Informação PIA

PIA
Site Venda de Artigos de Vestuário

Nome do autor
Tiago Gonçalves

Nome do assessor
Pedro Silva

Nome do validador
Pedro Silva

Data de criação
18/04/2019

Nome do DPO
Pedro Silva

Opinião do DPO
Aplicável.

Procura da opinião de partes interessadas
A opinião das partes em questão foi solicitada.

Opiniões de partes interessadas
Tiago Gonçalves

Status de pessoas em questão
O tratamento deve ser implementado.

Opiniões de partes interessadas
Aplicável.

Contexto

Visão geral

Qual é a finalidade de tratamento considerada no âmbito da análise?

O nosso projeto é um site de artigos de vestuário. Assim, o tipo de processamento que será feito é o de dados pessoais dos utilizadores, assim como os seus usernames e passwords, dados sobre pagamentos de artigos e ainda a recolha de informação preferencial de cada utilizador, para a seleção de artigos semelhantes para cada utilizador e também publicidade.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

Garantir que os dados seram processados de forma responsável e que não serão partilhados com terceiros.

Quais são as normas aplicáveis à finalidade de tratamento?

Os dados recolhidos e armazenados deveram ser cifrados e como tal, é escolhido um standard disponível para a cifragem.

Avaliação : Aceitável

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Dados pessoais dos utilizadores, assim como os seus usernames e passwords, dados sobre pagamentos de artigos e ainda a recolha de informação preferencial de cada utilizador. Todos os dados irão se manter até o utilizador encerrer a conta.

Como funciona o ciclo de vida dos dados pessoais e dos processos inerentes?

Inicialmente os dados serão recolhidos através do histórico de navegação dos utilizadores no site, assim como o uso de cookies.
Quando os utilizadores pretendem fazer uma compra, necessitam de registo, passando a ser clientes e aí serão recolhidos dados pessoais sobre os utilizadores. Todos os dados recolhidos serão guardados nos nossos servidores.
Apenas os dados pessoais de cada utilizador poderam ser modificados ou apagados, se assim entenderem, sendo que todos os outros dados recolhidos são apagados quando o utilizador eliminar a sua conta.
O processamento dos dados pessoais dos utilizadores são considerados de alto risco.

Quais são os ativos de informação utilizados na finalidade de tratamento?

Sistema Operativo Linux
Base de Dados mySQL

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

Todos os dados recolhidos e pedidos aos utilizadores são os minimos necessários para adequar as preferências dos utilizadores aos artigos no site.

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

Sempre que um utilizador cria uma nova conta tem de dar consentimento sobre as políticas da empresa, garantido que o utilizador tem conhecimento do processo. Desta forma os processos legais são cumpridos.

Avaliação : Aceitável

Os dados pessoais recolhidos são adequados, relevantes e limitados para o propósito de tratamento realizado (princípio da minimização de dados)?

Apenas seram recolhidos os dados necessários para o nosso processamento, de forma a fornecer aos utilizadores aquilo que eles procuram e da melhor maneira possível.

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Sempre que o utilizador mudar os seus dados pessoais, como a morada, será sempre possível alterar esses dados na área de utilizador no site.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

Os dados serão sempre guardados. O histórico é essencial para a empresa e para o utilizador.

Avaliação : Aceitável

Controlos para proteger os direitos pessoais dos titulares dos dados

Como é que os titulares dos dados são informados sobre o tratamento dos seus dados?

O histórico de compras do cliente e o registo de pesquisas, oferecem uma publicidade adequada a cada cliente.

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

O consentimento fornecido pelos clientes é dado quando a conta é criada.

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

O acesso e portabilidade serão garantidos na área reservada a cada utilizador disponível no site.

Avaliação : Aceitável

Como é garantida a atualização/retificação e apagamento dos dados pessoais pedida pelo titular dos mesmos?

Os utilizadores tem uma área de cliente onde podem alterar os seus dados.

Avaliação : Aceitável

Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos?

Quando é criada a conta, o utilizador pode discordar com alguns dos termos de utilização.

Avaliação : Aceitável

As obrigações dos subcontratrantes são claramente identificadas e regulados por contrato ou outro ato normativo?

Não é aplicado.

Avaliação : Aceitável

No caso de transferência de dados fora da União Europeia, os dados são adequadamente protegidos?

Como o domínio do site se encontra na União Europeia, qualquer transferência de dados para fora terá de ser aprovado pelos administradores, sendo que estes devem assegurar a proteção dos mesmos.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

Crifração

Todos os dados serão cifrados, de forma a que não haja acesso à informação de cada cliente.

Avaliação : Aceitável

Autenticação

Para a realização de uma compra no site, assim como na secção de pagamento, será necessário o uso de credências pessoais. Assim como na secção de pagamento

Avaliação : Aceitável

Acesso ilegítimo dos dados

Quais poderiam ser os principaisimpactos nos dados dos titulares se o risco ocorrer?

Alguns dados pessoais ficariam disponiveis, assim como dados sobre pagamentos.

Quais são os principaisameaçasque poderiam levar ao risco?

Fuga de informação pessoal, dados sobre pagamnetos, compras efetuadas.

Quais são as fontesde risco?

Desenvolvimento do site.

Quais são os controlos identificados que contribuem para abordar o risco?

Crifração, Autenticação

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante, Importante

Como estimas a probabilidade de risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Significante, Importante

Avaliação : Aceitável

Modificação indesejada dos dados

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?

Modificação e roubo dos dados pessoais dos clientes.

Quais são as principais ameaças que poderiam levar ao risco?

Acesso aos dados dos clientes.

Quais são as fontesde risco?

Desenvolvimento do site.

Quais são os controlos identificados que contribuem para abordar o risco?

Crifração, Autenticação

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante, Importante

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Insignificante, Caso a cifração seja feita corretamente.

Avaliação : Aceitável

Desaparecimento de dados

Quais são os principaisimpactos nos dados dos titulares se o risco ocorrer?

Perdido todo o histórico de cada cliente no site.

Quais são as principais ameaças que poderiam levar ao risco

Não existência de backups.

Quais são as fontesde risco?

Desenvolvimento do sie.

Quais são os controlos identificados que contribuem para abordar o risco?

Autenticação, Crifração

Como estimas a gravidade de risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante, Importante

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Máximo, Um dos principais objetivos

Avaliação : Aceitável

Plano de ação

Visão geral

Princípios fundamentais

Objetivos
Base legal
Dados adequados
Precisão de dados
Duração dos dados
Informação para os titulares dos dados
Obtenção do consentimento
Informação para os titulares dos dados
Direito à retificação e apagamento
Direito à restrição e à oposição
Subcontratação
Transferências

Medidas existentes ou planeadas

Crifração
Autenticação

Riscos

Acesso ilegítimo de dados
Modificação indesejada de dados
Desaparecimento de dados

Medidas Improváveis
Medidas Aceitáveis

Princípios fundamentais

Nenhum plano de ação registado.

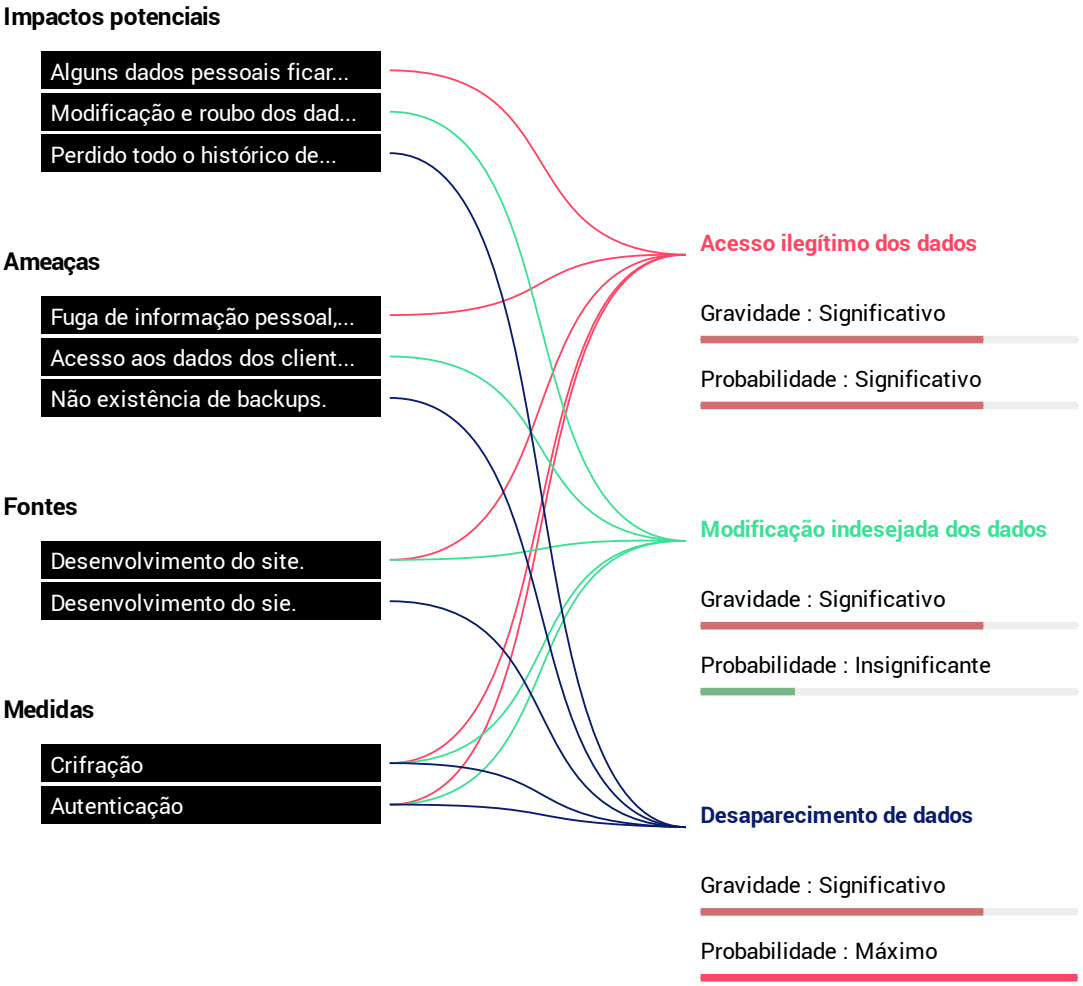
Medidas existentes e planeadas

Nenhum plano de ação registado.

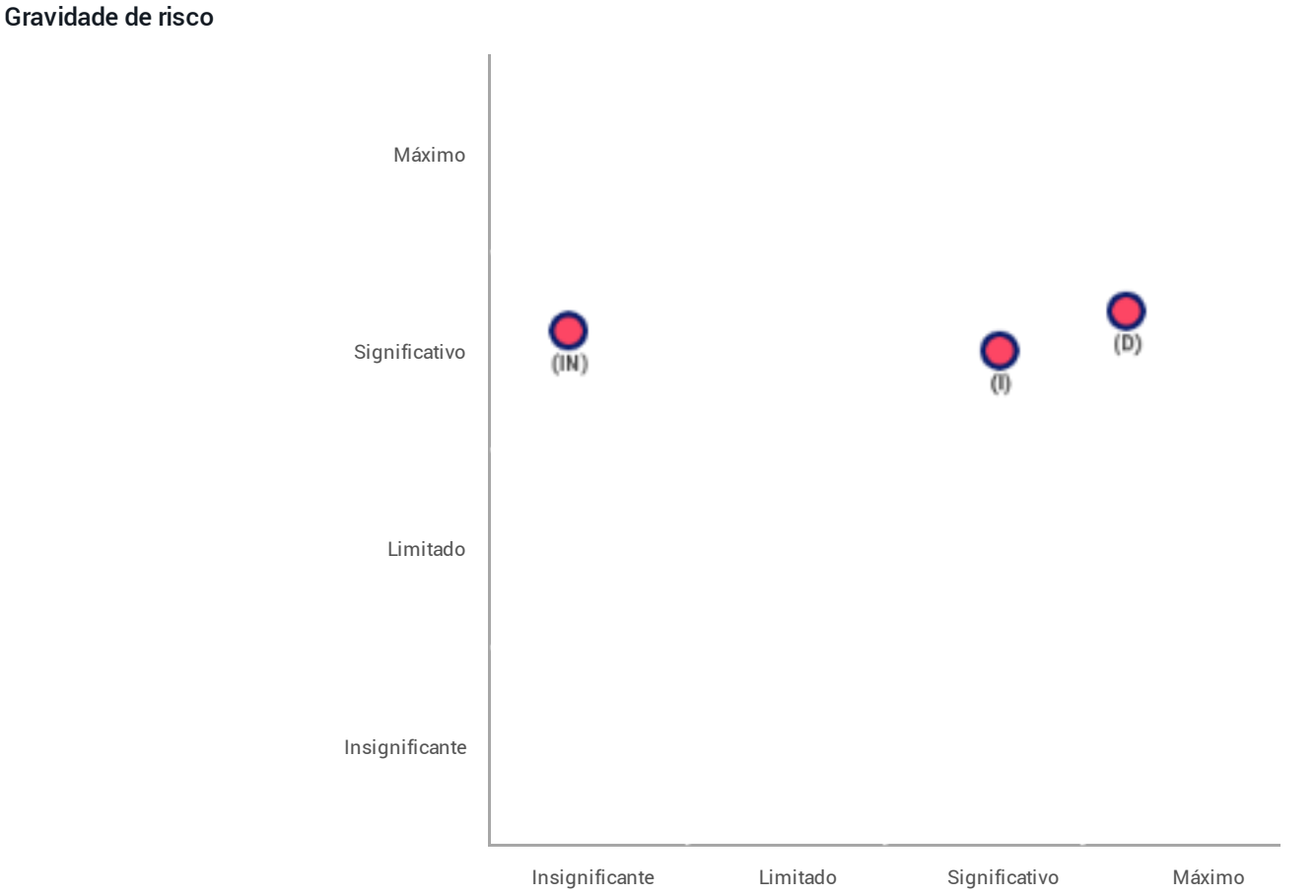
Riscos

Nenhum plano de ação registado.

Visão geral dos riscos



Mapeamento de riscos



- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

18/04/2019