Manual de Boas Práticas de Segurança da Informação e Proteção de Dados Pessoais

Elaborado por: Roberta Ribeiro

RGM: 39708471

São Paulo, 2025

1. O que é a LGPD?

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) regula o tratamento de dados pessoais em meios físicos e digitais. Define princípios, direitos e deveres que empresas e colaboradores devem respeitar.

Exemplo prático: quando um jogador se cadastra em um game, fornecer nome, e-mail e idade já caracteriza tratamento de dados pessoais.

2. Princípios da LGPD (Art. 6º)

• Finalidade: uso específico e legítimo;

• Adequação: compatibilidade com a finalidade informada;

• Necessidade: coleta apenas dos dados mínimos necessários;

• Transparência: clareza ao informar o uso;

• Segurança: medidas para proteger os dados;

• Prevenção: evitar incidentes.

Exemplo prático: ao pedir CPF do jogador, explicar que será usado apenas para emissão de nota fiscal.

3. Responsabilidades dos Colaboradores

- Senhas: usar senhas fortes, não compartilhar, trocar periodicamente.

Exemplo: ao sair para o almoço, bloquear o computador com Win+L.

- Equipamentos: manter antivírus atualizado, não usar dispositivos pessoais sem autorização.

Exemplo: não salvar dados de jogadores em pen drive pessoal.

- E-mails: desconfiar de anexos suspeitos, não enviar dados sensíveis sem criptografia.

Exemplo: se receber e-mail pedindo senha, encaminhar ao DPO.

- Dados de jogadores: coletar apenas o necessário e nunca compartilhar sem autorização.

Exemplo: não repassar lista de e-mails de jogadores a empresas terceiras sem consentimento.

4. Boas Práticas no Desenvolvimento de Jogos

• Adotar privacy by design;

• Usar anonimização e pseudonimização de dados;

• Garantir segurança de APIs e servidores;

• Aplicar acesso mínimo.

Exemplo: limitar acesso ao banco de dados de jogadores apenas para equipe autorizada.

5. Medidas de Segurança da Empresa

• Política de backups;

• Controle de acessos;

• Monitoramento de atividades;

• Treinamentos regulares.

Exemplo: backup diário criptografado e armazenado em servidor seguro.

6. Consequências do Não Cumprimento

O descumprimento pode causar multas, danos à reputação, sanções administrativas e até responsabilização civil.

Exemplo: um colaborador que compartilha indevidamente dados pode gerar multa milionária para a empresa.

7. Canal de Comunicação e Denúncias

Qualquer incidente deve ser reportado imediatamente ao DPO (Encarregado de Dados):

■ dpo@empresaexemplo.com.br

Exemplo: ao identificar invasão de conta de jogador, comunicar o DPO imediatamente.

8. Compromisso do Colaborador

TERMO DE COMPROMISSO Eu, , matrícula nº 39, declaro que:

• Li e compreendi o Manual de Segurança da Informação;

• Estou ciente das obrigações da LGPD;

• Comprometo-me a manter sigilo, não compartilhar senhas, respeitar os princípios e comunicar incidentes. Local e data: _____ Assinatura do colaborador: _____