GUIA ORIENTATIVO

SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

VERSÃO 1.0
OUT. 2021

ANPD

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

GUIA ORIENTATIVO SOBRE SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

Versão 1.0

OUTUBRO DE 2021

Equipe de elaboração

Andressa Girotto Vargas - Servidora da Coordenação-Geral de Normatização

Fabrício Lopes - Coordenador-Geral de Fiscalização

Isabela Maiolino - Coordenadora-Geral de Normatização

Jeferson Dias Barbosa - Gerente de Projeto do Conselho Diretor

Marcelo Santiago Guedes - Coordenador-Geral de Tecnologia e Pesquisa

Maria Luiza Duarte Sa - Estagiária da Coordenação de Tecnologia e Pesquisa

Rodrigo Santana dos Santos - Coordenador de Normatização

Thiago Moraes - Coordenador de Tecnologia e Pesquisa

Colaboradores externos

Cristine Hoepers - CERT.br/NIC.br

Klaus Steding-Jessen - CERT.br/NIC.br

Histórico de versões - Versão 1.0 – outubro/2021.

SUMÁRIO

1. APRESENTAÇÃO E OBJETIVO

1. A Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), representa um marco regulatório sobre o tratamento de dados pessoais. Um dos seus pilares é a proteção desses dados, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

2. Como competência da ANPD, a LGPD determinou em seu art. 55-J, XVIII, a edição de normas, orientações e procedimentos simplificados e diferenciados para microempresas e empresas de pequeno porte[1], bem como para iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação. A resolução com esse fim pode incluir no conceito de agentes de pequeno porte outras categorias de organizações além das anteriormente mencionadas[2].

3. O presente guia de boas práticas é endereçado aos agentes de tratamento de pequeno porte que, em razão de seu tamanho e eventuais limitações, muitas vezes não possuem dentre o seu corpo de funcionários, pessoas especializadas em segurança da informação e necessitam aprimorá-la em relação ao tratamento de dados pessoais, nos termos dos artigos 46, 47, 48[3] e 49 da LGPD.

4. Nesse sentido, o Guia apresenta algumas medidas de segurança da informação, com o fim de proteger os dados pessoais sob a guarda dos agentes de pequeno porte.

5. Para facilitar a identificação da adoção das medidas sugeridas neste guia, segue como anexo uma lista para uso interno das organizações.

[1] Sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, com faturamento máximo nos termos do art. 3º da Lei Complementar nº 123 de 14 de dezembro de 2006.

[2] Para maiores informações acerca de quem pode ser considerado agente de tratamento de pequeno porte, acompanhar a publicação da respectiva resolução.

[3] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, será tratado em um Guia específico.

2. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

2.1. Segurança da informação

6. A segurança da informação pode ser definida como o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação. Esse conjunto de ações impacta todo o ambiente institucional das empresas, com objetivo de prevenir, detectar e combater as ameaças digitais.

7. Um importante ponto é o gerenciamento de riscos no âmbito da segurança da informação, que consiste no processo de identificar, quantificar e gerenciar os riscos relacionados à segurança da informação dentro da organização. Ele visa a obter um equilíbrio eficiente entre a concretização de oportunidades de ganhos e a minimização de vulnerabilidades e perdas.

8. Ainda que não seja obrigatório é indicado que o gerenciamento de riscos de segurança seja realizado periodicamente. Ele é parte integrante das práticas de gerenciamento e um importante elemento da boa governança, além de auxiliar na melhoria organizacional, no desempenho e na tomada de decisões.

2.2. Tratamento de dados pessoais

9. A LGPD define tratamento como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, nos termos do inciso X do art. 5º da norma.

10. Vale ressaltar que a LGPD conceitua os dados pessoais em seu art. 5º, inciso I, como sendo as informações relacionadas a pessoa natural identificada ou identificável; e dados sensíveis, nos termos do art. 5º, inciso II, são definidos como aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de

caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

11. Os dados sensíveis, por terem uma proteção especial conferida pela LGPD, possuem regras mais rigorosas para seu tratamento, a fim de evitar riscos ou danos relevantes aos titulares de dados, mesmo quando manipulados por agentes de tratamento de pequeno porte. Por esse motivo, o rol de bases legais do art. 7º que trata de dados pessoais é distinto das hipóteses descritas no art. 11, que trata de dados pessoais sensíveis.

2.3 Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais

12. A LGPD introduz em seu art. 6º, VII, o Princípio da Segurança, que consiste na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Posteriormente, a Lei detalha a questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

13. No art. 46, a lei estabelece que agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, ou seja, vulnerabilidades que podem expor os dados dos titulares a tratamento inadequado ou ilícito. Já o §2º do art. 46 determina que as medidas de que trata o caput do artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

14. O art. 47 define que agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na Lei em relação aos dados pessoais, mesmo após o seu término.

15. Uma importante obrigação relacionada à segurança de dados pessoais é tratada no art. 48 e consiste na comunicação à ANPD de incidentes de segurança que possam

acarretar risco ou dano relevante[4] aos titulares de dados. Ela será tratada em normatização específica sobre o assunto e, portanto, não será abordada neste Guia. Cabe destacar que a ANPD emitiu orientações sobre incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à Autoridade, disponível em seu sítio eletrônico[5] .

16. Por fim, o art. 49 estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e nas demais normas regulamentares.

2.4 Segurança da informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte

17. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[6] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

18. Como se sabe, a implementação e a manutenção de medidas que atendam a essas obrigações, considerando sua complexidade e especificidade em casos concretos, podem necessitar, em algumas situações, de elevado investimento, com potencial de causar impacto financeiro aos agentes de tratamento de pequeno porte.

19. Nesse sentido, são apresentadas a seguir sugestões de medidas de segurança da informação capazes de promover, em agentes de tratamento de pequeno porte, um ambiente institucional mais seguro quanto ao tratamento de dados pessoais.

20. As medidas sugeridas devem ser entendidas como boas práticas e devem ser complementadas com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização.

[4] Cabe explicar que não é todo incidente de segurança que deveria ser comunicado à ANPD, mas tão somente aquele com dados pessoais e com que possa acarretar risco ou dano relevante aos titulares.
[5] Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>.
[6] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado, não será abordado neste Guia.

3. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

3.1 Medidas administrativas

3.1.1 Política de segurança da informação

21. A política de segurança da informação - PSI, consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.

22. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Muito embora não seja obrigatória, a elaboração dessa política e sua implementação são incentivadas pela ANPD aos agentes de tratamento de pequeno porte porque evidenciam boa-fé e diligência na segurança dos dados pessoais sob sua custódia e fornecem as diretrizes para a gestão da segurança da informação.

23. O propósito fundamental da PSI é ser uma ferramenta que apoie a implementação de um processo estruturado de segurança da informação adequado a cada organização, considerando seu negócio e seu porte.

24. Nesse sentido, a ANPD sugere que, quando possível, seja estabelecida pela organização uma política de segurança da informação, ainda que simplificada, com previsão de revisão periódica e que contemple controles relacionados ao tratamento de dados pessoais, como por exemplo, cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de softwares; uso de correio eletrônico; uso de antivírus, entre outros.

3.1.2 Conscientização e Treinamento

25. Os recursos humanos de uma organização são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e à proteção de dados pessoais, já que efetivamente são as pessoas que trabalham para os agentes de tratamento de pequeno porte que realizarão o tratamento dos dados pessoais.

26. Assim, sugere-se que os agentes de tratamento de pequeno porte conscientizem os seus funcionários por meio de treinamentos e campanhas de conscientização sobre suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

27. Essa conscientização implica informar e sensibilizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.

28. Algumas informações úteis que podem ser passadas aos funcionários são:

- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- não compartilhar logins e senhas de acesso das estações de trabalho;
- bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- seguir as orientações da política de segurança da informação.

29. Também é importante criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas.

3.1.3. Gerenciamento de contratos

30. É recomendável que termos de confidencialidade (non-disclosure agreement - NDA) sejam assinados com os funcionários da empresa para que estes se comprometam a não

divulgar informações confidenciais que envolvam dados pessoais. Esta é uma medida de segurança importante contra abusos de privilégio.

31. É indicado que seja realizado o gerenciamento de contratos e aquisições, para atenção à distribuição de funções e responsabilidades entre as partes, com observância à LGPD e ao tratamento adequado dos dados pessoais.

32. No caso de agentes de tratamento de pequeno porte que terceirizam os serviços de TI, recomenda-se que estabeleçam com os fornecedores contratos que incluam dentre outras, cláusulas de segurança da informação que assegurem a adequada proteção de dados pessoais.

33. Tais instrumentos poderão conter, por exemplo, cláusulas que tratam de:

- Regras para fornecedores e parceiros;
- regras sobre compartilhamentos;
- relações entre controlador-operador;
- orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

3.2 Medidas técnicas

3.2.1 Controle de acesso

34. O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele consiste em processos de autenticação, autorização e auditoria.

- A autenticação identifica quem acessa o sistema ou os dados;
- a autorização determina o que o usuário identificado pode fazer;
- a auditoria registra o que foi feito pelo usuário.

35. Sobre esse aspecto, a ANPD sugere que, caso o agente de tratamento de pequeno porte possua rede interna de computadores, seja implementado um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da

necessidade de trabalhar com o sistema e de acessar dados pessoais. Esse sistema de controle de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários.

36. Além disso, sugere-se que o sistema de controle de acesso seja configurado com funcionalidades que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade. Isso significa que é importante que o sistema possa estabelecer o número de caracteres para se criar uma senha, definir se é necessário o uso de um caractere especial ou outros fatores que o agente de tratamento considere necessários.

37. É importante, ainda, na implementação de sistemas de segurança, utilizar um adequado gerenciamento de senhas, evitando o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos, tendo em vista que geralmente os atacantes utilizam estas senhas padronizadas (default) para tentativas de conexão e realizar os seus ataques. As senhas precisam ser alteradas por outras com requisitos mais seguros.

38. Outra medida sugerida é que os agentes de tratamento de pequeno porte não permitam o compartilhamento de contas ou de senhas entre funcionários, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação.

39. A premissa que deve ser aplicada é a do princípio do menos privilégio (need to know), ou seja, os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades. Funções de alto nível, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade.

40. Nesse sentido, importante mencionar que o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[7] publicado pelo Centro de Estudos, Resposta

[7] Segurança digital: uma análise da gestão de riscos em empresas brasileiras, Núcleo de Informação e Coordenação do Ponto BR, 1ª ed., São Paulo: Comitê Gestor da Internet no Brasil, 2020. ISBN 978-65-86949-20-9. Disponível em: <https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/>.

e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[8] em conjunto com o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), apontou que melhorar processos de identificação e autenticação em serviços e sistemas, incluindo a não reutilização de senhas, estão entre as três medidas de maior impacto na segurança da informação em empresas.[9]

41. Por fim, sugere-se que os agentes considerem, preferencialmente, utilizar a autenticação multi-fatores (MFA) para acessar sistemas ou base de dados que contenham dados pessoais. Essa autenticação consiste em estabelecer uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.

42. A título de exemplo de autenticação multi-fatores, podemos citar o envio de códigos de segurança por short message service (SMS) ou por e-mail e o uso de aplicativos autenticadores ou tokens de segurança.

3.2.2 Segurança dos dados pessoais armazenados[10]

43. Pode-se dizer que as etapas descritas até o momento visam a contribuir justamente com a segurança dos dados pessoais armazenados, a fim de diminuir o risco de incidentes e aumentar a segurança que os agentes de pequeno porte devem ter ao longo do tratamento de dados pessoais.

44. Inicialmente, cabe salientar que, muitas vezes, os agentes de tratamento coletam mais dados do que o necessário para a realização de suas atividades ou para uma finalidade

[8] Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. O NIC.br é uma organização privada sem fins lucrativos criada para implementar as decisões e os projetos do CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no país.

[9] As três medidas recomendadas pelo CERT.br e pelo CETIC.br estão contempladas nas boas práticas apresentadas neste Guia. São elas: (i) manter todos os softwares (sistemas operacionais e aplicativos) atualizados; (ii) fazer o hardening de todos os sistemas e dispositivos, ou seja, desabilitar serviços desnecessários para a função dos dispositivos, mudar todas as senhas padrão, configurar todos os serviços expostos na Internet de forma segura e constantemente rever as configurações; (iii) melhorar os processos de identificação e autenticação em serviços e sistemas.

[10] A segurança dos dados pessoais armazenados está relacionada com a segurança de dados em repouso, expressão utilizada pela comunidade técnico-científica.

específica. Para se evitar riscos de incidentes de segurança e outros comprometimentos, e em atenção ao princípio da necessidade previsto no art. 6º, III, da LGPD, os agentes de tratamento de pequeno porte devem coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida.

45. No contexto atual da LGPD, tratar (coletar e guardar, por exemplo) dados pessoais sem uma utilidade imediata e concreta, apenas porque um dia poderão ser úteis (sem se saber exatamente para quê), não é uma prática adequada, considerando os princípios da finalidade e da necessidade previstos na referida Lei.

46. Além disso, tendo em vista que os dados pessoais sensíveis gozam de uma proteção especial pela LGPD, sugere-se que os agentes de tratamento de pequeno porte que armazenam dados dessa natureza implementem soluções que dificultem a identificação do titular, como as técnicas de pseudonimização[11]. Um exemplo dessa técnica é a criptografia.

47. Em relação às estações de trabalho, sugere-se que seja orientado aos funcionários a importância das configurações de segurança, a fim de que eles não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites.

48. Um importante ponto a ser considerado é evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives, discos rígidos externos, dentre outros, tendo em vista o risco de se perder a guarda dos dados pessoais transferidos. Caso essa operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como inventariá-los, cifrar os dados e armazená-los em locais seguros.

[11] Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art.13 §4 da LGPD). Sobre o assunto, veja: COMISSÃO DE PROTEÇÃO DE DADOS PESSOAIS DE SINGAPURA. Guide to Basic Data Anonymization Techniques – PDPC. 25 jan 2018. Disponível em: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf>; e COMISSÃO EUROPEIA. Opinion 05/2014 on Anonymization Techniques. Article 29 Data Protection Working Party – 0829/EN – WP216. Adotada em 10 abr 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

49. Em relação às cópias de segurança, comumente chamadas de backups, é importante que elas sejam realizadas regularmente de forma completa e armazenadas em locais seguros e distintos dos dispositivos de armazenamento principais. Também é importante que essas cópias não sejam sincronizadas online (em tempo real), para evitar a perda de dados em casos de infecções por códigos maliciosos que sequestram os dados (ransomware).

50. Por fim, sobre a eliminação de dados pessoais, sugere-se que em todas as mídias que contenham dados pessoais seja executado o método de formatar antes de descartá-las. Quando isso não for possível, como em CDs e DVDs, sugere-se que seja realizada a destruição física da mídia – o que também se aplica para destruição de papel e de mídia portátil para armazenar dados pessoais.

51. Além disso, para os agentes que fazem uso de serviço de terceiros para o descarte, seja de mídia ou registro de papel, sugere-se que seja estabelecido um contrato de serviço com cláusulas de registro da destruição que for realizada.

3.2.3 Segurança das comunicações[12]

52. As comunicações são um importante ponto relacionado à segurança de dados pessoais, tendo em vista a possibilidade da existência de vulnerabilidades no processo de transmissão de dados ou informações. Por exemplo, aplicativos de mensageria podem comprometer a segurança de qualquer negócio se houver troca de links maliciosos ou se o usuário receber algum arquivo infectado.

53. Sobre o assunto, destaca-se a relevância de se utilizar conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim. Isso se aplica também ao uso de e-mails, por exemplo, para envio de informações de funcionários como salários ou de prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

[12] A segurança das comunicações está relacionada com a segurança de dados em trânsito, expressão utilizada pela comunidade técnico-científica.

54. Além disso, sugere-se que o tráfego de rede seja gerenciado. Algumas formas de fazer isso, são:

- instalar e manter um sistema de firewall[13], que monitore, detecte e bloqueie ameaças, impedindo conexões a redes não confiáveis. Caso serviços web sejam utilizados, sugere-se o uso de firewalls de aplicação web (Web Application Firewall – WAF).
- Proteger serviços de e-mail, utilizando antivírus integrados, ferramentas anti-spam e filtros de e-mail;

55. Outro cuidado importante é remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas, por exemplo, o site da empresa. Caso o negócio da empresa envolva o tratamento de dados sensíveis (ex. serviços de saúde) recomenda-se criar um canal de acesso restrito para que o cliente acesse essas informações.

3.2.4 Manutenção de programa de gerenciamento de vulnerabilidades

56. Em relação à manutenção de um programa de gerenciamento de vulnerabilidades, entende-se que um importante ponto é o monitoramento da existência de novas versões e correções disponíveis em todos os sistemas e aplicativos. Nesse sentido, é também relevante manter todos os sistemas e aplicativos em suas últimas versões, bem como instalar todas as correções de segurança disponíveis (patches[14]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

57. Uma medida adicional de segurança e detecção de comprometimentos consiste na adoção e atualização de softwares antivírus ou antimalwares, que detectam, impedem e atuam na remoção de programas maliciosos, como vírus. Diante disso, sugere-se que os agentes de tratamento de pequeno porte implementem antivírus em seus sistemas, em especial em computadores e laptops.

[13] Dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
[14] Programa de computador criado para atualizar ou corrigir um software de forma a corrigir vulnerabilidades ou falhas.

58. Além disso, é importante que esses mecanismos sejam mantidos funcionando ativamente e atualizados e que realizem varreduras periódicas nos dispositivos, bem como que não possam ser desativados ou alterados pelos usuários.

3.3 Medidas relacionadas ao uso de dispositivos móveis

59. Em relação aos dispositivos móveis, como smartphones e laptops, caso seu uso seja necessário para fins institucionais, sugere-se que estejam sujeitos aos mesmos procedimentos de controle de acesso que os outros equipamentos de TI, como o uso da autenticação multi fator para acesso aos dispositivos e sistemas de informação da organização, além de serem guardados em locais seguros quando não estiverem em uso.

60. É importante que, quando possível, os agentes de tratamento de pequeno porte separem os dispositivos móveis de uso privado daqueles de uso institucional. Dispositivos móveis de uso privado estão sujeitos a mais vulnerabilidades, por exemplo, pelo uso de aplicativos potencialmente inseguros para fins pessoais. Já em dispositivos para uso exclusivamente institucional, pode-se ter mais gerenciamento no acesso e nos aplicativos utilizados.

61. Caso não seja possível implementar medidas de segurança equivalentes às da organização, recomenda-se que dispositivos móveis pessoais não sejam utilizados para fins institucionais.

62. Tendo em vista que dispositivos móveis podem ser comprometidos mais facilmente em eventual perda ou roubo, e que isso pode colocar em risco a guarda dos dados pessoais, sugere-se também que os agentes avaliem e implementem funcionalidades que permitam apagar remotamente os dados pessoais relacionados à sua atividade de processamento. Isso poderá diminuir a chance de eventual incidente de segurança com dados pessoais. As medidas sugeridas nessa seção valem tanto para dispositivos móveis de propriedade institucional quanto os pessoais.

3.4. Medidas relacionadas ao serviço em nuvem

63. Serviço em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet ("a nuvem").

64. A seguir, são descritas medidas consideradas prioritárias para que agentes de pequeno porte contratem serviço em nuvem com maior garantia na proteção de dados pessoais.

65. Cabe salientar que, devido ao porte dos provedores de serviço de computação em nuvem e à especificidade do trabalho exercido, é esperado que essas empresas observem e implementem as recomendações internacionais e as boas práticas de segurança da informação.

66. Com relação à prestação de serviços de computação em nuvem, sugere-se que o agente de tratamento de pequeno porte realize um contrato de acordo de nível de serviço[15], contemplando a segurança dos dados armazenados.

67. Além disso, a partir dos requisitos de segurança da informação definidos pelo agente de tratamento de pequeno porte, sugere-se que seja avaliado se o serviço oferecido pelo provedor do serviço em nuvem atende os requisitos estabelecidos.

68. Por fim, sugere-se que sejam especificados os requisitos para o acesso do usuário a cada serviço em nuvem utilizado, bem como que sejam usadas técnicas de autenticação multi fator, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

4. CONSIDERAÇÕES FINAIS

69. O presente guia orientativo foi elaborado com o objetivo de disseminar boas práticas e medidas básicas de segurança da informação para apoiar os agentes de

[15] Em inglês Service Level Agreement (SLA).

tratamento de pequeno porte no desenvolvimento de suas atividades organizacionais em um ambiente institucional mais seguro no que se refere ao tratamento de dados pessoais.

70. Neste Guia, foram apresentadas medidas administrativas que envolvem a política de segurança da informação relacionada a dados pessoais e a segurança em recursos humanos; e medidas técnicas, que tratam, entre outros, do controle de acesso aos dados; segurança nos dados armazenados; manutenção de programa de gerenciamento de vulnerabilidades; e segurança das comunicações. Também se deu destaque a medidas relacionadas ao serviço em nuvem (de ordem técnica ou administrativa), tendo em vista a frequência com que esses serviços são utilizados por agentes de tratamento de pequeno porte.

71. Espera-se que essas medidas contribuam para estabelecer um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, para um aumento na confiança dos titulares de dados nos agentes de tratamento de dados pessoais de pequeno porte.

72. Por fim, cabe ressaltar que este documento não tem efeito normativo vinculante e deve ser entendido como um guia de boas práticas, que poderá ser atualizado e aperfeiçoado sempre que necessário.

5. REFERÊNCIAS

AWS SECURITY BLOG. Ransomware mitigation: Top 5 protections and recovery preparation actions. Disponível em: <https://aws.amazon.com/it/blogs/security/ransomware-mitigation-top-5-protections-and-recovery-preparation-actions/>. Acesso em 17 set. 2021.

CENTER FOR INTERNET SECURITY. Ransomware: The Data Exfiltration and Double Extortion Trends. Disponível em: <https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/>. Acesso em 17 set. 2021.

COMISSÃO DE PROTEÇÃO DE DADOS PESSOAIS DE SINGAPURA. Guide to Basic Data Anonymization Techniques – PDPC. 25 jan 2018. Disponível em: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf>. Acesso em 06 jul. 2021.

COMISSÃO EUROPEIA. Opinion 05/2014 on Anonymization Techniques. Article 29 Data Protection Working Party – 0829/EN – WP216. Adotada em 10 abr 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em 06 jul. 2021.

ENISA. Guidelines for SMEs on the security of personal data processing, 2016. Disponível em https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. Acesso em 29 abr. 2021.

ENISA. Non-disclosure agreement – NDA. Disponível em: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/tools/run/governing-rules/non-disclosure-agreement-2013-nda>. Acesso em 17 set. 2021.

HISCOX. Data exfiltration during ransomware attacks. Disponível em: <https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf>. Acesso em 17 set. 2021.

MICROSOFT. Backup and restore plan to protect against ransomware, 2021. Disponível em: <https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware>. Acesso em 17 set. 2021.

NCSC.uk. Phishing attacks: defending your organization. Disponível em: <https://www.ncsc.gov.uk/guidance/phishing>. Acesso em 17 set. 2021.

NIST. National Institute of Standards and Technology Special Publication 800-145 - The NIST Definition of Cloud Computing. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em 25 mai.2021.

NIST. National Institute of Standards and Technology Special Publication 1800-25 - Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf>. Acesso em 17 set. 2021.

PCI. Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS): Requisitos e procedimentos da avaliação de segurança, 2018. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/PCI_DSS_v3-2-1_PT-BR.PDF>. Acesso em 29 abr. 2021.

SECURITY BOULEVARD. Privilege Abuse: Don't Let Employee Access 'Level Up', 2021. Disponível em: <https://securityboulevard.com/2021/01/privilege-abuse-dont-let-employee-access-level-up/>. Acesso em 17 set. 2021.

UC BERKELEY. Information Security Office. What do I do to protect against Ransomware? Disponível em: <https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware>. Acesso em 17 set. 2021.

US HHS Office. FACT SHEET: Ransomware and HIPAA. Disponível em: <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>. Acesso em 17 set. 2021.