TEMPLATE – AMPLIANDO A CONSISTÊNCIA DO NEGÓCIO

Patrícia Maura Angelini

Versão 1

HISTÓRICO DE VERSÕES

Versão	Data	Responsável	Descrição
1	19/08/2024	Patrícia Maura Angelini	Versão Inicial Template PBL Fase 3 - CAP 01 – A**MPLIANDO A CONSISTENCIA DO NEGOCIO**
	19/08/2024	Rita de Cássia Rodrigues	Revisão acadêmica

FICHA CATALOGRÁFICA

[NÃO PREENCHER - PARA USO DO DEPTO DE EAD E BIBLIOTECA]

A000a Sobrenome, Nome

Título [livro eletrônico] / Nome Sobrenome. -- São Paulo : Fiap, 2016.
x MB ; ePUB

Bibliografia.
ISBN 000-00-00000-00-0

Categoria. 2. Subcategoria. S., Nome. II. Título.

CDU 000.000.00

Formatado: Italiano (Itália)

RESUMO

Template para atividade de PBL fase 3 1º ano TSC.

Palavras-chave: PBL. FASE 3. TEMPLATE

LISTA DE FIGURAS

Formatado: Inglês (Estados Unidos)

Código de campo alterado

LISTA DE QUADROS

LISTA DE TABELAS

Formatado: Português (Brasil)

LISTA DE CÓDIGOS-FONTE

Formatado: Inglês (Estados Unidos)

Código de campo alterado

LISTA DE COMANDOS DE PROMPT DO SISTEMA OPERACIONAL

Formatado: Português (Brasil)

SUMÁRIO

POTENCIALIZANDO O DESEMPENHO COM NOSQL

1 INSTRUÇÕES PARA USO DO TEMPLATE

1.1 Template

Um template é um modelo predefinido que simplifica e padroniza a criação de documentos, páginas da web ou outros elementos de design, permitindo que usuários preencham apenas as partes específicas, economizando tempo e garantindo consistência visual ou estrutural.

Para seu uso leia as instruções nesse e use o template a partir da seção 2

1.1 Instruções

O template está dividido por seções que representam pedidos feitos para o PBL. No template iremos encontrar exemplos ilustrativos de entregas, cujo contexto não tem relação ao que está sendo solicitado no PBL.

Ao usar o template, apague por completo a seção 1 de instruções para que o seu trabalho fique mais organizado.

Não se esqueça de salvar o template em .pdf para a entrega.

A seguir um Quadro Resumo das tarefas:

Solicitação.

1. Um roteiro de trabalho para a empresa Melhores Compras se adequar a LGPD .

A partir deles desenvolva os passos:

- Contextualização do papel da TI em relação à LGPD
  - Frente as tarefas diárias da própria TI
  - Frente à plataforma de eCommerce
- Recomendações de proteção aos dados
  - Destacar no mínimo duas recomendações
  - Descrever o benefício de cada recomendação
- Anonimização
  - Relacionar todos os dados de clientes disponíveis
  - Definir dois dados para serem anonimizados

~~o Justificar as escolha~~

~~Quadro 1 – Quadro resumo das tarefas do PBL~~
~~Fonte: Elaborado pelo autora (2024)~~

2 CONTEXTUALIZAÇÃO DO PAPEL DA TI EM RELAÇÃO À LGPD

A área de Tecnologia da Informação (TI) exerce papel fundamental na aplicação prática da Lei Geral de Proteção de Dados (LGPD), sendo responsável tanto pelo suporte técnico quanto pela sustentação dos processos que asseguram o cumprimento da norma. Desde o planejamento até as operações cotidianas, a TI atua como pilar essencial para a proteção de dados, implementando soluções que automatizam consentimentos, gerenciam os direitos dos titulares, fortalecem a segurança da informação e promovem o monitoramento constante.

Em termos gerais, a TI garante a viabilidade técnica da LGPD por meio de práticas que integram tecnologia, governança e conformidade legal.

Existem algumas funções que são determinantes para resumir o papel da TI, por exemplo, Automatização de processos de consentimento, gerenciamento de direitos dos titulares, implementação de medidas técnicas e operacionais, treinamentos e monitoramento e auditoria continua.

Em resumo, a Tecnologia da Informação é o alicerce fundamental para a implementação da LGPD, pois envolve a criação, implementação e manutenção de soluções técnicas e operacionais que garantam a conformidade com a legislação

~~Descreva o papel da TI frente a LGPD.~~

2.1 Aplicação da LGPD nas tarefas da TI

As rotinas operacionais da TI são decisivas para garantir que a organização esteja em conformidade com a LGPD. Isso inclui a proteção dos dados de colaboradores e demais partes interessadas. A TI deve assegurar que as informações sejam coletadas e utilizadas de forma transparente, limitada à finalidade para a qual

foram obtidas, e resguardadas por mecanismos robustos de segurança.

Entre as práticas recomendadas estão a criptografia de dados sensíveis, o controle rigoroso de permissões de acesso com base na função de cada usuário, além do uso de logs que possibilitem rastrear as atividades realizadas. Também é papel da TI participar da definição das políticas de privacidade internas, promover treinamentos e realizar auditorias regulares. Assim, o setor atua de forma estratégica, reduzindo riscos e garantindo um ambiente seguro e conforme à legislação.

~~Descreva como as operações diárias do setor de TI impactam o cumprimento da LGPD.~~

~~Explique como a TI deve assegurar a conformidade com a proteção de dados pessoais no tratamento de dados internos, como registros de colaboradores, controle de acessos, e outras operações rotineiras.~~

2.2 Aplicação da LGPD na plataforma de eCommerce

No ambiente do comércio eletrônico, a proteção de dados ganha ainda mais relevância devido à grande quantidade de informações pessoais envolvidas. Cabe à equipe de TI implementar políticas e práticas que assegurem o correto tratamento desses dados, com foco em segurança, controle e resposta a incidentes.

É necessário armazenar apenas o essencial, com o uso de criptografia e autenticação multifatorial para evitar acessos não autorizados. O controle de acesso deve ser bem definido, com permissões específicas para cada nível de usuário. A rastreabilidade de ações, backups seguros e o descarte adequado de arquivos também são pontos críticos.

Além disso, é essencial que a equipe de TI esteja preparada para lidar com eventuais vazamentos de dados, por meio de planos de resposta ágeis e eficazes. A constante atualização dos sistemas e a capacitação da equipe completam o processo, garantindo que a organização atue de maneira preventiva e esteja alinhada à LGPD.

Para assegurar a conformidade com a LGPD, a TI deve adotar práticas que garantam o tratamento adequado dos dados pessoais de colaboradores e demais usuários internos. Isso inclui armazenar apenas as informações realmente necessárias, protegê-las com mecanismos como criptografia e autenticação multifator, e controlar rigorosamente quem pode acessá-las. No caso de registros de colaboradores, por exemplo, é essencial que a equipe de TI assegure que esses

dados estejam armazenados em ambientes seguros, com acesso restrito apenas a profissionais autorizados, sempre com base em uma justificativa legal clara e legítima.

Além disso, o controle de acessos deve ser estruturado de forma que cada colaborador tenha acesso apenas às informações que são relevantes para sua função. Isso exige a implementação de políticas de segurança, gestão de identidade e rastreamento de atividades, de modo que qualquer acesso ou alteração em dados sensíveis possa ser auditado. Mesmo atividades rotineiras como envio de e-mails, realização de backups ou descarte de arquivos devem ser conduzidas com atenção à proteção de dados, adotando práticas que evitem exposições acidentais ou intencionais de informações pessoais.

O setor de TI também deve estar preparado para lidar com incidentes de segurança, mantendo planos de resposta e comunicação que permitam agir rapidamente em caso de vazamento ou uso indevido de dados, conforme exige a LGPD. Por fim, a constante atualização dos sistemas, bem como a capacitação da equipe de TI sobre boas práticas e obrigações legais, é essencial para manter um ambiente tecnológico alinhado às exigências da lei. Dessa forma, a área de TI não apenas apoia a conformidade com a LGPD, como também fortalece a governança de dados e a confiança na organização.

~~Explique como a TI deve gerenciar a segurança e o cumprimento da LGPD em relação à plataforma de eCommerce da empresa.~~

~~Discuta as práticas de segurança e privacidade que precisam ser implementadas para garantir a proteção dos dados pessoais dos clientes.~~

3 RECOMENDAÇÕES DE PROTEÇÃO AOS DADOS

3.1 Recomendação 1

Uma das formas mais eficazes de proteger dados pessoais é por meio da criptografia. Informações como dados bancários e de cartões devem ser protegidas tanto no armazenamento quanto durante a transmissão. A aplicação de protocolos como SSL/TLS e criptografia AES ajuda a evitar que terceiros consigam interpretar os dados em caso de acesso indevido.

Formatado: Recuo: Primeira linha: 0 cm

Vantagem: Mesmo que ocorra uma violação, os dados criptografados se tornam

inutilizáveis, protegendo a privacidade dos titulares e cumprindo os requisitos da LGPD.

Como Implantar: A criptografia deve ser aplicada a todos os **dados sensíveis** dos consumidores, como informações de pagamento, dados de cartão de crédito e qualquer outra informação que possa ser considerada confidencial. A Melhores Compras pode utilizar criptografia de ponta a ponta (end-to-end) para garantir que os dados sejam criptografados tanto em trânsito (durante a transmissão) quanto em repouso (armazenados nos servidores).
Passos:

Aplicar criptografia **SSL/TLS** no site para proteger a comunicação entre o navegador do cliente e o servidor da plataforma.

Utilizar criptografia **AES** para dados armazenados nos bancos de dados, garantindo que apenas usuários autorizados possam descriptografar essas informações.

Benefício: A criptografia de dados sensíveis assegura que, mesmo que haja um **acesso não autorizado** aos servidores ou ao banco de dados, os dados estarão protegidos e ilegíveis, evitando o vazamento de informações privadas e cumprindo com a LGPD ao garantir a segurança dos dados pessoais dos consumidores.

~~Descreva a recomendação.~~

~~Benefícios: Explique como essa recomendação ajudará a proteger os dados pessoais dos clientes e/ou colaboradores, destacando o impacto positivo na conformidade com a LGPD~~

3.2 Recomendação 2

O acesso aos dados deve ser controlado com base em funções específicas dentro da organização. Isso garante que cada colaborador visualize apenas as informações necessárias para sua atuação. A autenticação multifatorial adiciona uma camada extra de segurança, dificultando o acesso não autorizado.

Formatado: Recuo: Primeira linha: 0 cm

Vantagem: Reduz significativamente o risco de exposição acidental ou mal-intencionada de informações sensíveis, reforçando a confiança dos usuários e a conformidade legal.

Como Implantar: Para garantir que apenas os colaboradores autorizados tenham acesso aos dados pessoais dos clientes, é fundamental implementar um **controle de acesso granular** nos sistemas da plataforma. Isso inclui a definição de permissões baseadas na função de cada usuário (RBAC - **Role-Based Access Control**). Além disso, a autenticação multifatorial (MFA) deve ser implementada para garantir uma camada extra de segurança.
Passos:

Definir papéis e permissões: A plataforma deve permitir que diferentes níveis de acesso sejam definidos, como administradores, atendentes de suporte e desenvolvedores, com permissões específicas para cada grupo. Por exemplo, apenas o time de suporte pode visualizar dados de clientes, e somente administradores podem alterar configurações críticas.

Implementar MFA: O sistema de login da plataforma deve exigir não apenas uma senha, mas também um segundo fator de autenticação, como **código enviado por SMS ou aplicativo autenticador**, para aumentar a segurança.

Benefício: O controle de acesso adequado e a autenticação multifatorial reduzem o risco de **acesso indevido** aos dados pessoais, minimizando a chance de vazamentos ou abusos de dados e aumentando a confiança dos consumidores na plataforma. Isso também está em conformidade com a LGPD, que exige que as empresas protejam os dados pessoais de forma eficaz.

Formatado: Parágrafo da Lista

~~Descreva a recomendação.~~

~~Benefícios: Explique como essa recomendação ajudará a proteger os dados pessoais dos clientes e/ou colaboradores, destacando o impacto positivo na conformidade com a LGPD~~

4 ANONIMIZAÇÃO

4.1 Relação de Dados de Clientes Disponíveis

Nome completo;
CPF;
Data de nascimento;

Sexo Biológico;

Descrição Gênero;

Endereço completo (rua, número, complemento, bairro, cidade, estado, CEP);

Número de telefone;

Endereço de e-mail;

~~Liste todos os tipos de dados de clientes que estão disponíveis na plataforma e que são coletados, armazenados e processados pela empresa.~~

4.1 Definição de Dados para Anonimização

- Dado 1: Endereço completo (rua, bairro, cidade, estado). Justificativa: Pode ser substituído por informações mais genéricas, como apenas a cidade ou um código geográfico.

  Dado 2: Nome completo do cliente. Justificativa: Pode ser convertido em um identificador único ou código, mantendo a utilidade dos dados sem revelar a identidade.

  A anonimização reduz significativamente os riscos em caso de violação e mantém a conformidade com a LGPD ao inviabilizar a identificação direta dos indivíduos.

  Justificativa: O endereço completo dos clientes pode ser **anonimizado** por meio de uma técnica de **generalização** ou **pseudonimização**, transformando o dado em uma versão agregada, como a **cidade** ou **bairro**, ou então usando um código que represente uma localização sem permitir a identificação do indivíduo ~~Explique por que este dado foi escolhido para ser anonimizado, destacando a importância de sua proteção~~.

- Dado 2: Nome Completo do Cliente ~~[Descreva o dado 2]~~.

  Justificativa: O nome completo dos clientes pode ser **pseudonimizado**, substituindo-o por um **código único** ou **ID** atribuído a cada cliente, que

Formatado: Recuo: Primeira linha: 0 cm

Formatado: Fonte: Não Negrito

não revela a identidade real, mas ainda permite a análise dos dados para fins estatísticos ou de marketing.

~~Explique por que este dado foi escolhido para ser anonimizado, destacando a importância de sua proteção~~

A anonimização ou pseudonimização de dados permite que a Melhores Compras utilize essas informações de forma segura para análises internas e outras finalidades, sem comprometer a privacidade dos consumidores. Além disso, está em total conformidade com os princípios da LGPD, garantindo que, mesmo em casos de vazamento ou acesso indevido, os dados não possam ser utilizados para identificar diretamente o cliente

REFERÊNCIAS

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Forense, 2014.

MACHADO, Célio A. B. Privacidade e proteção de dados pessoais: uma abordagem à luz da LGPD. São Paulo: Saraiva Educação, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018

~~SOBRENOME, Nome do autor abreviado. **Título do livro.** Local da edição: Editora, ano.~~

Formatado: Corpo de texto

GLOSSÁRIO

~~Termo~~**Anonimização**	Processo que remove ou modifica dados pessoais de forma que o titular não possa ser identificado, direta ou indiretamente. Uma vez anonimizado, o dado deixa de estar sujeito à LGPD. ~~Explicação~~.

Autenticação Multifatorial (MFA) ~~**Termo**~~	Mecanismo de segurança que exige mais de um fator de verificação para conceder acesso a um sistema ou dado. Geralmente envolve senha e um código temporário enviado ao celular ou gerado por aplicativo.~~Explicação~~.
Criptografia	Técnica de codificação de informações, tornando os dados ilegíveis para terceiros não autorizados. Utilizada para proteger dados em trânsito ou em repouso.
Dados Pessoais	Qualquer informação relacionada a uma pessoa natural identificada ou identificável, como nome, CPF, endereço, e-mail, entre outros.
Dados Sensíveis	Categoria especial de dados pessoais que inclui informações sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados biométricos, entre outros. Requerem cuidados extras de proteção.
LGPD (Lei Geral de Proteção de Dados Pessoais)	Legislação brasileira (Lei nº 13.709/2018) que regulamenta o tratamento de dados pessoais, com foco na proteção da privacidade dos cidadãos.
Pseudonimização	Técnica de tratamento de dados em que as informações de identificação direta são substituídas por pseudônimos ou códigos. Permite análises sem revelar a identidade do titular.

TI (Tecnologia da Informação)	Conjunto de recursos tecnológicos e computacionais usados para criar, armazenar, processar e proteger informações em ambientes organizacionais.