidência de uma violação semelhante.

84. Medidas aconselháveis:

(*A seguinte lista de medidas não é, de modo algum, exclusiva ou exaustiva*. *Pelo contrário, o objetivo é apresentar ideias de prevenção e possíveis soluções. Cada atividade de tratamento é diferente, pelo que o responsável pelo tratamento deve tomar a decisão sobre quais as medidas que melhor se adequam à situação em causa*).

- Execução periódica de programas de formação, educação e sensibilização destinados aos trabalhadores sobre as suas obrigações em matéria de privacidade e segurança e a deteção e comunicação de ameaças à segurança dos dados pessoais[26]. Desenvolver um programa de sensibilização para recordar aos trabalhadores os erros mais comuns que conduzem a violações de dados pessoais e a melhor forma de os evitar.
- Implementar práticas, procedimentos e sistemas sólidos e eficazes em matéria de proteção de dados e privacidade[27].
- Avaliar as práticas, procedimentos e sistemas em matéria de privacidade, a fim de assegurar a continuidade da eficácia[28].
- Elaborar políticas adequadas de controlo do acesso e obrigar os utilizadores a respeitar as regras.
- Aplicar técnicas que obrigam à autenticação dos utilizadores quando acedem a dados pessoais sensíveis.
- Desativar a conta de utilizador na empresa assim que a pessoa deixe de trabalhar na empresa.
- Verificar o fluxo de dados invulgares entre o servidor de ficheiros e as estações de trabalho dos trabalhadores.
- Criar a segurança da interface I/O no BIOS ou através da utilização de *software* de controlo da utilização de interfaces de computador (bloqueio ou desbloqueio, por exemplo, USB/CD/DVD, etc.).
- Rever a política de acesso dos trabalhadores (por exemplo, registar o acesso a dados sensíveis e exigir que o utilizador introduza uma razão comercial, de modo a que tal esteja disponível para auditorias).
- Desativar os serviços de computação em nuvem abertos.
- Proibir e impedir o acesso a serviços de correio aberto conhecidos.
- Desativar a função de impressão de ecrã no SO.
- Aplicar uma política de mesa limpa.
- Bloqueio automático de todos os computadores após um certo período de inatividade.
- Utilizar mecanismos [por exemplo, *token* (sem fios) para iniciar sessão/abrir contas bloqueadas] para trocas rápidas de utilizador em ambientes partilhados.
- Utilização de sistemas próprios de gestão de dados pessoais que apliquem mecanismos adequados de controlo do acesso e que impeçam erros humanos, como o envio de comunicações ao destinatário errado. A utilização de folhas de cálculo e de outros documentos de escritório não é um meio adequado para gerir os dados dos clientes.

[26] Secção 2, alínea i), da resolução para abordar o papel dos erros humanos nas violações de dados pessoais.

[27] Secção 2, alínea ii), da resolução para abordar o papel dos erros humanos nas violações de dados pessoais.

[28] Secção 2, alínea iii), da resolução para abordar o papel dos erros humanos nas violações de dados pessoais.

5 DISPOSITIVOS PERDIDOS OU FURTADOS E DOCUMENTOS EM PAPEL

85. Um tipo de caso frequente é a perda ou o furto de dispositivos portáteis. Nestes casos, o responsável pelo tratamento tem de ter em conta as circunstâncias da operação de tratamento, tais como o tipo de dados armazenados no dispositivo, bem como os ativos de apoio, e as medidas tomadas antes da violação para garantir um nível de segurança adequado. Todos estes elementos afetam os potenciais impactos da violação de dados. A avaliação dos riscos pode ser difícil, uma vez que o dispositivo já não está disponível.

86. Este tipo de violação pode sempre ser classificado como uma violação da confidencialidade. No entanto, se não existir uma cópia de segurança para a base de dados roubada, o tipo de violação também pode ser considerado uma violação da disponibilidade e da integridade.

87. Os cenários a seguir apresentados demonstram de que forma as circunstâncias acima mencionadas influenciam a probabilidade e a gravidade da violação de dados.

5.1 CASO n.º 10: Material roubado que armazena dados pessoais cifrados

Durante um assalto a um jardim de infância, foram roubados dois tábletes. Estes continham uma aplicação onde eram armazenados os dados pessoais sobre as crianças que frequentam o jardim de infância, nomeadamente o nome, a data de nascimento e os dados pessoais sobre a educação das crianças. Tanto os tábletes cifrados que foram desligados no momento do assalto como a aplicação estavam protegidos por uma palavra-passe forte. Os dados da cópia de segurança estavam à disposição do responsável pelo tratamento. Pouco tempo depois de ter tomado conhecimento do assalto, o jardim de infância emitiu à distância um comando para limpar os tábletes.

5.1.1 CASO n.º 10 – Medidas prévias e avaliação dos riscos

88. Neste caso específico, o responsável pelo tratamento tomou medidas adequadas para prevenir e atenuar os impactos de uma potencial violação de dados através da cifragem de dispositivos, da introdução de uma proteção adequada da palavra-passe e da cópia de segurança dos dados armazenados nos tábletes. (A secção 5.7 contém uma lista de medidas aconselháveis).

89. Depois de tomar conhecimento de uma violação, o responsável pelo tratamento deve avaliar a fonte de risco, os sistemas de apoio ao tratamento de dados, o tipo de dados pessoais envolvidos e os potenciais impactos da violação de dados nas pessoas em causa. A violação de dados acima descrita poderia ter afetado a confidencialidade, a disponibilidade e a integridade dos dados em causa, mas, devido à aplicação de procedimentos adequados por parte do responsável pelo tratamento antes e depois da violação de dados, nenhum desses problemas se verificou.

5.1.2 CASO n.º 10 – Atenuação e obrigações

90. A confidencialidade dos dados pessoais incluídos nos dispositivos não foi comprometida devido à proteção por palavra-passe forte tanto nos tábletes como nas aplicações. Os tábletes foram configurados de tal forma que a configuração de uma palavra-passe também cifra os dados do dispositivo. O responsável pelo tratamento tentou ainda apagar à distância todos os dados constantes dos dispositivos roubados.

91. Devido às medidas tomadas, a confidencialidade dos dados também foi mantida intacta. Além disso, a cópia de segurança assegurou a disponibilidade contínua dos dados pessoais, pelo que não poderia ter ocorrido qualquer potencial impacto negativo.

92. Face às medidas tomadas, era pouco provável que a violação de dados acima descrita resultasse num risco para os direitos e liberdades dos titulares dos dados, pelo que não foi necessário efetuar qualquer notificação

à AC ou aos titulares dos dados em causa. No entanto, esta violação de dados deve também ser documentada em conformidade com o artigo 33.º, n.º 5.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

5.2 CASO n.º 11: Material furtado que armazena dados pessoais que não estão cifrados

O computador portátil eletrónico de um trabalhador de uma empresa prestadora de serviços foi furtado. O computador portátil furtado continha nomes, apelidos, sexo, endereços e data de nascimento de mais de 100 000 clientes. Devido à indisponibilidade do dispositivo furtado, não foi possível identificar se outras categorias de dados pessoais também foram afetadas. O acesso ao disco rígido do computador portátil não estava protegido por uma palavra-passe. Os dados pessoais podem ser restaurados a partir de cópias de segurança diárias.

5.2.1 CASO n.º 11 – Medidas prévias e avaliação dos riscos

93. O responsável pelo tratamento não adotou quaisquer medidas de segurança prévias, pelo que os dados pessoais armazenados no computador portátil furtado estavam à disposição do ladrão ou de qualquer outra pessoa que posteriormente viesse a estar na posse do dispositivo.

94. Esta violação de dados diz respeito à confidencialidade dos dados armazenados no dispositivo furtado.

95. Neste caso, o computador portátil que contém os dados pessoais estava vulnerável porque não possuía qualquer proteção por palavra-passe ou cifragem. A falta de medidas básicas de segurança aumenta o nível de risco para os titulares dos dados afetados. Além disso, a identificação dos titulares dos dados em causa é igualmente problemática, o que também aumenta a gravidade da violação. O número considerável de pessoas em causa aumenta o risco; no entanto, não estavam em causa categorias especiais de dados pessoais na violação de dados.

96. Durante a avaliação dos riscos[29], o responsável pelo tratamento deve ter em conta as potenciais consequências e os efeitos adversos da violação da confidencialidade. Em resultado da violação, os titulares dos dados em causa podem ser vítimas de fraude de identidade com base nos dados disponíveis incluídos no dispositivo furtado, pelo que o risco é considerado elevado.

5.2.2 CASO n.º 11 – Atenuação e obrigações

97. Acionar a cifragem dos dispositivos e utilizar uma proteção por palavra-passe forte na base de dados armazenada poderia ter impedido que a violação dos dados resultasse num risco para os direitos e liberdades dos titulares dos dados.

98. Devido a estas circunstâncias, é necessário notificar a AC, sendo igualmente necessária a notificação dos titulares dos dados em causa.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

[29] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

5.3 CASO n.º 12: Ficheiros em papel furtados que contêm dados sensíveis

Foi roubado um livro de registo em papel numa instituição de reabilitação de toxicodependentes. O livro continha dados relativos à identidade e à saúde dos doentes da instituição de reabilitação. Os dados foram armazenados apenas em papel e não existia uma cópia de segurança para os médicos que tratavam os doentes. O livro não estava guardado numa gaveta fechada nem numa sala, o responsável pelo tratamento dos dados não dispunha de um sistema de controlo de acesso nem de qualquer outra medida de segurança para a documentação em papel.

5.3.1 CASO n.º 12 – Medidas prévias e avaliação dos riscos

99. O responsável pelo tratamento não adotou quaisquer medidas de segurança prévias, pelo que os dados pessoais armazenados no livro estavam à disposição da pessoa que o encontrou. Além disso, a natureza dos dados pessoais armazenados no livro faz com que a falta de dados de segurança constitua um fator de risco muito grave.

100. Este caso serve de exemplo para uma violação de dados de elevado risco. Devido à falta de precauções de segurança adequadas, foram perdidos dados relativos à saúde sensíveis nos termos do artigo 9.º, n.º 1, do RGPD. Uma vez que, neste caso, estava em causa uma categoria especial de dados pessoais, os potenciais riscos para os titulares dos dados em causa foram agravados, o que deve igualmente ser tido em conta pelo responsável pelo tratamento que avalia o risco[30].

101. Esta violação diz respeito à confidencialidade, à disponibilidade e à integridade dos dados pessoais em causa. Em consequência da violação, o sigilo médico é violado e terceiros não autorizados podem ter acesso às informações médicas privadas dos doentes, o que pode ter um impacto grave na vida pessoal do doente. A violação da disponibilidade pode também perturbar a continuidade do tratamento dos doentes. Uma vez que a alteração/apagamento de partes do conteúdo do livro não pode ser excluída, a integridade dos dados pessoais também está comprometida.

5.3.2 CASO n.º 12 – Atenuação e obrigações

102. Durante a avaliação das medidas de segurança, o tipo de ativo de apoio também deve ser considerado. Uma vez que o livro de registo dos doentes era um documento físico, a sua segurança deveria ter sido organizada de forma diferente da de um dispositivo eletrónico. A pseudonimização dos nomes dos doentes, o armazenamento do livro numa instalação protegida e numa gaveta fechada ou numa sala, bem como um controlo de acesso adequado com autenticação no momento do acesso, poderiam ter impedido a violação dos dados.

103. A violação de dados acima descrita pode afetar gravemente os titulares dos dados em causa; por conseguinte, a notificação da AC e a comunicação da violação aos titulares dos dados em causa são obrigatórias.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	omunicação aos titulares dos dados
✓	✓	✓

[30] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

5.4 Medidas organizacionais e técnicas para prevenir/atenuar os impactos da perda ou roubo de dispositivos

104. Uma combinação das medidas a seguir mencionadas – aplicadas em função das características únicas do caso – deverá ajudar a reduzir a probabilidade de reincidência de uma violação semelhante.

105. Medidas aconselháveis:

(*A seguinte lista de medidas não é, de modo algum, exclusiva ou exaustiva*. *Pelo contrário, o objetivo é apresentar ideias de prevenção e possíveis soluções. Cada atividade de tratamento é diferente, pelo que o responsável pelo tratamento deve tomar a decisão sobre quais as medidas que melhor se adequam à situação em causa*).

- Acionar a cifragem do dispositivo (por exemplo, BitLocker, Veracrypt ou DM-Crypt).
- Utilizar o código de identificação/palavra-passe em todos os dispositivos. Cifrar todos os dispositivos eletrónicos móveis de uma forma que exija a introdução de uma palavra-passe complexa para decifragem.
- Utilizar uma autenticação multifatorial.
- Acionar as funcionalidades de dispositivos altamente móveis que permitem localizá-los em caso de perda ou extravio.
- Utilizar *software*/aplicação de gestão de dispositivos móveis (MDM) e localização. Utilizar filtros antiencandeamento. Desligar os dispositivos que não estiverem a ser utilizados.
- Se possível e adequado para o tratamento dos dados em questão, guardar dados pessoais não num dispositivo móvel, mas num servidor central de retaguarda.
- Se a estação de trabalho estiver ligada à LAN institucional, fazer uma cópia de segurança automática a partir das pastas de trabalho, desde que seja inevitável que os dados pessoais sejam aí armazenados.
- Utilizar uma VPN segura (por exemplo, que exige uma chave de autenticação de segundo fator separada para o estabelecimento de uma ligação segura) para ligar dispositivos móveis a servidores de retaguarda.
- Fornecer fechaduras físicas aos funcionários, a fim de lhes permitir proteger fisicamente os dispositivos móveis que utilizam enquanto não são utilizados.
- Regulação adequada da utilização dos dispositivos fora da empresa.
- Regulação adequada da utilização dos dispositivos na empresa.
- Utilizar *software*/aplicação MDM (gestão de dispositivos móveis) e ativar a função de limpeza à distância.
- Utilizar a gestão centralizada de dispositivos com direitos mínimos para os utilizadores finais instalarem *software*.
- Instalar controlos de acesso físico.
- Evitar armazenar informações sensíveis em dispositivos móveis ou discos rígidos. Se for necessário aceder ao sistema interno da empresa, devem ser utilizados canais seguros como anteriormente indicado.

6 ERRO NO CORREIO POSTAL

106. Neste caso, a fonte de risco é também um erro humano interno, mas a violação não foi causada por uma ação maliciosa, sendo resultado da falta de atenção. O responsável pelo tratamento pouco pode fazer após a sua ocorrência, pelo que a prevenção é ainda mais importante nestes casos do que noutros tipos de violação.

6.1 CASO n.º 13: Erro do correio postal

Uma empresa de venda a retalho preparou duas encomendas de calçado. Devido a erro humano, duas faturas foram trocadas, pelo que os dois produtos e as faturas foram enviados à pessoa errada. Isto significa que os dois clientes receberam as encomendas um do outro, incluindo as faturas que contêm dados pessoais. Depois de ter tomado conhecimento da violação, o responsável pelo tratamento dos dados recolheu as encomendas e enviou-as aos destinatários certos.

6.1.1 CASO n.º 13 – Medidas prévias e avaliação dos riscos

107. As faturas continham os dados pessoais necessários para uma entrega correta (nome, endereço, mais o artigo adquirido e o seu preço). É importante começar por identificar a forma como o erro humano poderia ter ocorrido e, de alguma forma, poderia ter sido evitado. Neste caso em concreto, o risco é descrito como reduzido, uma vez que não houve nenhuma categoria especial de dados pessoais ou outros dados cujo abuso possa ter efeitos negativos substanciais e a violação não resulta de um erro sistémico por parte do responsável pelo tratamento, estando envolvidas apenas duas pessoas. Não foi possível identificar qualquer efeito negativo sobre as pessoas.

6.1.2 CASO n.º 13 – Atenuação e obrigações

108. O responsável pelo tratamento deve prever a devolução gratuita dos artigos e das faturas que os acompanham, bem como solicitar aos destinatários errados que destruam/apaguem todas as eventuais cópias das faturas que contenham os dados pessoais da outra pessoa.

109. Mesmo que a violação por si só não constitua um risco elevado para os direitos e liberdades das pessoas afetadas e, por conseguinte, a comunicação aos titulares dos dados não seja obrigatória nos termos do artigo 34.º do RGPD, não é possível contornar a comunicação da violação aos mesmos, uma vez que a sua cooperação é necessária para atenuar o risco.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

6.2 CASO n.º 14: Dados pessoais altamente confidenciais enviados por correio eletrónico por engano

O instituto de emprego de um serviço da administração pública enviou uma mensagem de correio eletrónico – sobre futuras ações de formação – às pessoas inscritas no seu sistema como candidatos a emprego. Por engano, foi anexado a esta mensagem eletrónica um documento que continha todos os dados pessoais dos candidatos a emprego (nome, endereço eletrónico, endereço postal, número de segurança social). O número de pessoas afetadas é superior a 60 000. Posteriormente, o instituto contactou todos os destinatários e pediu-lhes que apagassem a mensagem anterior e que não utilizassem as informações nela contidas.

6.2.1 CASO n.º 14 – Medidas prévias e avaliação dos riscos

110. Deveriam ter sido aplicadas regras mais rigorosas para o envio dessas mensagens. É necessário ponderar a introdução de mecanismos de controlo adicionais.

111. O número de pessoas afetadas é considerável e o envolvimento do seu número de segurança social, juntamente com outros dados pessoais mais básicos, aumenta ainda mais o risco, que pode ser identificado

como elevado[31]. O responsável pelo tratamento não tem forma de impedir a posterior distribuição dos dados por algum dos destinatários.

6.2.2 CASO n.º 14 – Atenuação e obrigações

112. Tal como referido anteriormente, os meios para atenuar eficazmente os riscos de uma violação semelhante são limitados. Embora o responsável pelo tratamento tenha solicitado o apagamento da mensagem, não pode obrigar os destinatários a fazê-lo e, consequentemente, também não pode ter a certeza de que cumprem o pedido.

113. A execução das três ações abaixo indicadas deve ser evidente num caso como este.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

6.3 CASO n.º 15: Dados pessoais enviados por correio eletrónico por engano

Uma lista de participantes de um curso de inglês jurídico que decorre num hotel durante cinco dias foi enviada por engano a 15 antigos participantes do curso em vez do hotel. A lista contém nomes, endereços eletrónicos e preferências alimentares dos 15 participantes. Apenas dois participantes indicaram as suas preferências alimentares e informaram que são intolerantes à lactose. Nenhum dos participantes tem uma identidade protegida. O responsável pelo tratamento descobre o erro imediatamente após o envio da lista e informa os destinatários do erro e pede-lhes que apaguem a lista.

6.3.1 CASO n.º 15 – Medidas prévias e avaliação dos riscos

114. Deveriam ter sido aplicadas regras rigorosas para o envio de mensagens que contenham dados pessoais. É necessário ponderar a introdução de mecanismos de controlo adicionais.

115. Os riscos decorrentes da natureza, sensibilidade, volume e contexto dos dados pessoais são reduzidos. Os dados pessoais incluem dados sensíveis sobre as preferências alimentares de dois dos participantes. Mesmo que a informação de que alguém é intolerante à lactose configure dados relativos à saúde, o risco de estes dados serem utilizados de forma prejudicial deve ser considerado relativamente baixo. Embora, no caso de dados relativos à saúde, se presuma normalmente que a violação é suscetível de resultar num risco elevado para o titular dos dados[32], ao mesmo tempo, neste caso específico, não é possível identificar qualquer risco de que a violação cause danos físicos, materiais ou imateriais ao titular dos dados devido à divulgação não autorizada de informações relativas à intolerância à lactose. Contrariamente a outras preferências alimentares, a intolerância à lactose não pode normalmente ser associada a quaisquer convicções religiosas ou filosóficas. A quantidade de dados violados e o número de titulares de dados afetados também são muito reduzidos.

[31] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

[32] Ver Orientações WP250, p. 23.

6.3.2 CASO n.º 15 – Atenuação e obrigações

116. Resumidamente, pode afirmar-se que a violação não teve qualquer efeito significativo sobre os titulares dos dados. O facto de o responsável pelo tratamento ter contactado imediatamente os destinatários após ter tomado conhecimento do engano pode ser considerado um fator de atenuação.

117. Se for enviada uma mensagem de correio eletrónico a um destinatário errado/não autorizado, é recomendável que o responsável pelo tratamento de dados envie, com conhecimento oculto, uma mensagem de correio eletrónico de seguimento aos destinatários involuntários, com um pedido de desculpas, dando instruções para que o correio eletrónico ilícito seja apagado e informando os destinatários de que não têm o direito de continuar a utilizar os endereços de correio eletrónico que lhes foram identificados.

118. Face a esta situação, era pouco provável que a violação de dados acima descrita resultasse num risco para os direitos e liberdades dos titulares dos dados, pelo que não foi necessário efetuar qualquer notificação à AC ou aos titulares dos dados em causa. No entanto, esta violação de dados deve também ser documentada em conformidade com o artigo 33.º, n.º 5.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	X	X

6.4 CASO n.º 16: Erro do correio postal

Uma seguradora oferece seguros automóveis. Para o efeito, envia regularmente políticas de contribuição ajustadas por correio postal. Além do nome e endereço do tomador do seguro, a carta contém o número de matrícula do veículo sem algarismos ocultados, as taxas de seguro do ano de seguro em curso e do ano de seguro seguinte, a quilometragem anual aproximada e a data de nascimento do tomador de seguro. Os dados relativos à saúde em conformidade com o artigo 9.º do RGPD, os dados relativos aos pagamentos (dados bancários) e os dados económicos e financeiros não estão incluídos.

As cartas são embaladas por caixas automáticas. Devido a um erro mecânico, duas cartas endereçadas a diferentes tomadores de seguros são inseridas num envelope e enviadas a um tomador de seguro por correio postal. O tomador de seguro abre a carta em casa e vê que recebeu a carta que lhe pertencia, bem como a carta que devia ter sido entregue a outro tomador de seguro.

6.4.1 CASO n.º 16 – Medidas prévias e avaliação dos riscos

119. A carta incorretamente entregue contém o nome, endereço, data de nascimento, número de matrícula do veículo não ocultado e a classificação da taxa de seguro do ano em curso e do ano seguinte. Os efeitos sobre a pessoa afetada devem ser considerados médios, uma vez que as informações não acessíveis ao público, como a data de nascimento ou os números de matrícula não ocultados, e os pormenores sobre o aumento das taxas de seguro são comunicados ao destinatário não autorizado. Considera-se que a probabilidade de utilização abusiva destes dados se situa entre baixa e média. No entanto, embora muitos destinatários provavelmente coloquem a carta indevidamente recebida no lixo, em alguns casos não se pode excluir totalmente a possibilidade de a carta ser publicada nas redes sociais ou de o tomador de seguro ser contactado.

6.4.2 CASO n.º 16 – Atenuação e obrigações

120. A devolução do documento original deve ser paga pelo responsável pelo tratamento. O destinatário errado deve também ser informado de que não pode utilizar indevidamente as informações lidas.

121. Provavelmente, nunca será possível evitar completamente um erro de entrega postal numa expedição em massa se forem utilizadas máquinas totalmente automatizadas. No entanto, em caso de aumento da frequência, é necessário verificar se as máquinas embaladoras têm a configuração e a manutenção mais corretas ou se alguma outra questão sistémica conduz a tal violação.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	X

6.5 Medidas organizacionais e técnicas para prevenir/atenuar os impactos dos erros no correio postal

122. Uma combinação das medidas a seguir mencionadas – aplicadas em função das características únicas do caso – deverá ajudar a reduzir a probabilidade de reincidência de uma violação semelhante.

123. Medidas aconselháveis:

(*A seguinte lista de medidas não é, de modo algum, exclusiva ou exaustiva*. *Pelo contrário, o objetivo é apresentar ideias de prevenção e possíveis soluções. Cada atividade de tratamento é diferente, pelo que o responsável pelo tratamento deve tomar a decisão sobre quais as medidas que melhor se adequam à situação em causa*).

- Definir normas exatas – sem margem para interpretação – para o envio de cartas/mensagens de correio eletrónico.
- Formação adequada do pessoal sobre como enviar cartas/mensagens de correio eletrónico.
- Quando enviam mensagens de correio eletrónico a vários destinatários, estes são inseridos por defeito no campo «bcc».
- É necessário voltar a confirmar quando se enviam mensagens de correio eletrónico a vários destinatários, que não constam do campo «bcc».
- Aplicação do princípio dos «quatro olhos».
- Endereçamento automático em vez de manual, com dados extraídos de uma base de dados disponível e atualizada; o sistema de endereçamento automático deve ser revisto regularmente para verificar se existem erros ocultos e configurações incorretas.
- Aplicação do atraso da mensagem (por exemplo, a mensagem pode ser apagada/editada num determinado prazo após clicar no botão para enviar).
- Desativar o preenchimento automático quando se digitam endereços eletrónicos.
- Sessões de sensibilização sobre os erros mais comuns que conduzem a uma violação de dados pessoais.
- Sessões de formação e manuais sobre como lidar com incidentes que provoquem uma violação de dados pessoais e quem informar (envolver o encarregado da proteção de dados).

7 OUTROS CASOS – ENGENHARIA SOCIAL

7.1 CASO n.º 17: Roubo de identidade

O centro de contacto de uma empresa de telecomunicações recebe uma chamada telefónica de uma pessoa que se faz passar por cliente. O suposto cliente exige que a empresa mude o endereço de correio eletrónico para o qual devem ser enviados os dados de faturação. O trabalhador do centro de contacto valida a identidade do cliente solicitando determinados dados pessoais, tal como definido nos procedimentos da empresa. O assistente indica corretamente o número fiscal e o endereço postal do cliente (porque teve acesso a estes dados). Após a validação, o operador efetua a alteração solicitada e, a partir daí, os dados de faturação são enviados para o novo endereço de correio eletrónico. O procedimento não prevê qualquer notificação ao anterior contacto de correio eletrónico. No mês seguinte, o cliente legítimo contacta a empresa, numa tentativa de saber por que razão não está a receber a faturação no seu endereço de correio eletrónico e nega ter efetuado qualquer chamada a pedir a alteração do contacto de correio eletrónico. Mais tarde, a empresa apercebe-se de que os dados foram enviados a um utilizador ilegítimo e reverte a alteração.

7.1.1 CASO n.º 17 – Avaliação dos riscos, atenuação e obrigações

124. Este caso é um exemplo da importância de medidas prévias. A violação, do ponto de vista do risco, apresenta um elevado nível de risco33, uma vez que os dados de faturação podem fornecer informações sobre a vida privada do titular dos dados (por exemplo, hábitos, contactos) e pode causar danos materiais (por exemplo, perseguição, risco para a integridade física). Os dados pessoais obtidos durante este ataque também podem ser utilizados para facilitar a usurpação de conta nesta organização ou explorar outras medidas de autenticação noutras organizações. Tendo em conta estes riscos, a medida de autenticação «adequada» deve cumprir uma norma elevada, dependendo dos dados pessoais que podem ser tratados em resultado da autenticação.

125. Consequentemente, o responsável pelo tratamento deve efetuar tanto uma notificação à AC como uma comunicação ao titular dos dados.

126. O processo prévio de validação do cliente deve ser claramente aperfeiçoado à luz deste caso. Os métodos utilizados para a autenticação não foram suficientes. A parte mal-intencionada fez-se passar pelo utilizador previsto recorrendo a informações publicamente disponíveis e informações a que, de outro modo, teve acesso.

127. Não é recomendada a utilização deste tipo de autenticação estática baseada no conhecimento (se a resposta não for alterada e se a informação não for «secreta», como seria o caso com uma palavra-passe).

128. Em vez disso, a organização deve utilizar uma forma de autenticação que resulte num elevado grau de confiança de que o utilizador autenticado é a pessoa prevista e não outra pessoa qualquer. A introdução de um método de autenticação multifatorial fora da banda resolveria o problema, por exemplo, para verificar o pedido de alterações, enviando um pedido de confirmação para o anterior contacto; ou acrescentar perguntas adicionais e requerer informações apenas visíveis nas faturas anteriores. Cabe ao responsável pelo

[33] Para consultar as orientações sobre as operações de tratamento «suscetíveis de resultarem num risco elevado», ver a nota de rodapé 10 *supra*.

tratamento decidir quais as medidas a adotar, uma vez que conhece os pormenores e os requisitos do seu funcionamento interno.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓

7.2 CASO n.º 18: Exfiltração por correio eletrónico

Uma cadeia de hipermercados detetou, três meses após a sua configuração, que algumas contas de correio eletrónico tinham sido alteradas e que foram criadas regras para que todas as mensagens que contenham determinadas expressões (por exemplo, «fatura», «pagamento», «ordem de transferência bancária», «autenticação do cartão de crédito», «dados da conta bancária») fossem transferidas para uma pasta não utilizada e também enviadas para um endereço de correio eletrónico externo. Além disso, nessa altura, já tinha sido cometido um ataque de engenharia social, ou seja, o atacante, fazendo-se passar por um fornecedor, tinha alterado os dados da conta bancária de forma a introduzir dados seus. Por último, nessa altura, tinham sido enviadas várias faturas falsas que continham os novos dados da conta bancária. O sistema de monitorização da plataforma de correio eletrónico acabou por emitir um alerta sobre as pastas. A empresa não conseguiu detetar a forma como o atacante conseguiu aceder inicialmente às contas de correio eletrónico, mas presumiu que fora utilizada uma mensagem de correio eletrónico infetada para permitir o acesso ao grupo de utilizadores responsáveis pelos pagamentos.

Devido ao reencaminhamento de mensagens de correio eletrónico baseado em palavras-chave, o atacante recebeu informações sobre 99 trabalhadores: nome e salário de um determinado mês relativamente a 89 titulares de dados; nome, estado civil, número de filhos, salário, horário de trabalho e restante informação sobre o recibo salarial de dez trabalhadores cujos contratos cessaram. O responsável pelo tratamento apenas notificou os dez trabalhadores pertencentes a este último grupo.

7.2.1 CASO n.º 18 – Avaliação dos riscos, atenuação e obrigações

129. Mesmo que o atacante não tivesse provavelmente como objetivo a recolha de dados pessoais, uma vez que a violação poderia conduzir a danos materiais (por exemplo, perdas financeiras) e imateriais (por exemplo, usurpação ou fraude de identidade), ou que os dados podiam ser utilizados para facilitar outros ataques (por exemplo, mistificação da interface), a violação de dados pessoais é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares. Por conseguinte, a violação deve ser comunicada a todos os 99 trabalhadores e não apenas aos dez trabalhadores cujas informações salariais foram divulgadas.

130. Depois de ter tomado conhecimento da violação, o responsável pelo tratamento obrigou a alterar a palavra-passe das contas comprometidas, bloqueou o envio de mensagens de correio eletrónico para a conta de correio eletrónico do atacante, notificou o prestador de serviços da mensagem de correio eletrónico utilizada pelo atacante relativamente às suas ações, suprimiu as regras estabelecidas pelo atacante e aperfeiçoou os alertas do sistema de monitorização, a fim de emitir um alerta logo que fosse criada uma regra automática. Em alternativa, o responsável pelo tratamento pode suprimir o direito de os utilizadores definirem regras de reencaminhamento, exigindo que a equipa do serviço informático o faça apenas mediante pedido, ou introduzir uma política que permita aos utilizadores verificar e comunicar informações sobre as regras estabelecidas nas suas contas uma vez por semana ou mais frequentemente, em áreas que tratam dados financeiros.

131. O facto de uma violação poder ocorrer e não ser detetada durante tanto tempo e o facto de, num período mais longo, a engenharia social poder ter sido utilizada para alterar mais dados, evidenciaram problemas significativos no sistema de segurança informática do responsável pelo tratamento. Estas questões devem ser abordadas sem demora, como as análises de automatização e os controlos das alterações, a deteção de incidentes e as medidas de resposta. Os responsáveis pelo tratamento de dados sensíveis, informações financeiras, etc., têm uma maior responsabilidade de garantir uma segurança adequada dos dados.

Medidas necessárias com base nos riscos identificados		
Documentação interna	Notificação à AC	Comunicação aos titulares dos dados
✓	✓	✓