Grupo MACIEL

Cartilha de Privacidade, Segurança e Proteção de Dados Pessoais

Documento: V.2	Cartilha de Privacidade, Segurança e Proteção de Dados Pessoais	Data Aprovação: 16/10/2023 Vigência: outubro/2023

ÍNDICE

1. NOSSO COMPROMISSO

Nós somos o Grupo Maciel, uma organização especializada em fornecer serviços que auxiliam empresas a enfrentar seus maiores desafios de forma inovadora, responsável e sustentável. Aqui, prezamos pela privacidade dos titulares de dados pessoais e assumimos o compromisso de respeitar a autodeterminação informativa dos indivíduos, promovendo, interna e externamente, ações que garantam a segurança e proteção dos dados pessoais no tratamento das respectivas informações.

Construímos, de forma pioneira, uma equipe competente e transdisciplinar, com atuação conjunta das áreas de tecnologia da informação, segurança da informação, jurídico, administrativo, Compliance e auditoria, proporcionando, assim, um time preparado para agregar valor aos clientes no tratamento de dados pessoais, observando a privacidade e proteção dos dados pessoais dos titulares de dados.

Além de um grupo de trabalho robusto, que presta serviços de diagnóstico, implementação e aculturamento, visando à adequação da sua empresa à Lei Geral de Proteção de Dados Pessoais – LGPD, Lei 13.709/2018, DPO as a service, assessoria ao DPO, assessoria de segurança da informação, auditoria para LGPD, o Grupo Maciel conta com um Programa de Governança em Privacidade.

Este garante o adequado tratamento de dados pessoais pela organização, e nomeou seu Encarregado pelo Tratamento de Dados Pessoais (DPO), Luis Felipe Canto Barros, que poderá ser contactado, a qualquer momento, de forma facilitada, através do canal: http://grupomaciel.net.br/contato/.

Com o objetivo de difundir o conhecimento sobre privacidade e proteção de dados pessoais, o Grupo Maciel, disponibiliza diversos cursos e treinamentos para que os profissionais sejam conscientizados e se aprofundem nas peculiaridades sobre o tema, colaborando no desenvolvimento e disseminação de uma cultura em privacidade e proteção de dados.

Ampliando nossas ações, desenvolvemos e disponibilizamos nossa Cartilha de Privacidade, Segurança e Proteção de dados, que abordará, de forma clara e descomplicada, os principais conceitos da LGPD, fornecendo, ainda, dicas de boas práticas e materiais adicionais.

2. CONCEITOS

- **Agentes de Tratamento:** Controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e Operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador).
- **Autodeterminação Informativa:** faculdade do titular em exercer controle sobre seus dados pessoais, cabendo a este decidir, na medida do possível, sobre o tratamento de seus dados pessoais.
- **Autoridade Nacional de Proteção de Dados (ANPD):** autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio, responsável pela proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** dado pessoal 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.
- **Encarregado pelo Tratamento de Dados Pessoais (DPO): pessoa** indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Titular de Dados Pessoais:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento de Dados Pessoais:** 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.

- **Incidente de Segurança com Dados Pessoais:** qualquer evento adverso, 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.

3. DICAS DE BOAS PRÁTICAS

1. Os usuários têm obrigação de bloquear as estações de trabalho ao se afastarem do equipamento, impedindo eventual acesso não autorizado por terceiros.
2. Computadores e dispositivos similares devem ser configurados para usar protetores de tela ativados por tempo e protegidos por senha, impedindo acesso não autorizado em equipamentos desacompanhados.
3. As estações de trabalho são pessoais. Não utilize a estação de outro colaborador sem a autorização da liderança e a devida comunicação à equipe técnica.
4. Ao final do expediente, ou em caso de ausência prolongada do local de trabalho, a mesa de trabalho deve permanecer limpa, documentos guardados, gavetas e armários trancados e computador desligado.
5. Realize a manutenção da sua caixa de e-mail adequadamente, evitando acúmulo de e-mails e arquivos desnecessários.
6. Não utilize seu e-mail particular para fins corporativos.
7. Evite utilizar seu e-mail corporativo para fins particulares.
8. Não mantenha sua credencial de acesso salva automaticamente nos sistemas ou anotada em agendas e post it na tela no notebook.
09. Computadores e dispositivos similares devem estar posicionados de

forma a evitar que transeuntes identifiquem informações das telas.

10. Não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.
11. Não instale qualquer software em um computador local sem a permissão do gestor imediato ou da equipe técnica.
12. Os sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados se encontram na lista proibida e são bloqueados para acesso.
13. As credenciais de acesso são pessoais, intransferíveis e de responsabilidade do colaborador.
14. As senhas não devem ser compartilhadas ou anotadas, sendo necessário, utilize um gerenciador de senhas.
15. As senhas devem seguir um padrão complexo.
16. Evite senhas que tenham informações pessoais, como nomes, datas de aniversário, placa de automóvel, número de telefone etc.
17. Não utilize senhas de contas pessoais em contas corporativas.
18. Os documentos e arquivos físicos não devem permanecer sobre a mesa desnecessariamente, armazene a documentação em armários ou gavetas trancadas.
19. Anotações, recados e lembretes, que tenham dados pessoais, não devem ser deixados à mostra sobre a mesa, anotados em quadros brancos ou colados em paredes, divisórias, murais ou monitor do computador.
20. Guarde agendas e cadernos de anotações, assim como objetos pessoais, em gavetas ou armários trancados.
21. Devolva os documentos obtidos por empréstimos de outros departamentos.
22. Descarte, de forma segura, os documentos físicos que tenham dados pessoais. Sendo possível, utilize fragmentadoras.
23. Evite imprimir documentos apenas para lê-los ou desnecessariamente; priorize a documentação no formato digital.
24. Evite arquivar documentos e informações que tenham dados pessoais em arquivos duplicados. Mantenha apenas os arquivos atualizados.
25. Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente.
26. Impressões inutilizadas que tenham dados pessoais não devem ser reaproveitadas ou utilizadas como rascunho. O documento deverá ser picotado, de forma mecânica ou manual, e colocado no lixo de forma segura, caso

não tenha fragmentadora disponível.

27. Colete apenas os dados necessários ao desempenho de sua atividade e do escopo da empresa.

28. O acesso aos dados pessoais deverá ser autorizado apenas para usuários que necessitam das informações para desempenho de suas atividades profissionais.

29. Tenha controle e conhecimento sobre os dados pessoais que acessa, a finalidade do tratamento, eventuais compartilhamentos com terceiros, forma e prazo de armazenamento, meio de descarte, entre outras informações pertinentes.

30. Cada usuário deverá tratar apenas as informações e ambientes previamente permitidos. A tentativa consciente de acesso a ambientes/dados não autorizados será passível de punição.

31. Caso algum setor ou agente externo solicite dados pessoais dos titulares de dados tratados pelo seu departamento, verifique a finalidade da utilização pelo terceiro e se o procedimento está regularmente previsto. Havendo dúvida sobre a possibilidade de compartilhamento das informações, busque auxílio de seu gestor imediato ou, ainda, do Encarregado de Dados Pessoais da instituição.

32. Antes de fornecer informações com dados pessoais para terceiros, verifique a identidade do solicitante.

33. O uso de dispositivos de armazenamento externo (pendrive, HD) deve ser autorizado por seu gestor imediato ou pela equipe técnica. Ainda que o uso seja autorizado, evite fazer cópias de arquivos com dados pessoais para dispositivos de armazenamento externo.

34. Evite realizar sua atividade de seu dispositivo móvel particular.

35. Conforme determinado pela Alta Administração, apenas sócios e profissionais em nível de gestão têm autorização para instalação de ferramentas corporativas em dispositivos móveis.

36. O envio de documentos ou informações com dados pessoais não deverá ser realizado através de dispositivo pessoal ou contas pessoais.

37. Os métodos de troca de mensagens devem ser definidos de acordo com a Norma de Classificação da Informação. Caso tenha dúvida, consulte o gestor imediato para determinar o melhor método para troca de mensagens classificadas.

38. Caso haja eventual recebimento de documentos ou informações com dados pessoais em dispositivos pessoais, transmita, imediatamente, a mídia para

seu computador corporativo e exclua terminantemente do seu dispositivo pessoal.

39. Os dispositivos móveis, pessoais ou corporativos, deverão ser configurados para utilização de senhas, biometria e/ou reconhecimento facial para acesso – de preferência com duplo grau de segurança (a utilização de duas das opções de forma simultânea).

40. Não abra e-mails de desconhecidos e não baixe arquivos duvidosos. Se estiver em dúvida, apague-os ou reporte à equipe técnica.

41. Ao receber e-mails, para garantir a segurança do conteúdo, confirme a identificação do remetente, confira eventual URL enviada, não clique em links ou responda e-mails suspeitos, identifique a existência de mensagens em língua estrangeira, identifique a estética da mensagem (cores, assinatura, logo), identifique a existência de erros gramaticais nas mensagens. Sendo necessário, busque informações junto com a instituição que enviou a respectiva mensagem.

42. Não execute instruções recebidas por e-mail que não sejam da equipe da equipe técnica.

43. Não altere ou desative qualquer aplicativo ou sistema implementado pela empresa.

44. Tenha conhecimentos das políticas que se refiram a dados pessoais da sua empresa.

45. Conheça as medidas de segurança fornecidas pela empresa e execute suas atividades implementando as respectivas medidas, de acordo com a sensibilidade da informação tratada.

46. Participe ativamente de projetos, campanhas, treinamentos e ações de aculturamento promovidos pela sua empresa, visando a disseminação de uma cultura em privacidade e proteção de dados pessoais.

47. Você, colaborador, também é titular de dados pessoais. As ações de segurança e proteção de dados implementadas pela empresa garantem a sua própria proteção.

48. Caso verifique indícios de incidentes com dados pessoais ou algum procedimento em desacordo com as normas da empresa, reporte ao seu gestor imediato para providências junto ao Encarregado de Dados Pessoais da instituição.

49. Ao realizar a contratação de algum parceiro, siga as orientações relacionadas à proteção de dados, providenciando a devida análise da maturidade do parceiro e cláusulas contratuais adequadas.

50. Caso receba alguma solicitação de titulares de dados, redirecione ao

Encarregado de Dados Pessoais da instituição para que o respectivo responsável realize as providências necessárias.

51. Caso tenha dúvida sobre assuntos relacionados à proteção dos dados pessoais, converse com o DPO/Encarregado de Dados Pessoais.