Joyce Roysen
Advogados

MANUAL DE BOAS PRÁTICAS PARA PROTEÇÃO DE DADOS PESSOAIS

JOYCE ROYSEN ADVOGADOS

Classificação

Esta informação foi classificada como Pública, portanto, a sua divulgação foi permitida pelo JRA, desde que mantida a integridade da mensagem.

Classification

This information has been classified as public; therefore, its disclosure is allowed by JRA, as long as the integrity of the message is maintained.

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR	ALTERAÇÕES
16/09/2021	1.0	Primeira versão	Datablock Proteção de Dados	Documento original
01/06/2023	2.0	Segunda versão	Datablock Proteção de Dados	Inclusão de medidas técnicas de segurança
15/04/2024	3.0	Terceira versão	Datablock Proteção de Dados	Repaginação do texto e exclusão das medidas técnicas, que passam a integrar a PSI.

APROVAÇÃO

DATA	APROVADO POR
16/09/2021	Dr. Edgard Nejm
01/06/2023	Dr. Edgard Nejm
15/04/2024	Dr. Edgard Nejm

1 SUMÁRIO

1 Introdução 4
2. Política de Segurança da Informação 5
3. Tratamento de Dados Pessoais 6
3.1. Princípios da LGPD 6
3.2. Classificação da Informação 8
3.3. Descarte de Dados 8
4. Conscientização e Treinamento 0
5. Gerenciamento de Contratos 2
6. Medidas Técnicas 3
6.1 Controle de Acessos 3
6.2 Segurança dos Dados Pessoais Armazenados 4
6.3 Segurança das Comunicações 6
6.4 Manutenção de Programa de Gerenciamento de Vulnerabilidades 6
6.5 Medidas Relacionadas Ao Uso De Dispositivos Móveis 7
7. Plano de Resposta e Continuidade 9

1 INTRODUÇÃO

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 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.

O presente manual foi elaborado com o objetivo de, no cumprimento do disposto acima, disseminar boas práticas e medidas de segurança da informação para apoiar o JRA no desenvolvimento de suas atividades organizacionais em um ambiente institucional mais seguro no que se refere ao tratamento de dados e informações sigilosas, contribuindo para o aumento da confiança dos clientes, colaboradores e prestadores de serviços do Escritório.

Estas medidas são complementadas com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional do JRA, inclusive aquelas indicadas na Política de Segurança da Informação do Escritório.

Por fim, cabe ressaltar que este documento deverá ser atualizado e aperfeiçoado sempre que necessário.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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 no Escritório. Outrossim, ela prevê as regras de nomeação e funcionamento do Comitê de Segurança da Informação, órgão responsável por auxiliar na criação e revisão de políticas, normas e procedimentos gerais relacionados à segurança da informação.

O Comitê do Escritório é formado por um grupo de gestores dos departamentos de Tecnologia da Informação, Jurídico e Administrativo, além do Encarregado de Proteção de Dados (“DPO”). O Comitê possui autonomia para debater e/ou recomendar quaisquer aspectos relacionados à segurança da informação, oferecendo subsídio à Diretoria no processo de tomada de decisão.

As diretrizes da PSI deverão ser mandatoriamente observadas pelos sócios, advogados, estagiários e funcionários do JRA, bem como por terceiros que atuem em seu nome, como parceiros de negócios, fornecedores ou prestadores de serviços, de forma que todos estarão aptos a auxiliar na identificação de situações de risco e engajados no objetivo de mitigá-las.

Eventuais violações à PSI, bem como às demais normas e procedimentos de segurança da informação adotados pelo Escritório, são passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa, conforme análise do Comitê.

As medidas técnicas de proteção de dados trazidas neste documento são um extrato daquelas exigidas de forma detalhada pelo JRA em sua PSI, normas e procedimentos internos relacionados à proteção de dados e segurança da informação.

3. TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados - 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.

Vale ressaltar que a LGPD conceitua os dados pessoais como sendo as informações relacionadas a pessoa natural identificada ou identificável. Já os dados sensíveis, 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.

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. Nesse caso, o Escritório adota medidas de segurança reforçadas para seu tratamento.

Todos os colaboradores, sócios, estagiários, advogados, parceiros de negócios e prestadores de serviços que tenham acesso à dados pessoais e informações sigilosas de responsabilidade do JRA deverão observar as regras contidas na LGPD, sob pena de responderem nos termos estabelecidos na PSI.

3.1. PRINCÍPIOS DA LGPD

Ao estabelecer as medidas de segurança a serem implementadas, o JRA levou em consideração a natureza das informações tratadas, as características

específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos na LGPD. Nesse sentido, dados sensíveis, dados de menores de idade, de idosos ou analfabetos, assim como dados de crianças e adolescentes estão protegidos com medidas de segurança reforçadas, principalmente se são tratados a larga escala.

Os princípios da Lei, que deverão ser observados em todas as atividades de processamento de dados do Escritório, são os seguintes:

- ✓ Finalidade: o tratamento somente será realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- ✓ Adequação: o tratamento deverá ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- ✓ Necessidade: o tratamento deverá limitar-se ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- ✓ Livre acesso: é necessário garantir aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- ✓ Qualidade dos dados: é necessário garantir aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- ✓ Transparência: é necessário garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- ✓ Segurança: utilizar 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;

- ✓ Prevenção: adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- ✓ Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- ✓ Responsabilização e prestação de contas: a empresa deverá demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3.2. CLASSIFICAÇÃO DA INFORMAÇÃO

Informações estratégicas de caráter sigiloso do JRA, como dados pessoais de clientes e informações relacionadas aos serviços prestados, incluindo, mas não limitando-se a, boletins de ocorrência, inquéritos policiais e ações penais (ainda que não tramitem sob sigilo/segredo de justiça) estarão inventariadas, etiquetadas e classificadas de acordo com o grau de sigilo de cada documento como (i) confidencial, (ii) interna ou (iii) pública.

Esta classificação determinará quem está autorizado a acessar um determinado documento, como deverão ser armazenados e em que condições poderão ser transmitidos. Para mais informações, consulte a PSI.

3.3. DESCARTE DE DADOS

Os colaboradores, sócios, estagiários e advogados deverão observar os prazos de guarda de cada documento, os quais devem ser descartados após a ocorrências dos seguintes motivos:

- Quando alcançada a finalidade para a qual foram coletados.

- Quando já não sejam necessários ou pertinentes para o alcance da finalidade para a qual foram coletados.
- Quando o titular revogue o consentimento prestado para o tratamento de seus dados pessoais.
- Por solicitação da Autoridade Nacional de Proteção de Dados.

Nenhum documento relacionado a clientes e aos serviços prestados será descartado sem a devida autorização, prévia comunicação ao cliente, observância das medidas de segurança elencadas na PSI, ou quando sejam necessários para as seguintes finalidades:

- Cumprimento de obrigação legal ou regulatória pelo JRA;
- Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD.
- Para uso exclusivo do JRA, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Devem ser observados ainda eventuais prazos de retenção estabelecidos pela Ordem dos Advogados do Brasil. Em caso de dúvidas sobre o descarte de dados, o Comitê de Segurança da Informação deverá ser consultado.

4. CONSCIENTIZAÇÃO E TREINAMENTO

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 nela trabalham que realizarão o tratamento dos dados pessoais.

Por esta razão, o JRA promove periodicamente a conscientização de seus funcionários por meio de treinamentos e campanhas sobre suas obrigações e responsabilidades relacionadas à segurança e sigilo das informações.

Essa conscientização implica informar e sensibilizar os estagiários, sócios, advogados e colaboradores do Escritório sobre as obrigações legais existentes na LGPD, e em normas e orientações editadas pela Ordem dos Advogados do Brasil e pela Autoridade Nacional de Proteção de Dados (“ANPD”), entre elas:

- ✓ 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;
- ✓ não compartilhar informações com terceiros sem prévia e expressa autorização;

- ✓ seguir as regras de segurança da informação contidas na PSI, normas e procedimentos relacionados à segurança da informação do Escritório.

Além disso, o JRA incentiva os usuários de sistemas do Escritório a informar incidentes e vulnerabilidades detectadas por meio do canal lgpd@roysenadvogados.com e a comunicá-los ao Encarregado pelos Dados Pessoais (DPO) do Escritório: a empresa Datablock Proteção de Dados. O Encarregado deverá ser acionado sempre que existam dúvidas ou solicitações em relação ao tratamento dos dados pessoais realizados pelo Escritório ou por seus prestadores de serviços. A Datablock poderá ser acionada através do seguinte e-mail: dpo@datablock.com.br.

5. GERENCIAMENTO DE CONTRATOS

O JRA realiza 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.

Todos os colaboradores, sócios, estagiários, advogados e parceiros do Escritório deverão assinar termos de confidencialidade (*non-disclosure agreement* - NDA) comprometendo-se formalmente a não divulgar informações confidenciais. Esta é uma medida de segurança importante contra abusos de privilégio.

No caso de terceirização de serviços de tecnologia, de contabilidade, de marketing, entre outros, o Escritório estabelece contratos que incluem cláusulas que exigem um padrão mínimo de maturidade em segurança da informação e a implementação de medidas técnicas e organizacionais específicas e capazes de assegurar a adequada proteção de dados pessoais.

Nenhum fornecedor ou prestador de serviços poderá atuar para o JRA sem contrato escrito onde fiquem estabelecidas suas obrigações em relação à segurança da informação e proteção dos dados pessoais.

No que tange à prestação de serviços de computação em nuvem, o Escritório mantém contratos de acordo de nível de serviço (*Service Level Agreement*, ou SLA), contemplando a segurança dos dados armazenados, e os tempos de resposta em caso de indisponibilidade dos serviços.

6. MEDIDAS TÉCNICAS

6.1 CONTROLE DE ACESSOS

O controle de acesso consiste em uma medida técnica que garante 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.

Sobre esse aspecto, foi 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 e informações relacionadas aos serviços prestados pelo Escritório. Esse sistema de controle de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários.

Além disso, o sistema de controle de acesso foi configurado com funcionalidades que podem detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade, como um determinado número de caracteres, o uso de um caractere especial ou outros fatores considerados necessários.

Ainda, para um adequado gerenciamento de senhas, os colaboradores, sócios, estagiários e advogados deverão evitar 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.

O JRA não permite o compartilhamento de contas ou de senhas entre usuários, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação. A premissa aplicada é a do princípio do menor 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, são restringidas apenas àqueles colaboradores que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade.

Quando possível e necessário, o JRA utiliza a autenticação multi-fator (MFA) para acesso a sistemas ou base de dados que contenham dados pessoais e/ou informações sigilosas. 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.

6.2 SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

Inicialmente, cabe salientar que, muitas vezes, as organizações 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 na LGPD, os colaboradores, sócios, estagiários, advogados, parceiros e prestadores de serviços do Escritório devem coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos pretendidos.

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.

Além disso, tendo em vista que os dados pessoais sensíveis gozam de uma proteção especial pela LGPD, o JRA implementou soluções que dificultam a identificação do titular, como técnicas de pseudonimização, como por exemplo, a criptografia.

Em relação às estações de trabalho, os colaboradores, estagiários, sócios e advogados devem atender à importância das configurações de segurança, a fim de que não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites.

Os colaboradores, estagiários, sócios e advogados devem, também, 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, devem adotar controles adicionais a esses dispositivos externos, como inventariá-los, cifrar os dados e armazená-los em locais seguros.

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

Sobre a eliminação de dados pessoais, todas as mídias que contenham dados pessoais devem ser formatadas antes de descartas. Quando isso não for possível, como em CDs e DVDs, deve ser realizada a destruição física da mídia – o que também se aplica para destruição de papel e de mídia portátil para armazenar dados pessoais e/ou informações sigilosas.

Além disso, caso se faça uso de serviço de terceiros para o descarte, seja de mídia ou papel, é estabelecido um contrato de serviço com cláusulas de registro

da destruição que for realizada.

6.3 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 das informações se houver troca de links maliciosos ou se o usuário receber algum arquivo infectado.

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 sobre os serviços prestados aos clientes. Nesses casos, os e-mails ou os arquivos serão, sempre que possível, cifrados.

Além disso, o Escritório realiza o gerenciamento de sua rede da seguinte forma:

- ✓ Instala e mantem um sistema de firewall, que monitora, detecta e bloqueia ameaças, impedindo conexões a redes não confiáveis. No caso de serviços web, são utilizados firewalls de aplicação web (*Web Application Firewall* – WAF).
- ✓ Protege serviços de e-mail, utilizando antivírus integrados, ferramentas anti-spam e filtros de e-mail.

6.4 MANUTENÇÃO DE PROGRAMA DE GERENCIAMENTO DE VULNERABILIDADES

Em relação ao gerenciamento de vulnerabilidades, o JRA monitora constantemente a existência de novas versões e correções disponíveis em todos os sistemas e aplicativos. Com o objetivo de manter todos os sistemas e aplicativos utilizados no Escritório em suas últimas versões, bem como instalar todas as correções de segurança disponíveis (*patches*) lançadas pelo desenvolvedor do sistema operacional e aplicativos. Outra medida adotada é a atualização de softwares antivírus ou antimalwares, que detectam, impedem e atuam na remoção de programas maliciosos, como vírus.

Por último, o JRA trabalha para 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.

6.5 MEDIDAS RELACIONADAS AO USO DE DISPOSITIVOS MÓVEIS

Em relação aos dispositivos móveis, como smartphones e laptops, caso seu uso seja necessário para fins institucionais, devem estar sujeitos aos mesmos procedimentos de controle de acesso que os outros equipamentos de TI, como o uso da autenticação para acesso aos dispositivos e sistemas de informação do Escritório, além de serem guardados em locais seguros quando não estiverem em uso.

Os colaboradores, estagiários e advogados não devem utilizar dispositivos móveis de uso privado para fins institucionais. 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 um maior gerenciamento do acesso e dos 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 e/ou de informações sigilosas, o JRA implementou funcionalidades que permitem a remoção remota dos dados pessoais relacionados à sua atividade. Isso diminuir a chance de eventual incidente de segurança com dados pessoais e divulgação de informações confidenciais.

7. PLANO DE RESPOSTA E CONTINUIDADE

Em que pese a todas as precauções e medidas de segurança técnicas e administrativas implementadas pelo Escritório, é necessário estar preparados para reagir caso um incidente de segurança se materialize. Essa reação deve ser assertiva e rápida, visando anular ou reduzir o risco de um eventual acesso não autorizado aos dados. Por essa razão, o JRA elaborou um Plano de Resposta a Incidentes, nomeando pessoas responsáveis por detectar, notificar e corrigir o incidente, bem como os protocolos que deverão ser seguidos nestes casos.

O protocolo de atuação consiste em identificar, avaliar e classificar a vulnerabilidade, segundo uma escala de impacto *versus* urgência, onde estão pré-estabelecidas as prioridades e prazos de solução, segundo o nível de criticidade do incidente. Caso seja necessário, em razão da extensão do incidente, poderá ser ativado, ainda, o Plano de Continuidade de Negócios.

O objetivo do Plano de Continuidade do Negócio é manter a integridade e a disponibilidade dos dados do Escritório, bem como a disponibilidade dos serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento das atividades.

Possui ainda como objetivo garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos. O Plano prevê a possibilidade de dar continuidade nas operações produtivas do Escritório em um ambiente de backup.

Por último, será realizada uma avaliação sobre a necessidade de comunicar o incidente à Autoridade Nacional de Proteção de Dados e aos titulares dos dados

afetados, bem como de implementar novas medidas de segurança para evitar que o incidente volte a ocorrer.