Segurança da Informação nas ações cotidianas

LGPD | Manual de boas práticas

Elaborado por: Ingrid Martinez – Governança Corporativa - Data: 16/09/2024 - Nº da Revisão: 00

www.digix.com.br

Sumário

Introdução

Bem-vindo ao Manual de “Boas Práticas de Segurança da Informação”. Ele foi elaborado com o objetivo de orientar a implementação e manutenção de práticas que garantam a proteção e a privacidade dos dados pessoais, em conformidade com a “Política de Segurança da informação” e proteção de dados da Digix, a legislação vigente, Regulamento Interno, especialmente a Lei Geral de Proteção de Dados (LGPD).

A responsabilidade pelo cumprimento deste manual é compartilhada entre todos os níveis da organização.

Certas áreas possuem maior capacidade para implementar e monitorar as diretrizes, assegurando uma abordagem integrada e colaborativa.

Nosso compromisso é assegurar que todas as operações de tratamento de dados pessoais sejam realizadas de forma transparente, segura e ética, promovendo a confiança de nossos clientes, parceiros e colaboradores. Acreditamos que a proteção de dados é um pilar essencial para a sustentabilidade e o sucesso de nossa organização.

Leia o “Manual” e ajude a fortalecer a proteção dos dados na Digix.

1. Senhas

Responsável: todos os colaboradores.

- Criação de Senhas Fortes: Utilizar senhas complexas, com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- Troca Regular de Senhas: Alterar senhas periodicamente e nunca reutilizar senhas antigas.
- Armazenamento Seguro: Nunca anotar senhas em papéis, locais de fácil acesso ou compartilhá-las com outras pessoas. Utilizar gerenciadores de senhas/cofres digitais.

2. Mesa Limpa

Responsável: todos os colaboradores.

- Documentos Físicos: Manter a mesa de trabalho limpa de documentos quando não estiverem em uso. Não deixar documentos em papéis, anotações, recados e lembretes importantes, incluindo aqueles colados em seu monitor ou divisórias (post-it) e mídias removíveis (pendrives e HDs externos) sobre a mesa desnecessariamente. Guardar documentos em locais seguros.
- Descarte Seguro: Destruir documentos sensíveis de forma segura, utilizando trituradores de papel.
- Sala de Reunião: Verificar ao final das reuniões se todos os papéis foram retirados, se o quadro foi apagado e se a folha do *flipchart* foi descartada apropriadamente.

3. Anonimização de Dados

Responsável: todos os colaboradores e OPTI.

- Minimização de Dados: Coletar e armazenar apenas os dados necessários para a finalidade específica.
- Anonimização: Sempre que possível, anonimizar dados pessoais para reduzir os riscos associados ao tratamento de dados sensíveis.

4. E-mails

Responsável: todos os colaboradores.

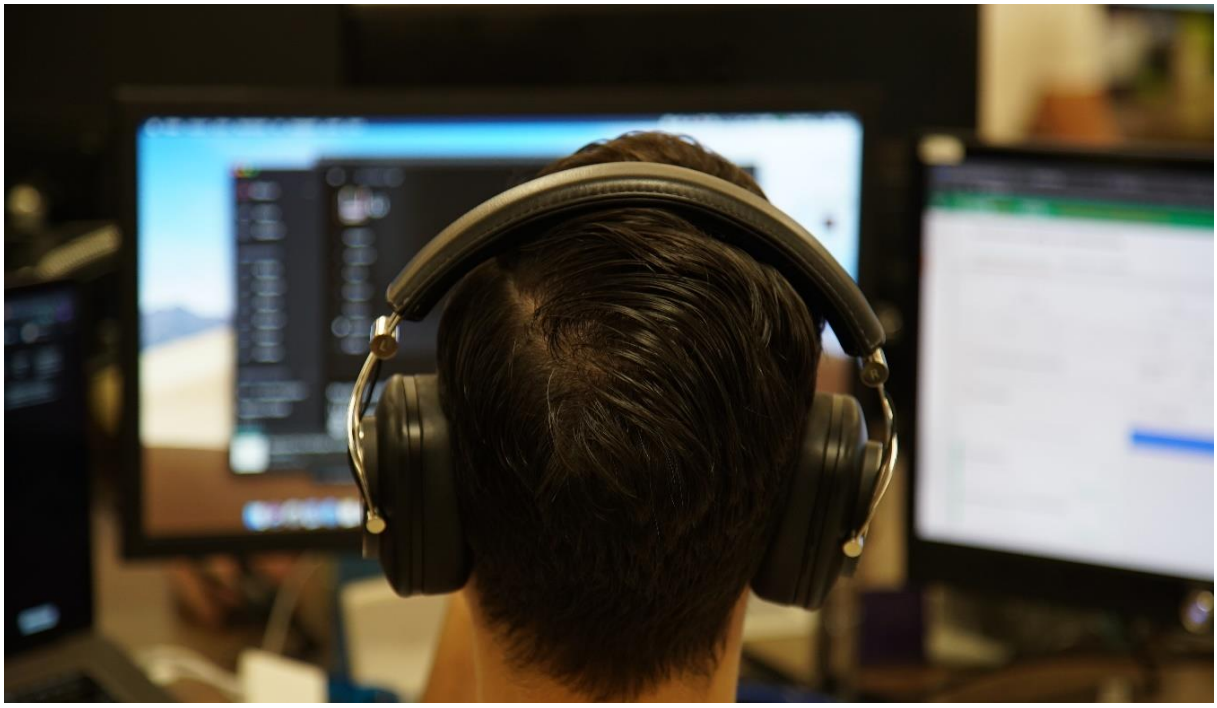
- Cuidado com Phishing: Ser cauteloso com e-mails suspeitos e não clicar em links ou abrir anexos de remetentes desconhecidos.
- Confidencialidade: Não compartilhar informações sensíveis por e-mail sem as devidas precauções, como criptografia.
- Limpeza: Periodicamente realizar a limpeza da caixa de e-mail, deletando correspondências que contenham dados pessoais e/ou sensíveis que já atingiram a finalidade do uso.

5. Proteção contra ameaças - Antivírus e Antimalware

Responsável: todos os colaboradores e OPTI.

- Instalação e Atualização: Manter soluções de antivírus e antimalware instaladas e atualizadas em todos os dispositivos (estações de trabalho e servidores).
- Verificações Regulares: Realizar verificações regulares para identificar e remover possíveis ameaças, como vírus, códigos maliciosos e *ransomware*.
- Backup: Realizar backups regulares e testes de recuperação.

6. Home Office



Responsável: todos os colaboradores e OPTI.

- Ambiente Seguro: Garantir que o ambiente de trabalho em casa seja seguro e livre de interrupções.
- Acesso Remoto Seguro: Utilizar VPNs e outras medidas de segurança para acessar sistemas corporativos.
- Criptografia: Criptografar dispositivos utilizados em home office.
- Equipamentos: Utilizar apenas equipamentos fornecidos pela Digix ou autorizados para o trabalho remoto.

7. Licenciamento de Softwares e Softwares Não Autorizados

Responsável: todos os colaboradores e OPTI.

- Softwares Licenciados: Utilizar apenas softwares licenciados e autorizados pela Digix.
- Proibição de Softwares Não Autorizados: Não instalar ou utilizar softwares não autorizados nos dispositivos da Digix.
- Licenças: Regularmente verificar e atualizar licenças.

8. Uso e Controle de Equipamentos

Responsável: todos os colaboradores, Facilidades e OPTI.

- Responsabilidade: Manter os equipamentos fornecidos pela Digix em boas condições e reportar qualquer problema imediatamente.
- Segurança: Não deixar equipamentos desprotegidos em locais públicos ou de fácil acesso.
- Inventário: Manter uma lista atualizada de todos os equipamentos.
- Equipamento pessoais: Restringir o uso de dispositivos pessoais para fins corporativos. Armazenar arquivos pessoais em rede distinta a da Digix.
- Bloquear a tela: Sempre que se ausentar do computador, bloqueie a tela para prevenir acessos não autorizados.

9. Uso de Internet

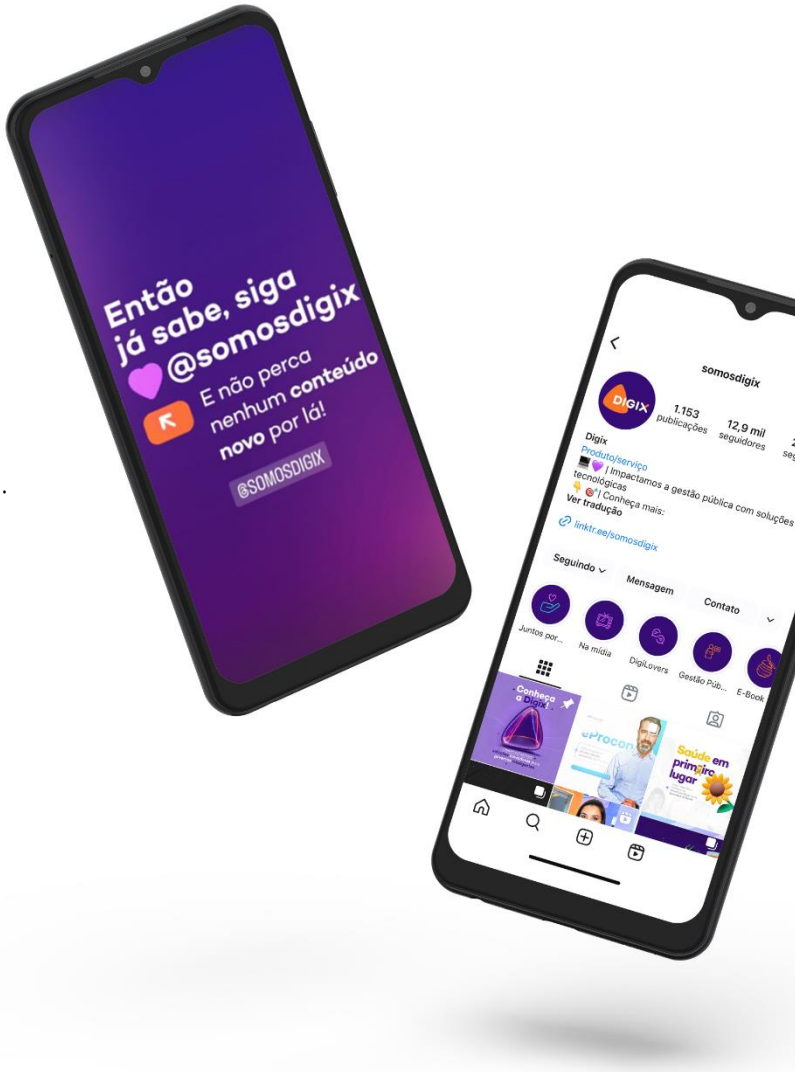
Responsável: todos os colaboradores.

- Uso Adequado: Utilizar a internet e o correio eletrônico da Digix apenas para fins profissionais.
- Segurança: Evitar acessar sites suspeitos ou baixar arquivos de fontes não confiáveis. Monitorar o uso da internet.

10. Redes Sociais

Responsável: todos os colaboradores.

- Cuidado com Informações: Não compartilhar informações sensíveis ou confidenciais da Digix em redes sociais.
- Segurança: Monitorar o uso de redes sociais.



11. Participação em Eventos e Feiras

Responsável: todos os colaboradores e gestão.

- Confidencialidade: Manter a confidencialidade das informações da Digix durante eventos e feiras. Proteger dispositivos e documentos utilizados em eventos.
- Autorização: Obter autorização antes de compartilhar qualquer informação sensível em eventos externos. Ao coletar dados pessoais, seja para fins de prospecção, sorteio, etc, obter o consentimento. Se pessoa jurídica, não precisa do consentimento.

12. Plano de Backup e Cópias de Segurança

Responsável: todos os colaboradores e OPTI.

- Backup Regular: Realizar backups regulares dos dados importantes.
- Armazenamento Seguro: Armazenar as cópias de segurança em locais seguros e protegidos.
- Criptografia: Criptografar todos os backups, os discos dos notebooks utilizados pelos colaboradores para em caso de roubo ou extravio, as informações contidas nos dispositivos permanecerem seguras e protegidas contra acessos não autorizados.

13. Lista de Contatos

Responsável: todos os colaboradores, gestão e OPTI.

- Manutenção Atualizada: Manter uma lista atualizada de contatos vitais, incluindo colaboradores, fornecedores e clientes.
- Acesso Restrito: Garantir que a lista de contatos seja acessível apenas a pessoas autorizadas.

14. Segurança Física

Responsável: Facilidades.

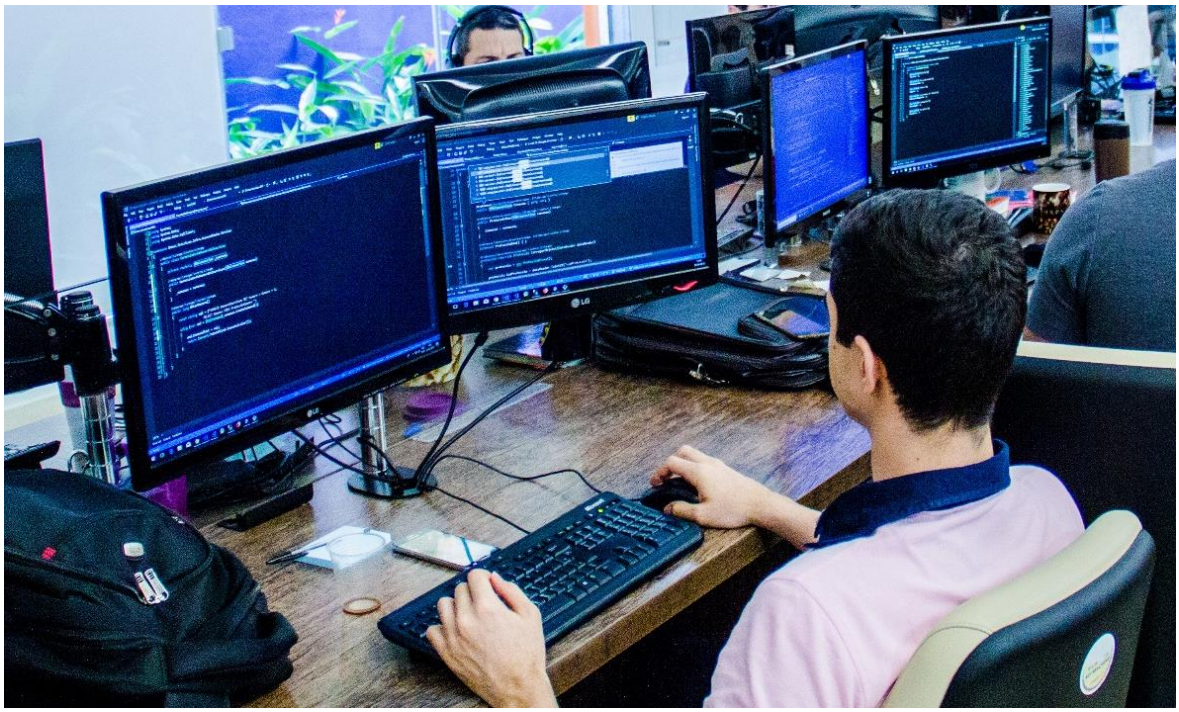
- Controle de Acesso: Implementar sistemas de controle de acesso para áreas críticas, garantindo que apenas pessoas autorizadas possam entrar.
- Identificação: Utilizar métodos de identificação para todos os colaboradores e visitantes, tais como, mas não se limitando a biometria, crachás, códigos QR, aplicativos móveis, senhas, entre outros.
- Registro de Acessos: Manter um registro detalhado de todos os acessos a áreas críticas, incluindo data, hora e identidade da pessoa.
- Monitoramento: Instalar câmeras de segurança em áreas estratégicas e garantir que as imagens sejam armazenadas de forma segura e acessíveis apenas a pessoas autorizadas. Informar as pessoas que estão sendo filmadas.

15. Imagens de Câmeras de Segurança

Responsável: Facilidades.

- Armazenamento Seguro: Garantir que as imagens das câmeras de segurança sejam armazenadas de forma segura e protegidas contra acesso não autorizado.
- Prazo de Retenção: Definir o prazo de retenção e descarte das imagens, em conformidade com a legislação aplicável.

16. Exclusão de Acessos



Responsável: todos os colaboradores e o OPTI.

- Desativação de Acessos: Garantir que os acessos às ferramentas e tecnologias da Digix sejam desativados imediatamente após o desligamento de um colaborador.

- Revisão Periódica: Realizar revisões periódicas dos acessos para garantir que apenas pessoas autorizadas tenham acesso às ferramentas e tecnologias.

17. Utilização de E-mail Corporativo

Responsável: todos os colaboradores.

- Ferramentas de Trabalho: Utilizar, sempre que possível, o e-mail corporativo para acessar as ferramentas de trabalho, tais como, mas não se limitando a: Adm Sites, Adobe, All Strategy, Analytics, Anchor, Aprecie.me, Auth0, Bitly, Bubble, Canva, Cap Cut, ChatGPT, Ekyte, Envato, Feedz, Figma, Flickr, FlutterFlow, Google ADS, Google Analytics, Google Tag Manager, Hotjar, InHire, Instagram, X, Sênior, JetBrains, Mindsight, Miro, Nave, Notion, Pipe Drive, Plano, RD Station, Shutterstock, Spotify, StreamYard, Supabase, Taggo, Trello, Vault e YouTube.

18. Uso de MFA – Múltiplo Fator de Autenticação

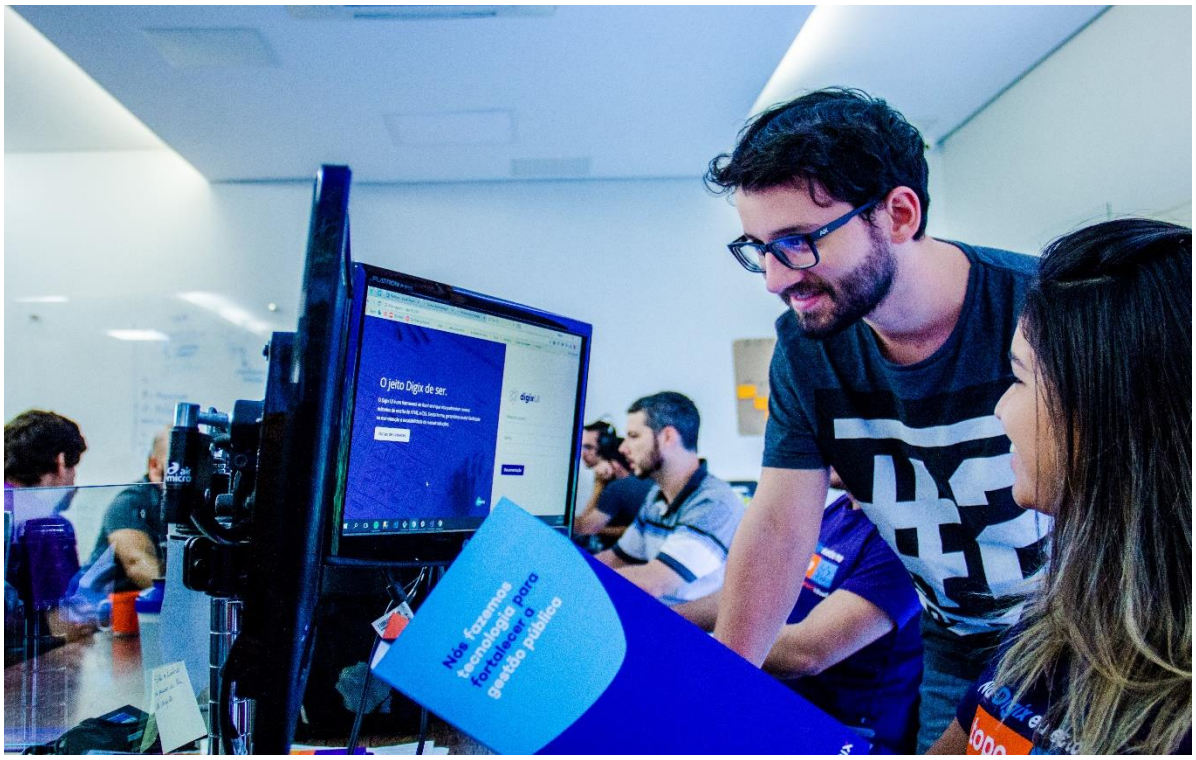
Responsável: todos os colaboradores.

- Implementar MFA: habilitar em todas as plataformas que forneçam este método, independente da criticidade. Reforçar a autenticação com fatores adicionais (ex.: SMS, aplicativos autenticadores).

19. Confidencialidade e Necessidade de Conhecimento

Responsável: todos os colaboradores, Gestão e Governança.

- Comunicação Segura: É essencial que os dados pessoais sob sua responsabilidade não sejam revelados ou compartilhados com indivíduos que não tenham uma necessidade legítima de conhecê-los para a execução de suas funções, devendo ser tratados com o mais alto nível de confidencialidade.
- Acordos de confidencialidade: São estabelecidos acordos de confidencialidade, termos de responsabilidade ou cláusula de confidencialidade com os colaboradores, clientes e prestadores de serviços.
- Minimização de Dados: Compartilhe apenas a quantidade mínima de dados pessoais necessária para a realização da tarefa específica. Evite a divulgação de informações excessivas ou irrelevantes.



20 - Exceções

Responsável: Gestão, Encarregado de dados e o OPTI.

- Avaliar exceções caso a caso.
- Documentar e justificar exceções.

21 – Relato de Incidentes

Responsável: todos os colaboradores.

- Relato de Incidentes: Caso ocorra qualquer incidente de segurança ou suspeita de violação de dados, comunique a Digix imediatamente através do Encarregado de Proteção de Dados (DPO) ou o substituto, através do canal oficial – lgpd@digix.com.br. A rápida comunicação é crucial para mitigar possíveis danos.

22 - Conclusão

A implementação das boas práticas e diretrizes de governança para privacidade de dados, conforme estabelecido neste manual, é fundamental para garantir a conformidade com a LGPD e proteger os direitos dos titulares

de dados. A adesão a essas práticas não apenas fortalece nossa reputação e confiança no mercado, mas também contribui para a construção de um ambiente de negócios mais seguro e ético.

Reforçamos a importância do compromisso de cada colaborador em seguir as orientações aqui apresentadas e em participar ativamente dos treinamentos e atualizações sobre privacidade de dados. A proteção de dados é uma responsabilidade coletiva e contínua, que exige vigilância e dedicação constantes.

Juntos podemos garantir que a Digix continue a operar de maneira responsável e em conformidade com as exigências legais, protegendo os dados pessoais de todos os nossos stakeholders.

23 - Nosso contato

Se você tiver dúvidas ou preocupações em relação à sua privacidade ou ao tratamento de seus dados pessoais pela Digix, entre em contato com a nossa Encarregada de Dados – Ingrid Roberta Martinez, através do e-mail lgpd@digix.com.br.

Telefone: +55 (67) 3345-6500

24 – Revisões

Eventualmente poderemos fazer alterações neste manual de “Boas Práticas de Segurança da Informação”. Se fizermos qualquer alteração substancial no documento, publicaremos essas alterações. Consulte também a nossa “Política de Segurança da informação e Proteção de Dados” e a “Política de Privacidade” regularmente.

Controle de alterações

Revisão	Data publicação	Descrição
00	16/09/2024	Versão Inicial