PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Nota Técnica nº 19/2021/CGN/ANPD

Assunto: **Proposta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte**

Referência: Processo SEI nº 00261.000821/2021-16

1. RELATÓRIO

1. Trata-se de proposta de guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte, que tem por finalidade apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais.

2. Nos termos do que dispõe o art. 55-J, XVIII da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), a Autoridade Nacional de Proteção de Dados (ANPD) tem competência para editar normas específicas, com procedimentos simplificados e diferenciados, bem como os critérios de elegibilidade, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à LGPD.

3. O Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, em seu art. 16, atribui a esta Coordenação-Geral de Normatização as competências de elaboração de guias e recomendações, bem como proposições normativas, regulamentos, orientações e procedimentos simplificados, nos termos da LGPD, a serem submetidas à aprovação pelo Conselho Diretor.

4. Diante das competências acima mencionadas, em 05 de maio de 2021 foi realizada reunião com Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo NIC.br para apresentar a primeira versão da minuta e coletar contribuições. A partir daí a ANPD e CERT.br trabalharam em conjunto no aprimoramento da minuta do guia orientativo.

5. A primeira versão da minuta foi submetida a comentários e sugestões dos demais servidores da ANPD entre os dias 06 de julho e 16 de julho de 2021. As contribuições recebidas foram analisadas pela equipe de trabalho criada, que procedeu ajustes na minuta.

6. Após a revisão dos ajustes realizados, elaborou-se a presente versão do guia, que segue para avaliação pela Assessoria Jurídica da ANPD e, posteriormente, será submetida à apreciação do Conselho Diretor para deliberação da matéria.

7. É o relatório.

2. ANÁLISE

2.1 Contextualização

8. A LGPD inaugurou um novo regime jurídico referente ao tratamento de dados pessoais no país e introduziu novos conceitos, direitos e obrigações ao estruturar nacionalmente um sistema efetivo de proteção de dados pessoais.

9. Dado que a aplicação desses novos conceitos, direitos e obrigações ao cotidiano do cidadão nem sempre é simples, mormente considerando a complexidade do objeto tutelado em si, percebe-se um espaço farto para interpretações e regulamentação pela ANPD, a quem incumbe zelar pelos dados pessoais, bem como regulamentar a LGPD e a sua implementação.

10. A confecção de um guia com esse propósito, por conseguinte, é tanto conveniente quanto oportuna.

11. Entre as competências da ANPD, está estabelecer normas e diretrizes para a interpretação e implementação da LGPD, conforme autoriza o parágrafo único do art. 55-J da própria LGPD:

> Art. 55-J. Compete à ANPD:
>
> (...)
>
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

12. Adicionalmente, o Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, prevê como competência da Coordenação-Geral de Normatização a elaboração de guias e recomendações:

> Art. 16. São competências da Coordenação-Geral de Normatização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:
>
> (...)
>
> II - elaborar guias e recomendações, bem como proposições normativas, orientações e procedimentos simplificados nos termos da Lei nº 13.709, de 2018, a serem submetidas à aprovação pelo Conselho Diretor;

13. Sendo assim, o guia visa disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte, cumprindo o que está disposto na LGPD e no Regimento Interno da ANPD.

2.2 Da Minuta do Guia Orientativo

14. O presente guia foi escrito buscando proporcionar uma linguagem mais acessível aos agentes de tratamento de pequeno porte, bem como identificar medidas organizacionais e técnicas que não sejam de alta complexidade e custo reduzido, sendo, portanto, mais adequado à realidade dos agentes de tratamento de pequeno porte.

Apresentação

15. Apresenta a visão geral do guia e a previsão legal do art. 55-J, XVIII, da LGPD para elaboração do guia orientativo de segurança da informação para agentes de tratamento de pequeno porte.

Escopo e Objetivo

2.1. Neste item é definido o principal público alvo do guia, sendo eles:

i. Microempresas e Empresas de Pequeno Porte: 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

ii. Startup: Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.

iii. Agente de Tratamento de Pequeno Porte: microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.

Segurança da Informação Relacionada a Dados Pessoais

16. Neste tópico busca-se esclarecer o conceito de segurança da informação e sua importância dentro de uma organização, independentemente do porte, apresentando, inclusive o conceito de gestão de riscos.

17. Apresenta-se também as obrigações relacionadas à segurança da informação relacionada a dados pessoais na LGPD, nos termos do disposto nos artigos 46 a 49 da lei.

Medidas de segurança da informação

18. Este é o principal tópico do guia, que apresenta as medidas de segurança da informação que se entende mais adequadas aos agentes de tratamento de pequeno porte, considerando a sua realidade e o impacto que estas medidas podem trazer para a proteção dos dados dos titulares de dados pessoais.

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

20. Espera-se que as medidas sugeridas pelo guia proporcionem um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, um aumento na confiança dos titulares de dados nos agentes de tratamento de pequeno porte.

21. Por fim, cabe ressaltar que o guia não tem efeito normativo vinculante e deve ser entendido como um guia de boas práticas, que poderá ser atualizado e aperfeiçoado sempre que necessário. Assim, não se pretende submeter o referido guia ao procedimento de consulta pública e audiência pública.

3. CONCLUSÃO

22. A presente Nota Técnica submete à Assessoria Jurídica a proposta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte (SEI nº 2734320), que busca estabelecer diretrizes não-vinculantes aos agentes de tratamento de pequeno porte sobre segurança da informação.

23. Diante do exposto, encaminha-se à Assessoria Jurídica para análise do Guia Orientativo.

4. ANEXO

24. Anexo - Minuta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte - SEI nº 2734320.

RODRIGO SANTANA DOS SANTOS
Coordenador de Normatização

De acordo.

ISABELA MAIOLINO
Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenadora-Geral de Normatização**, em 20/07/2021, às 15:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)**, em 20/07/2021, às 15:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2728509** e o código CRC **E95CE10D** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

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

VERSÃO PARA ASSESSORIA JURÍDICA

JULHO DE 2021

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

Equipe de elaboração

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

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

Sumário

1. APRESENTAÇÃO

1. A publicação da 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 pilares desse marco regulatório é a proteção dos dados pessoais, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

2. Um importante ponto da LGPD é a previsão de tratamento diferenciado para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, tendo determinado a edição de norma específica para esse grupo, nos termos do inciso XVIII do art. 55-J da LGPD. No momento, a norma se encontra em consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD).

3. De modo a melhor identificar estas categorias de empresas, a ANPD atribuiu o nome de agentes de tratamento de pequeno porte às micro e pequenas empresas e *startups*. Existe um enorme desafio em flexibilizar algumas obrigações desses agentes contidas na LGPD sem aumentar os riscos e danos aos titulares dos dados, bem como conscientizar as empresas sobre a relevância da proteção de dados pessoais.

4. Diante desse cenário, a ANPD elaborou o presente guia orientativo, que busca apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais. Destaca-se que este guia poderá ser atualizado de forma periódica à medida em que a ANPD entender necessário.

2. ESCOPO E OBJETIVO

5. Este 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 aprimorar o processo de segurança da informação relacionada a dados pessoais, nos termos dos artigos 46, 47, 48[1] e 49 da LGPD.

6. No âmbito deste guia orientativo, adotam-se os conceitos de microempresa, pequena empresa e *startup* trazidos pela Lei Complementar nº 123/2006 e pela Lei Complementar nº 182, de 1º de junho de 2021.

7. Diante das duas leis mencionadas, pode-se estabelecer os seguintes conceitos:

> Microempresas e Empresas de Pequeno Porte
>
> 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.
>
> Startup

[1] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, como explicado mais a frente, será tratado em um Guia específico.

Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.

Agente de Tratamento de Pequeno Porte

Microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.

8. Tendo em vista estas definições, o objetivo desse Guia é disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte.

3. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

3.1. Segurança da informação

9. A *International Organization for Standardization* (ISO) é uma organização internacional que desenvolve e publica normas técnicas que são utilizadas por inúmeros países, incluindo o Brasil. Uma das normas da organização é a Norma ABNT NBR ISO/IEC 27001,[2] que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.

10. Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio globais da organização.

11. De acordo com a norma, a segurança da informação pode ser definida como o conjunto de ações que visam a preservação da confidencialidade, integridade e disponibilidade da informação.

12. Este conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais, ou seja, estão relacionadas às camadas de tecnologia, processos e pessoas e não somente ao ambiente de tecnologia da informação.

13. 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.

14. Ainda que não seja obrigatório é indicado que, se possível, 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] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

3.2. Tratamento de dados pessoais

15. A LGPD define tratamento de dados pessoais como toda operação realizada com dados pessoais, como as que se referem a 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.

16. Vale ressaltar que dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, conforme disposto no art. 5º, I da LGPD.

17. A título exemplificativo, os conjuntos de dados que incluem dados pessoais podem conter identificadores diretos e indiretos, que permitem que um indivíduo seja identificado ou se torne identificável. Um identificador direto é uma informação específica que se refere a um indivíduo, como por exemplo nome e apelido, endereço de uma residência, endereço de correio eletrônico, número de um cartão de identificação, cookies em sítios eletrônicos. Por outro lado, um identificador indireto (também chamado de quase-identificador) é qualquer informação que pode ser usada, individualmente ou em combinação com outros quase-identificadores, por alguém que tem conhecimento sobre aquele indivíduo com o propósito de identificá-lo no conjunto de dados, como por exemplo, uma posição geográfica em um determinado momento ou uma opinião sobre um determinado assunto, dentre outros.

18. Cabe destacar que a LGPD define como dados pessoais sensíveis 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, nos termos do art. 5º, inciso II.

19. Os dados sensíveis, por terem uma proteção especial conferida pela LGPD, possuem regras mais rigorosas para seu tratamento, **a fim de evitar risco ou danos relevantes aos titulares de dados, mesmo manipulados por agentes de tratamento de pequeno porte.** Como exemplo, verifica-se que o rol de hipóteses legais dispostos no art. 7, que trata de dados pessoais, é distinto das hipóteses descritas no art. 11, que trata de dados sensíveis, ambos da mesma norma. Ademais, a citada lei estabelece algumas regras para tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14.

3.4. Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais

20. A LGPD trata da questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

21. 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.

22. 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.

23. O art. 48 trata de uma importante obrigação relacionada à segurança de dados pessoais, e à comunicação à ANPD de incidentes de segurança que possam acarretar risco ou dano relevante[3] 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 institucional (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

24. 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 às demais normas regulamentares.

3.5. Segurança de informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte

25. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[4] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

26. Como se sabe, a implementação e manutenção de medidas que atendam a essas obrigações, considerando sua complexidade e especificidade em casos concretos, podem necessitar, em alguns casos, de elevado investimento e recursos. Este fato pode causar impacto financeiro aos agentes de tratamento de pequeno porte.

27. Nesse sentido, são apresentadas, a seguir, sugestões de medidas de segurança da informação relacionadas a dados pessoais capazes de promover em agentes de tratamento de pequeno porte um ambiente institucional mais seguro quanto ao tratamento de dados pessoais. As medidas sugeridas devem ser entendidas como boas práticas a serem adotadas.

4. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

4.1 Medidas organizacionais

4.1.1 Política de segurança da informação

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

29. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Entretanto, pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis. A PSI, formalmente instituída, pode ser mais aplicável às organizações de médio e grande porte que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Cabe a cada instituição avaliar

[3] Cabe explicar que não é todo incidente que deveria ser comunicado à ANPD. No caso, devem ser comunicados apenas aqueles que envolvam dados pessoais e, mesmo assim, somente aqueles que se refiram a um evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

[4] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado acima, não será abordado neste Guia.

os impactos e recursos necessários e decidir sobre a sua formalização, sendo que esta Autoridade estimula a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

30. 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.

31. Ressalta-se que, no âmbito deste guia, não é exigido que agentes de tratamento de pequeno porte, em especial os que tratem dados de forma incidental, estabeleçam uma política de segurança da informação que contemple tratamento de dados pessoais.

32. No entanto, é recomendado que agentes de pequeno porte que tratem dados como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao tratamento de dados pessoais com diretrizes e regras mínimas relacionadas ao planejamento, implementação e controle.

33. Nesse sentido, a ANPD sugere que, quando possível, seja estabelecida uma política de segurança da informação simplificada 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 e uso de antivírus. Essas ações estariam integradas como parte da política de segurança da informação da empresa, com destaque a esta categoria especial de dados – os dados pessoais.

34. Sugere-se, ainda, que essa política seja **revisada periodicamente (a cada 1 ou 2 anos, por exemplo)**.

35. Além disso, é indicado que seja realizado o gerenciamento de contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

4.1.2 Segurança em recursos humanos

36. Os recursos humanos de uma empresa são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e 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.

37. Assim, quanto aos recursos humanos, sugere-se que os agentes de tratamento de pequeno porte **conscientizem os seus funcionários por meio de treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais**. Essa conscientização implica em **informar os funcionários diretamente envolvidos na atividade de tratamento de dados sobre as obrigações legais existentes na LGPD e normas editadas pela ANPD**.

38. Além disso, **sugere-se também que os funcionários sejam informados sobre os controles de segurança dos sistemas de TI que são relacionados ao seu trabalho diário**. Por exemplo, se um funcionário é responsável por incluir os dados de um grupo de clientes em um sistema no computador da empresa, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte, que serão sugeridas no tópico seguinte.

4.2 Medidas técnicas

4.2.1 Controle de acesso

39. O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele é composto pelos 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 e a auditoria registra o que foi feito pelo usuário.

40. 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 que acessam o sistema de TI**. Esse sistema de controle de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários que acessam o sistema de TI.

41. 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 o sistema estabelecerá o número de caracteres necessários para se criar uma senha, se é necessário o uso de um caractere especial ou outros fatores que o agente de tratamento considere importante.

42. Outro importante ponto sugerido 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.

43. Nesse sentido, o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[5] publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[6] 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.

44. Por fim, sugere-se que os agentes considerem, preferencialmente, **utilizar a autenticação de dois fatores** 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.

45. A título de exemplo de autenticação de dois 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.

4.2.2 Segurança dos dados pessoais armazenados

46. Pode-se dizer que as etapas descritas até o momento visam contribuir justamente com a segurança dos dados pessoais armazenados, a fim de diminuir o risco de vazamento e aumentar

[5] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

[6] 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.

a segurança que os agentes de pequeno porte devem ter ao longo do tratamento de dados pessoais.

47. 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 específica. Para se evitar riscos de vazamento e outros comprometimentos, sugere-se que os agentes de tratamento de pequeno porte **coletem e processem apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados**.

48. 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 lidam com dados dessa natureza **implementem soluções de pseudonimização[7], como por exemplo a criptografia** para cifrar os dados sob sua responsabilidade.

49. Em relação as 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.

50. Além disso, **é importante que os aplicativos antivírus sejam atualizados** quando necessário e que sejam instaladas regularmente as atualizações para última versão e as correções de segurança (*patches*[8]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

51. 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 esta operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como por exemplo, inventariá-los, cifrar os dados e armazená-los em locais seguros.

52. 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*).

53. Em relação aos dispositivos móveis, como celulares e laptops, sugere-se que estejam sujeitos, se possível, aos **mesmos procedimentos de controle de acesso que os outros equipamentos de TI**, **como o uso da autenticação de dois fatores para acesso aos dispositivos e sistemas de informação** além de serem guardados em locais seguros quando não estiverem em uso. Caso não seja possível implementar essas medidas de segurança recomenda-se que esses dispositivos não sejam utilizados para fins institucionais.

[7] 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>.

[8] Programa de computador criado para atualizar ou corrigir um software de forma a corrigir vulnerabilidades ou falhas.

54. Neste sentido, 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, como 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 aplicativos utilizados. 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 vazamento de dados.

55. Por fim, sobre a eliminação de dados pessoais, sugere-se que **em todas as mídias que contenham dados pessoais seja executado o método de sobrescrever todos os dados 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.

56. 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 um registro da destruição que for realizada**.

4.2.3 Manutenção de programa de gerenciamento de vulnerabilidades

57. 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.

58. 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**.

59. 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.

60. Por fim, para manter sistemas e aplicativos seguros, é importante que os agentes se certifiquem que todos os componentes do sistema estejam protegidos de vulnerabilidades, instalando *patches* de segurança disponibilizados pelos fornecedores.

4.2.4 Segurança das comunicações

61. 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.

62. Sobre o assunto, destaca-se a relevância de se **utilizar somente 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, prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

63. Além disso, sugere-se que **seja instalado e mantido um sistema de firewall**[9], que consiste, por exemplo, na restrição de conexões entre redes não confiáveis e quaisquer componentes do sistema. Adicionalmente convém considerar o uso de ferramenta anti-spam, adotar filtros de e-mail, integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

64. É importante, ainda, na implementação desses 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.

4.3. Medidas relacionadas ao serviço em nuvem

65. 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”).

66. 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.

67. 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.

68. 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 com o provedor do serviço em nuvem, contemplando a segurança dos dados armazenados.**

69. 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**.

70. 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 de dois fatores**, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

5. CONSIDERAÇÕES FINAIS

71. 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 tratamento de pequeno

[9] 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.

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

72. Neste guia foram apresentadas medidas de segurança de natureza organizacional, que envolvem a política de segurança da informação relacionada a dados pessoais e segurança em recursos humanos; e medidas técnicas, que tratam 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 organizacional), tendo em vista a frequência que esses serviços são utilizados por empresas de pequeno porte.

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

74. 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.

6. REFERÊNCIAS

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.

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.

ABNT. Norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

ABNT. Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ABNT. Norma ABNT NBR ISO/IEC 27018: 2021, Tecnologia da informação — Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.

ABNT. Norma ABNT NBR ISO/IEC27005:2019, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT. Norma ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem.

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 25/05/2021.

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

VERSÃO PARA ASSESSORIA JURÍDICA

JULHO DE 2021

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

Equipe de elaboração

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

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

Sumário

1. APRESENTAÇÃO

1. A publicação da 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 pilares desse marco regulatório é a proteção dos dados pessoais, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

2. Um importante ponto da LGPD é a previsão de tratamento diferenciado para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, tendo determinado a edição de norma específica para esse grupo, nos termos do inciso XVIII do art. 55-J da LGPD. No momento, a norma se encontra em consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD).

3. De modo a melhor identificar estas categorias de empresas, a ANPD atribuiu o nome de agentes de tratamento de pequeno porte às micro e pequenas empresas e *startups*. Existe um enorme desafio em flexibilizar algumas obrigações desses agentes contidas na LGPD sem aumentar os riscos e danos aos titulares dos dados, bem como conscientizar as empresas sobre a relevância da proteção de dados pessoais.

4. Diante desse cenário, a ANPD elaborou o presente guia orientativo, que busca apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais. Destaca-se que este guia poderá ser atualizado de forma periódica à medida em que a ANPD entender necessário.

2. ESCOPO E OBJETIVO

5. Este 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 aprimorar o processo de segurança da informação relacionada a dados pessoais, nos termos dos artigos 46, 47, 48[1] e 49 da LGPD.

6. No âmbito deste guia orientativo, adotam-se os conceitos de microempresa, pequena empresa e *startup* trazidos pela Lei Complementar nº 123/2006 e pela Lei Complementar nº 182, de 1º de junho de 2021.

7. Diante das duas leis mencionadas, pode-se estabelecer os seguintes conceitos:

> Microempresas e Empresas de Pequeno Porte
>
> 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.
>
> Startup

[1] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, como explicado mais a frente, será tratado em um Guia específico.

Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.

Agente de Tratamento de Pequeno Porte

Microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.

8. Tendo em vista estas definições, o objetivo desse Guia é disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte.

3. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

3.1. Segurança da informação

9. A *International Organization for Standardization* (ISO) é uma organização internacional que desenvolve e publica normas técnicas que são utilizadas por inúmeros países, incluindo o Brasil. Uma das normas da organização é a Norma ABNT NBR ISO/IEC 27001,[2] que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.

10. Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio globais da organização.

11. De acordo com a norma, a segurança da informação pode ser definida como o conjunto de ações que visam a preservação da confidencialidade, integridade e disponibilidade da informação.

12. Este conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais, ou seja, estão relacionadas às camadas de tecnologia, processos e pessoas e não somente ao ambiente de tecnologia da informação.

13. 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.

14. Ainda que não seja obrigatório é indicado que, se possível, 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] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

3.2. Tratamento de dados pessoais

15. A LGPD define tratamento de dados pessoais como toda operação realizada com dados pessoais, como as que se referem a 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.

16. Vale ressaltar que dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, conforme disposto no art. 5º, I da LGPD.

17. A título exemplificativo, os conjuntos de dados que incluem dados pessoais podem conter identificadores diretos e indiretos, que permitem que um indivíduo seja identificado ou se torne identificável. Um identificador direto é uma informação específica que se refere a um indivíduo, como por exemplo nome e apelido, endereço de uma residência, endereço de correio eletrônico, número de um cartão de identificação, cookies em sítios eletrônicos. Por outro lado, um identificador indireto (também chamado de quase-identificador) é qualquer informação que pode ser usada, individualmente ou em combinação com outros quase-identificadores, por alguém que tem conhecimento sobre aquele indivíduo com o propósito de identificá-lo no conjunto de dados, como por exemplo, uma posição geográfica em um determinado momento ou uma opinião sobre um determinado assunto, dentre outros.

18. Cabe destacar que a LGPD define como dados pessoais sensíveis 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, nos termos do art. 5º, inciso II.

19. Os dados sensíveis, por terem uma proteção especial conferida pela LGPD, possuem regras mais rigorosas para seu tratamento, **a fim de evitar risco ou danos relevantes aos titulares de dados, mesmo manipulados por agentes de tratamento de pequeno porte.** Como exemplo, verifica-se que o rol de hipóteses legais dispostos no art. 7, que trata de dados pessoais, é distinto das hipóteses descritas no art. 11, que trata de dados sensíveis, ambos da mesma norma. Ademais, a citada lei estabelece algumas regras para tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14.

3.4. Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais

20. A LGPD trata da questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

21. 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.

22. 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.

23. O art. 48 trata de uma importante obrigação relacionada à segurança de dados pessoais, e à comunicação à ANPD de incidentes de segurança que possam acarretar risco ou dano relevante[3] 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 institucional (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

24. 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 às demais normas regulamentares.

3.5. Segurança de informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte

25. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[4] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

26. Como se sabe, a implementação e manutenção de medidas que atendam a essas obrigações, considerando sua complexidade e especificidade em casos concretos, podem necessitar, em alguns casos, de elevado investimento e recursos. Este fato pode causar impacto financeiro aos agentes de tratamento de pequeno porte.

27. Nesse sentido, são apresentadas, a seguir, sugestões de medidas de segurança da informação relacionadas a dados pessoais capazes de promover em agentes de tratamento de pequeno porte um ambiente institucional mais seguro quanto ao tratamento de dados pessoais. As medidas sugeridas devem ser entendidas como boas práticas a serem adotadas.

4. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

4.1 Medidas organizacionais

4.1.1 Política de segurança da informação

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

29. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Entretanto, pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis. A PSI, formalmente instituída, pode ser mais aplicável às organizações de médio e grande porte que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Cabe a cada instituição avaliar

[3] Cabe explicar que não é todo incidente que deveria ser comunicado à ANPD. No caso, devem ser comunicados apenas aqueles que envolvam dados pessoais e, mesmo assim, somente aqueles que se refiram a um evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

[4] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado acima, não será abordado neste Guia.

os impactos e recursos necessários e decidir sobre a sua formalização, sendo que esta Autoridade estimula a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

30. 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.

31. Ressalta-se que, no âmbito deste guia, não é exigido que agentes de tratamento de pequeno porte, em especial os que tratem dados de forma incidental, estabeleçam uma política de segurança da informação que contemple tratamento de dados pessoais.

32. No entanto, é recomendado que agentes de pequeno porte que tratem dados como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao tratamento de dados pessoais com diretrizes e regras mínimas relacionadas ao planejamento, implementação e controle.

33. Nesse sentido, a ANPD sugere que, quando possível, seja estabelecida uma política de segurança da informação simplificada 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 e uso de antivírus. Essas ações estariam integradas como parte da política de segurança da informação da empresa, com destaque a esta categoria especial de dados – os dados pessoais.

34. Sugere-se, ainda, que essa política seja **revisada periodicamente (a cada 1 ou 2 anos, por exemplo)**.

35. Além disso, é indicado que seja realizado o gerenciamento de contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

4.1.2 Segurança em recursos humanos

36. Os recursos humanos de uma empresa são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e 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.

37. Assim, quanto aos recursos humanos, sugere-se que os agentes de tratamento de pequeno porte **conscientizem os seus funcionários por meio de treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais**. Essa conscientização implica em **informar os funcionários diretamente envolvidos na atividade de tratamento de dados sobre as obrigações legais existentes na LGPD e normas editadas pela ANPD**.

38. Além disso, **sugere-se também que os funcionários sejam informados sobre os controles de segurança dos sistemas de TI que são relacionados ao seu trabalho diário**. Por exemplo, se um funcionário é responsável por incluir os dados de um grupo de clientes em um sistema no computador da empresa, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte, que serão sugeridas no tópico seguinte.

4.2 Medidas técnicas

4.2.1 Controle de acesso

39. O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele é composto pelos 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 e a auditoria registra o que foi feito pelo usuário.

40. 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 que acessam o sistema de TI**. Esse sistema de controle de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários que acessam o sistema de TI.

41. 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 o sistema estabelecerá o número de caracteres necessários para se criar uma senha, se é necessário o uso de um caractere especial ou outros fatores que o agente de tratamento considere importante.

42. Outro importante ponto sugerido 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.

43. Nesse sentido, o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[5] publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[6] 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.

44. Por fim, sugere-se que os agentes considerem, preferencialmente, **utilizar a autenticação de dois fatores** 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.

45. A título de exemplo de autenticação de dois 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.

4.2.2 Segurança dos dados pessoais armazenados

46. Pode-se dizer que as etapas descritas até o momento visam contribuir justamente com a segurança dos dados pessoais armazenados, a fim de diminuir o risco de vazamento e aumentar

[5] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

[6] 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.

a segurança que os agentes de pequeno porte devem ter ao longo do tratamento de dados pessoais.

47. 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 específica. Para se evitar riscos de vazamento e outros comprometimentos, sugere-se que os agentes de tratamento de pequeno porte **coletem e processem apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados**.

48. 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 lidam com dados dessa natureza **implementem soluções de pseudonimização[7], como por exemplo a criptografia** para cifrar os dados sob sua responsabilidade.

49. Em relação as 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.

50. Além disso, **é importante que os aplicativos antivírus sejam atualizados** quando necessário e que sejam instaladas regularmente as atualizações para última versão e as correções de segurança (*patches*[8]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

51. 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 esta operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como por exemplo, inventariá-los, cifrar os dados e armazená-los em locais seguros.

52. 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*).

53. Em relação aos dispositivos móveis, como celulares e laptops, sugere-se que estejam sujeitos, se possível, aos **mesmos procedimentos de controle de acesso que os outros equipamentos de TI**, **como o uso da autenticação de dois fatores para acesso aos dispositivos e sistemas de informação** além de serem guardados em locais seguros quando não estiverem em uso. Caso não seja possível implementar essas medidas de segurança recomenda-se que esses dispositivos não sejam utilizados para fins institucionais.

[7] 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>.

[8] Programa de computador criado para atualizar ou corrigir um software de forma a corrigir vulnerabilidades ou falhas.

54. Neste sentido, 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, como 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 aplicativos utilizados. 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 vazamento de dados.

55. Por fim, sobre a eliminação de dados pessoais, sugere-se que **em todas as mídias que contenham dados pessoais seja executado o método de sobrescrever todos os dados 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.

56. 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 um registro da destruição que for realizada**.

4.2.3 Manutenção de programa de gerenciamento de vulnerabilidades

57. 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.

58. 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**.

59. 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.

60. Por fim, para manter sistemas e aplicativos seguros, é importante que os agentes se certifiquem que todos os componentes do sistema estejam protegidos de vulnerabilidades, instalando *patches* de segurança disponibilizados pelos fornecedores.

4.2.4 Segurança das comunicações

61. 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.

62. Sobre o assunto, destaca-se a relevância de se **utilizar somente 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, prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

63. Além disso, sugere-se que **seja instalado e mantido um sistema de firewall**[9], que consiste, por exemplo, na restrição de conexões entre redes não confiáveis e quaisquer componentes do sistema. Adicionalmente convém considerar o uso de ferramenta anti-spam, adotar filtros de e-mail, integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

64. É importante, ainda, na implementação desses 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.

4.3. Medidas relacionadas ao serviço em nuvem

65. 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").

66. 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.

67. 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.

68. 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 com o provedor do serviço em nuvem, contemplando a segurança dos dados armazenados.**

69. 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**.

70. 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 de dois fatores**, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

5. CONSIDERAÇÕES FINAIS

71. 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 tratamento de pequeno

[9] 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.

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

72. Neste guia foram apresentadas medidas de segurança de natureza organizacional, que envolvem a política de segurança da informação relacionada a dados pessoais e segurança em recursos humanos; e medidas técnicas, que tratam 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 organizacional), tendo em vista a frequência que esses serviços são utilizados por empresas de pequeno porte.

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

74. 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.

6. REFERÊNCIAS

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.

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.

ABNT. Norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

ABNT. Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ABNT. Norma ABNT NBR ISO/IEC 27018: 2021, Tecnologia da informação — Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.

ABNT. Norma ABNT NBR ISO/IEC27005:2019, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT. Norma ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem.

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 25/05/2021.

PARECER n. 00014/2021/GAB/ASJUR-ANPD/CGU/AGU

NUP: 01030.000029/2021-30
INTERESSADOS: Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Normatização.
ASSUNTOS: Minuta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

EMENTA: PROCESSO DE EDIÇÃO DE NORMA ESPECÍFICA NO ÂMBITO DA ANPD. REGULAMENTAÇÃO DO ART. 55-J, INCISO XVIII DA LEI GERAL DE PROTEÇÃO DE DADOS - APLICABILIDADE DA LGPD.

1. Exame de minuta de Guia Orientativo *sobre segurança da informação para agentes de tratamento de pequeno porte, que tem por finalidade apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais*

2. Higidez do procedimento normativo.

3. Análise da regularidade jurídica e da coerência das regras propostas com o ordenamento jurídico.

3. Recomendações de avaliação de conteúdo normativo e de aspectos redacionais, de acatamento discricionário pela Administração.

4. Exame que não abrange a matéria reservada ao juízo de conveniência e de oportunidade da Administração, nos termos da recomendação contida no Enunciado de Boas Práticas Consultivas nº 7 da Consultoria-Geral da União.

1. RELATÓRIO

1. Trata-se de processo instaurado no Sistema Eletrônico de Informações - SEI/PR/ANPD (processo nº 00261.000821/2021-16), pela Coordenação-Geral de Normatização - CGN/ANPD, com a finalidade de editar *proposta de guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte, que tem por finalidade apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais* (seq. Sapiens 01, p. 01).

2. A Coordenação-Geral de Normatização encaminhou o feito a esta Assessoria Jurídica por meio da Nota Técnica nº 19/2021/CGN/ ANPD (SEI nº 2728509 / seq. Sapiens 01, p. 01 a 04), solicitando manifestação sobre a minuta de Guia Orientativo apresentado (SEI nº 2734320 / seq. Sapiens p. 05 a 18), *que busca estabelecer diretrizes não-vinculantes aos agentes de tratamento de pequeno porte sobre segurança da informação.*

3. A área demandante objetiva formalizar a divulgação do indigitado guia orientativo, com fulcro no artigo 55-J da Lei nº 13.709, de 14.08.2018.

4. Com efeito, compete a este Órgão de Execução da Advocacia-Geral da União se pronunciar nos termos do art. 11, incisos I, III, IV e V da Lei Complementar nº 73, de 21 de junho de 1993, e do art. 23, incisos I, II, III, IV e V do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020.

5. Instruem os autos:

* Nota Técnica nº 19/2021/CGN/ANPD (SEI nº 2728509);
* Minuta de Guia Orientativo sobre Segurança da Informação (SEI nºs 2734311 e 2734320).

6. É o relato.

2. ARCABOUÇO NORMATIVO DE REGÊNCIA

7. Lei nº 13.709, de 14.08.2018 - Lei Geral de Proteção de Dados (LGPD);
8. Lei Complementar nº 182, de 01.06.2021 - Marco legal das startups e empreendedorismo inovador;
9. Lei Complementar nº 123, de 14.12.2006 - Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte;
10. Lei nº 12.527, de 18.11.2011 - Lei de Acesso à Informação;
11. Lei nº 12.965, de 23.04.2014 - Marco Civil da Internet;
12. Decreto nº 10.474, de 26.08.2020 - Aprova estrutura da ANPD;
13. Portaria ANPD nº 1, de 08.03.2021 - Estabelece Regimento da ANPD.

3. CONSIDERAÇÕES PRELIMINARES

14. Inicialmente, convém salientar que o exame da demanda em tela se restringe aos seus aspectos jurídicos, excluídos, portanto, aqueles de natureza técnica, porquanto, parte-se da premissa de que a autoridade administrativa competente se municiou dos conhecimentos específicos imprescindíveis para sua adequação às necessidades da Administração, observando os requisitos legalmente impostos. Sobre o tema, destaca-se o que preceitua o Enunciado n° 07 do Manual de Boas Práticas Consultivas da CGU/AGU, no sentido de que o Órgão Consultivo deve evitar *"(...) posicionamentos conclusivos sobre temas não jurídicos, tais como os técnicos, administrativos ou de conveniência ou oportunidade. (...) ".*

15. Nesse ponto, ressalta-se que determinadas observações são feitas sem caráter vinculativo, mas em prol da segurança da própria autoridade administrativa assessorada a quem incumbe, dentro da margem de discricionariedade que lhe é conferida pela lei, avaliar e acatar, ou não, tais ponderações. Não obstante, as questões relacionadas à legalidade serão apontadas para fins de sua correção. O prosseguimento do feito sem a observância destes apontamentos será de responsabilidade exclusiva da autoridade administrativa competente.

4. EXAME JURÍDICO

4.1 Análise da conformidade e legalidade da minuta.

16. *Ab initio,* cumpre destacar que a **forma** escolhida para exteriorização do conteúdo constante da minuta em análise (SEI nº 2734311) revela a intenção da área consulente em não conferir ao ora previsto a densidade normativa suficiente para revesti-lo do tratamento jurídico vinculante, outrossim, por ser um guia, apresenta-se como manifestação técnica não cogente, mas veiculadora de boas práticas, destinadas *a apoiar e orientar* os agentes de tratamento de pequeno porte *no que se refere à segurança da informação relacionada à proteção de dados pessoais*, nos termos do quanto consignado nos tópicos "APRESENTAÇÃO" e "ESCOPO E OBJETIVO" da Nota Técnica nº 19/2021/CGN/ANPD. Outrossim, a utilização da forma de Guia atende ao exigido na LGPD e Regimento Interno da ANPD.

17. Igualmente, quanto ao quesito da **competência** para produção do ato normativo, verifica-se que o conteúdo do guia é expressão do delineado nos incisos VI e XVIII do art. 55-J da Lei nº 13.709 (LGPD). Semelhantemente, no âmbito interno, observa-se que recaiu à Coordenação-Geral de Normatização (CGN/ANPD) a atribuição da respectiva elaboração, *ex vi* do art. 16 do Regimento Interno.

18. Por seu turno, em relação ao **objeto** proposto, a CGN/ANPD *intenciona disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte*, desse modo, os efeitos materiais a serem perseguidos pelo ato em exame são lícitos, possíveis e hígidos, assim como o guia é instrumento normativo adequado para o mister.

19. Quanto à **motivação** do ato proposto, a Coordenação-Geral de Normatização providenciou a sua fundamentação técnica e jurídica, conforme exposto na Nota Técnica nº 19/2021/CGN/ANPD. Assim, os pressupostos de fato e os elementos de direito que precedem a realização do ato administrativo encontram-se fundamentados na Lei nº 13.709, de 2018, no Decreto 10.474, de 2020, e na Portaria nº 1, de 8 de março de 2021, que estabelece o Regimento Interno da ANPD.

20. No que pertine à **finalidade**, o interesse público a ser perseguido encontra-se exteriorizado nas normas que impuseram à Autoridade Nacional de Proteção de Dados os deveres de zelar e implementar o cumprimento da Lei nº 13.709, de 2018, em todo o território nacional, assegurando-lhe, para tanto, competência normativa.

4.2 Análise do conteúdo da minuta.

21. De início, considerando a tramitação simultânea, na ANPD, de ato normativo destinado a regulamentar a aplicação da LGPD para microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo, isto é, com idênticos destinatários aos em questão, **afigura-se prudente destacar a importância e necessidade do devido diálogo entre não somente os dois atos destacados, mas sim sobre toda a produção normativa editada (vinculante ou não) pela autoridade regulatória**, porquanto, como cediço, a unidade e a harmonia *interna corporis* são pressupostos imprescindíveis na construção normativa de qualquer sistema pautado na segurança jurídica.

22. A minuta do Guia Orientativo foi colacionada ao seq. Sapiens 01 (p. 05 a 18), e restou dividida em 6 partes, embora as últimas duas não reclamem exame:

1. APRESENTAÇÃO
2. ESCOPO E OBJETIVO
3. SEGURANÇA DA INFORMAÇÃO
4. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO
5. CONSIDERAÇÕES FINAIS
6. REFERÊNCIAS

23. "APRESENTAÇÃO": é iniciada com a previsão legislativa oriunda da LGPD que determina a edição de normas específicas que contemplem o tratamento diferenciado destinado às microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo, categoria denominada pela CGN/ANPD como "agentes de tratamento de pequeno porte", nos

termos do firmado no tópico seguinte "ESCOPO E OBJETIVO", responsável por endereçar o guia a esse público-alvo, visando *disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais* protagonizado por aludidos atores.

24. "SEGURANÇA DA INFORMAÇÃO": campo subdividido em quatro tópicos, quais sejam:

(3.1) Segurança da informação: desponta trazendo a relevância das normas técnicas da *International Organization for Standardization* (ISO), organização internacional, e sua contribuição na formulação de conceitos uniformizados (segurança da informação e gerenciamento de riscos) e endossados por diversos países;

(3.2) Tratamento de dados pessoais: replica conceituação apresentada pela LGPD e a exemplifica;

(3.4) Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais: **nessa passagem, sugere-se avaliar o acréscimo de alguns exemplos que ilustrem didaticamente o conteúdo dos comandos legais previstos nos arts. 46 a 49 da LGPD, ademais, deve ser corrigida a numeração para "3.3."**;

(3.5) Segurança da informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte: **demonstra que as determinações impostas pelos arts. 46, 47, 49 e 50 da LGPD foram baseadas em boas práticas internacionais, e que, a despeito de seus reconhecidos benefícios, em razão do potencial custo para implementação em certos casos, pode gerar impacto financeiro desproporcional ao mercado dos agentes de tratamento de pequeno porte, motivo pela qual são sugeridas as medidas do capítulo seguinte. A numeração também deverá ser revista para "3.4", se permanecerem tão somente as quatros subdivisões.**

Informa-se que foi feita recomendação no parágrafo 37 do Parecer nº 00013/2021/GAB/ASJUR-ANPD/CGU/AGU[1] a respeito da nomenclatura "agente de tratamento de pequeno porte" e que, em caso de acolhimento dessa recomendação, seja feita a devida avaliação no Guia em análise.

25. "MEDIDAS DE SEGURANÇA DA INFORMAÇÃO": capítulo organizado em três perspectivas de abordagem, a saber:

(4.1) Medidas organizacionais;

(4.2.) Medidas técnicas;

(4.3.) Medidas relacionadas ao serviço em nuvem.

26. As medidas organizacionais abarcam a política de segurança da informação (4.1.1.), concebida como *conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, implementação e controle de ações relacionadas à segurança da informação em uma organização* e que pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis, cabendo a cada instituição avaliar (...) e decidir sobre sua formalização, todavia, a ANPD recomenda que agentes de tratamento de pequeno porte que *tratem dados como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao tratamento de dados pessoais.* **Ainda que seja inquestionável a conformação das diretrizes negritadas ao microssistema protetivo legalmente arquitetado, registra-se a orientação para que a área técnica introduza esclarecimento (mesmo indireto como nota de rodapé) apto a auxiliar o intérprete a compreender a concepção binária "atividade principal e atividade incidental" ali sinalizada**, **visto se tratar de uma categorização que não foi apresentada pela legislação e jurisprudência ou minimamente desenvolvida pela doutrina, podendo causar incompreensões desnecessárias nos operadores**; e (4.1.2) segurança em recursos humanos, evidenciada por meio da conscientização dos funcionários a respeito da temática.

27. As medidas técnicas, por sua vez, congregam mecanismos e rotinas de proteção, que devem ser implementadas por todos os agentes de tratamento de pequeno porte, e que restaram agrupadas em: controle de acesso (4.2.1), segurança dos dados pessoais armazenados (4.2.2), manutenção de programa de gerenciamento de vulnerabilidades (4.2.3) e segurança das comunicações (4.2.4).

28. Ao final, foram apontadas as medidas e precauções relacionadas ao serviço em nuvem (4.3), retratadas, uma vez mais, de modo simples e convidativo, atendendo aos objetivos instrutivos de um guia.

29. Em comum, constata-se que as medidas constantes do capítulo 4 se revelam como ferramentas e fluxos que visam diminuir a probabilidade de que vulnerabilidades, omissões e incidentes de segurança possam afetar o ciclo de tratamento informacional patrocinado pelos agentes de pequeno porte, tornando o correspondente ecossistema de proteção de dados pessoais mais seguro.

30. Constata-se que as diversas diretrizes técnicas elencadas evidenciam a preocupação da ANPD em ilustrar, mediante linguagem acessível e pedagógica, como princípios insculpidos, sobretudo, no art. 6º da Lei Geral de Proteção de Dados, poderão ser materializados e respeitados.

31. Dessarte, assente ao evidenciado, extrai-se que o conteúdo da minuta em questão atendeu aos limites normativos impostos, sem exorbitar das balizas regulamentares e diretivas pertinentes, desnudando-se hígido e obediente ao arcabouço normativo de regência.

32. De igual modo, até o momento, o processo de produção do indigitado guia respeitou o rito procedimental correlato.

5. CONCLUSÃO

33. Em face do exposto, **observadas as recomendações consignadas nos parágrafos 21, 24 e 26**, conclui-se, nos limites da análise jurídica, excluídos os aspectos técnicos, assim como juízo de conveniência e oportunidade, que o presente Guia Orientativo não transborda as competências institucionais destinadas à ANPD, tampouco inova indevidamente no ordenamento jurídico, merecendo, por conseguinte, prosseguimento do feito.

À consideração superior.

RAPHAEL RODRIGUES VALENÇA DE OLIVEIRA
ADVOGADO DA UNIÃO
ASSESSORIA JURÍDICA - ASJUR
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

Atenção, a consulta ao processo eletrônico está disponível em http://sapiens.agu.gov.br mediante o fornecimento do Número Único de Protocolo (NUP) 01030000029202130 e da chave de acesso e9604dc3

Notas

1. ^ *"37. Sugere-se, pois, para evitar possíveis equívocos interpretativos, avaliar a utilização da expressão"de pequeno porte" para qualificar os agentes de tratamento abrangidos pelo regime diferenciado previsto na resolução, recomendando-se que tal qualificação espelhe, da forma mais próxima possível, a previsão legal (que fala em "procedimentos simplificados e diferenciados"), considerando que o poder normativo exercido pela ANPD decorre de lei e deve ser exercido a partir da referida previsão legal." (Parecer n. 00013/2021/GAB/ASJUR-ANPD/CGU/AGU).*

Documento assinado eletronicamente por RAPHAEL RODRIGUES VALENCA DE OLIVEIRA, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 695239960 no endereço eletrônico http://sapiens.agu.gov.br. Informações adicionais: Signatário (a): RAPHAEL RODRIGUES VALENCA DE OLIVEIRA. Data e Hora: 09-08-2021 12:23. Número de Série: 434213278927595946452065068 93. Emissor: Autoridade Certificadora SERPRORFBv5.

ADVOCACIA-GERAL DA UNIÃO
CONSULTORIA-GERAL DA UNIÃO
ASSESSORIA JURÍDICA JUNTO A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
GABINETE
ESPLANADA DOS MINISTÉRIOS, BLOCO C, 2º ANDAR.

DESPACHO n. 00002/2021/GAB/ASJUR-ANPD/CGU/AGU

NUP: 01030.000029/2021-30
INTERESSADOS: PRESIDÊNCIA DA REPÚBLICA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
ASSUNTOS: DIREITO REGULATÓRIO

1. Aprovo o PARECER n. 00014/2021/GAB/ASJUR-ANPD/CGU/AGU.

Brasília, 09 de agosto de 2021.

GABRIEL NETTO BIANCHI
CONSULTOR JURÍDICO
ASSESSORIA JURÍDICA - ASJUR
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

Atenção, a consulta ao processo eletrônico está disponível em http://sapiens.agu.gov.br mediante o fornecimento do Número Único de Protocolo (NUP) 01030000029202130 e da chave de acesso e9604dc3

Documento assinado eletronicamente por GABRIEL NETTO BIANCHI, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 696815145 no endereço eletrônico http://sapiens.agu.gov.br. Informações adicionais: Signatário (a): GABRIEL NETTO B I A N C H I . Data e Hora: 09-08-2021 15:38. Número de Série: 842020452684248905864199958840008302 34. Emissor: AC OAB G2.

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Nota Técnica nº 27/2021/CGN/ANPD

Assunto: **Proposta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte**

Referência: Processo SEI nº 00261.000821/2021-16

1. RELATÓRIO

1. Trata-se de proposta de Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, que tem por finalidade apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais.

2. Nos termos do que dispõe o art. 55-J, XVIII da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), a Autoridade Nacional de Proteção de Dados (ANPD) tem competência para editar normas específicas, com procedimentos simplificados e diferenciados, bem como os critérios de elegibilidade, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à LGPD.

3. Diante da competência acima mencionada, em 05 de maio de 2021 foi realizada reunião com Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo NIC.br para apresentar a primeira versão da minuta e coletar contribuições. A partir daí a ANPD e CERT.br trabalharam em conjunto no aprimoramento da minuta do Guia Orientativo.

4. Para fins de elaboração do Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, criou-se uma equipe composta pelos seguintes servidores: Fabrício Lopes (Coordenador de Normatização), Isabela Maiolino (Coordenadora-Geral de Normatização), Jeferson Dias Barbosa (Gerente de Projeto do Conselho Diretor), Marcelo Santiago Guedes (Coordenador-Geral de Tecnologia e Pesquisa), Rodrigo Santana dos Santos (Coordenador de Normatização) e Thiago Moraes (Coordenador de Tecnologia e Pesquisa). Posteriormente, a servidora Andressa Girotto Vargas passou a

integrar a equipe de projeto. Houve ainda a contribuição dos seguintes representantes do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), na condição de colaboradores externos: Cristine Hoepers (CERT.br/NIC.br) e Klaus Steding-Jessen (CERT.br/NIC.br).

5. A Assessoria Jurídica da ANPD se manifestou sobre a minuta e realizou recomendações de ajustes, nos termos do Parecer nº 00014/2021/GAB/ASJUR-ANPD/CGU/AGU (2789975).

6. É o relatório.

2. ANÁLISE

7. O Parecer exarado pela Assessoria Jurídica (2789975) sugeriu as seguintes recomendações:

> I - realizar devido diálogo entre toda a produção normativa editada (vinculante ou não) pela Autoridade, não se restringindo apenas ao ato normativo destinado a regulamentar a aplicação da LGPD para microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo (item 21);
>
> II - avaliar a inserção de exemplos no item 3.4 do Guia, que ilustrem o conteúdo dos comandos legais previstos nos arts. 46 a 49 da LGPD (item 24);
>
> III - retificar numeração do item 3.4 para “3.3” (item 24);
>
> IV - retificar numeração do item 3.5 para “3.4” (item 24);
>
> V - reavaliar a utilização da expressão "de pequeno porte" para qualificar os agentes de tratamento abrangidos pelo regime diferenciado previsto na resolução, recomendando-se que tal qualificação espelhe, da forma mais próxima possível, a previsão legal (que fala em "procedimentos simplificados e diferenciados" (item 24);
>
> VI - esclarecer, ainda que de forma indireta, por meio de nota de rodapé, os conceitos de “atividade principal” e “atividade incidental” no item 4.1.1 do Guia, tendo em vista se tratar de uma categorização que não apresentada pela legislação e jurisprudência ou minimamente desenvolvida pela doutrina, podendo causar incompreensões desnecessárias nos operadores. (item 26).

8. As recomendações relativas aos aspectos formais referentes aos itens III e IV listados acima foram acatadas na nova versão do Guia, nos termos da minuta SEI nº 2836728.

9. No tocante as demais recomendações, as justificativas serão apresentadas a seguir.

2.1 - Realizar devido diálogo entre toda a produção normativa editada (vinculante ou não) pela Autoridade.

10. O Parecer sinalizou para a tramitação simultânea, na ANPD, de ato normativo destinado a regulamentar a aplicação da LGPD para microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo, tendo destacado a importância e a necessidade do devido diálogo não somente com aquele ato normativo, mas para com toda a produção normativa editada (vinculante ou não) pela autoridade regulatória.

11. Diante disso, a fim de acatar a recomendação da Assessoria Jurídica, considera-se pertinente referenciar o "Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado" no parágrafo 5 do Guia Orientativo objeto da presente nota, no qual é feito o endereçamento do normativo, de modo a auxiliar o leitor a identificar seu papel no tratamento e consequentemente, reforçar a divulgação daquele Guia para aqueles que, porventura, ainda não possuíam conhecimento de sua existência.

12. Relativamente às demais as produções normativas já publicadas (a maioria de caráter não vinculante), considerando que são majoritariamente direcionadas aos titulares de dados pessoais, entende-se que não necessitam ser referenciadas neste Guia Orientativo, tendo em vista que os principais destinatários deste são os agentes de tratamento de pequeno porte.

2.2 - Avaliar a inserção de exemplos no item 3.4 do Guia.

13. O Parecer sugeriu para que fosse avaliado o acréscimo de alguns exemplos no item 3.4 do Guia, que ilustrassem didaticamente o conteúdo dos comandos legais previstos nos arts. 46 a 49 da LGPD.

14. Não obstante o caráter orientativo do presente Guia, entende-se que as sugestões de medidas de segurança da informação elencadas no item 4, as quais restaram apresentadas sob a forma de medidas organizacionais, técnicas e relacionadas ao serviço de nuvem, foram

capazes de exemplificar os comandos legais supramencionados.

15. Ademais, considerando que o objetivo do Guia é disseminar as medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte, acredita-se que as orientações ali constantes alcançaram o resultado pretendido, revelando, pois, prescindível o acréscimo de exemplos.

2.3 - Reavaliar a utilização da expressão "de pequeno porte".

16. A Assessoria Jurídica sinalizou para recomendação realizada no âmbito do Parecer nº 00013/2021/GAB/ASJUR-ANPD/CGU/AGU (2779400), constante no Processo SEI nº 00261.000054/2021-37, a fim de que fosse avaliado o uso da expressão “de pequeno porte” para qualificar os agentes de tratamento abrangidos pelo regime diferenciado previsto naquela minuta de Resolução. Ademais, foi recomendado que tal qualificação espelhasse de forma mais próxima possível a previsão legal (que fala em "procedimentos simplificados e diferenciados"), uma vez que o poder normativo exercido pela ANPD decorre de lei e deve ser exercido a partir desta.

17. Cumpre mencionar que esta Coordenação-Geral de Normatização, em Nota Técnica nº 25/2021/CGN/ANPD (2810848), manifestou-se pela manutenção da expressão “agentes de tratamento de pequeno porte”, considerando que esta não se confundiria com o conceito de “empresa de pequeno porte”, apresentado pela Lei Complementar nº 123/2006, tendo em vista a abrangência conferida à expressão, ainda que lhe tome parte do termo emprestada. Outrossim, em que pese o ato normativo não se restrinja às empresas de pequeno porte, entendeu-se que sendo essa a categoria majoritária a qual a norma se destina, pareceu oportuno prestigiá-la nesta identificação.

18. Informa-se, ainda, que a referida Nota Técnica nº 25/2021/CGN/ANPD (2810848) foi encaminhada para apreciação do Conselho Diretor.

19. A respeito da apreciação por parte do Conselho Diretor, cabe destacar que no voto do Relator do processo SEI nº 00261.000054/2021-37, Diretor Arthur Sabbat, não houve manifestação contrária à utilização da expressão “agentes de tratamento de pequeno porte”, na minuta de resolução já submetida à consulta pública. Assim, entende-se que a expressão deve ser mantida, para guardar relação direta aos termos usados na minuta de resolução que trata sobre o tema, sem prejuízo de eventual atualização do guia em caso de alterações na norma pós realização de consulta pública e audiência pública.

2.4 - Esclarecer os conceitos de “atividade principal” e “atividade incidental” no item 4.1.1.

20. O Parecer sugeriu para que fosse esclarecida a concepção binária de "atividade principal" e "atividade incidental", visto se tratar de uma categorização que não foi apresentada pela legislação e jurisprudência ou, ainda, minimamente desenvolvida pela doutrina, podendo causar incompreensões desnecessárias.

21. A esse respeito, é necessário mencionar que esta Coordenação-Geral de Normatização adotou um entendimento diverso ao anteriormente proposto na minuta do presente Guia Orientativo, quando da elaboração do Relatório de Análise de Impacto Regulatório (AIR) para aplicação da LGPD a microempresas e empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais (2811023).

22. Apenas para fins de esclarecimento, o tratamento como atividade principal consistiria naquele realizado para obtenção de 50% (cinquenta por cento) ou mais da receita bruta anual; e o de forma incidental consistiria naquele realizado para fins administrativos ou para contato com usuários de bens e serviços ofertados. Tal classificação tem como inspiração a norma estabelecida pelo *California Consumer Privacy Act*, de 2018.

23. No que tange a utilização de tal critério para aplicação da norma, verificou-se que ainda que este possa parecer objetivo, é de difícil aferição, seja em razão da dificuldade de acesso à documentação contábil da empresa, seja em razão da dificuldade de se aferir (mesmo de posse dos documentos contábeis) o quanto, de fato, de sua receita advém da atividade de tratamento de dados pessoais.

24. Ademais, entendeu-se que a regra poderia criar incentivos econômicos para que empresas elenquem determinadas receitas para outras classificações contábeis, a fim de obter um tratamento diferenciado na legislação de proteção de dados.

25. Outrossim, concluiu-se que o potencial de risco e a probabilidade de danos graves para titulares de dados pessoais não possui relação direta com a receita bruta (ou, ainda, com o percentual de faturamento que decorre da atividade de tratamento de dados pessoais).

26. Diante do exposto, optou-se por adotar um outro critério relacionado ao risco que o tratamento de dados pessoais acarreta ao titular de dados, tendo em vista ser um modelo que resguarda de forma mais efetiva os titulares de dados pessoais, sem impedir que os agentes de tratamento de pequeno porte se beneficiem de um tratamento diferenciado, em especial

aqueles que realizam apenas o tratamento de dados de funcionários ou relacionados à sua gestão administrativa. Além disso, entendeu-se que o novo critério sugerido geraria menos insegurança para fins do trabalho de fiscalização da ANPD.

27. Nesse sentido, uma vez que o trecho sob análise foi suprimido na versão atualizada do Guia, desconsiderar-se-á essa recomendação.

2.5 Alterações feitas por esta Coordenação-Geral de Normatização

28. Além das sugestões acima feitas pela Assessoria Jurídica, esta Coordenação-Geral entendeu por bem realizar pequenas alterações no texto.

29. Foi realizada retificação no parágrafo 7 da minuta do Guia Orientativo, para fins de adequação à alteração realizada na minuta de "Resolução para a aplicação da LGPD para agentes de tratamento de pequeno porte", considerando o voto do relator (2833113), Diretor Arthur Sabbat, no processo SEI n° 00261.000054/2021-37.

30. Assim, foi atualizado o conceito dado aos agentes de tratamento de pequeno porte nos termos da minuta publicada para consulta pública, nos termos a seguir:

> Agente de Tratamento de Pequeno Porte: ~~Microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.~~
>
> Agente de Tratamento de Pequeno Porte: Microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

31. Além disso, foi feita a seguinte alteração no parágrafo 12 do Guia, para fins de conferir maior clareza ao texto:

> Este conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais. A segurança da informação, ~~ou seja,~~ está~~ão~~ relacionada~~s~~ às camadas de tecnologia, processos e pessoas, deve receber atenção de todos que lidam com dados pessoai**s** e não somente daqueles ~~a~~ no ambiente de tecnologia da informação.

32. Ainda, tendo em vista a mudança de entendimento desta Coordenação-Geral de Normatização no que tange ao critério adotado para aplicação da norma a esse grupo de agentes de tratamento, optou-se por suprimir os parágrafos 31 e 32. Conforme já mencionado na presente Nota Técnica, considerando o disposto no Relatório de Análise de Impacto Regulatório (SEI nº 2811023), passou-se a considerar o risco que o tratamento realizado apresenta aos titulares, em detrimento do tipo de tratamento realizado. A seguir, os trechos que foram excluídos da nova versão:

> 31. Ressalta-se que, no âmbito deste guia, não é exigido que agentes de tratamento de pequeno porte, em especial os que tratem dados de forma incidental, estabeleçam uma política de segurança da informação que contemple tratamento de dados pessoais.
>
> 32. No entanto, é recomendado que agentes de pequeno porte que tratem dados como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao tratamento de dados pessoais com diretrizes e regras mínimas relacionadas ao planejamento, implementação e controle.

33. Por fim, foi acrescido o trecho abaixo no parágrafo 45 da nova versão do Guia, a fim de complementar a redação:

> 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 específica. Para se evitar riscos de vazamento e outros comprometimentos, sugere-se que os agentes de tratamento de pequeno porte coletem e processem apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados. 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 necessidade previstos na referida Lei.

3. CONCLUSÃO

34. Considerando que todas as recomendações de alteração realizadas pela Assessoria Jurídica foram devidamente acatadas ou justificadas, nos termos da fundamentação acima e da nova minuta de resolução anexa já disponibilizada para consulta pública (2833149), proponho o encaminhado do processo à Secretaria Geral do Conselho Diretor da ANPD,

com a nova versão do Guia (2836728)

35. À consideração superior.

ANDRESSA GIROTTO VARGAS

Servidora da Coordenação-Geral de Normatização

RODRIGO SANTANA DOS SANTOS

Coordenador de Normatização

36. De acordo. Encaminha-se o presente processo à Secretaria Geral do Conselho Diretor da ANPD para providências.

ISABELA MAIOLINO

Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenadora-Geral de Normatização**, em 30/08/2021, às 19:33, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)**, em 30/08/2021, às 19:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Andressa Girotto Vargas**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 30/08/2021, às 19:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2834720** e o código CRC **115BAE16** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Formatado: Centralizado, Espaçamento entre linhas: Múltiplos 1,07 lin.

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

VERSÃO PARA O CONSELHO DIRETOR ~~ASSESSORIA JURÍDICA~~

~~JULHO~~ AGOSTO DE 2021

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

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

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

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Fonte: Negrito
Formatado: Fonte: 12 pt

SUMÁRIO

1. APRESENTAÇÃO

1. A publicação da 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 pilares desse marco regulatório é a proteção dos dados pessoais, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

2. Um importante ponto da LGPD é a previsão de tratamento diferenciado para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, tendo determinado a edição de norma específica para esse grupo, nos termos do inciso XVIII do art. 55-J da LGPD. No momento, a norma se encontra em consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD).

3. De modo a melhor identificar estas categorias de empresas, a ANPD atribuiu o nome de agentes de tratamento de pequeno porte às micro e pequenas empresas e *startups*. Existe um enorme desafio em flexibilizar algumas obrigações desses agentes contidas na LGPD sem aumentar os riscos e danos aos titulares dos dados, bem como conscientizar as empresas sobre a relevância da proteção de dados pessoais.

4. Diante desse cenário, a ANPD elaborou o presente guia orientativo, que busca apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais. Destaca-se que este guia poderá ser atualizado de forma periódica à medida em que a ANPD entender necessário.

~~4.~~

2. ESCOPO E OBJETIVO

5. Este guia de boas práticas é endereçado aos agentes de tratamento[1] 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 aprimorar o processo de segurança da informação relacionada a dados pessoais, nos termos dos artigos 46, 47, 48[2] e 49 da LGPD.

6. No âmbito deste guia orientativo, adotam-se os conceitos de microempresa, pequena empresa e *startups* trazidos pela Lei Complementar nº 123/2006 e pela Lei Complementar nº 182, de 1º de junho de 2021.

7. Diante das duas leis mencionadas, pode-se estabelecer os seguintes conceitos:

~~7.~~

[1] Para maiores informações acerca de quem pode ser considerado agente de tratamento, ver Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, mai.2021, p.5-6. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em 23 ago.2021

[2] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, como explicado mais a frente, será tratado em um Guia específico.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo, Espaçamento entre linhas: Múltiplos 1,07 lin.
Formatado: Normal, Sem marcadores ou numeração
Formatado: Espaço Depois de: 12 pt
Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo
Formatado: Sem marcadores ou numeração
Formatado: Texto de nota de rodapé

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

Microempresas e Empresas de Pequeno Porte

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.

Startups

Formatado: Fonte: Itálico

Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.

Agente de Tratamento de Pequeno Porte

~~Microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.~~

Microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

Formatado: Fonte: 9 pt
Formatado: Fonte: (Padrão) +Corpo (Calibri), 9 pt
Formatado: Fonte: 9 pt
Formatado: Fonte: 9 pt

Formatado: Normal, Sem marcadores ou numeração

8. Tendo em vista estas definições, o objetivo desse Guia é disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte.

~~8.~~

Formatado: Normal, Sem marcadores ou numeração

3. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

3.1. Segurança da informação

9. A *International Organization for Standardization* (ISO) é uma organização internacional que desenvolve e publica normas técnicas que são utilizadas por inúmeros países, incluindo o Brasil. Uma das normas da organização é a Norma ABNT NBR ISO/IEC 27001,[3] que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.

Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo

10. Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio globais da organização.

[3] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

11. De acordo com a norma, a segurança da informação pode ser definida como o conjunto de ações que visam a preservação da confidencialidade, integridade e disponibilidade da informação.

12. Este conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais. A segurança da informação~~, no que se refere à proteção de dados pessoais, ou seja,~~ está~~ão~~ relacionada~~s~~ às camadas de tecnologia, processos e pessoas, deve receber atenção de todos que lidam com dados pessoais e não somente daqueles ~~an~~o ambiente de tecnologia da informação.

13. 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.

14. Ainda que não seja obrigatório é indicado que, se possível, 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.

~~14.~~

Formatado: Normal, Sem marcadores ou numeração

3.2. Tratamento de dados pessoais

Formatado: Espaço Depois de: 12 pt

15. A LGPD define tratamento de dados pessoais como toda operação realizada com dados pessoais, como as que se referem a 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.

Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo, Espaçamento entre linhas: Múltiplos 1,07 lin.

16. Vale ressaltar que dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, conforme disposto no art. 5º, I da LGPD.

17. A título exemplificativo, os conjuntos de dados que incluem dados pessoais podem conter identificadores diretos e indiretos, que permitem que um indivíduo seja identificado ou se torne identificável. Um identificador direto é uma informação específica que se refere a um indivíduo, como por exemplo nome e apelido, endereço de uma residência, endereço de correio eletrônico, número de um cartão de identificação, cookies em sítios eletrônicos. Por outro lado, um identificador indireto (também chamado de quase-identificador) é qualquer informação que pode ser usada, individualmente ou em combinação com outros quase-identificadores, por alguém que tem conhecimento sobre aquele indivíduo com o propósito de identificá-lo no conjunto de dados, como por exemplo, uma posição geográfica em um determinado momento ou uma opinião sobre um determinado assunto, dentre outros.

18. Cabe destacar que a LGPD define como dados pessoais sensíveis 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, nos termos do art. 5º, inciso II.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

19. Os dados sensíveis, por terem uma proteção especial conferida pela LGPD, possuem regras mais rigorosas para seu tratamento, **a fim de evitar risco ou danos relevantes aos titulares de dados, mesmo quando manipulados por agentes de tratamento de pequeno porte.** Como exemplo, verifica-se que o rol de hipóteses legais dispostos no art. 7º, que trata de dados pessoais, é distinto das hipóteses descritas no art. 11, que trata de dados sensíveis, ambos da mesma norma. Ademais, a citada lei estabelece algumas regras para tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14.

~~3.4.~~ 3.3 Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais

Formatado: Espaço Depois de: 12 pt

20. A LGPD trata da questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo

21. 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.

22. 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.

23. O art. 48 trata de uma importante obrigação relacionada à segurança de dados pessoais, e à 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 institucional (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

24. 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 às demais normas regulamentares.

[4] Cabe explicar que não é todo incidente que deveria ser comunicado à ANPD. No caso, devem ser comunicados apenas aqueles que envolvam dados pessoais e, mesmo assim, somente aqueles que se refiram a um evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Espaço Depois de: 12 pt
Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo

~~3.5.~~3.4 Segurança de informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte

25. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[5] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

26. Como se sabe, a implementação e manutenção de medidas que atendam a essas obrigações, considerando sua complexidade e especificidade em casos concretos, podem necessitar, em alguns casos, de elevado investimento e recursos. Este fato pode causar impacto financeiro aos agentes de tratamento de pequeno porte.

27. Nesse sentido, são apresentadas, a seguir, sugestões de medidas de segurança da informação relacionadas a dados pessoais capazes de promover em agentes de tratamento de pequeno porte um ambiente institucional mais seguro quanto ao tratamento de dados pessoais. As medidas sugeridas devem ser entendidas como boas práticas a serem adotadas.

4. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

4.1 Medidas organizacionais

Formatado: Espaço Depois de: 12 pt

4.1.1 Política de segurança da informação

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

29. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Entretanto, pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis. A PSI, formalmente instituída, pode ser mais aplicável às organizações de médio e grande porte que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Cabe a cada instituição avaliar os impactos e recursos necessários e decidir sobre a sua formalização, sendo que esta Autoridade estimula a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

30. 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.

~~31. Ressalta-se que, no âmbito deste guia, não é exigido que agentes de tratamento de pequeno porte, em especial os que tratem dados de forma incidental, estabeleçam uma política de segurança da informação que contemple tratamento de dados pessoais.~~

~~32. No entanto, é recomendado que agentes de pequeno porte que tratem dados, como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao~~

[5] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado acima, não será abordado neste Guia.

~~tratamento de dados pessoais com diretrizes e regras mínimas relacionadas ao planejamento, implementação e controle.~~

~~33.~~31. Nesse sentido, a ANPD sugere que, quando possível, seja estabelecida uma política de segurança da informação simplificada 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 e uso de antivírus. Essas ações estariam integradas como parte da política de segurança da informação da empresa, com destaque a esta categoria especial de dados – os dados pessoais.

~~34.~~32. Sugere-se, ainda, que essa política seja **revisada periodicamente (a cada 1 ou 2 anos, por exemplo)**.

~~35.~~33. Além disso, é indicado que seja realizado o gerenciamento de contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

4.1.2 Segurança em recursos humanos

~~36.~~34. Os recursos humanos de uma empresa são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e 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.

~~37.~~35. Assim, quanto aos recursos humanos, sugere-se que os agentes de tratamento de pequeno porte **conscientizem os seus funcionários por meio de treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais**. Essa conscientização implica em **informar os funcionários diretamente envolvidos na atividade de tratamento de dados sobre as obrigações legais existentes na LGPD e normas editadas pela ANPD.**

~~38.~~36. Além disso, **sugere-se, também, que os funcionários sejam informados sobre os controles de segurança dos sistemas de TI que são relacionados ao seu trabalho diário**. Por exemplo, se um funcionário é responsável por incluir os dados de um grupo de clientes em um sistema no computador da empresa, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte, que serão sugeridas no tópico seguinte.

4.2 Medidas técnicas

4.2.1 Controle de acesso

~~39.~~37. O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele é composto pelos 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 e a auditoria registra o que foi feito pelo usuário.

~~40.~~38. 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 que acessam o sistema de TI**. Esse sistema de controle de acesso

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Justificado, Espaço Depois de: 12 pt
Formatado: Parágrafo da Lista, Recuo: Primeira linha: 0 cm
Formatado: Espaço Depois de: 12 pt
Formatado: Recuo: Primeira linha: 0 cm, Adicionar espaço entre parágrafos do mesmo estilo

pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários que acessam o sistema de TI.

~~41.~~39. 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 o sistema estabelecerá o número de caracteres necessários para se criar uma senha, se é necessário o uso de um caractere especial ou outros fatores que o agente de tratamento considere importante.

~~42.~~40. Outro importante ponto sugerido 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.

~~43.~~41. Nesse sentido, o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[6] publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[7] 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.

~~44.~~42. Por fim, sugere-se que os agentes considerem, preferencialmente, **utilizar a autenticação de dois fatores** 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.

43. A título de exemplo de autenticação de dois 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.

~~45.~~

4.2.2 Segurança dos dados pessoais armazenados

~~46.~~44. Pode-se dizer que as etapas descritas até o momento visam contribuir justamente com a segurança dos dados pessoais armazenados, a fim de diminuir o risco de vazamento e aumentar a segurança que os agentes de pequeno porte devem ter ao longo do tratamento de dados pessoais.

~~47.~~45. 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 específica. Para se evitar riscos de vazamento e outros comprometimentos, sugere-se que os agentes de tratamento de pequeno porte **coletem e processem apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados**. No contexto atual da LGPD, tratar (coletar e guardar, por exemplo) dados pessoais sem uma utilidade imediata e concreta, apenas porque um dia poderão

[6] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

[7] 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.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Fonte: Não Negrito
Formatado: Normal, Sem marcadores ou numeração
Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo

ser úteis (sem se saber exatamente para quê), não é uma prática adequada ~~permitida~~, considerando ~~conforme~~ os princípios da finalidade e necessidade previstos na referida ~~l~~Lei.

~~48.~~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 lidam com dados dessa natureza **implementem soluções de pseudonimização[8], como por exemplo a criptografia** para cifrar os dados sob sua responsabilidade.

~~49.~~47. Em relação as 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.

~~50.~~48. Além disso, **é importante que os aplicativos antivírus sejam atualizados** quando necessário e que sejam instaladas regularmente as atualizações para última versão e as correções de segurança (*patches*[9]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

~~51.~~49. 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 es~~t~~ta operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como por exemplo, inventariá-los, cifrar os dados e armazená-los em locais seguros.

~~52.~~50. 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*).

~~53.~~51. Em relação aos dispositivos móveis, como celulares e *laptops*, sugere-se que estejam sujeitos, se possível, aos **mesmos procedimentos de controle de acesso que os outros equipamentos de TI**, **como o uso da autenticação de dois fatores para acesso aos dispositivos e sistemas de informação**, além de serem guardados em locais seguros quando não estiverem em uso. Caso não seja possível implementar essas medidas de segurança, recomenda-se que esses dispositivos não sejam utilizados para fins institucionais.

~~54.~~52. Neste sentido, 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, ~~como~~ 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 aplicativos utilizados. 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**

[8] 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>.

[9] Programa de computador criado para atualizar ou corrigir um *software* de forma a corrigir vulnerabilidades ou falhas.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

os dados pessoais relacionados à sua atividade de processamento. Isso poderá diminuir a chance de eventual vazamento de dados.

~~55.~~53. Por fim, sobre a eliminação de dados pessoais, sugere-se que **em todas as mídias que contenham dados pessoais seja executado o método de sobrescrever todos os dados 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.

~~56.~~54. 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 um registro da destruição que for realizada**.

4.2.3 Manutenção de programa de gerenciamento de vulnerabilidades

~~57.~~55. 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.

~~58.~~56. 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**.

~~59.~~57. 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.

~~60.~~58. Por fim, para manter sistemas e aplicativos seguros, é importante que os agentes se certifiquem que todos os componentes do sistema estejam protegidos de vulnerabilidades, instalando *patches* de segurança disponibilizados pelos fornecedores.

4.2.4 Segurança das comunicações

~~61.~~59. 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.

~~62.~~60. Sobre o assunto, destaca-se a relevância de se **utilizar somente 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, prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada
Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo
Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo

~~63.~~61. Além disso, sugere-se que **seja instalado e mantido um sistema de *firewall***[10], que consiste, por exemplo, na restrição de conexões entre redes não confiáveis e quaisquer componentes do sistema. Adicionalmente convém considerar o uso de ferramenta *anti-spam*, adotar filtros de e-mail, integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

~~64.~~62. É importante, ainda, na implementação desses 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.

4.3. Medidas relacionadas ao serviço em nuvem

~~65.~~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").

~~66.~~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.

~~67.~~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.

~~68.~~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 com o provedor do serviço em nuvem, contemplando a segurança dos dados armazenados.**

~~69.~~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 de dois fatores**, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

~~70.~~

5. CONSIDERAÇÕES FINAIS

~~71.~~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 tratamento de pequeno porte no desenvolvimento de suas atividades empresariais em um ambiente institucional mais seguro, no que se refere ao tratamento de dados pessoais.

[10] 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.

Formatado: Fonte: 9 pt

Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm

Formatado: Cabeçalho, Centralizado

Tabela formatada

Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo

Formatado: Normal, Sem marcadores ou numeração

Formatado: Recuo: Primeira linha: 0 cm, Espaço Depois de: 6 pt, Adicionar espaço entre parágrafos do mesmo estilo

Formatado: Fonte: 9 pt
Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm
Formatado: Cabeçalho, Centralizado
Tabela formatada

~~72.~~70. Neste guia, foram apresentadas medidas de segurança de natureza organizacional, que envolvem a política de segurança da informação relacionada a dados pessoais e segurança em recursos humanos; e medidas técnicas, que tratam 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 organizacional), tendo em vista a frequência com que esses serviços são utilizados por empresas de pequeno porte.

~~73.~~71. Espera-se que essas medidas estabeleçam um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, um aumento na confiança dos titulares de dados nos agentes de tratamento de dados pessoais de pequeno porte.

~~74.~~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.

6. REFERÊNCIAS

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.

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.

ABNT. Norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

ABNT. Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ABNT. Norma ABNT NBR ISO/IEC 27018: 2021, Tecnologia da informação — Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.

ABNT. Norma ABNT NBR ISO/IEC27005:2019, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT. Norma ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem.

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. ~~/05/~~2021.

Formatado: Fonte: 9 pt

Formatado: Cabeçalho, Recuo: À esquerda: -0,2 cm

Formatado: Cabeçalho, Centralizado

Tabela formatada

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

VERSÃO PARA O CONSELHO DIRETOR

AGOSTO DE 2021

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

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

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

SUMÁRIO

1. APRESENTAÇÃO

1. A publicação da 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 pilares desse marco regulatório é a proteção dos dados pessoais, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

2. Um importante ponto da LGPD é a previsão de tratamento diferenciado para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, tendo determinado a edição de norma específica para esse grupo, nos termos do inciso XVIII do art. 55-J da LGPD. No momento, a norma se encontra em consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD).

3. De modo a melhor identificar estas categorias de empresas, a ANPD atribuiu o nome de agentes de tratamento de pequeno porte às micro e pequenas empresas e *startups*. Existe um enorme desafio em flexibilizar algumas obrigações desses agentes contidas na LGPD sem aumentar os riscos e danos aos titulares dos dados, bem como conscientizar as empresas sobre a relevância da proteção de dados pessoais.

4. Diante desse cenário, a ANPD elaborou o presente guia orientativo, que busca apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais. Destaca-se que este guia poderá ser atualizado de forma periódica à medida em que a ANPD entender necessário.

2. ESCOPO E OBJETIVO

5. Este guia de boas práticas é endereçado aos agentes de tratamento[1] 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 aprimorar o processo de segurança da informação relacionada a dados pessoais, nos termos dos artigos 46, 47, 48[2] e 49 da LGPD.

6. No âmbito deste guia orientativo, adotam-se os conceitos de microempresa, pequena empresa e *startups* trazidos pela Lei Complementar nº 123/2006 e pela Lei Complementar nº 182, de 1º de junho de 2021.

7. Diante das duas leis mencionadas, pode-se estabelecer os seguintes conceitos:

[1] Para maiores informações acerca de quem pode ser considerado agente de tratamento, ver Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, mai.2021, p.5-6. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em 23 ago.2021

[2] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, como explicado mais a frente, será tratado em um Guia específico.

Microempresas e Empresas de Pequeno Porte

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.

Startups

Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.

Agente de Tratamento de Pequeno Porte

Microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

8. Tendo em vista estas definições, o objetivo desse Guia é disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte.

3. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

3.1. Segurança da informação

9. A *International Organization for Standardization* (ISO) é uma organização internacional que desenvolve e publica normas técnicas que são utilizadas por inúmeros países, incluindo o Brasil. Uma das normas da organização é a Norma ABNT NBR ISO/IEC 27001,[3] que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.

10. Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio globais da organização.

11. De acordo com a norma, a segurança da informação pode ser definida como o conjunto de ações que visam a preservação da confidencialidade, integridade e disponibilidade da informação.

12. Este conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais. A segurança da informação está relacionada às camadas de tecnologia, processos e pessoas, deve receber atenção de todos que lidam com dados pessoais e não somente daqueles no ambiente de tecnologia da informação.

[3] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

13. 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.

14. Ainda que não seja obrigatório é indicado que, se possível, 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.

3.2. Tratamento de dados pessoais

15. A LGPD define tratamento de dados pessoais como toda operação realizada com dados pessoais, como as que se referem a 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.

16. Vale ressaltar que dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, conforme disposto no art. 5º, I da LGPD.

17. A título exemplificativo, os conjuntos de dados que incluem dados pessoais podem conter identificadores diretos e indiretos, que permitem que um indivíduo seja identificado ou se torne identificável. Um identificador direto é uma informação específica que se refere a um indivíduo, como por exemplo nome e apelido, endereço de uma residência, endereço de correio eletrônico, número de um cartão de identificação, cookies em sítios eletrônicos. Por outro lado, um identificador indireto (também chamado de quase-identificador) é qualquer informação que pode ser usada, individualmente ou em combinação com outros quase-identificadores, por alguém que tem conhecimento sobre aquele indivíduo com o propósito de identificá-lo no conjunto de dados, como por exemplo, uma posição geográfica em um determinado momento ou uma opinião sobre um determinado assunto, dentre outros.

18. Cabe destacar que a LGPD define como dados pessoais sensíveis 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, nos termos do art. 5º, inciso II.

19. Os dados sensíveis, por terem uma proteção especial conferida pela LGPD, possuem regras mais rigorosas para seu tratamento, **a fim de evitar risco ou danos relevantes aos titulares de dados, mesmo quando manipulados por agentes de tratamento de pequeno porte.** Como exemplo, verifica-se que o rol de hipóteses legais dispostos no art. 7º, que trata de dados pessoais, é distinto das hipóteses descritas no art. 11, que trata de dados sensíveis, ambos da mesma norma. Ademais, a citada lei estabelece algumas regras para tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14.

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

20. A LGPD trata da questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

21. 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.

22. 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.

23. O art. 48 trata de uma importante obrigação relacionada à segurança de dados pessoais, e à 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 institucional (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

24. 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 às demais normas regulamentares.

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

25. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[5] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

26. Como se sabe, a implementação e manutenção de medidas que atendam a essas obrigações, considerando sua complexidade e especificidade em casos concretos, podem necessitar, em alguns casos, de elevado investimento e recursos. Este fato pode causar impacto financeiro aos agentes de tratamento de pequeno porte.

[4] Cabe explicar que não é todo incidente que deveria ser comunicado à ANPD. No caso, devem ser comunicados apenas aqueles que envolvam dados pessoais e, mesmo assim, somente aqueles que se refiram a um evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

[5] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado acima, não será abordado neste Guia.

27. Nesse sentido, são apresentadas, a seguir, sugestões de medidas de segurança da informação relacionadas a dados pessoais capazes de promover em agentes de tratamento de pequeno porte um ambiente institucional mais seguro quanto ao tratamento de dados pessoais. As medidas sugeridas devem ser entendidas como boas práticas a serem adotadas.

4. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

4.1 Medidas organizacionais

4.1.1 Política de segurança da informação

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

29. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Entretanto, pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis. A PSI, formalmente instituída, pode ser mais aplicável às organizações de médio e grande porte que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Cabe a cada instituição avaliar os impactos e recursos necessários e decidir sobre a sua formalização, sendo que esta Autoridade estimula a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

30. 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.

31. Nesse sentido, a ANPD sugere que, quando possível, seja estabelecida uma política de segurança da informação simplificada 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 e uso de antivírus. Essas ações estariam integradas como parte da política de segurança da informação da empresa, com destaque a esta categoria especial de dados – os dados pessoais.

32. Sugere-se, ainda, que essa política seja **revisada periodicamente (a cada 1 ou 2 anos, por exemplo)**.

33. Além disso, é indicado que seja realizado o gerenciamento de contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

4.1.2 Segurança em recursos humanos

34. Os recursos humanos de uma empresa são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e 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.

35. Assim, quanto aos recursos humanos, sugere-se que os agentes de tratamento de pequeno porte **conscientizem os seus funcionários por meio de treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais**. Essa conscientização implica em **informar os funcionários diretamente envolvidos na atividade de tratamento de dados sobre as obrigações legais existentes na LGPD e normas editadas pela ANPD**.

36. Além disso, **sugere-se, também, que os funcionários sejam informados sobre os controles de segurança dos sistemas de TI que são relacionados ao seu trabalho diário**. Por exemplo, se um funcionário é responsável por incluir os dados de um grupo de clientes em um sistema no computador da empresa, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte, que serão sugeridas no tópico seguinte.

4.2 Medidas técnicas

4.2.1 Controle de acesso

37. O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele é composto pelos 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 e a auditoria registra o que foi feito pelo usuário.

38. 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 que acessam o sistema de TI**. Esse sistema de controle de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários que acessam o sistema de TI.

39. 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 o sistema estabelecerá o número de caracteres necessários para se criar uma senha, se é necessário o uso de um caractere especial ou outros fatores que o agente de tratamento considere importante.

40. Outro importante ponto sugerido 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.

41. Nesse sentido, o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[6] publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[7] em conjunto com o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), apontou que melhorar processos de

[6] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

[7] 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.

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.

42. Por fim, sugere-se que os agentes considerem, preferencialmente, **utilizar a autenticação de dois fatores** 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.

43. A título de exemplo de autenticação de dois 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.

4.2.2 Segurança dos dados pessoais armazenados

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

45. 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 específica. Para se evitar riscos de vazamento e outros comprometimentos, sugere-se que os agentes de tratamento de pequeno porte **coletem e processem apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados**. 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 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 lidam com dados dessa natureza **implementem soluções de pseudonimização[8], como por exemplo a criptografia** para cifrar os dados sob sua responsabilidade.

47. Em relação as 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.

48. Além disso, **é importante que os aplicativos antivírus sejam atualizados** quando necessário e que sejam instaladas regularmente as atualizações para última versão e as correções de segurança (*patches*[9]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

[8] 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>.

[9] Programa de computador criado para atualizar ou corrigir um *software* de forma a corrigir vulnerabilidades ou falhas.

49. 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 por exemplo, inventariá-los, cifrar os dados e armazená-los em locais seguros.

50. 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*).

51. Em relação aos dispositivos móveis, como celulares e *laptops*, sugere-se que estejam sujeitos, se possível, aos **mesmos procedimentos de controle de acesso que os outros equipamentos de TI**, **como o uso da autenticação de dois fatores para acesso aos dispositivos e sistemas de informação,** além de serem guardados em locais seguros quando não estiverem em uso. Caso não seja possível implementar essas medidas de segurança, recomenda-se que esses dispositivos não sejam utilizados para fins institucionais.

52. Neste sentido, 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 aplicativos utilizados. 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 vazamento de dados.

53. Por fim, sobre a eliminação de dados pessoais, sugere-se que **em todas as mídias que contenham dados pessoais seja executado o método de sobrescrever todos os dados 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.

54. 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 um registro da destruição que for realizada**.

4.2.3 Manutenção de programa de gerenciamento de vulnerabilidades

55. 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.

56. 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**.

57. 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.

58. Por fim, para manter sistemas e aplicativos seguros, é importante que os agentes se certifiquem que todos os componentes do sistema estejam protegidos de vulnerabilidades, instalando *patches* de segurança disponibilizados pelos fornecedores.

4.2.4 Segurança das comunicações

59. 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.

60. Sobre o assunto, destaca-se a relevância de se **utilizar somente 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, prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

61. Além disso, sugere-se que **seja instalado e mantido um sistema de *firewall***[10], que consiste, por exemplo, na restrição de conexões entre redes não confiáveis e quaisquer componentes do sistema. Adicionalmente convém considerar o uso de ferramenta *anti-spam*, adotar filtros de e-mail, integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

62. É importante, ainda, na implementação desses 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.

[10] 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.

4.3. 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 com o provedor do serviço em nuvem, 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 de dois fatores**, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

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

70. Neste guia, foram apresentadas medidas de segurança de natureza organizacional, que envolvem a política de segurança da informação relacionada a dados pessoais e segurança em recursos humanos; e medidas técnicas, que tratam 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 organizacional), tendo em vista a frequência com que esses serviços são utilizados por empresas de pequeno porte.

71. Espera-se que essas medidas estabeleçam um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, 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.

6. REFERÊNCIAS

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.

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.

ABNT. Norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

ABNT. Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ABNT. Norma ABNT NBR ISO/IEC 27018: 2021, Tecnologia da informação — Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.

ABNT. Norma ABNT NBR ISO/IEC27005:2019, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT. Norma ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem.

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.

Certidão de Distribuição - 2856195

Processo:
00261.000821/2021-16 - Normatização - Elaboração e revisão de normativos

Data da Distribuição:
02/09/2021 16:15:16

Colegiado:
Conselho Diretor da ANPD (CD/ANPD)

Composição do Colegiado:
Arthur Pereira Sabbat (DIR/AS/ANPD)
Miriam Wimmer (DIR/MW/ANPD)
Joacil Basilio Rael (DIR/JR/ANPD)
Nairane Farias Rabelo Leitão (DIR/NR/ANPD)
Waldemar Gonçalves Ortunho Junior (GABPR/ANPD) - Impedido: Diretor-Presidente em exercício, gerando impossibilidade de receber processos para relatoria de receber processos para relatoria conforme previsto no caput do art. 22 do Regimento Interno da ANPD

Relator:
Nairane Farias Rabelo Leitão (DIR/NR/ANPD)

PRESIDÊNCIA DA REPÚBLICA

PR/PROTOCOLO/ANPD/DIR/NR/ANPD

VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR

PROCESSO Nº 00261.000821/2021-16

INTERESSADO: Autoridade Nacional de Proteção de Dados

CONSELHEIRO

Nairane Farias Rabelo Leitão

1. ASSUNTO

1.1. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

2. EMENTA

2.1. PUBLICAÇÃO DE GUIA ORIENTATIVO. SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS. AGENTES DE TRATAMENTO DE PEQUENO PORTE. TUTELA DA PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS. BOAS PRÁTICAS. PAPEL ORIENTATIVO DA ANPD.

3. REFERÊNCIA

3.1. Processo SEI nº 00261.000821/2021-16.

4. RELATÓRIO

4.1. Trata-se da publicação de guia orientativo sobre boas práticas de segurança da informação para agentes de tratamento de pequeno porte, compreendidos como as microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, além daqueles que venham a ser assim entendidos por resolução pertinente.

4.2. Segundo dados disponibilizados pelo Sebrae, mais de 90% das empresas brasileiras se enquadram em microempresas e empresas de pequeno porte, o que torna ainda mais relevante a publicação de um guia orientativo direcionada a este público e aos demais que vierem a ser enquadrados como agentes de pequeno porte.

4.3. Em reunião realizada entre a Autoridade Nacional de Proteção

de Dados (ANPD) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo NIC.br, constatou-se a necessidade de elaboração conjunta do guia para orientação aos agentes de tratamento de pequeno porte, em razão de suas limitações estruturais e financeiras.

4.4. Ambas as instituições trabalharam para a elaboração do guia, que consiste em fruto dessa cooperação interinstitucional, ratificada pelo Acordo de Cooperação Técnica (ACT) firmado entre as instituições posteriormente, em 20 de julho de 2021.

4.5. O ACT firmado entre as instituições possui como objetivos ações conjuntas, conforme sua cláusula 1.1, item 'e':

> "1.1. O presente Acordo tem por objeto a cooperação técnica entre a ANPD e o NIC.br, através do CERT.br, com vistas a promover ações conjuntas sobre assuntos de interesse recíproco, nos termos da Lei e desde que não violem obrigações de confidencialidade, dentre as quais se incluem:e) Elaboração conjunta e intercambio de estudos, análises, notas técnicas e projetos de pesquisa sobre proteção de dados pessoais segurança da informação e tecnologia."

4.6. A publicação do referido guia está em consonância com as competências institucionais atribuídas pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) à ANPD, conforme exposto no art. 55-J I, VI, VII e XVIII:

> "Art. 55-J. Compete à ANPD:
>
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
>
> (...)
>
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
>
> VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade (...)
>
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei"

4.7. Ressalta-se que as competências estabelecidas no art. 55-J da LGPD convergem com o disposto nas competências especificadas no art. 16, II, do regimento interno da ANPD, publicado na Portaria nº 1, de 8 de março de 2021.

4.8. A emissão deste guia, além de contribuir para a competência orientativa, atende também a agenda regulatória da ANPD, que estabelece

como prioritário o tema de proteção de dados para agentes de tratamento de pequeno porte e pessoas físicas.

4.9. Ademais, as ações orientativas consistem em estratégias da fiscalização responsiva (conforme norma de fiscalização em processo de regulamentação), com o objetivo de alcançar a efetividade no cumprimento da LGPD, em concordância com o princípio da prevenção (art. 6º, VIII da LGPD) e da responsabilização (art. 6º, X da LGPD).

4.10. Portanto, a elaboração do presente guia contribui para a concretização das competências da ANPD com a finalidade máxima de proteção dos direitos dos titulares de dados pessoais.

4.11. Distribuído à relatoria deste Gabinete, foram procedidas algumas alterações na redação e no conteúdo do guia, tendo sido algumas delas resultado da gentil colaboração de outros membros do Conselho Diretor e da equipe técnica, conforme versão com marcas de revisão no documento SEI nº 2892323.

4.12. Em sua maioria, as alterações visam facilitar a leitura, por meio de redações mais simples ou reduzidas; sugerir mais algumas medidas que podem ser adotadas pelos agentes de pequeno porte; ou redistribuir as medidas para seções individualizadas. As alterações mais relevantes passarão a ser descritas a seguir.

4.13. Os capítulos 1 e 2 foram unificados para conferir uma redação mais objetiva da apresentação do guia e seu escopo.

4.14. Informações relacionadas à normas técnicas da ISO (*International Organization for Standardization*) foram removidas do guia por se tratar de entidade emissora de normas relacionadas a boas práticas não vinculantes, as quais a LGPD e a ANPD não se sujeitam. Portanto, compreende-se que não devem constar de guia orientativo emitido pela sua autoridade regulamentadora.

4.15. Termos técnicos, como “identificadores diretos e indiretos”, foram removidos por falta de previsão na LGPD, bem como em razão da complexidade dos conceitos e do objetivo de simplificação do guia, já que é direcionado a um público com menor porte operacional e financeiro no que se refere à segurança da informação.

4.16. Em relação às obrigações da LGPD, foi adicionado parágrafo que se refere ao princípio da segurança, obrigação legal intrinsecamente relacionada ao texto.

4.17. Menções à não obrigatoriedade da elaboração da política de segurança da informação pelos agentes de tratamento foram realizadas, embora com a devida ressalva de que a ANPD incentiva sua elaboração e

implementação.

4.18. A esse respeito, sugiro a elaboração e divulgação de proposta de modelo de Política de Segurança da Informação (PSI) simplificada, em momento oportuno, pela ANPD, sem pretensão de esgotar a matéria, mesmo porque, para a plena adequação da PSI à organização, faz-se necessário entender como funciona o fluxo operacional para que nenhum elemento de segurança necessário à proteção dos dados pessoais deixe de ser contemplado.

4.19. Exemplos práticos sobre medidas de segurança foram adicionados à redação, para facilitar a compreensão dos agentes de tratamento na leitura do guia.

4.20. Outras medidas de segurança, além daquelas já constantes da minuta proposta a este Gabinete, também foram acrescidas, como é o caso de recomendações para operacionalizar a informação por clientes e funcionários sobre vulnerabilidades detectadas, a assinatura de termos de confidencialidade com funcionários da empresa e o gerenciamento de contratos com clientes e fornecedores para a adequada proteção de dados.

4.21. Por fim, recomendações de governança foram incluídas, contendo exemplos de medidas que trazem segurança jurídica aos tratamentos de dados realizados pelos agentes de tratamento de pequeno porte.

4.22. Além das alterações, foi adicionado o anexo I ao guia, que é parte integrante deste para todos os fins. O anexo contém um *checklist* para facilitar a conferência e a aplicação prática das medidas de segurança técnicas e administrativas do guia.

4.23. Ressalta-se que o presente guia não é vinculante e nem constitui regulamentação à LGPD, mas apenas a esclarece e objetiva dar orientações aos entes regulados na busca pela adequação ao novo ecossistema de proteção de dados criado pela lei.

4.24. Desta forma, o guia orientativo segue para publicação no site da Autoridade, sem que se constitua em regulamentação de fato.

4.25. Para que não haja prejuízos aos direitos dos titulares em razão do descumprimento legal, e em seguimento à construção da cultura de proteção de dados no país, a ANPD entende que se trata de publicação urgente.

4.26. É recomendado que o documento seja amplamente publicizado e que seja disponibilizado um canal de contato para recebimento de sugestões de aprimoramento, as quais poderão ser incorporadas em versões

subsequentes do documento.

4.27. Também é recomendado que modelos, como o da PSI, sejam disponibilizados em seguida para facilitar a estruturação dos agentes de pequeno porte.

5. CONCLUSÃO

5.1. É de competência da ANPD zelar pela proteção de dados pessoais e por promover orientação aos titulares e aos agentes de tratamento brasileiros que, em sua maior parte, poderão ser classificadas como agentes de pequeno porte.

5.2. O cumprimento da LGPD por esses agentes é primordial para o país e, por isso mesmo, também o é a sua orientação, especialmente diante do fato de que normalmente não possuem estrutura operacional e financeira robusta.

5.3. O guia de segurança da informação tem como objetivo orientar os agentes de pequeno porte e de obter maior adesão ao cumprimento da LGPD e à proteção aos direitos dos titulares de dados.

5.4. Dessa forma, voto pela publicação do guia orientativo (documento SEI nº 2892324) sobre segurança da informação para agentes de tratamento de pequeno e seu anexo (documento SEI nº 2892325) e submeto o presente voto para aprovação dos demais membros do Conselho Diretor, mediante votação por circuito deliberativo, nos termos do § 1º do art. 40 do Regimento Interno da ANPD.

5.5. É como voto.

Documento assinado eletronicamente por **Nairane Farias Rabelo Leitão**, **Diretor(a)**, em 19/09/2021, às 19:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2892319** e o código CRC **16DD77FB** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2892319

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

~~VERSÃO PARA~~ O CONSELHO DIRETOR ~~ASSESSORIA JURÍDICA~~

~~JULHO~~ AGOSTO

SETEMBRO DE 2021

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

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

~~Maria Luiza - Estagiária de Tecnologia e Pesquisa~~

Colaboradores externos

Cristine Hoepers - CERT.br/NIC.br

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

SUMÁRIO

1. APRESENTAÇÃO E OBJETIVO

1. A publicação dAa 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 desse marco regulatório é a proteção dos dados pessoaisdesses 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 Um importante ponto da LGPD é a previsão de tratamento diferenciado 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[obs], tendo a Lei determinado a edição de norma específica para esse grupo. [obs]No momento, a norma se encontra em consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD).A resolução com esse fim pode incluir no conceito de agentes de pequeno porte outras categorias de organizações além das anteriormente mencionadas[2].

3. que até a data de publicação deste documento se encontra 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 presente Guia apresenta algumas medidas de segurança da informação, com o fim de proteger os dados pessoais sob a guarda dos agentes de pequeno porte sua guarda.

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

Nesse sentido, o presente Guia apresenta algumas medidas ns mecanismosrequisitos mínimos de segurança da informação, considerados pela Autoridade como possíveis de serem adotados pelos agentes de tratamento de pequeno porte, com o fim de proteger os dados pessoais sob a sua guarda. P

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

De modo a melhor identificar esstas categorias de empresas, a ANPD atribuiu o nome de agentes de tratamento de pequeno porte às micro e pequenas empresas e *startups*, entre outras entidades. Existe um enorme desafio em flexibilizar algumas obrigações desses agentes contidas

[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.

~~na LGPD sem aumentar os riscos e danos aos titulares dos dados, bem como conscientizar as empresas sobre a relevância da proteção de dados pessoais.~~

~~Diante desse cenário, o presente guia traz orientações específicas aos agentes de tratamento de pequeno porte sobre segurança da informação relacionada à proteção de dados pessoais.~~

~~Diante desse cenário, a ANPD elaborou o presente guia orientativo, que busca apoiar e orientar esses agentes de tratamento no que se refere à segurança da informação relacionada à proteção de dados pessoais. Destaca-se que este Gguia poderá ser atualizado de forma periódica à medida em que a ANPD entender necessário.~~

~~2. ESCOPO E OBJETIVO~~

~~Este guia de boas práticas é endereçado aos agentes de tratamento[4] 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 aprimorar o processo dae segurança da informaçãoaprimorá-la relacionada em relação ao tratamento de dados pessoais realizado por esses agentes, nos termos dos artigos 46, 47, 48[5] e 49 da LGPD.~~

~~2. Nesse sentido, o presente Guia apresenta os requisitos mínimos de segurança da informação, considerados pela Autoridade como possíveis de serem adotados pelos agentes de tratamento de pequeno porte, com o fim de proteger adequadamente os dados pessoais sob a guarda desses agentes.~~

~~3. No âmbito deste guia orientativo, adotam-se os conceitos de microempresa, empresa depequena empresa porte e *startups* trazidos pela Lei Complementar nº 123/2006 e pela Lei Complementar nº 182, de 1º de junho de 2021, e o conceito de agentes de tratamento de pequeno porte, proposto pela ANPD em resolução, ora em consulta pública..~~

~~Diante das duas leis mencionadas, pode-se estabelecer os seguintes conceitos:~~

> ~~Microempresas e Empresas de Pequeno Porte~~
>
> ~~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.~~
>
> ~~*Startups*~~
>
> ~~Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021.~~

~~[4]Para maiores informações acerca de quem pode ser considerado agente de tratamento, ver Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, mai.2021, p.5-6. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em 23 ago.2021~~

~~[5] O art. 48 também é uma obrigação relacionada à segurança da informação. Todavia, como explicado mais a frente, será tratado em um Guia específico.~~

~~Agente de Tratamento de Pequeno Porte~~

~~Microempresas, empresas de pequeno porte, startups, sociedades simples, pessoas jurídicas sem fins lucrativos, demais entidades equiparadas sem personalidade jurídica e outras sociedades empresárias, assim como pessoas físicas que tratem dados para fins econômicos, levando em consideração também a bruta máxima estabelecida no art. 4º, §1º, inciso I, da Lei Complementar nº 182, de 1º de junho de 2021.~~

~~Microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.~~

~~Tendo em vista esstas definições, o objetivo destse Guia é disseminar medidas básicas sobre segurança da informação e boas práticas relacionadas ao tratamento de dados pessoais para agentes de tratamento de pequeno porte.~~

2. ~~3.~~ SEGURANÇA DA INFORMAÇÃO RELACIONADA A DADOS PESSOAIS

2~~3~~.1. Segurança da informação

~~A *International Organization for Standardization* (ISO) é uma organização internacional que desenvolve e publica normas técnicas que são utilizadas por inúmeros países, incluindo o Brasil. Uma das normas da organização é a Norma ABNT NBR ISO/IEC 27001,[6] que dispõe sobre sistema de gestão de segurança da informação e técnicas de segurança.~~

~~Em síntese, a Norma ABNT NBR ISO/IEC 27001 tem como princípio geral a adoção de um conjunto de requisitos, processos e controles que visam a gerir adequadamente os riscos de segurança da informação presentes nas organizações. Além disso, esta norma foi preparada paracom o fim de prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio globais da organização.~~

~~4.~~6. ~~De acordo com a norma ABNT NBR ISO/IEC 27001, a~~A segurança da informação pode ser definida como o conjunto de ações que visam à~~s~~ 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.

~~5. Esste conjunto de ações impacta todo o ambiente institucional das empresas com objetivo de prevenir, detectar e combater as ameaças digitais. A segurança da informação, no que se refere à proteção de dados pessoais, ou seja, estáão relacionadas às camadas de tecnologia, processos e pessoas, e deve receber atenção de todos que lidam com dados pessoais e não somente daqueles ano ambiente de tecnologia da informação.~~

~~6.~~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

~~[6] Norma ABNT NBR ISO/IEC 27001 - Norma internacional para Sistema de Gestão de Segurança da Informação (SGSI) - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.~~

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 , se possível, 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.

23.2. Tratamento de dados pessoais

9. A LGPD define tratamento de dados pessoais como toda operação realizada com dados pessoais, como as que se referem àa 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.

7.11. 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.

Vale ressaltar que a LGPD define econceituam seu art. 5º, I, os dados pessoais em seu art. 5º, inciso I, como sendo são as informações relacionadas a pessoa natural identificada ou identificável; e dados sensíveis, nos termos do art. 5º, inciso II, são definidos como , conforme disposto no art. 5º, I da LGPD.

como sendo 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., nos termos do art. 5º, inciso II.

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. Como exemplo, verifica-se que o rol de hipóteses legais dispostos dispostas noTtanto que 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, ambos da mesma norma. Ademais, a citada lei estabelece algumas regras para tratamento de dados pessoais de crianças e adolescentes, nos termos do art. 14.

3.4. 23.3 Obrigações da LGPD sobre segurança da informação relacionada a dados pessoais

8.12. A LGPD introduz, em seu art. 6º, inciso 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 trata da questão de segurança da informação relacionada aos dados pessoais nos artigos 46 a 49.

9.13. 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.

10.14. 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.

11.15. O art. 48 trata de uUma importante obrigação relacionada à segurança de dados pessoais é tratada no art. 48 e, e à que consiste na comunicação à ANPD de incidentes de segurança que possam acarretar risco ou dano relevante[7] 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 institucionaleletrônico[8] (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca).

12.16. 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 naàs demais normas regulamentares.

[7] 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. No caso, devem ser comunicados apenas aqueles que envolvam dados pessoais e, mesmo assim, somente aqueles que se refiram a um evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco ou dano relevante para os direitos e liberdades do titular dos dados pessoais.

[8] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

2.43.5.3.4 Segurança dae informação relacionada a dados pessoais nos agentes de tratamento de pequeno porte

13.17. As obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD,[9] referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

14.18. 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 algumasns situaçõescasos, de elevado investimento e recursos. Esste fato, o que podecom 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 relacionadas a dados pessoais capazes de promover, em agentes de tratamento de pequeno porte, um ambiente institucional mais seguro quanto ao tratamento de dados pessoais.

15.20. As medidas sugeridas devem ser entendidas como boas práticas a serem adotadase devem ser complementadas com outras que possam ser identificadas como necessárias para promover a segurança nao fluxo operacional informacional da organização.

34. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

3.1 Medidas organizacionaisadministrativas

34.1.1 Política de segurança da informação

16.21. 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.

17.22. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Entretanto, pode não ser aplicável às organizações de pequeno porte que não tratam dados sensíveis. A PSI, formalmente instituída, pode ser mais aplicável às organizações de médio e grande porte que necessitam direcionar a atuação institucional relacionada à segurança de forma mais abrangente. Muito embora não seja obrigatória, a elaboração dessa política e sua implementação são incentivadas pela ANPD aos agentes de tratamento de pequeno porte, a elaboração dessa política e, sua implementação são incentivadas pela ANPD, porque evidenciam a boa-fé e a diligência desses agentes na segurança dos dados pessoais sob sua custódia e fornecem as diretrizes para a gestão da segurança da informação. Nesse contexto, cCabe a cada instituição avaliar os impactos e os recursos necessários e decidir sobre a sua formalização desse instrumento, sendo que esta Autoridade estimulaincentiva a elaboração de uma política institucional que forneça as diretrizes para a gestão da segurança da informação.

[9] O art. 48 também é uma obrigação igualmente baseada em boas práticas internacionais. Todavia, como explicado acima, não será abordado neste Guia.

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.

18. 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; e uso de antivírus, entre outros.

19. Ressalta-se que, no âmbito deste guia, não é exigido que agentes de tratamento de pequeno porte, em especial os que tratem dados de forma incidental, estabeleçam uma política de segurança da informação que contemple tratamento de dados pessoais.

20. No entanto, é recomendado que agentes de pequeno porte que tratem dados, como atividade principal estabeleçam uma política simplificada de segurança que traga destaque ao tratamento de dados pessoais com diretrizes e regras mínimas relacionadas ao planejamento, implementação e controle.

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, por exemplo, cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de *softwares;* uso de correio eletrônico; e uso de antivírus, entre outros. cópias de segurança;, uso de senhas;, acesso à informação;, compartilhamento de dados;, atualização de *softwares;*, uso de correio eletrônico; e uso de antivírus. Essas ações estariam integradas como parte da política de segurança da informação da empresaorganização, com destaque a essta categoria especial de dados – os dados pessoais.

21. Um modelo proposto de PSI simplificada pode ser encontrado no Anexo I a este Guia.

22. Sugere-se, ainda, que essa política seja revisada periodicamente (a cada 1 ou 2 anos, por exemplo).

Além disso, é indicado que seja realizado o gerenciamento de contratos e aquisições com observância ao tratamento adequado dos dados pessoais.; tais instrumentos poderiam conter cláusulas que tratassem 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.

Uma proposta de PSI simplificada deve ser divulgada pela ANPD, sem pretensão de esgotar a matéria, mesmo porque, para a plena adequação da PSI à organização, faz-se necessário entender como funciona o fluxo operacional para que nenhum elemento de segurança necessário à proteção dos dados pessoais deixe de ser contemplado.

23. Como boa prática, recomenda-se à organização que elabore a PSI simplificada e que os itens abordados a seguir constem dessa Política, cuja elaboração pode seguir o modelo proposto no Anexo a este Guia.

24.

4.1.2 Plano de resposta a incidentes

O plano de respostas a incidentes é um documento que apresenta um conjunto de ferramentas e procedimentos para que a empresa possa lidar com incidentes de segurança que ocorram, garantindo a proteção dos ativos institucionais e os dados pessoais de titulares. Embora seu escopo envolva todos os eventos adversos que afetem o negócio da empresa, ele deve ser capaz de fornecer instruções que auxiliem a identificar se um determinado incidente de segurança está relacionado a dados pessoais, ou seja, se o incidente detectado acarreta risco ou dano relevante aos titulares de dados.

Algumas das informações que um plano de respostas a incidentes deve conter são: (i) instruções para garantir o sigilo de informações sensíveis quanto ao incidente; (ii) definição de funções e responsabilidades de unidades organizacionais durante o incidente; (iii) escalonamento de possíveis problemas e relato de atividades suspeitas; (iv) classificações de gravidade de incidentes; (v) orientações para comunicações externas (por exemplo, com a ANPD, fornecedores de serviços, seguradoras, titulares de dados, etc.).

4.1.3 Plano de recuperação de desastres e Plano de continuidade do negócio

Estes importantes documentos de governança estão correlacionados mas possuem suas particularidades. A finalidade do plano de recuperação de desastre é definir precisamente como a organização irá recuperar sua infraestrutura e serviços de TI dentro dos prazos estabelecidos no caso de um desastre ou outro incidente disruptivo. Assim, o foco desse documento está em garantir a restauração rápida de sistemas de TI que sustentam processos críticos de negócio.

Por sua vez, o plano de continuidade dos negócios possui escopo mais amplo e ajuda a empresa a minimizar os impactos de uma crise e permitir o uso de processos alternativos quando os processos usuais estiverem indisponíveis. Seu objetivo é garantir a continuidade de processos e serviços vitais do negócio.

34.1.2 Segurança em recursos humanosConscientização e Treinamento

24.25. Os recursos humanos de uma empresa 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, quanto aos recursos humanos, sugere-se que os agentes de tratamento de pequeno porte conscientizem os seus funcionários por meio de treinamentos e campanhas de conscientização sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

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

28. Além disso, sugere-se, também, que os funcionários sejam informados sobre os controles de segurança dos sistemas de TI que são relacionados ao seu trabalho diário, além de como evitar que sejam 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.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.

. Por exemplo, se um funcionário é responsável por incluir os dados de um grupo de clientes em um sistema no computador da empresaorganização, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte, que serão sugeridas no tópico seguinte.

29. Também é importante criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informarcomunicar incidentes e vulnerabilidades detectadas. No caso dos últimos, esses devem se sentir seguros de que não sofrerão retaliações ao realizarem a comunicação.

– *NDA*

34.1.3. 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.

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. Nesse sentido, 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.

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

- Regras para fornecedores e parceiros;
- regras sobre compartilhamentos;
- relações entre controlador-operador;

- 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

Exemplo 1: se um funcionário é responsável por incluir os dados de um grupo de clientes pessoas físicas em um sistema no computador da organização, é importante que ele siga as medidas técnicas de segurança do agente de tratamento de pequeno porte.

Exemplo 2: Os funcionários devem manter documentos físicos que contenham dados pessoais, dentro de gavetas, e não sobre as mesas.

Exemplo 3: Os funcionários não devem compartilhar devem memorizar seus logins e senhas de acesso às suas estações de trabalho; devem, ainda, evitar ao máximo escrever esses dados. Caso tenham de fazê-lo, tais dados devem ficar em local protegido.

Exemplo 4: Ao se afastar do computador de trabalho, o funcionário que trata dados pessoais deve bloqueá-lo para evitar que outros acessem as informações.

Medidas técnicas

34.2.1 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 é compostoconsiste em pelos 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; ~~e a~~
- ~~–~~a auditoria registra o que foi feito pelo usuário.

~~26.~~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 ~~que acessam o sistema de TI~~, 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 ~~que acessam esse o sistema de TI~~.

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~~á~~ o número de caracteres ~~necessários~~ 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~~importante~~.

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.

~~É importante, ainda, na implementação desses 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.~~

~~27.~~ 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.

38.

39. ~~Outro importante ponto sugerido~~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.~~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.

~~28.~~40. Nesse sentido, importante mencionar que o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[10] publicado pelo Centro de Estudos, Resposta e

[10] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Tratamento de Incidentes de Segurança no Brasil (CERT.br)[11] 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.[12]

29.1. Nesse sentido, importante mencionar que o estudo "Segurança Digital: uma análise de gestão de risco em empresas brasileiras",[13] publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[14] 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.[15]

30.41. Por fim, sugere-se que os agentes considerem, preferencialmente, utilizar a autenticação de doismulti- 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 de doismulti- 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.

34.2.2 Segurança dos dados pessoais armazenados[16]Segurança dos dados pessoais armazenados[17]

31.43. Pode-se dizer que as etapas descritas até o momento visam contribuir justamente com a segurança dos dados pessoais armazenados, a fim de diminuir o risco de incidentesvazamento e

[11] 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.

[12] 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.

[13] 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. https://www.cgi.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

[14] 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.

[15] 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.

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

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

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

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 permitida, considerando conforme os princípios da finalidade e da necessidade previstos na referida lLei.

32. 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

33.46. 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 lidam comarmazenam dados dessa natureza implementem soluções que dificultem a identificação do titular, como as técnicas de pseudonimização.[18] Um exemplo dessa técnica é a criptografia. Um exemplo dessa técnica é a criptografia. e de, como, por exemplo, a criptografia, por exemplo. para cifrar os dados sob sua responsabilidade.

Em relação àas 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.

34. Mostra-se de grande valor também a orientação dos funcionários para que não cliquem em links que aparecem na forma de pop-up de promoções ou em links desconhecidos recebidos por e-mail.

47. Além disso, é importante que aplicativos antivírus sejam instalados em todos os equipamentos e atualizados quando necessário. Da mesma forma, devem ser instaladas regularmente as atualizações para última versão e as correções de segurança (patches) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

[18] 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>.

~~35. Além disso, é importante que os aplicativos antivírus sejam atualizados quando necessário e que sejam instaladas regularmente as atualizações para última versão e as correções de segurança (*patches*[19]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.~~

~~36.~~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 es~~t~~a operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como ~~por exemplo,~~ inventariá-los, cifrar os dados e armazená-los em locais seguros.

~~37.~~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*).

~~38. Em relação aos dispositivos móveis, como celulares e *laptops*, caso seu uso seja necessário para fins institucionais, sugere-se que estejam sujeitos, se possível, aos mesmos procedimentos de controle de acesso que os outros equipamentos de TI, como o uso da autenticação de dois multi-fatores para acesso aos dispositivos e sistemas de informação da organização, além de serem guardados em locais seguros quando não estiverem em uso. Caso não seja possível implementar essas medidas de segurança equivalentes às da organização, recomenda-se que taisesses dispositivos não sejam utilizados para esses fins. institucionais.~~

~~Nesste sentido, 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, como 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.~~

~~39. 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 vazamento de dados.~~

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 ~~sobrescrever~~ formatar ~~todos os dados~~essas mídias 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.

~~40.~~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.

[19] ~~Programa de computador criado para atualizar ou corrigir um *software* de forma a corrigir vulnerabilidades ou falhas.~~

41. 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 um registro da destruição que for realizada.

4.2.3 Segurança no uso de dispositivos móveis

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.

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 vazamento de dados.

34.2.34 Segurança das comunicações[20]

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 dee prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

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

- Para isto, pode-ser-ser instaladoinstalar e mantertido um sistema de *firewall*[21], que consiste, por exemplo, namonitore, detecte e bloqueie ameaças, impedindo restrição de conexões entrea redes não confiáveis. Caso serviços web sejam utilizados, sugere-se o uso de *firewalls* de aplicação *web* (Web Application Firewall – WAF) e quaisquer componentes do sistem.a.
- Proteger serviços de e-mail, Adicionalmente convém considerar o utilizandoso antivírus integrados, de ferramentas *anti-spam* e ,adotar filtros de e-mail;
  - , integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

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

[21] 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.

É importante, ainda, na implementação desses 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.

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.

34.2.453 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*[22]) lançadas pelo desenvolvedor do sistema operacional e aplicativos.

42. .

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.

43.58. 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.

44. 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.

45. Por fim, para manter sistemas e aplicativos seguros, é importante que os agentes se certifiquem que todos os componentes do sistema estejam protegidos de vulnerabilidades, instalando *patches* de segurança disponibilizados pelos fornecedores.

4.2.4 Segurança das comunicações

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

[22] Programa de computador criado para atualizar ou corrigir um *software* de forma a corrigir vulnerabilidades ou falhas.

qualquer negócio se houver troca de *links* maliciosos ou se o usuário receber algum arquivo infectado.

Sobre o assunto, destaca-se a relevância de se utilizar somente 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 e prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

Além disso, sugere-se que o tráfego de rede seja gerenciado. Para isto, pode ser sejaser

instalado e mantido um sistema de *firewall*, que consiste, por exemplo, na restrição de conexões entre redes não confiáveis e quaisquer componentes do sistema. Adicionalmente convém considerar o uso de ferramenta *anti-spam*, adotar filtros de e-mail, integrar o antivírus ao sistema de e-mail ou fazer uso de *Web Application Firewall* (WAF – Filtro de Aplicação).

É importante, ainda, na implementação desses 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.

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.

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.

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

Nesse sentido, 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.

Tais instrumentos poderiam 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.

43.3.2.3 Segurança nMedidas 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.

46. 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 pessoaisvazamento de dados.

62. As medidas sugeridas nessa seção valem tanto para dispositivos móveis de propriedade institucional quanto os pessoais.

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

1. As medidas sugeridas nessa seção valem tanto para dispositivos móveis de propriedade institucional quanto os pessoais. Caso não seja possível implementar medidas de segurança equivalentes às da organização, recomenda-se que dispositivos móveis pessoais não sejam utilizados para esses fins.

4.3.43. Medidas relacionadas ao serviço em nuvem

47.63. 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”).

48.64. 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.

49.65. 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.

50.66. 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[23] com o provedor do serviço em nuvem, contemplando a segurança dos dados armazenados.

51.67. 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 de dois multi fatores, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

5. GERENCIAMENTO DE CONTRATOS

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.
Nesse sentido, 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.
Tais instrumentos poderiam 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.

4565. CONSIDERAÇÕES FINAIS

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

53.70. Neste Gguia, foram apresentadas medidas de segurança de natureza organizacionaladministrativas, que envolvem a política de segurança da informação relacionada a dados pessoais e a segurança em recursos humanos; e medidas técnicas, que tratam, entre

[23] Em inglês, *Service Level Agreement* (SLA).

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 organizacionaladministrativa), tendo em vista a frequência com que esses serviços são utilizados por empresas agentes de tratamento de pequeno porte.

54.71. Espera-se que essas medidas estabeleçam um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, 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.

56. REFERÊNCIAS

CI Security - https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/;

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-

Código de campo alterado

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.

NIC.br. – http://https://nic.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras

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.

ABNT. Norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

Código de campo alterado

ABNT. Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ABNT. Norma ABNT NBR ISO/IEC 27018: 2021, Tecnologia da informação — Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP.

ABNT. Norma ABNT NBR ISO/IEC27005:2019, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT. Norma ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem.

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./05/2021.

NIST - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf;

NIC.br - http://https:/nic.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileir

Berkeley ISO https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware;

Security Boulevard - https://securityboulevard.com/2021/01/privilege-abuse-dont-let-employee-access-level-up/;

CI Security - https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/;

HISCOX - https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf;

Microsoft - https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware;

NCSC.uk - https://www.ncsc.gov.uk/guidance/phishing;

US HHS Office ;

AWS https://aws.amazon.com/it/blogs/security/ransomware-mitigation-top-5-protections-and-recovery-preparation-actions/

Código de campo alterado

Código de campo alterado

Código de campo alterado

Código de campo alterado

Código de campo alterado

Código de campo alterado

Código de campo alterado

Código de campo alterado

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (Simplificada)

(MODELO)

FINALIDADE

Estabelecer os aspectos de segurança da informação a serem seguidos pela (organização).

2. OBJETIVOS

A presente Política de Segurança da Informação possui os seguintes objetivos:

- elevar o nível de segurança dos sistemas e dos processos;

- promover, para todos os integrantes, a cultura de segurança da informação; e

- elevar a proteção dos dados pessoais tratados pela (organização).

3. MEDIDAS ADMINISTRATIVAS

Com o fim de viabilizar a presente Política, a (organização) adotará as seguintes medidas administrativas:

3.1. a Chefia (ou similar) designará um funcionário para revisar periodicamente[24]elaborar a PSI;

3.2. a Chefia (ou similar) apreciará e aprovará a PSI, devendo divulgá-la a todos os funcionários;

3.3. a Chefia (ou similar), caso julgue necessário complementar as orientações da PSI, poderá buscar orientações junto a outras normas e metodologias de segurança da informação, reconhecidas no mercado; e

3.4. a Chefia promoverá, mensalmenteperiodicamente[25], eventos de conscientização para todos os funcionários.

4. MEDIDAS TÉCNICAS

4.1. Controles de acesso

- protocolo de autenticação[26]: os logins deverão ter no máximo (x)6 caracteres alfabéticos e as senhas deverão ter (x)10 caracteres alfanuméricos. Para acesso a sistemas que contenham dados pessoais, deve ser utilizada autenticação de dois fatores, por SMS/e-mail.

[24] É importante que se estabeleça o período, por exemplo, anualmente.
[25] É importante que se estabeleça o período, por exemplo bimestralmente.
[26] É importante fazer referência para qual sistema foi definido o controle de acesso e o número de caracteres para logins e senhas

- protocolo de autorização: o administrador da rede (ou do sistema) deverá conceder autorização de acesso aos funcionários, de acordo com sua "necessidade de conhecer".

- protocolo de auditoria: as atividades dos funcionários na rede corporativa devem ser registradas, por meio de ferramenta específica.

4.2. Backup

Deve ser realizado backup completo dos dados organizacionais e pessoais, de 10 em dias 10 diasperiodicamente[27], e esse backup deve ficar na sala (em local distinto do sistema original).

4.3. Antivírus

Os sistemas e redes devem ter antivírus original, atualizado e com varreduras programadas periodicamentede 10 em 10 dias.[28]

4.4. Sistema Operacional e Software de uso contínuo

O sistema operacional e os softwares de uso contínuo, como o de escritório, devem ser atualizados sempre que possível.

4.5. Firewall

Deve ser implementado firewall pra proteção dos sistemas computacionais.

5. PROCEDIMENTOS

5.1. Login e Senha

Devem ser trocados a cada 4 meses e memorizadas;periodicamente[29] e não devem ser compartilhadas.

As senhas devem ser comportas de no mínimo (X)[30] caracteres, alfanuméricas, com letras maiúsculas e minúsculas.

5.2. Coleta de dados pessoais

Devem ser coletados somente os dados pessoais estritamente necessários ao atendimento da finalidade pretendida.

5.3. Dados pessoais sensíveis

Devem ser armazenados e trafegados, preferencialmente, criptografados.

[27] É importante que se estabeleça o período, por exemplo, a cada 10 dias.
[28] É importante que se estabeleça o período, por exemplo, a cada 10 dias.
[29] É importante que se estabeleça o período, por exemplo, bimestralmente.
[30] Trata-se de exemplo de como definir a senha.

~~5.4. Estação de Trabalho~~

~~Ao deixar a estação de trabalho, o funcionário deve realizar o log off.~~

~~5.5. Armazenamento em mídias externas~~

~~Não devem ser armazenados dados pessoais em dispositivos de armazenamento externo, como HDs e pen drives. Caso tenham de ser armazenados nessas mídias, esses dados devem ser criptografados.~~

~~5.6. Dispositivos móveis corporativos~~

~~Devem ser submetidos às mesmas regras de controle de acesso de computadores tipo desk top. Caso não seja possível fazê-lo, não devem ser utilizados.~~

~~5.7. Dispositivos móveis pessoais~~

~~Devem ser submetidos às mesmas regras de controle de acesso de computadores tipo desk topcorporativos, inclusive por meio de Termo de Compromisso por parte do usuário. Caso não seja possível fazê-lo, não devem ser utilizados para fins institucionais.~~

~~5.8. Descarte de mídias~~

~~Antes de serem descartadas, as mídias que contêêm dados pessoais devem ser formatadas. Aquelas que não podem sofrer formatação, como CDs e DVDs, devem ser destruídas.~~

~~5.9. Aplicativos de Mensageria~~

~~Devem somente ser utilizados aqueles aplicativos com recursos criptográficos na transmissão das mensagens. Deve, ainda, ser evitada a transmissão de dados pessoais, especialmente os sensíveis, assim como também deve ser evitada a abertura de links desconhecidos..~~

~~5.10. Senhas padrão de firewall e de modens~~

~~As senhas padrão de firewall e de modens, que vêm dos fabricantes, devem ser trocadas no momento da configuração desses dispositivos, para dificultar a invasão e o comprometimento desses meios.~~

~~5.11. Para serviços em Nuvem~~

~~- Devem ser implementados os mesmos controles de acesso utilizados para os computadores e para os dispositivos móveis corporativos.~~

~~- Devem ser incluídas cláusulas de segurança com relação aos dados armazenados, especialmente com relação aos dados pessoais.~~

~~- Devem ser realizadas avaliações periódicas do serviço, preferencialmente de 30 em 30 dias, para verificar se atende aos requisitos de segurança estabelecidos em contrato.~~

~~5.12. Segurança Física~~

~~- O local de armazenamento dos dados pessoais deverá permanecer trancado. O acesso a esse local dependerá de autorização do responsável (ou similar).~~

~~(Caso possível, poderão ser previstas outras medidas de segurança física, como instalação de câmeras, controle de acesso eletrônico à organização etc).~~

~~6. DISPOSIÇÕES GERAIS~~

~~- A presente PSI, após aprovada pela Chefia (ou similar) entrará em vigor imediatamente.~~

~~Casos não tratados nesta PSI serão decididos pela Chefia (ou similar).~~

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

SETEMBRO DE 2021

Presidente da República

Jair Messias Bolsonaro

Diretor-Presidente

Waldemar Gonçalves Ortunho Júnior

Diretores

Arthur Pereira Sabbat

Joacil Basílio Rael

Miriam Wimmer

Nairane Farias Rabelo Leitão

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

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 porte1, 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.

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

[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.

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.

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

[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] ANPD. Comunicação de incidentes de segurança. 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.

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 em 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 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 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.

[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/>.

[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.

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 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.

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.

[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>.

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.

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.

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

[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.

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

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 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 estabeleçam um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, 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.

CHECKLIST DE MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Estabelecer uma política de segurança da informação simplificada, que estabeleça 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 e uso de antivírus. ☐
- Realizar revisões periódicas da política de segurança da informação. ☐
- Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais. ☐

CONSCIENTIZAÇÃO E TREINAMENTO

- Realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD. ☐
- 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. ☐

CONSCIENTIZAÇÃO E TREINAMENTO

- Informar os funcionários sobre:
  - 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. ☐

- Criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas. ☐

GERENCIAMENTO DE CONTRATOS

- Estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como: ☐
  - 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.

- Assinar termos de confidencialidade (non-disclosure agreement - NDA) com os funcionários da empresa. ☐

CONTROLE DE ACESSO

- Implementar 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. ☐

- Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade. ☐

- Implementar um adequado gerenciamento de senhas, estabelecendo controles tais como: ☐
  - evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos;
  - utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos;
  - não reutilizar senhas.

- Proibir o compartilhamento de contas ou de senhas entre funcionários. ☐

- Aplicar o princípio do menor privilégio (need to know). ☐

- Utilizar a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais. ☐

- Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores). ☐

SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

- Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados. ☐
- Implementar soluções de pseudonimização, como por exemplo, a criptografia, para cifrar dados pessoais. ☐
- Orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho. ☐
- Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos. ☐
- Inventariar e cifrar dados de dispositivos externos e armazena-los em locais seguros. ☐
- Realizar backups offline, periódicos e armazená-los de forma segura. ☐
- Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas. ☐
- Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte). ☐

SEGURANÇA DAS COMUNICAÇÕES

- Utilizar conexões cifradas *(TLS/HTTPS)* ou aplicativos com criptografia fim-a- fim para serviços de comunicação. ☐
- Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall *(WAF – Filtro de Aplicação)*. ☐
- Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e, integrar o antivírus ao sistema de e-mail. ☐
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas. ☐

GERENCIAMENTO DE VULNERABILIDADES

- Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores). ☐
- Adotar e atualizar periodicamente softwares antivírus e antimalwares. ☐
- Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados. ☐

DISPOSITIVOS MÓVEIS

- Utilizar técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops. ☐
- Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível. ☐
- Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis. ☐

SERVIÇOS EM NUVEM

- Realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados. ☐
- Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos. ☐
- Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado. ☐
- Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais. ☐

ANPD
Autoridade Nacional de Proteção de Dados

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados

Brasília, 20 de setembro de 2021.

SOLICITAÇÃO DE ABERTURA DE CIRCUITO DELIBERATIVO

Encaminho os autos do processo nº 00261.000821/2021-16 a essa Secretaria-Geral para adoção das providências cabíveis para submissão desta matéria à deliberação do Conselho Diretor por meio de Circuito Deliberativo.

Dados para decisão:

Período de Circuito Deliberativo	Início: 20/09/2021	Fim: 20/10/2021
Natureza da matéria:	Finalística	
Interessados:	ANPD	
Assunto:	Guia orientativo sobre segurança da informação para agentes de pequeno porte	
Dados da Análise:	VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (2892319)	
Conclusão Análise/Voto	**Aprovo** a publicação do guia orientativo sobre segurança, conforme descrito no voto, documento SEI nº 2892319	

Documento assinado eletronicamente por **Nairane Farias Rabelo Leitão**, **Diretor(a)**, em 20/09/2021, às 10:33, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2893363** e o código CRC **4AFD3726** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Brasília, 21 de setembro de 2021.

DESPACHO DECISÓRIO Nº 38/2021/SG/ANPD

Processo nº 00261.000821/2021-16

Interessado: Conselho Diretor

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL D PROTEÇÃO DE DADOS, no uso de suas atribuições legais e regulamentares, em especial a disposta no art. 6°, §2°, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do Processo em epígrafe, decide aprovar a abertura de Circuito Deliberativo n° 11/2021 nos termos do Documento Solicitação de Abertura do Circuito Deliberativo (2893363).

Encaminhe-se os autos à Secretaria-Geral para acompanhamento.

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 21/09/2021, às 15:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2897270** e o código CRC **1382E033** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Brasília, 21 de setembro de 2021.

PAUTA DE CIRCUITO DELIBERATIVO Nº 11/2021

Processo nº: 00261.000821/2021-16
Interessado: Autoridade Nacional de Proteção de Dados

Período de Circuito Deliberativo	Início: 21/09/2021	Fim: 21/10/2021
Natureza da matéria:	Finalística	
Assunto:	Guia orientativo sobre segurança da informação para agentes de pequeno porte	
Conselheiro (a) Relator(a)	Nairane Farias Rabelo Leitão	
Presidente	Waldemar Gonçalves Ortunho Junior	

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 21/09/2021, às 15:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2897282** e o código CRC **34F709F7** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA

PR/PROTOCOLO/ANPD/DIR/AS/ANPD

VOTO Nº 15/2021/ANPD/AS/DIR/ANPD/PROTOCOLO/PR

PROCESSO Nº 00261.000821/2021-16

INTERESSADO: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

ASSUNTO: Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

VOTO EM CIRCUITO DELIBERATIVO Nº 11/2021

DIRETOR ARTHUR PEREIRA SABBAT

Caso o prazo do Circuito Deliberativo seja inferior a 7 dias, nos termos do § 1º do art. 41 do Regimento Interno:	
	Concordo com a redução do prazo
	Não concordo com a redução do prazo
X	**Não aplicável à hipótese**

Voto no Circuito Deliberativo:	
X	**Acompanho a Relatora (Voto nº 14/2021/ANPD/JR/DIR/ANPD/PROTOCOLO/PR, SEI nº 2892319)**

Não acompanho a Relatora, nos termos do Voto indicado a seguir:

Documento assinado eletronicamente por **Arthur Pereira Sabbat**, **Diretor(a)**, em 21/09/2021, às 18:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2898542** e o código CRC **43861C8C** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2898542

PRESIDÊNCIA DA REPÚBLICA

PR/PROTOCOLO/ANPD/SG/ANPD

VOTO Nº 12/2021/ANPD/JR/DIR/ANPD/PROTOCOLO/PR

PROCESSO Nº 00261.000821/2021-16

INTERESSADO: Autoridade Nacional de Proteção de Dados

ASSUNTO: Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte

VOTO EM CIRCUITO DELIBERATIVO N. 12/2021 -

DIRETOR JOACIL RAEL

Voto no Circuito Deliberativo:	
X	**Acompanho a Relatora (VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR, SEI nº 2892319)**
	Não acompanho a Relatora, nos termos do Voto indicado a seguir:

Documento assinado eletronicamente por **Joacil Basilio Rael**, **Diretor(a)**, em 21/09/2021, às 16:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2898586** e o código CRC **864D2E71** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA

PR/PROTOCOLO/ANPD/SG/ANPD

VOTO Nº 13/2021/ANPD/MW/DIR/ANPD/PROTOCOLO/PR

PROCESSO Nº 00261.000821/2021-16

INTERESSADO: Autoridade Nacional de Proteção de Dados

ASSUNTO: Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

VOTO EM CIRCUITO DELIBERATIVO N. 13/2021 -

DIRETORA MIRIAM WIMMER

Voto no Circuito Deliberativo:	
X	**Acompanho a Relatora (Voto nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR, SEI nº 2892319)**
	Não acompanho o Relator, nos termos do Voto indicado a seguir:

Documento assinado eletronicamente por **Miriam Wimmer**, **Diretor(a)**, em 28/09/2021, às 15:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2900329** e o código CRC **A4169F3E** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2900329

PRESIDÊNCIA DA REPÚBLICA

PR/PROTOCOLO/ANPD/SG/ANPD

VOTO Nº 12/2021/ANPD/GABPR/ANPD/PROTOCOLO/PR

PROCESSO Nº 00261.000821/2021-16

INTERESSADO: Autoridade Nacional de Proteção de Dados

ASSUNTO: Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

VOTO EM CIRCUITO DELIBERATIVO N. 13/2021 -

DIRETOR PRESIDENTE WALDEMAR GONÇALVES

Voto no Circuito Deliberativo:	
X	**Acompanho a Relatora (Voto nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR, SEI nº 2892319)**
	Não acompanho o Relator, nos termos do Voto indicado a seguir:

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 01/10/2021, às 15:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2924654** e o código CRC **F660C0E6** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2924654

PRESIDÊNCIA DA REPÚBLICA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

ATA DE CIRCUITO DELIBERATIVO DO CONSELHO DIRETOR Nº 11/2021

Período do Circuito Deliberativo:	21/09/2021	21/10/2021
Natureza da Matéria:	Finalística	
Assunto:	Guia orientativo sobre segurança da informação para agentes de pequeno porte	
Conselheiro Relator:	Nairane Farias Rabelo Leitão	
Voto do Conselheiro Relator:	VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (2892319)	
Presidente:	Waldemar Gonçalves Ortunho Junior	

Decisão do Circuito Deliberativo		
Resumo dos votos	Acompanha o relator	4
	Não acompanha o relator	0
	Levar à Reunião Deliberativa	0

Votos proferidos no Circuito Deliberativo	
Diretor	Nairane Farias Rabelo Leitão
Voto	VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (2892319)
Diretor	Waldemar Gonçalves Ortunho Junior

Voto	VOTO Nº 12/2021/ANPD/GABPR/ANPD/PROTOCOLO/PR (2924654)
Diretor	Joacil Basilio Rael
Voto	VOTO Nº 12/2021/ANPD/JR/DIR/ANPD/PROTOCOLO/PR (2898586)
Diretor	Miriam Wimmer
Voto	VOTO Nº 13/2021/ANPD/MW/DIR/ANPD/PROTOCOLO/PR (2900329)
Diretor	Arthur Pereira Sabbat
Voto	VOTO Nº 15/2021/ANPD/AS/DIR/ANPD/PROTOCOLO/PR (2898542)

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 01/10/2021, às 17:20, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2926671** e o código CRC **BB696FC7** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2926671

PRESIDÊNCIA DA REPÚBLICA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Secretaria-Geral

Brasília, 01 de outubro de 2021.

Certidão de Julgamento

Certifico que o presente processo foi julgado conforme abaixo:

Processo	00261.000821/2021-16
Data da Sessão	01/10/2021 - Circuito Deliberativo nº 11/2021
Colegiado	Conselho Diretor
Relator	Nairane Farias Rabelo Leitão
Dispositivo	O Colegiado Conselho Diretor, por unanimidade, decidiu aprovar a proposta, nos termos do voto do relator - VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (2892319)

NUBIA AUGUSTO DE SOUSA ROCHA

Secretária-Geral

Documento assinado eletronicamente por **Nubia Augusto de Sousa Rocha**, **Secretária-Geral**, em 01/10/2021, às 17:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Secretaria-Geral

Brasília, 04 de outubro de 2021.

À CGN

Assunto: **Publicação de Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**

Senhora Coordenadora-Geral,

1. Em atenção à Nota Técnica n° 27 2834720, informo que o Circuito Deliberativo n° 11/2021 foi encerrado nos termos da Ata 2926671. Informa-se que o guia em tela foi pulicado e no site da ANPD (acesso à matéria) e também está publicado na aba de Documentos e Publicações.

2. Diante do exporto, encaminho os autos para ciência e providências subsequentes.

Núbia Augusto de Sousa Rocha
Secretária-Geral

Documento assinado eletronicamente por **Nubia Augusto de Sousa Rocha**, **Secretária-Geral**, em 04/10/2021, às 16:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2929927** e o código CRC **7BBCCE4E** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Diretora Nairane Farias Rabelo Leitão

Brasília, 07 de outubro de 2021.

À CGTP

C/C Secretaria-Geral

Assunto: **Elaboração de modelo de Política de Segurança da Informação**

Senhor Coordenador-Geral,

1. Tendo em vista as competências desta Autoridade, exaradas nos arts. 55-J, I, VI e XVIII da LGPD, e em atenção ao disposto no parágrafo n. 4.27 do VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (SEI n. 2892319), este Gabinete encaminha o presente processo para providências por parte da Coordenação-Geral de Tecnologia e Pesquisa.

2. As providências a serem tomadas pela Coordenação-Geral de Tecnologia e Pesquisa consistem em estudos e elaboração de modelo de Política de Segurança da Informação direcionado aos agentes de tratamento de pequeno porte, conforme suas competências atribuídas pelo art. 18, XVI do regimento interno desta Autoridade (PORTARIA Nº 1, DE 8 DE MARÇO DE 2021), ouvida a Coordenação-Geral de Normatização, no que couber.

3. Após a elaboração dos documentos, estes deverão ser remetidos à apreciação do Conselho Diretor da ANPD, por meio de distribuição para deliberação, nos termos do art. 40 do regimento interno.

NAIRANE FARIAS RABELO LEITÃO
Diretora da Autoridade Nacional de Proteção de Dados

Documento assinado eletronicamente por **Nairane Farias Rabelo Leitão**,

Diretor(a), em 03/11/2021, às 07:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **2937141** e o código CRC **887E8F33** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 2937141

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Tecnologia e Pesquisa

Brasília, 03 de fevereiro de 2022.

À Coordenação-Geral de Normatização

Assunto: **Minuta da Política de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**

1. Nos termos do Despacho da Diretora Nairane Farias Rabelo Leitão (2937141), encaminho para manifestação a essa Coordenação-Geral de Normatização os estudos e a minuta de modelo de Política de Segurança da Informação direcionado aos agentes de tratamento de pequeno porte.

2. Após, retorne-se os autos para as devidas análises e alterações na minuta por parte desta CGTP e subsequente encaminhamento ao Conselho Diretor.

MARCELO SANTIAGO GUEDES
Coordenador-Geral de Tecnologia e Pesquisa

Documento assinado eletronicamente por **Marcelo Santiago Guedes**, **Coordenador(a)-Geral**, em 03/02/2022, às 15:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **3166017** e o código CRC **398011A7** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Projeto para elaboração de Modelo de Política de Segurança da Informação para Agentes de Pequeno Porte

1. ORIGEM

Coordenação-Geral de Tecnologia e Pesquisa (CGTP/ANPD).

2. OBJETIVO

2.1. Executar estudos e elaborar modelo de Política de Segurança da Informação – PSI – para Agentes de Pequeno Porte – EPP – em atendimento ao despacho 2937141 da Diretora Nairane Farias Rabelo Leitão, constante no processo SEI nº 00261.000821/2021-16 (Anexo-01).

3. JUSTIFICATIVA

3.1 Justifica-se este projeto de construção de modelo de política de segurança da informação para agentes de pequeno porte em função de solicitação da Diretoria da ANPD registrada no processo SEI nº 00261.000821/2021-16 (documento nº 2937141), pelas competências exaradas nos artigos 55-J, I, VI e XVIII da Lei Geral de Proteção de Dados, e também em atenção ao disposto no parágrafo n. 4.27 do VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (documento nº 2892319).

3.2 De acordo com o *Guidance for Information Security Managers* do *Information Security Governance*, as políticas são "declarações de alto nível das intenções, expectativas e direcionamento da administração" e "pode ser considerada a 'constituição' da governança de segurança".

4. RESULTADOS ESPERADOS

4.1 Modelo de Política de Segurança da Informação (PSI) direcionado aos agentes de tratamento de pequeno porte.

5. ETAPAS DE EXECUÇÃO DO PROJETO / CONTROLE DE VERSÕES

5.1 As etapas de execução do projeto de curta duração estão descritas na tabela abaixo:

5.1.1 Histórico

Data	Descrição
25-11-2021	Apresentação da demanda para produção da PSI para EPP.
26-11-2021	Reunião para alinhamento dos detalhes e prazo de entrega.
27-11-2021	Início das pesquisas e levantamentos de normas existentes.
03-12-2021	Entrega da primeira versão, apresentação para equipe CGTP e revisão.
17-12-2021	Revisão do texto pela Diretora Nairane Farias Rabelo Leitão.
22-12-2021	Ajuste do texto sobre a revisão apresentada.

5.1.2 Controle de versões deste documento

Data Reunião	Versão nº	Descrição
03-12-2021	01	Alterações sugeridas para a versão 02: (1) incluir uma seção referendado o Guia ANPD para Agentes de Pequeno Porte; (2) retirar do modelo a questão relacionada à propriedade intelectual; (3) pesquisar a legislação trabalhista além das questões penais/cívicas; (4) incluir no glossário os termos já utilizados pelo guia do GSI; (5) trocar a nomenclatura da ISO para a da ANPD quando em referência aos conceitos de documento sensível, "alto risco", dado sensível, etc;
17-12-2021	03	Diversas correções textuais a partir da revisão apresentada.
22-12-2021	04	Atualização e ajustes no texto. Troca de ABNT para ISO; troca de "empresa" para "agente".

6. EQUIPE DO PROJETO

6.1 A demanda está direcionada ao servidor da CGPT/ANPD João Batista Ribas de Moura e versões revisadas por toda equipe CGTP.

7. METODOLOGIA DE PESQUISA E REFERENCIAL UTILIZADO

7.1 Para elaboração do Modelo de PSI a agentes de pequeno porte, foram pesquisados os principais referenciais normativos nacionais e internacionais e apresentados nesta sequência. Cabe destacar que normalmente a política é o primeiro documento a surgir em organizações visto apresentar os princípios e diretrizes que serão basilares à construção dos demais artefatos - guias procedimentais, checklists, controles, etc -. Para ISACA, "as políticas fornecem orientações sobre comportamentos e ações aceitáveis e inaceitáveis para uma organização"[1]. Os padrões e procedimentos suportam os requisitos definidos inicialmente pelas políticas.

7.2 **Norma ISO/IEC 27001** – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos [1], traz requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). De acordo com a norma 27001:

7.2.1 a política de segurança (PSI) deve estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para todas as partes interessadas.

7.2.2 as pessoas que realizam trabalho sob controle da organização devem estar cientes da existência da política de segurança da informação;

7.2.3 a PSI deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

7.2.4 a PSI deve apoiar a segurança da informação (SI) para gerenciar riscos decorrentes do uso de dispositivos móveis;

7.2.5 deve ser solicitado aos funcionários e partes externas que pratiquem a SI de acordo com o estabelecido nas políticas e procedimentos da organização; e

7.2.6 todos os funcionários devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

[1] Manual *Certified in Risk and Information Systems Control* 6ª Ed., ISACA,

7.3 **Norma ISO/IEC 27002** – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação é um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. De acordo com a norma 27002:

7.3.1 Convém que a PSI contemple requisitos oriundos de:

- Estratégia do negócio;
- Regulamentações, legislação e contratos;
- Ambientes de ameaça da SI, atual e futuro;
- Definição de SI, objetivos e princípios para orientar todas as atividades relativas à SI;
- Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da SI para os papéis definidos; e
- Processos para o tratamento dos desvios e exceções.

7.3.2 No nível mais baixo, convém que a PSI seja apoiada por política específica do tema, que exige implementação de controles de segurança e que seja estruturada para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos. São exemplos de tais temas de política:

a) controle de acesso;
b) classificação e tratamento da informação;
c) segurança física e do ambiente;
d) tópicos orientados aos usuários finais:
    1) uso aceitável dos ativos;
    2) mesa limpa e tela limpa;
    3) transferência de informações;
    4) dispositivos móveis e trabalho remoto; e
    5) restrições sobre o uso e instalação de software.
e) backup;
f) transferência da informação;
g) proteção contra malware;
h) gerenciamento de vulnerabilidades técnicas;
i) controles criptográficos;
j) segurança nas comunicações;
k) proteção e privacidade da informação de identificação pessoal; e
l) relacionamento na cadeia de suprimento.

7.3.3 Considerações para uso de dispositivo móvel:

7.3.3.1 Convém que, ao se utilizar dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas e a política considere:

a) Registros dos dispositivos móveis;
b) Requisitos para a proteção física;
c) Restrições quanto à instalação de software;
d) Requisitos para as versões dos softwares a aplicações de patches;
e) Restrições para conexão aos serviços de informação;
f) Controle de acesso;
g) Técnicas criptográficas;
h) Proteção contra malware;
i) Desativação, bloqueio e exclusão de forma remota;
j) Backups; e
k) Uso dos serviços web e aplicações web.

7.3.4 Considerações para trabalho remoto:

7.3.4.1 Convém que uma política e medidas que apoiem a segurança da informação sejam implementadas para proteger as informações acessadas, processadas, ou armazenadas em locais de trabalho remoto, considerando:

a) a segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;
b) o ambiente físico proposto para o trabalho remoto;
c) os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;
d) o fornecimento de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;
e) a ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;
f) o uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;
g) políticas e procedimentos para prevenir disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;
h) acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), o qual pode ser restringido por lei;
i) acordos de licenciamento de software que podem tonar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou partes externas; e
j) requisitos de firewall e proteção antivírus.

7.3.4.2 Convém que as diretrizes e providências considerem:

a) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto, onde o uso de equipamentos de propriedade particular que não esteja sob controle da organização não seja permitido;
b) uma definição do trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;
c) provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;
d) segurança física;
e) regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;
f) a provisão de suporte e manutenção de hardware e software;
g) a provisão de seguro;
h) os procedimentos para cópias de segurança e continuidade de negócio;
i) auditoria e monitoramento da segurança; e
j) revogação de autoridade e direitos de acesso, e devolução do equipamento quanto as atividades de trabalho remoto encerrarem.

7.3.5 Considerações para segurança em recursos humanos:

7.3.5.1 Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:

a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação;
b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados;
c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas;
d) as responsabilidades dos funcionários ou partes externas pelo tratamento da informação recebida de outras companhias ou partes interessadas; e
e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.

7.3.6 Considerações em relação aos proprietários ou direção da organização:
(...)
c) sejam motivados para cumprir com as políticas de segurança da informação da organização;

(...)
e) cumpram com os termos e condições de trabalho, que incluam a política de segurança da informação da organização e métodos apropriados de trabalho;
(...)

7.2.6.1 É recomendado que a direção demonstre seu apoio às políticas, procedimentos e controles, e aja como tal, de forma exemplar.

7.3.7 Considerações em relação à conscientização, educação e treinamento:

7.3.7.1 Convém quem um programa de conscientização em segurança da informação seja estabelecido e alinhado com a PSI e procedimentos da organização, levando em consideração as informações da organização a serem protegidas e os controles que foram implementados para proteger a informação.

7.3.8 Considerações em relação ao processo disciplinar:

7.3.8.1 Convém que o processo disciplinar também seja usado como uma forma de dissuasão, para evitar que os funcionários e partes externas violem os procedimentos e a PSI, e quaisquer outras violações na segurança da informação.

7.3.9 Considerações sobre proteção contra malware:

7.3.9.1 Convém estabelecer uma política forma proibindo o uso de softwares não autorizados.

7.3.10 Considerações sobre cópias de segurança da informação:

7.3.10.1 Convém que a política de backup seja estabelecida para definir requisitos da organização relativos às cópias de segurança das informações, dos softwares e dos sistemas;

7.3.10.2 Convém que a política de backup defina os requisitos para a proteção e retenção; e

7.3.10.3 Convém que os procedimentos operacionais monitorem a execução dos backups e apontem falhas de backup programado, para garantir a integralidade dos backups, de acordo com a política de backup.

7.3.11 Considerações sobre proteção das informações dos registros de eventos (logs):

7.3.11.1 Alguns registros (log) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência.

7.3.13 Considerações sobre a transferência de informação:

7.3.13.1 Convém que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

7.3.13.2 Convém que políticas, procedimentos e normas para proteger as informações e as mídias em trânsito sejam estabelecidos e mantidos, além de serem referenciados nos mencionados acordos para transferência de informações.

7.3.14 Considerações sobre a cadeia de suprimento:

7.3.14.1 Convém que a organização identifique e exija os controles de SI para tratar, especificamente, do acesso do fornecedor às informações da organização, através de uma política.

7.3.15 Considerações sobre notificação de eventos de segurança da informação:

7.3.15.1 Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade ao notificar qualquer evento de SI o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de SI e do ponto de contato, ao qual os eventos devem ser notificados.

7.3.15.2 Situações a serem consideradas para notificar um evento de segurança da informação incluem:

I) controle de segurança ineficaz;
II) violação da disponibilidade, confidencialidade e integridade da informação;
III) erros humanos;
IV) não conformidade com políticas ou diretrizes;
V) violações de procedimentos de segurança física;
VI) mudanças descontroladas de sistemas;
VII) mau funcionamento de software ou hardware; e
VIII) violação de acesso.

7.3.16 Considerações sobre aprendizagem com incidentes de SI:

7.3.16.1 a avaliação de incidentes de SI pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de futuras ocorrências, ou ser levada em conta no processo de análise crítica da política de segurança.

7.3.17 Considerações sobre análise crítica da segurança da informação:

7.3.17.1 Convém que a análise crítica independente seja iniciada pela direção. Tal análise crítica independente é necessária para assegurar a contínua pertinência, adequação e eficácia do enfoque da organização para gerenciar a SI. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, incluindo a política e os objetivos de controle.

7.3.18 Sobre a conformidade com a PSI e procedimentos de SI:

7.3.18.1 Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de SI.

7.4 **Norma ISO/IEC 27701** – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27702 para gestão da privacidade de informação – Requisitos e diretrizes - é um documento que apresenta requisitos e diretrizes adicionais que permitem a geração de evidências documentais de como a organização lida com o tratamento de Dados Pessoais (DP). De acordo com a norma 27701:

7.4.1 As diretrizes adicionais para implementação da Política de Segurança da Informação, da ABNT 27002, são:

7.4.1.1 Seja para o desenvolvimento de políticas de privacidade separadas, seja para acréscimo de políticas de segurança da informação, convém que a organização produza uma declaração quanto ao apoio e comprometimento para alcançar *compliance* com as regulamentações e legislações de proteção de DP aplicáveis, e com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores etc.), para os quais convém que se especifiquem claramente as responsabilidades entre eles.

7.4.1.2 Para qualquer organização que trate DP, seja um controlador de DP seja um operador de DP, convém que seja considerada a regulamentação e/ou legislação de proteção de DP aplicável, durante o desenvolvimento e a manutenção de políticas de segurança da informação.

7.4.1.3 A norma ABNT 27002 é baseada nas normas ABNT 27001 e 27002 e estende os seus requisitos e diretrizes para considerar, em contemplação à segurança da informação, a proteção da privacidade dos titulares de DP, que podem ser potencialmente afetados pelo tratamento de DP. Isto significa que, onde o termo "segurança da informação" for usado nas normas 27001 ou 27002, o termo "**segurança da informação e privacidade**" se aplica.

7.4 De acordo com o **Infosec Institute**[2] existem cinco elementos em uma política de segurança da informação:

7.4.1 **Propósito**: organizações desenvolvem políticas de segurança por várias razões:

- Para estabelecer uma abordagem geral para a segurança da informação;
- Para detectar e prevenir falhas na segurança da informação;
- Para proteger a reputação da organização no que diz respeito às suas responsabilidades éticas e legais; e
- Para respeitar os direitos dos usuários.

7.4.2 **Escopo**: Uma política de segurança da informação deveria atuar sobre dados, programas, sistemas, infraestrutura de tecnologia, usuários de tecnologia e terceiras partes.

7.4.3 **Objetivos**: Uma organização que pretender desenvolver uma PSI funcional precisa ter objetivos bem definidos em relação à segurança e à estratégia. A gerência deve concordar com esses objetivos porque quaisquer divergências existentes neste contexto podem tornar todo o projeto disfuncional. Idealmente, a redação da política deve ser breve e direta. O texto redundante torna os documentos prolixos ou mesmo ilegíveis. A segurança da informação é considerada como salvaguarda de três objetivos principais: confidencialidade, integridade e disponibilidade.

7.4.4 **Política de autorização e controle de acesso**: Normalmente, uma política de segurança possui um padrão hierárquico onde cada posição com especificações e autorizações são esclarecidas. Por exemplo, um usuário pode ter a necessidade de saber um tipo específico de informação. Portanto, os dados devem ter granularidade suficiente para permitir o acesso autorizado apropriado e nada mais. Trata-se de encontrar o delicado equilíbrio entre permitir o acesso a quem precisa usar os dados como parte de seu trabalho e negá-lo a entidades não autorizadas.

7.4.5 **Classificação dos dados**: Os dados podem ter valores diferentes. Gradações no índice de valor podem impor separação nos procedimentos de manuseio específicos para cada tipo. Um sistema de classificação de informações, portanto, ajudará na proteção de dados que têm uma importância significativa para a organização e deixará de fora informações insignificantes que, de outra forma, sobrecarregariam os recursos da organização.

[2] https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/#gref

7.4.5.1 Uma política de classificação de dados pode organizar todo o conjunto de informações da seguinte forma:

i) **Classe de alto risco**: Dados protegidos por legislação estadual e federal (a Lei de Proteção de Dados, HIPAA, FERPA), bem como financeiros, folha de pagamento e pessoal (requisitos de privacidade) estão incluídos aqui;]

ii) **Classe confidencial**: os dados nesta classe não têm o privilégio de serem protegidos por lei, mas o proprietário dos dados julga que devem ser protegidos contra divulgação não autorizada; e

iii) **Classe pública**: essas informações podem ser distribuídas gratuitamente Os proprietários dos dados devem determinar a classificação dos dados e as medidas exatas que um guardião dos dados precisa tomar para preservar a integridade de acordo com aquele nível.

7.4.5.2 Os proprietários de dados (*data owners*) devem determinar a classificação dos dados e as medidas exatas que o custodiante dos dados precisa executar para preservar a integridade de acordo com determinada classificação.

7.4.6 **Suporte de dados e operações**: Refere-se a parte de uma PSI onde são estipuladas cláusulas referentes a:

- A regulamentação dos mecanismos gerais do sistema responsável pela proteção de dados;
- O backup de dados; e
- O transporte/movimento de dados.

7.4.7 **Conscientização de segurança**: A divulgação da PSI com as equipes é uma etapa crítica. Fazer os colaboradores ler e reconhecer um documento não significa necessariamente que estejam familiarizados e compreendam a nova política. Por outro lado, uma sessão de treinamento envolveria os funcionários de forma a garantiria que eles entendessem os procedimentos e mecanismos em vigor para proteger os dados.

7.4.8 **Responsabilidades, direitos e deveres do pessoal**: Os itens a serem considerados nesta área da PSI geralmente se concentram na responsabilidade das pessoas nomeadas para realizar a implementação, educação, resposta a incidentes, análises de acesso do usuário e atualizações periódicas de uma política de segurança da informação.

7.4.10 **Outros itens que podem ser incluídos em uma política de segurança da informação**: Uma PSI incluir vários itens diferentes que incluem, mas não se limitam a: procedimento de proteção de vírus, procedimento de detecção de intrusão, resposta a incidentes, procedimento de trabalho remoto, diretrizes técnicas, auditoria, requisitos de funcionários, consequências para não conformidade, ações disciplinares, funcionários desligados, segurança física de TI, referências a documentos de apoio e muito mais.

7.5 **National Institute of Standards and Technology (NIST)** publicou o documento *Special Publication (SP) – **NIST SP 800-53** - Security and Privacy Controls for Information Systems and Organizations* sendo considerado padrão de referência para segurança da informação.

7.5.1 De acordo com o documento de referência NIST SP-800 Rev. 5[3], há 20 famílias de controles operacionais, técnicos e gerenciais para garantir a privacidade, integridade e a segurança em sistemas de informação: Acess Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Assessment, Authorization and Monitoring (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environment Protection (PE), Planning (PL), Program Management (PM), Personnel Security (PS), Processing and Transparency (PT), Risk Assessment (RA), System and Services Aquisition (SA), System and Communications Protection (SC), System and Information Integrity (SI), Supply Chain Risk Management (SR).

7.5.2 Muitas organizações optaram por usar os controles NIST SP 800-53 como basilar aos seus controles de segurança e privacidade porque os controles descritos no catálogo são em maioria neutros em termos de política, tecnologia e setor; eles se concentram nas medidas fundamentais necessárias para proteger as informações e a privacidade dos indivíduos em todo o ciclo de vida das informações.

7.5.3 Existem 05 (cinco) princípios-chave na construção de políticas de segurança de acordo com NIST:

1) Políticas necessitam ser escritas. Embora pareça óbvio, muitas organizações falham na documentação de suas próprias políticas de segurança;
2) Devem existir procedimentos descritos para facilitar a implementação de controles associados à política;
3) Políticas devem ser periodicamente revisadas;
4) Políticas devem ser disseminadas na organização porque serão consideradas não efetivas se não direcionarem o comportamento organizacional; e
5) Políticas devem ser gerenciadas a partir de processos definidos: revisão, coordenação, *compliance* etc.

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

7.6 O **Gabinete de Segurança Institucional (GSI)** da Presidência da República traz orientações para Política de Segurança da Informação em sua Instrução Normativa Nº1, de 27 de maio de 2020 que, embora direcionadas aos órgãos e entidades da administração federal, trazem valiosos ensinamentos para todas as organizações.

7.6.1 De acordo com o GSI-PR, a PSI deverá ser composto, no mínimo, pelos seguintes itens[4]:

"**I – escopo**: descreve o objetivo e a abrangência da Política, definindo o limite dentro do qual as ações de segurança da informação serão desenvolvidas no órgão ou na entidade;

II - conceitos e definições: relaciona e descreve os conceitos e definições a serem utilizados na Política do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade, devendo ser utilizadas as definições contidas no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República;

III - princípios: relaciona os princípios que regem a segurança da informação no órgão ou na entidade;

IV - diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:

a) Tratamento da Informação;
b) Segurança Física e do Ambiente;
c) Gestão de Incidentes em Segurança da Informação;
d) Gestão de Ativos;
e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
f) Controles de Acesso;
g) Gestão de Riscos;
h) Gestão de Continuidade; e
i) Auditoria e Conformidade.

V - competências: define as atribuições e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação;

[4] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215

VI - penalidades: estabelece as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto; e

VII - política de atualização: estabelece a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos.

(...)"

7.7 **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte da Autoridade Nacional de Proteção de Dados (ANPD)** define a política de segurança da informação (PSI) como um "conjunto de diretrizes e regras que tem por objetivo o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização".

7.7.1 ANPD diz que "o propósito fundamental da PSI é ser uma ferramenta que apoie a implementação de um processo estruturado de SI adequado a cada organização, considerando seu negócio e seu porte" sugerindo que a política 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.

7.7.2 O Guia da ANPD sugere ações de conscientização e treinamento inclusive para que funcionários sigam as orientações da PSI.

7.7.3 São apresentadas medidas técnicas que tratam, entre outros temas, do controle de acesso aos dados; segurança nos dados armazenados; manutenção de programa de gerenciamento de vulnerabilidades; segurança das comunicações; e serviços em nuvem.

7.7.3 Em complemento ao guia orientativo, a ANPD disponibilizou o "Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte", oferecendo aos Agentes de Tratamento de Pequeno Porte uma visão objetiva e concreta de controles de segurança aplicável a esse contexto.

7.7.4 Considerando essa visão e buscando uma visão harmônica, a elaboração desse modelo de PSI ponderou as proposições contidas nos seguintes documentos:

- a Minuta de Resolução ANPD que aprova o regulamento de aplicação da Lei nº 13.709/2018 para agentes de tratamento de pequeno porte;
- o capítulo de "medidas técnicas" existente no "Guia ANPD Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte"; e
- "Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte".

7.7.5 É preciso observar, contudo, que, na medida em que se crie maturidade em processos de governança de privacidade e proteção de dados, é adequado que processos de gestão de riscos e de gestão da privacidade sejam considerados.

10. REFERENCIAIS BIBLIOGRÁFICO

8. ENCAMINHAMENTO

Brasília, 22 de dezembro de 2021.

À consideração superior,

João Batista Ribas de Moura

De acordo, encaminhe-se ao Conselho Diretor da ANPD,

Marcelo Santiago Guedes
Coordenador-Geral de Tecnologia e Pesquisa

Thiago Guimarães Moraes
Coordenador de Tecnologia e Pesquisa

ANEXO I

MODELO DE POLÍTICA DE SEGURANÇA DA INFORMÇÃO PARA EPP

A Política de Segurança da Informação (PSI) é uma declaração formal da organização manifestando compromisso com a proteção dos dados e informações sob sua responsabilidade devendo estar disponível como informação documentada e comunicada a todos.

Escopo

Os objetivos, princípios e diretrizes aqui estabelecidos devem ser observados por todos os empregados, colaboradores, fornecedores e prestadores de serviços que tenham acesso aos dados, informações e recursos tecnológicos desta organização para prover segurança da informação e redução do risco a níveis aceitáveis, buscando continuamente a disponibilidade, a integridade e confidencialidade aos objetivos estratégicos.

Conceitos e Definições[5]

I – ameaça: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;
II – ativo: tudo que tenha valor para a organização, material ou não;
III – ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
IV – autenticidade: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
V- backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;
VI – confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
VII – consentimento:
computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);
VIII – custodiante da informação:
IX – disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
X- firewall: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;
XI - hardware: parte física do computador ou de seus componentes eletrônicos;
XII - cloud computing: ver nuvem – computação;

[5] https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370

XIII – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XIV – malware: software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits;
XV - multi-fator (MFA) - autenticação: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital,tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);
XVI – phishing: técnica de envio de e-mail falso para enganar usuários com informações aparentemente corretas e direcioná-los a ambientes criados para capturar informações e senhas;
XVII - pseudonimização: 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;
XVIII - ransomware: tipo de malware que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados;
XIX – segurança orgânica: conjunto de medidas passivas, com o objetivo de prevenir e, até mesmo, obstruir as ações que visem o comprometimento ou a quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;
XX – serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;
XXI – sistema de proteção física: sistema composto por pessoas, equipamentos e procedimentos, para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ação humana não autorizada, conforme gestão da segurança física e ambiental; e software
XXII – tratamento: 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.

<u>Princípios</u>

As ações de segurança da informação são norteadas pela ética profissional e princípios:

I – disponibilidade, integridade, confidencialidade das informações;
II – continuidade dos processos e serviços essenciais para o funcionamento da organização; e
III – responsabilidade dos colaboradores, constituída no dever de conhecer e respeitar esta Política de Segurança da Informação.

<u>Diretrizes Gerais</u>

Recomenda-se que a PSI apresente os seguintes temas específicos que repercutirão na implementação de controles de segurança proporcionais:

i) Copias de segurança (backup);

ii) Controle de acesso;
iii) Atualização de software e gerenciamento de vulnerabilidades;
iv) Uso de correio eletrônico;
v) Proteção contra malware;
vi) Gerenciamento de contratos e aquisições;
vii) Segurança das comunicações;
viii) Dispositivos móveis e teletrabalho;
ix) Serviços em nuvem;
x) Conscientização e treinamento; e
xi) Segurança dos dados armazenados.

Considerações sobre Cópia de Segurança (backup):

Devem ser definidas rotinas para realização de cópias de segurança de dados e softwares em períodos regulares e proporcionais à quantidade de novos dados gerados diariamente. Deve ser levado em consideração a segurança dos dados copiados – criptografia e armazenamento em local seguro – além do tempo de retenção.
Devem ser realizados registros para monitoramento e garantia da correta execução das cópias de segurança nos intervalos de tempo programados.

Considerações sobre Controle de Acesso:

Devem ser estabelecidas medidas técnicas que garantam acesso aos dados e informações somente às pessoas autorizadas para execução das atividades laborais abrangendo processos de concessão, revisão e suspensão de acessos aos usuários.

Recomenda-se ativação de recurso técnico para bloqueio de tela e proteção por senha, token ou mecanismo de autenticação semelhante para acesso aos sistemas computacionais.

O acesso aos sistemas e bases de dados devem possuir autenticação multifator.

Usuários afastados ou desligados da empresa devem ter sua autorização de acesso imediatamente cancelada.

Considerações sobre atualização de software e gerenciamento de vulnerabilidades:

Devem ser criadas rotinas e controles para verificação de novas versões de softwares (*patches*) corrigindo falhas detectadas pelos fabricantes.

É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas à instância superior assim que identificadas.

A instalação de software não autorizado em dispositivos computadorizados pode introduzir vulnerabilidades e causar vazamento de informações, perda de integridade ou outros incidentes de segurança da informação.

Considerações sobre uso de correio eletrônico:

O correio eletrônico deverá ser utilizado somente para fins laborais. Os colaboradores devem ser conscientizados quanto ao risco de *phishing*,

Considerações sobre proteção contra malware:

Devem ser utilizados softwares antivírus e antimalwares com controles de atualização e registro de varreduras.

Considerações sobre gerenciamento de contratos e aquisições:

Devem existir cláusulas contratuais que:

i) determinem a observância desta Política;
ii) garantam compromisso com o sigilo das informações organizacionais a que tenham acesso; e
iii) garantam, quando for o caso, a confidencialidade, integridade e disponibilidade dos dados hospedados em seus sistemas.

Considerações sobre segurança das comunicações:

Devem ser adotados controles e medidas técnicas para garantir a confidencialidade das informações trafegadas interna ou externamente.

Convém que informações do negócio – sensíveis ou críticas – em papel ou mídia sejam guardadas em local seguro quando não em uso.

Recomenda-se informativos de conscientização para que documentos contendo informação sensível sejam removidos da impressora imediatamente.

Considerações sobre dispositivos móveis e teletrabalho:

Convém os dispositivos móveis utilizados e relacionados às atividades da EPP estejam submetidos a controles que garantam:

a) Registro dos dispositivos móveis;
b) Restrições à instalação de softwares;
c) Acompanhamento para aplicação de patches críticos;
d) Controle de acesso;
e) Proteção contra malware;
f) Backups;
g) Segurança física no ambiente doméstico; e
h) Requisitos de segurança nas comunicações sobre, por exemplo, uso de VPN para acesso remoto aos sistemas organizacionais.

Considerações sobre serviços em nuvem:

É de responsabilidade do(s) proprietário(s) a divulgação desta Política.

Todos os colaboradores são responsáveis pela segurança dos ativos de informação que esteja sob sua responsabilidade.

Considerações sobre Conscientização, Educação e Treinamento de colaboradores:

Devem ser estabelecidos momentos – reuniões presenciais, palestra, e-mails, cartazes etc. – objetivando a divulgação deste política e conscientização em segurança da informação levando-se em consideração o porte da organização e a quantidade de colaboradores.

Disposições Finais:

Esta PSI deverá ser revisada em função de alterações na legislação, de diretrizes da Autoridade Nacional de Proteção de Dados, ou a cada doze meses a conta da data de sua publicação.

O(s) proprietário(s) da Empresa de Pequeno Porte deve(m) se comprometer com o desenvolvimento e implementação desta política.

Esta política entre em vigor na data de sua publicação.

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Brasília, 22 de março de 2022.

À Coordenação-Geral de Tecnologia e Pesquisa

Assunto: **Minuta da Política de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**

1. Em atenção ao Despacho dessa Coordenação-Geral de Tecnologia e Pesquisa (CGTP), encaminho a manifestação desta Coordenação-Geral de Normatização (CGN) sobre o estudo e a minuta de modelo de Política de Segurança da Informação direcionada aos Agentes de Tratamento de Pequeno Porte (ATPP).

2. Na análise da minuta buscou-se harmonizar o teor do documento com o do Guia Orientativo sobre Segurança de Informação para ATPP e o Regulamento de aplicação da LGPD para ATPP, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

3. As contribuições foram inseridas diretamente na minuta do documento (SEI nº 3223883).

4. Ademais, cabe destacar que o Despacho (SEI nº 2937141), exarado pela Diretora Nairane, solicitou a elaboração de estudo e de modelo de Política de Segurança da Informação direcionado aos agentes de tratamento de pequeno porte, mas a minuta elaborada não está estruturada de forma a ser um modelo conforme solicitado, mas, sim, um texto orientativo para elaboração e execução de política de segurança da informação.

5. Sobre esse ponto, ressalta-se que nem o regulamento (art. 13) nem o guia orientativo (item 3.1.1) dispuseram que a Autoridade disponibilizaria modelo de política de segurança da informação. No entanto, em acordo com o despacho acima mencionado, entende-se que a disponibilização de um modelo facilitaria a compreensão desse grupo de agentes de tratamento sobre esse tema.

6. Estamos à disposição para esclarecimentos e análises adicionais.

RODRIGO SANTANA DOS SANTOS

Coordenador de Normatização

ISABELA MAIOLINO

Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenador(a)-Geral**, em 22/03/2022, às 16:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)**, em 22/03/2022, às 16:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **3203619** e o código CRC **2DA67630** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 3203619

Projeto para elaboração de Modelo de Política de Segurança da Informação para Agentes de Pequeno Porte

1. ORIGEM

Coordenação-Geral de Tecnologia e Pesquisa (CGTP/ANPD).

2. OBJETIVO

2.1. Executar estudos e elaborar modelo de Política de Segurança da Informação – PSI – para Agentes de Pequeno Porte – EPP – em atendimento ao despacho 2937141 da Diretora Nairane Farias Rabelo Leitão, constante no processo SEI nº 00261.000821/2021-16 (Anexo-01).

3. JUSTIFICATIVA

3.1 Justifica-se este projeto de construção de modelo de política de segurança da informação para agentes de pequeno porte em função de solicitação da Diretoria da ANPD registrada no processo SEI nº 00261.000821/2021-16 (documento nº 2937141), pelas competências exaradas nos artigos 55-J, I, VI e XVIII da Lei Geral de Proteção de Dados, e também em atenção ao disposto no parágrafo n. 4.27 do VOTO Nº 14/2021/ANPD/NR/DIR/ANPD/PROTOCOLO/PR (documento nº 2892319).

3.2 De acordo com o *Guidance for Information Security Managers* do *Information Security Governance*, as políticas são "declarações de alto nível das intenções, expectativas e direcionamento da administração" e "pode ser considerada a 'constituição' da governança de segurança".

4. RESULTADOS ESPERADOS

4.1 Modelo de Política de Segurança da Informação (PSI) direcionado aos agentes de tratamento de pequeno porte.

5. ETAPAS DE EXECUÇÃO DO PROJETO / CONTROLE DE VERSÕES

5.1 As etapas de execução do projeto de curta duração estão descritas na tabela abaixo:

5.1.1 Histórico

Data	Descrição
25-11-2021	Apresentação da demanda para produção da PSI para EPP.
26-11-2021	Reunião para alinhamento dos detalhes e prazo de entrega.
27-11-2021	Início das pesquisas e levantamentos de normas existentes.
03-12-2021	Entrega da primeira versão, apresentação para equipe CGTP e revisão.
17-12-2021	Revisão do texto pela Diretora Nairane Farias Rabelo Leitão.
22-12-2021	Ajuste do texto sobre a revisão apresentada.

5.1.2 Controle de versões deste documento

Data Reunião	Versão nº	Descrição
03-12-2021	01	Alterações sugeridas para a versão 02: (1) incluir uma seção referendado o Guia ANPD para Agentes de Pequeno Porte; (2) retirar do modelo a questão relacionada à propriedade intelectual; (3) pesquisar a legislação trabalhista além das questões penais/cívicas; (4) incluir no glossário os termos já utilizados pelo guia do GSI; (5) trocar a nomenclatura da ISO para a da ANPD quando em referência aos conceitos de documento sensível, "alto risco", dado sensível, etc;
17-12-2021	03	Diversas correções textuais a partir da revisão apresentada.
22-12-2021	04	Atualização e ajustes no texto. Troca de ABNT para ISO; troca de "empresa" para "agente".

6. EQUIPE DO PROJETO

6.1 A demanda está direcionada ao servidor da CGPT/ANPD João Batista Ribas de Moura e versões revisadas por toda equipe CGTP.

7. METODOLOGIA DE PESQUISA E REFERENCIAL UTILIZADO

7.1 Para elaboração do Modelo de PSI a agentes de pequeno porte, foram pesquisados os principais referenciais normativos nacionais e internacionais e apresentados nesta sequência. Cabe destacar que normalmente a política é o primeiro documento a surgir em organizações visto apresentar os princípios e diretrizes que serão basilares à construção dos demais artefatos - guias procedimentais, checklists, controles, etc -. Para ISACA, "as políticas fornecem orientações sobre comportamentos e ações aceitáveis e inaceitáveis para uma organização"[1]. Os padrões e procedimentos suportam os requisitos definidos inicialmente pelas políticas.

7.2 **Norma ISO/IEC 27001** – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos [1], traz requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). De acordo com a norma 27001:

7.2.1 a política de segurança (PSI) deve estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para todas as partes interessadas.

7.2.2 as pessoas que realizam trabalho sob controle da organização devem estar cientes da existência da política de segurança da informação;

7.2.3 a PSI deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

7.2.4 a PSI deve apoiar a segurança da informação (SI) para gerenciar riscos decorrentes do uso de dispositivos móveis;

7.2.5 deve ser solicitado aos funcionários e partes externas que pratiquem a SI de acordo com o estabelecido nas políticas e procedimentos da organização; e

7.2.6 todos os funcionários devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

[1] Manual *Certified in Risk and Information Systems Control* 6ª Ed., ISACA,

7.3 **Norma ISO/IEC 27002** – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação é um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. De acordo com a norma 27002:

7.3.1 Convém que a PSI contemple requisitos oriundos de:

- Estratégia do negócio;
- Regulamentações, legislação e contratos;
- Ambientes de ameaça da SI, atual e futuro;
- Definição de SI, objetivos e princípios para orientar todas as atividades relativas à SI;
- Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da SI para os papéis definidos; e
- Processos para o tratamento dos desvios e exceções.

7.3.2 No nível mais baixo, convém que a PSI seja apoiada por política específica do tema, que exige implementação de controles de segurança e que seja estruturada para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos. São exemplos de tais temas de política:

a) controle de acesso;
b) classificação e tratamento da informação;
c) segurança física e do ambiente;
d) tópicos orientados aos usuários finais:
    1) uso aceitável dos ativos;
    2) mesa limpa e tela limpa;
    3) transferência de informações;
    4) dispositivos móveis e trabalho remoto; e
    5) restrições sobre o uso e instalação de software.
e) backup;
f) transferência da informação;
g) proteção contra malware;
h) gerenciamento de vulnerabilidades técnicas;
i) controles criptográficos;
j) segurança nas comunicações;
k) proteção e privacidade da informação de identificação pessoal; e
l) relacionamento na cadeia de suprimento.

7.3.3 Considerações para uso de dispositivo móvel:

7.3.3.1 Convém que, ao se utilizar dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas e a política considere:

a) Registros dos dispositivos móveis;
b) Requisitos para a proteção física;
c) Restrições quanto à instalação de software;
d) Requisitos para as versões dos softwares a aplicações de patches;
e) Restrições para conexão aos serviços de informação;
f) Controle de acesso;
g) Técnicas criptográficas;
h) Proteção contra malware;
i) Desativação, bloqueio e exclusão de forma remota;
j) Backups; e
k) Uso dos serviços web e aplicações web.

7.3.4 Considerações para trabalho remoto:

7.3.4.1 Convém que uma política e medidas que apoiem a segurança da informação sejam implementadas para proteger as informações acessadas, processadas, ou armazenadas em locais de trabalho remoto, considerando:

a) a segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;
b) o ambiente físico proposto para o trabalho remoto;
c) os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;
d) o fornecimento de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;
e) a ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;
f) o uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;
g) políticas e procedimentos para prevenir disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;
h) acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), o qual pode ser restringido por lei;
i) acordos de licenciamento de software que podem tonar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou partes externas; e
j) requisitos de firewall e proteção antivírus.

7.3.4.2 Convém que as diretrizes e providências considerem:

a) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto, onde o uso de equipamentos de propriedade particular que não esteja sob controle da organização não seja permitido;
b) uma definição do trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;
c) provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;
d) segurança física;
e) regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;
f) a provisão de suporte e manutenção de hardware e software;
g) a provisão de seguro;
h) os procedimentos para cópias de segurança e continuidade de negócio;
i) auditoria e monitoramento da segurança; e
j) revogação de autoridade e direitos de acesso, e devolução do equipamento quanto as atividades de trabalho remoto encerrarem.

7.3.5 Considerações para segurança em recursos humanos:

7.3.5.1 Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:

a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação;
b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados;
c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas;
d) as responsabilidades dos funcionários ou partes externas pelo tratamento da informação recebida de outras companhias ou partes interessadas; e
e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.

7.3.6 Considerações em relação aos proprietários ou direção da organização:
(...)
c) sejam motivados para cumprir com as políticas de segurança da informação da organização;

(...)
e) cumpram com os termos e condições de trabalho, que incluam a política de segurança da informação da organização e métodos apropriados de trabalho;
(...)

7.2.6.1 É recomendado que a direção demonstre seu apoio às políticas, procedimentos e controles, e aja como tal, de forma exemplar.

7.3.7 Considerações em relação à conscientização, educação e treinamento:

7.3.7.1 Convém quem um programa de conscientização em segurança da informação seja estabelecido e alinhado com a PSI e procedimentos da organização, levando em consideração as informações da organização a serem protegidas e os controles que foram implementados para proteger a informação.

7.3.8 Considerações em relação ao processo disciplinar:

7.3.8.1 Convém que o processo disciplinar também seja usado como uma forma de dissuasão, para evitar que os funcionários e partes externas violem os procedimentos e a PSI, e quaisquer outras violações na segurança da informação.

7.3.9 Considerações sobre proteção contra malware:

7.3.9.1 Convém estabelecer uma política forma proibindo o uso de softwares não autorizados.

7.3.10 Considerações sobre cópias de segurança da informação:

7.3.10.1 Convém que a política de backup seja estabelecida para definir requisitos da organização relativos às cópias de segurança das informações, dos softwares e dos sistemas;

7.3.10.2 Convém que a política de backup defina os requisitos para a proteção e retenção; e

7.3.10.3 Convém que os procedimentos operacionais monitorem a execução dos backups e apontem falhas de backup programado, para garantir a integralidade dos backups, de acordo com a política de backup.

7.3.11 Considerações sobre proteção das informações dos registros de eventos (logs):

7.3.11.1 Alguns registros (log) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência.

7.3.13 Considerações sobre a transferência de informação:

7.3.13.1 Convém que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

7.3.13.2 Convém que políticas, procedimentos e normas para proteger as informações e as mídias em trânsito sejam estabelecidos e mantidos, além de serem referenciados nos mencionados acordos para transferência de informações.

7.3.14 Considerações sobre a cadeia de suprimento:

7.3.14.1 Convém que a organização identifique e exija os controles de SI para tratar, especificamente, do acesso do fornecedor às informações da organização, através de uma política.

7.3.15 Considerações sobre notificação de eventos de segurança da informação:

7.3.15.1 Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade ao notificar qualquer evento de SI o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de SI e do ponto de contato, ao qual os eventos devem ser notificados.

7.3.15.2 Situações a serem consideradas para notificar um evento de segurança da informação incluem:

I) controle de segurança ineficaz;
II) violação da disponibilidade, confidencialidade e integridade da informação;
III) erros humanos;
IV) não conformidade com políticas ou diretrizes;
V) violações de procedimentos de segurança física;
VI) mudanças descontroladas de sistemas;
VII) mau funcionamento de software ou hardware; e
VIII) violação de acesso.

7.3.16 Considerações sobre aprendizagem com incidentes de SI:

7.3.16.1 a avaliação de incidentes de SI pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de futuras ocorrências, ou ser levada em conta no processo de análise crítica da política de segurança.

7.3.17 Considerações sobre análise crítica da segurança da informação:

7.3.17.1 Convém que a análise crítica independente seja iniciada pela direção. Tal análise crítica independente é necessária para assegurar a contínua pertinência, adequação e eficácia do enfoque da organização para gerenciar a SI. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, incluindo a política e os objetivos de controle.

7.3.18 Sobre a conformidade com a PSI e procedimentos de SI:

7.3.18.1 Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de SI.

7.4 **Norma ISO/IEC 27701** – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27702 para gestão da privacidade de informação – Requisitos e diretrizes - é um documento que apresenta requisitos e diretrizes adicionais que permitem a geração de evidências documentais de como a organização lida com o tratamento de Dados Pessoais (DP). De acordo com a norma 27701:

7.4.1 As diretrizes adicionais para implementação da Política de Segurança da Informação, da ABNT 27002, são:

7.4.1.1 Seja para o desenvolvimento de políticas de privacidade separadas, seja para acréscimo de políticas de segurança da informação, convém que a organização produza uma declaração quanto ao apoio e comprometimento para alcançar *compliance* com as regulamentações e legislações de proteção de DP aplicáveis, e com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores etc.), para os quais convém que se especifiquem claramente as responsabilidades entre eles.

7.4.1.2 Para qualquer organização que trate DP, seja um controlador de DP seja um operador de DP, convém que seja considerada a regulamentação e/ou legislação de proteção de DP aplicável, durante o desenvolvimento e a manutenção de políticas de segurança da informação.

7.4.1.3 A norma ABNT 27002 é baseada nas normas ABNT 27001 e 27002 e estende os seus requisitos e diretrizes para considerar, em contemplação à segurança da informação, a proteção da privacidade dos titulares de DP, que podem ser potencialmente afetados pelo tratamento de DP. Isto significa que, onde o termo "segurança da informação" for usado nas normas 27001 ou 27002, o termo "**segurança da informação e privacidade**" se aplica.

7.4 De acordo com o **Infosec Institute**[2] existem cinco elementos em uma política de segurança da informação:

7.4.1 **Propósito**: organizações desenvolvem políticas de segurança por várias razões:

- Para estabelecer uma abordagem geral para a segurança da informação;
- Para detectar e prevenir falhas na segurança da informação;
- Para proteger a reputação da organização no que diz respeito às suas responsabilidades éticas e legais; e
- Para respeitar os direitos dos usuários.

7.4.2 **Escopo**: Uma política de segurança da informação deveria atuar sobre dados, programas, sistemas, infraestrutura de tecnologia, usuários de tecnologia e terceiras partes.

7.4.3 **Objetivos**: Uma organização que pretender desenvolver uma PSI funcional precisa ter objetivos bem definidos em relação à segurança e à estratégia. A gerência deve concordar com esses objetivos porque quaisquer divergências existentes neste contexto podem tornar todo o projeto disfuncional. Idealmente, a redação da política deve ser breve e direta. O texto redundante torna os documentos prolixos ou mesmo ilegíveis. A segurança da informação é considerada como salvaguarda de três objetivos principais: confidencialidade, integridade e disponibilidade.

7.4.4 **Política de autorização e controle de acesso**: Normalmente, uma política de segurança possui um padrão hierárquico onde cada posição com especificações e autorizações são esclarecidas. Por exemplo, um usuário pode ter a necessidade de saber um tipo específico de informação. Portanto, os dados devem ter granularidade suficiente para permitir o acesso autorizado apropriado e nada mais. Trata-se de encontrar o delicado equilíbrio entre permitir o acesso a quem precisa usar os dados como parte de seu trabalho e negá-lo a entidades não autorizadas.

7.4.5 **Classificação dos dados**: Os dados podem ter valores diferentes. Gradações no índice de valor podem impor separação nos procedimentos de manuseio específicos para cada tipo. Um sistema de classificação de informações, portanto, ajudará na proteção de dados que têm uma importância significativa para a organização e deixará de fora informações insignificantes que, de outra forma, sobrecarregariam os recursos da organização.

[2] https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/#gref

7.4.5.1 Uma política de classificação de dados pode organizar todo o conjunto de informações da seguinte forma:

i) **Classe de alto risco**: Dados protegidos por legislação estadual e federal (a Lei de Proteção de Dados, HIPAA, FERPA), bem como financeiros, folha de pagamento e pessoal (requisitos de privacidade) estão incluídos aqui;]

ii) **Classe confidencial**: os dados nesta classe não têm o privilégio de serem protegidos por lei, mas o proprietário dos dados julga que devem ser protegidos contra divulgação não autorizada; e

iii) **Classe pública**: essas informações podem ser distribuídas gratuitamente. Os proprietários dos dados devem determinar a classificação dos dados e as medidas exatas que um guardião dos dados precisa tomar para preservar a integridade de acordo com aquele nível.

7.4.5.2 Os proprietários de dados (*data owners*) devem determinar a classificação dos dados e as medidas exatas que o custodiante dos dados precisa executar para preservar a integridade de acordo com determinada classificação.

7.4.6 **Suporte de dados e operações**: Refere-se a parte de uma PSI onde são estipuladas cláusulas referentes a:

- A regulamentação dos mecanismos gerais do sistema responsável pela proteção de dados;
- O backup de dados; e
- O transporte/movimento de dados.

7.4.7 **Conscientização de segurança**: A divulgação da PSI com as equipes é uma etapa crítica. Fazer os colaboradores ler e reconhecer um documento não significa necessariamente que estejam familiarizados e compreendam a nova política. Por outro lado, uma sessão de treinamento envolveria os funcionários de forma a garantiria que eles entendessem os procedimentos e mecanismos em vigor para proteger os dados.

7.4.8 **Responsabilidades, direitos e deveres do pessoal**: Os itens a serem considerados nesta área da PSI geralmente se concentram na responsabilidade das pessoas nomeadas para realizar a implementação, educação, resposta a incidentes, análises de acesso do usuário e atualizações periódicas de uma política de segurança da informação.

7.4.10 **Outros itens que podem ser incluídos em uma política de segurança da informação**: Uma PSI incluir vários itens diferentes que incluem, mas não se limitam a: procedimento de proteção de vírus, procedimento de detecção de intrusão, resposta a incidentes, procedimento de trabalho remoto, diretrizes técnicas, auditoria, requisitos de funcionários, consequências para não conformidade, ações disciplinares, funcionários desligados, segurança física de TI, referências a documentos de apoio e muito mais.

7.5 **National Institute of Standards and Technology (NIST)** publicou o documento *Special Publication (SP)* – ***NIST SP 800-53*** **-** *Security and Privacy Controls for Information Systems and Organizations* sendo considerado padrão de referência para segurança da informação.

7.5.1 De acordo com o documento de referência NIST SP-800 Rev. 5[3], há 20 famílias de controles operacionais, técnicos e gerenciais para garantir a privacidade, integridade e a segurança em sistemas de informação: Acess Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Assessment, Authorization and Monitoring (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environment Protection (PE), Planning (PL), Program Management (PM), Personnel Security (PS), Processing and Transparency (PT), Risk Assessment (RA), System and Services Aquisition (SA), System and Communications Protection (SC), System and Information Integrity (SI), Supply Chain Risk Management (SR).

7.5.2 Muitas organizações optaram por usar os controles NIST SP 800-53 como basilar aos seus controles de segurança e privacidade porque os controles descritos no catálogo são em maioria neutros em termos de política, tecnologia e setor; eles se concentram nas medidas fundamentais necessárias para proteger as informações e a privacidade dos indivíduos em todo o ciclo de vida das informações.

7.5.3 Existem 05 (cinco) princípios-chave na construção de políticas de segurança de acordo com NIST:

1) Políticas necessitam ser escritas. Embora pareça óbvio, muitas organizações falham na documentação de suas próprias políticas de segurança;
2) Devem existir procedimentos descritos para facilitar a implementação de controles associados à política;
3) Políticas devem ser periodicamente revisadas;
4) Políticas devem ser disseminadas na organização porque serão consideradas não efetivas se não direcionarem o comportamento organizacional; e
5) Políticas devem ser gerenciadas a partir de processos definidos: revisão, coordenação, *compliance* etc.

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

7.6 O **Gabinete de Segurança Institucional (GSI)** da Presidência da República traz orientações para Política de Segurança da Informação em sua Instrução Normativa Nº1, de 27 de maio de 2020 que, embora direcionadas aos órgãos e entidades da administração federal, trazem valiosos ensinamentos para todas as organizações.

7.6.1 De acordo com o GSI-PR, a PSI deverá ser composto, no mínimo, pelos seguintes itens[4]:

"**I – escopo**: descreve o objetivo e a abrangência da Política, definindo o limite dentro do qual as ações de segurança da informação serão desenvolvidas no órgão ou na entidade;

II - conceitos e definições: relaciona e descreve os conceitos e definições a serem utilizados na Política do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade, devendo ser utilizadas as definições contidas no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República;

III - princípios: relaciona os princípios que regem a segurança da informação no órgão ou na entidade;

IV - diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:

a) Tratamento da Informação;
b) Segurança Física e do Ambiente;
c) Gestão de Incidentes em Segurança da Informação;
d) Gestão de Ativos;
e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
f) Controles de Acesso;
g) Gestão de Riscos;
h) Gestão de Continuidade; e
i) Auditoria e Conformidade.

V - competências: define as atribuições e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação;

[4] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215

VI - penalidades: estabelece as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto; e

VII - política de atualização: estabelece a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos.

(...)"

7.7 **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte da Autoridade Nacional de Proteção de Dados (ANPD)** define a política de segurança da informação (PSI) como um "conjunto de diretrizes e regras que tem por objetivo o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização".

7.7.1 ANPD diz que "o propósito fundamental da PSI é ser uma ferramenta que apoie a implementação de um processo estruturado de SI adequado a cada organização, considerando seu negócio e seu porte" sugerindo que a política 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.

7.7.2 O Guia da ANPD sugere ações de conscientização e treinamento inclusive para que funcionários sigam as orientações da PSI.

7.7.3 São apresentadas medidas técnicas que tratam, entre outros temas, do controle de acesso aos dados; segurança nos dados armazenados; manutenção de programa de gerenciamento de vulnerabilidades; segurança das comunicações; e serviços em nuvem.

7.7.3 Em complemento ao guia orientativo, a ANPD disponibilizou o "Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte", oferecendo aos Agentes de Tratamento de Pequeno Porte uma visão objetiva e concreta de controles de segurança aplicável a esse contexto.

7.7.4 Considerando essa visão e buscando uma visão harmônica, a elaboração desse modelo de PSI ponderou as proposições contidas nos seguintes documentos:

- a Minuta de Resolução ANPD que aprova o regulamento de aplicação da Lei nº 13.709/2018 para agentes de tratamento de pequeno porte;
- o capítulo de "medidas técnicas" existente no "Guia ANPD Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte"; e
- "Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte".

7.7.5 É preciso observar, contudo, que, na medida em que se crie maturidade em processos de governança de privacidade e proteção de dados, é adequado que processos de gestão de riscos e de gestão da privacidade sejam considerados.

10. REFERENCIAIS BIBLIOGRÁFICO

8. ENCAMINHAMENTO

Brasília, 22 de dezembro de 2021.

À consideração superior,

João Batista Ribas de Moura

De acordo, encaminhe-se ao Conselho Diretor da ANPD,

Marcelo Santiago Guedes
Coordenador-Geral de Tecnologia e Pesquisa

Thiago Guimarães Moraes
Coordenador de Tecnologia e Pesquisa

ANEXO I

MODELO DE POLÍTICA DE SEGURANÇA DA INFORMÇÃO PARA ~~EPP~~Agentes de Tratamento de Pequeno Porte (ATPP)

Objetivo

~~A~~

Esta Política de Segurança da Informação (PSI) estabelece conceitos, diretrizes e regras de segurança da informação e tem objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação do ATPP. Assim, deve ser entendida como uma declaração formal da ORGANIZAÇÃO acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os funcionários, estagiários e colaboradores terceirizados do ATPP. ~~é uma declaração formal da organização manifestando compromisso com a proteção dos dados e informações sob sua responsabilidade devendo estar disponível como informação documentada e comunicada a todos.~~

Escopo

Os objetivos, princípios, ~~e~~ diretrizes e regras aqui estabelecidos devem ser observados por todos os empregados, colaboradores, fornecedores e prestadores de serviços que tenham acesso aos dados, informações e recursos tecnológicos desta organização para prover segurança da informação e redução do risco a níveis aceitáveis, buscando continuamente a disponibilidade, a integridade e confidencialidade aos objetivos estratégicos.

Conceitos e Definições[5]

I – ameaça: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;
II – ativo: tudo que tenha valor para a organização, material ou não;
III – ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
IV – autenticidade: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
V- backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;
VI – confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
VII – consentimento:
computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);
VIII – custodiante da informação:

[5] https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370

Formatado: Sublinhado

Comentado [RSdS1]: Não pode existir uma ameaça interna?

Comentado [RSdS2]: Essa é a definição de consentimento, segundo a LGPD

Comentado [IM3]: Não tem o conceito de consentimento.

Comentado [RSdS4]: Falta a numeração

Comentado [RSdS5]: Falta a definição

IX – disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X- firewall: 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; ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XI - hardware: parte física do computador ou de seus componentes eletrônicos;

XII - cloud computing: ver nuvem – computação;

XIII – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIV – malware: software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits;

XV – autenticação multi-fatores (MFA) ~~– 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~~utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema~~. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital,tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

XVI – phishing: técnica de envio de e-mail falso para enganar usuários com informações aparentemente corretas e direcioná-los a ambientes criados para capturar informações e senhas;

XVII - pseudonimização: 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;

XVIII - ransomware: tipo de malware que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados;

XIX – segurança orgânica: conjunto de medidas passivas, com o objetivo de prevenir e, até mesmo, obstruir as ações que visem o comprometimento ou a quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

XX – serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XXI – sistema de proteção física: sistema composto por pessoas, equipamentos e procedimentos, para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ação humana não autorizada, conforme gestão da segurança física e ambiental; e software

XXII – tratamento: 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.

Princípios

Comentado [RSdS6]: Definição constante no Guia de Segurança p APP

Comentado [RSdS7]: Melhor colocar somente a definição de computação em nuvem

Comentado [RSdS8]: Alinhando com a definição do guia

As ações de segurança da informação são norteadas pela ética profissional e princípios:

I – atender as propriedade de disponibilidade, integridade, confidencialidade das informações;
II – continuidade dos processos e serviços essenciais para o funcionamento da organização; e
III – responsabilidade dos colaboradores, constituída no dever de conhecer e respeitar esta Política de Segurança da Informação.

Comentado [RSdS9]: Para ter maior harmonização com a Norma ISO 27001, que define disponibilidade e integridade como propriedades.

Formatado: À esquerda

Diretrizes Gerais

As informações de titulares devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pelo PPPDP – Política de Privacidade e Proteção de Dados Pessoais da ORGANIZAÇÃO e das leis vigentes.

A ORGANIZAÇÃO ~~Recomenda-se que a PSI~~ mantém compromisso em adotar técnicas e meios de segurança mais adequados e disponíveis em relação à segurança dos dados trafegados, processados e/ou armazenados em sua base de dados~~-~~.

A ORGANIZAÇÃO deve classificar as informações com objetivo de apoiar a proteção de dados que têm uma importância significativa para a organização.

A ORGANIZAÇÃO deve realizar treinamentos de forma regular e periódica, de conscientização sobre a Lei Geral de Proteção de Dados, em especial à Segurança da Informação.

Cabe à ORGANIZAÇÃO promover a divulgação e revisão desta Política para todos os funcionários, estagiários e colaboradores terceirizados.

A ORGANIZAÇÃO, considerando os custos de implementação, bem como a estrutura, a escala e o volume das operações realizadas, nos termos do art. 13, §1º do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, adota as seguintes medidas de segurança: ~~apresente os seguintes temas específicos que repercutirão na implementação de controles de segurança proporcionais:~~
A seguir segue lista sugestiva de medidas adotadas pela ORGANIZAÇÃO:

i) Copias de segurança (backup);
ii) Controle de acesso;
iii) Atualização de software e gerenciamento de vulnerabilidades;
iv) Uso de correio eletrônico;
v) Proteção contra malware;
vi) Gerenciamento de contratos e aquisições;
vii) Segurança das comunicações;
viii) Dispositivos móveis e teletrabalho;
ix) Serviços em nuvem;
x) Conscientização e treinamento; e
xi) Segurança dos dados armazenados.

Considerações sobre Cópia de Segurança (backup):

Devem ser definidas rotinas para realização de cópias de segurança de –dados e softwares em períodos regulares e proporcionais à quantidade de novos dados gerados

diariamente. Deve ser levado em consideração a segurança dos dados copiados – criptografia e armazenamento em local seguro – além do tempo de retenção.
Devem ser realizados registros para monitoramento e garantia da correta execução das cópias de segurança nos intervalos de tempo programados.

Considerações sobre Controle de Acesso:

Devem ser estabelecidas medidas técnicas que garantam acesso aos dados e informações somente às pessoas autorizadas para execução das atividades laborais abrangendo processos de concessão, revisão e suspensão de acessos aos usuários.

Recomenda-se ativação de recurso técnico para bloqueio de tela e proteção por senha, token ou mecanismo de autenticação semelhante para acesso aos sistemas computacionais.

O acesso aos sistemas e bases de dados devem possuir autenticação multifator.

Usuários afastados ou desligados da empresa devem ter sua autorização de acesso imediatamente cancelada.

Considerações sobre atualização de software e gerenciamento de vulnerabilidades:

Devem ser criadas rotinas e controles para verificação de novas versões de softwares (*patches*) corrigindo falhas detectadas pelos fabricantes.

É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas à instância superior assim que identificadas.

A instalação de software não autorizado em dispositivos computadorizados pode introduzir vulnerabilidades e causar vazamento de informações, perda de integridade ou outros incidentes de segurança da informação.

Considerações sobre uso de correio eletrônico:

O correio eletrônico deverá ser utilizado somente para fins laborais. Os colaboradores devem ser conscientizados quanto ao risco de *phishing*.

Considerações sobre proteção contra malware:

Devem ser utilizados softwares antivírus e antimalwares com controles de atualização e registro de varreduras.

Considerações sobre gerenciamento de contratos e aquisições:

Devem existir cláusulas contratuais que:

i) determinem a observância desta Política;
ii) garantam compromisso com o sigilo das informações organizacionais a que tenham acesso; e
iii) garantam, quando for o caso, a confidencialidade, integridade e disponibilidade dos dados hospedados em seus sistemas.

Considerações sobre segurança das comunicações:

Devem ser adotados controles e medidas técnicas para garantir a confidencialidade das informações trafegadas interna ou externamente.

Convém que informações do negócio – sensíveis ou críticas – em papel ou mídia sejam guardadas em local seguro quando não em uso.

Recomenda-se informativos de conscientização para que documentos contendo informação sensível sejam removidos da impressora imediatamente.

Considerações sobre dispositivos móveis e teletrabalho:

Convém os dispositivos móveis utilizados e relacionados às atividades da ~~EPP~~ ORGANIZAÇÃO estejam submetidos a controles que garantam:

a) Registro dos dispositivos móveis;
b) Restrições à instalação de softwares;
c) Acompanhamento para aplicação de patches críticos;
d) Controle de acesso;
e) Proteção contra malware;
f) Backups;
g) Segurança física no ambiente doméstico; e
h) Requisitos de segurança nas comunicações sobre, por exemplo, uso de VPN para acesso remoto aos sistemas organizacionais.

Considerações sobre serviços em nuvem:

É de responsabilidade do(s) proprietário(s) ou da alta administração a divulgação desta Política.

Todos os colaboradores são responsáveis pela segurança dos ativos de informação que esteja sob sua responsabilidade.

Comentado [RSdS10]: O texto relacionado à responsabilidade não possui relação com o título de serviços em nuvem

Considerações sobre Conscientização, Educação e Treinamento de colaboradores:

Devem ser estabelecidos momentos – reuniões presenciais, palestra, e-mails, cartazes etc. – objetivando a divulgação ~~deste política~~desta política e conscientização em segurança da informação levando-se em consideração o porte da organização e a quantidade de colaboradores.

Responsabilidades

De forma geral, cabe a todos os funcionários, estagiários e colaboradores terceirizados cumprir fielmente esta política, sob pena de responsabilização de eventuais danos causados à ORGANIZAÇÃO e/ou aos titulares de dados pessoais, conforme dispositivo do Código Civil brasileiro, observadas outras disposições legais.

Formatado: Justificado, Recuo: À esquerda: 2 cm

Disposições Finais:

Esta PSI deverá ser revisada em função de alterações na legislação, de diretrizes da Autoridade Nacional de Proteção de Dados, ou a cada doze meses a conta da data de sua publicação.

O(s) proprietário(s) ou alta administração da ORGANIZAÇÃO~~Da Empresa de Pequeno Porte~~ deve(m) se comprometer com o desenvolvimento e implementação desta política.

Esta política entre em vigor na data de sua publicação.

PRESIDÊNCIA DA REPÚBLICA
Protocolo da Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Brasília, 01 de julho de 2022.

À Secretaria-Geral,

Assunto: **Desarquivamento de Processo em virtude de necessidade de alteração em documento e solicitação de publicação de nova versão em razão de período de Defeso Eleitoral**

1. Em atendimento ao art. 73, inciso VI, alínea b da Lei nº 9.504, de 1997, a qual dispõe, dentre outras questões, sobre condutas vedadas aos agentes públicos durante os pleitos eleitorais, às diretrizes disciplinadas pela Instrução Normativa Secom nº 1 de 11 de abril de 2018, bem como pelo Manual de Condutas Vedadas aos Agentes Públicos Federais em Eleições 2022, às orientações recebidas pela Assessoria de Comunicação (ASCOM) junto à Corregedoria desta Autoridade Nacional de Proteção de Dados em reunião sobre "Adequação dos Canais Digitais da ANPD", realizada em 30/06/2022, e, ainda, considerando a iminência do período de Defeso Eleitoral, o qual inicia-se em 02 de julho de 2022 e perdurará até o encerramento do período eleitoral de 2022, ou seja, até 30 de outubro em caso de segundo turno, desarquiva-se o presente processo a fim de que sejam feitas as alterações necessárias no documento em questão para fins de adequação à legislação eleitoral.

2. Junta-se ao processo a nova versão do **Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte** (SEI nº 3472474), na qual resta suprimida a logomarca "Pátria Amada, Brasil", sem quaisquer alterações quanto ao conteúdo do documento.

3. Por fim, encaminha-se o processo à Secretaria-Geral, para publicação da nova versão do documento no site da ANPD.

Atenciosamente,

ISABELA MAIOLINO
Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenador(a)-Geral**, em 01/07/2022, às 16:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

A autenticidade do documento pode ser conferida informando o código verificador **3471127** e o código CRC **2781DF8A** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.000821/2021-16 SEI nº 3471127

GUIA ORIENTATIVO

SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

VERSÃO 1.0
OUT. 2021

Capa atualizada para atendimento à Legislação Eleitoral 2022

ANPD

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.

Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

FORMULÁRIO PARA EXPEDIÇÃO DE DOCUMENTOS PARA O PROTOCOLO CENTRAL

Ao Protocolo da ANPD.

Encaminho o presente processo para expedição conforme a seguir:

(X) Enviar o processo integralmente;

( ) Enviar apenas os documentos listados abaixo:

Identificação do documento PRINCIPAL 1	**Link SUPER do documento PRINCIPAL 1**
Identificação do anexo do documento PRINCIPAL 1	**Link SUPER do anexo do documento PRINCIPAL 1**

Identificação do documento PRINCIPAL 2 (se houver)	**Link SUPER do documento PRINCIPAL 2 (se houver)**
Identificação do anexo do documento PRINCIPAL 2	**Link SUPER do anexo do documento PRINCIPAL 2**

Prazo de envio			
( )	Urgente	( )	Não urgente

Nível de Acesso			
( )	Público	( )	Restrito

Indicação da forma de remessa	
( )	E-mail Informar e-mail (s) de destino:

( )	Protocolo Digital ou Peticionamento Eletrônico · Solução que possibilita aos órgãos e entidades da Administração Pública de todas as esferas, pessoas físicas e jurídicas, encaminhar documentos pela Internet, de forma eletrônica. · Envio de documentos avulsos. · O processo eletrônico que possui o(s) documento(s) continua aberto na Unidade no SUPER-PR.		
(X)	Barramento · Solução que permite a comunicação entre os órgãos públicos que utilizam o SUPER ou outras soluções de processo eletrônico (desde que também estejam integrados ao Barramento). · Envio de todo o processo. · O processo eletrônico enviado fica bloqueado no SUPER-PR e não pode ser editado nem tramitado, mas fica disponível para consulta.		
( )	Via Postal * Colocar endereço(s) do(s) destinatário(s)	( )	SEDEX
		( )	Aviso de recebimento
( )	Qualquer das opções		

ATENÇÃO: Caso a opção escolhida seja envio por meio de protocolo digital ou de peticionamento eletrônico, barramento ou e-mail e o Órgão de destino não ofereça essas opções de recebimento, o documento será enviado fisicamente ou por via postal.

INSTRUÇÕES:

a) este formulário deve ser assinado pelo colaborador responsável e o

respectivo processo encaminhado à unidade PROTOCOLO CENTRAL para atendimento;

b) não é necessário incluir despacho de encaminhamento - apenas o formulário devidamente preenchido e assinado é suficiente para o atendimento da demanda;

c) os documentos a serem expedidos devem compor os autos dos processos enviados à expedição. Havendo documentos em processo diverso, estes deverão estar disponíveis para consulta da unidade PROTOCOLO CENTRAL.

Em caso de dúvida, por favor, entre em contato com o Protocolo Central: 2487/2488 ou acesse o menu Documentação e Arquivo, opção PROTOCOLO CENTRAL na Intranet.

Documento assinado eletronicamente por **Fabíola de Gabriel Soares Pinto**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 17/01/2024, às 11:11, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida informando o código verificador **4905205** e o código CRC **A68ABB83** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
