Informação PIA

PIA
Aplicação Vocacional

Nome do autor
Zita Abreu

Nome do assessor
Zita Abreu

Nome do validador
Zita Abreu

Data de criação
17/04/2019

Nome do DPO
GRUPO 2

Opinião do DPO
O tratamento pode ser facilmente implementado e inclusive melhorado, com o decorrer da utilização da aplicação e com o aumento dos dados a serem recolhidos.

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

Razão pela qual a opinião de partes interessadas não foi pedida
A dimensão e estrutura da aplicação não exige solicitação de partes interessadas

Contexto

Visão geral

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

O projeto consiste numa aplicação de orientação académica para alunos que estejam numa determinada etapa de transição, seja ensino básico-secundário, ensino secundário-universitário, entre outras.

Esta aplicação permite a disponibilização de informações, de modo a impulsionar reflexão nos alunos, e testes de carácter pedagógico e vocacionais, supervisionados por especialistas qualificados.

Adicionalmente, esta aplicação terá a intervenção de psicólogos e professores, que durante o processo de apoio na tomada de decisão do aluno, têm acesso ao respetivo desenvolvimento do mesmo, com base nos resultados dos testes efetuados por este.

As credenciais de acesso dos alunos são disponibilizadas pelas escolas, que aderem à presente aplicação, e as credências de acesso dos especialistas sãos disponibilizadas pelos mesmos, no momento em que se disponibilizam para serem orientadores neste projeto.

Cada aluno terá o seu perfil, acompanhado de informações básicas como: nome da escola, ano, turma, número de aluno, nome completo, nome de utilizador, endereço de email, foto, *password*; e cada especialista será caracterizado por: nome completo, nome de utilizador, profissão, endereço de email e *password*.

Após a autenticação dos alunos, estes serão abordados com algumas questões, de modo a efetuar-se uma primeira triagem de opções, tanto vocacionais como de selecção do especialista que melhor o consegue acompanhar. Posteriormente, o aluno será convidado, pelo especialista que lhe foi atribuído, a efectuar determinados testes.

Todos esses testes serão armazenados de acordo com o nome da escola, ano e turma que o aluno frequenta, ano letivo e especialista responsável pelo seu acompanhamento. Mais ainda, estes testes são analisados e acrescentados ao respetivo histórico. Este, por sua vez, apenas está acessível ao aluno e ao seu especialista, tendo este último ainda acesso às estatísticas extraídas dos testes.

A escola possui a capacidade de eliminar a conta de um dado aluno, sendo, nesses casos, removidos todos os dados associados a este, à excepção do respetivo histórico anónimo, que é conservado para fins estatísticos.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

Os responsáveis por controlar os dados são os responsáveis por garantir que os dados pessoais recolhidos apenas são utilizados no contexto concreto da aplicação. Adicionalmente, este deve garantir que terceiros não conseguem aceder a nenhum tipo de dados e que os utilizadores da aplicação só conseguem aceder aos dados para os quais possuem permissão. Estes devem ainda garantir que eliminar um dado de um aluno não implique remover o mesmo do histórico, pois existe necessidade de preservar o histórico para fins estatísticos .

Assim, os processadores de dados deverão, por exemplo, cifrar os dados armazenados e transmitidos, durante todo o processo, de modo a permitir o anonimato do histórico.

Note-se que não existe necessidade em responsáveis conjuntos de tratamento.

Quais são as normas aplicáveis à finalidade de tratamento?

Os códigos de conduta aprovados passariam pela cifragem dos dados e por certificações de proteção de dados e segurança de informação.

Para a cifragem dos dados sugere-se técnicas *standards*, como o algoritmo de criptografia AES, para o armazenamento, e o TLS para o estabelecimento da comunicação segura.

Para proceder ao anonimato várias técnicas podem ser adoptadas, como: *hashing with key or salt, encryption as pseudonymization technique ou tokenisation.* Na primeira pode-se recorrer ao uso do *standard* HMAC, com SHA-3, e na segunda o *standard* AES.

Avaliação : Aceitável

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Os dados pessoais recolhidos dos alunos são: nome da escola, ano, turma, número de aluno, nome completo, nome de utilizador, endereço de *email*, foto e *password.*

Os dados pessoais recolhidos dos especialistas são: nome completo, nome de utilizador, profissão, endereço de *email* e *password.*

Os dados do administrador são apenas o nome do utilizador e a *password*.

Note-se que além destes dados, a cada aluno é associado um histórico, com todo o processo do seu acompanhamento e a cada especialista é associado o histórico dos acompanhamentos por si efetuados.

A conservação dos dados admite um prazo variável para cada aluno, pois os acompahamentos são personalizáveis e com duração igual à necessária para que cada um tome a sua decisão final. Observe-se no entanto que os dados pessoais dos alunos, quando já não precisam mais dos serviços fornecidos pela aplicação, são eliminados, acontecendo o mesmo quando algum dos especialistas já não quer disponibilizar os seus serviços. O tempo de vida dos alunos e especialistas é assim limitado, pois são apagados pelo administrador, caso seja esse o caso.

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

Os dados podem ser inseridos ou por uma entidade individual ou por um administrador de uma escola. Mais detalhadamente, são introduzidos os dados pessoais dos alunos e especialistas, e os dados resultantes da relação estabelecida por eles (análises dos questionários e possíveis testes, respostas a estes, entre outros).
Os dados serão recolhidos das credenciais dos intervenientes da aplicação. Os especialistas são responsáveis pelos testes vocacionais propostos e pela respetiva análise e os alunos pelas respostas aos testes mencionados. Note-se que inserção de dados é indispensável para a autenticação e posterior identificação dos intervenientes na aplicação.
Observe-se ainda que os testes são elaborados para que os mesmos possam ser preenchidos pelos alvos da análise vocacional, os alunos, e consequentemente, a fonte de dados para o funcionamento da aplicação consiste assim no preenchimento dos testes que os alunos serão submetidos.
As respostas dadas pelos mesmo são objeto de análise por parte dos especialistas e são mantidas no histórico dos alunos, para que se proceda à elaboração de análises vocacionais, a longo prazo, e ainda se efetue análises estatísticas.
Todos os dados aqui referidos são armazenados numa base de dados única, sendo que é permitido ao administrador anonimizar o histórico dos alunos, através da remoção dos dados pessoais destes.
Adicionalmente, existe partilha de dados apenas entre o aluno e o especialista, mas nunca os mesmos serão divulgados a terceiros.
O tipo de processamento identificado como de alto risco está associado ao facto dos dados pertencerem a sujeitos vulneráveis (menores de idade).

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

Os dados pessoais dependem de ativos de informação, como o equipamento informático, as pessoas intervenientes, o *software,* entre outros.

Existe a necessidade de sistemas operativos (sendo a aplicação em causa desenvolvida para todos), um sistema gestor de base de dados e um sistema de desenvolvimento da aplicação.

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

O armazenamento dos dados tem como objetivo extrair estatísticas e efetuar uma análise vocacional progressiva, durante um considerável prazo (mínimo 3 meses). Adicionalmente, permite que os intervenientes da aplicação possam consultar o seu acompanhamento.

Por fim, esta aplicação vem possibilitar uma automatização e um acompanhamento muito pessoal aos seus utilizadores, contrariamente ao método tradicional, que para além de impessoal exige a presença física.

Pretende-se alcançar que as escolas aderentes a este programa, possam dispor de um acompanhamento de orientação vocacional de excelência para os seus alunos. Pretende-se ainda que os mesmos sejam de tal maneira bem orientados e acompanhados, que o numero de alunos que ingressam, por exemplo no ensino superior, e mudam de curso ao fim de x tempo seja reduzido.

O objetivo principal passa por ajudar os alunos na tomada de decisão, que é muitas vezes encarada por eles com muita pressão.

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

O fundamento para o tratamento dos dados pessoais é inerente ao objetivo da aplicação por si só, sendo necessário, no caso dos alunos menores de idade o consentimento dos seus encarregados de educação, para que os seus dados sejam tratados.
Caso os desenvolvedores da aplicação queiram torná-la 100% digital e *online,* podem optar por recorrer a assinaturas digitais.

Avaliação : Aceitável

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

Todos os dados recolhidos admitem um propósito para o tratamento a ser realizado:

Alunos:
- Nome de utilizador: autenticação; - *Password*: autenticação; Endereço de *email:* autenticação;- Foto: autenticação; - Nome da escola: útil na organização dos dados por diferentes escolhas que usem a aplicação; - Ano: útil na organização dos dados por anos; Turma: útil na organização dos dados por diferentes turmas.

Especialistas:
- Nome de utilizador: autenticação;Profissão: necessário para o acompanhamento; -Endereço de *email*: autenticação; e *password*: autenticação.

Administrador:
-Nome do utilizador: autenticação; *password*: autenticação.

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Os dados tanto dos alunos como dos especialistas estão aptos a serem atualizados, mediante pedido feito ao administrador da aplicação, que por sua vez vai requerer autorização, caso haja necessidade disso.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

O especialista vai manter os dados consigo até que dos mesmos se retire alguma conclusão confiável, posteriormente serão removidos todos os dados pessoais dos antigos alunos, que já não precisam dos serviços que esta aplicação fornece.

O armazenamento dos dados tem como objetivo extrair estatísticas e efetuar uma análise vocacional progressiva, durante um considerável prazo (mínimo 3 meses). Adicionalmente, permite que os intervenientes da aplicação possam consultar o seu acompanhamento.

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?

Os utilizadores da aplicação estão cientes do tratamento feito aos dados que fornecem, sendo informados através da constante comunicação estabelecids entre os mesmos e os respetivos especialistas.

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

O consentimento dos titulares é obtido através da incrição inicial, i.e do preenchimento das credenciais. No entanto esta pré inscrição só é válida após a autorização por parte das entidades intervenientes.

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

Os utilizadores facilmente onseguem aceder aos seus dados pessoais na página de perfil da aplicação.

Avaliação : Aceitável

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

Qualquer alteração, seja adição ou remoção de dados, deve ser solicitada à administração, se aplicável. Pois observe-se que a existência de um administrador é inerente à inscrição do aluno por parte de uma autoridade coletiva (como uma escola), ou não.

Avaliação : Aceitável

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

Não é aplicável.

Avaliação : Aceitável

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

Não é aplicável.

Avaliação : Aceitável

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

Não é aplicável.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

DPO

- Contratar um responsável qualificado para o tratamento de informações e um encarregado de proteção de dados: DPO (Data Protection Officer);

Avaliação : Aceitável

Cifragem de dados

- Cifrar os dados enquanto os alunos estiverem inscritos, permitindo que estes apenas tenham acesso aos mesmos depois de efetuada a autenticação e validação de permissões. Deste modo apenas os especialistas e os próprios alunos têm acesso aos seus dados e históricos. Quando removidos os dados dos utilizadores da aplicação, optar pelo anonimato.

Avaliação : Aceitável

Minimizar

-Minimizar os dados recolhidos, o acesso aos mesmos e o tempo de armazenamento associado a estes.

Avaliação : Aceitável

Proteção de dados

-Optar por usar algum método útil na proteção de todos os dados pessoais envolventes, não só a cifragem mas também, por exemplo, a pseudonimização, que consiste em substituir dados pessoais por códigos.

Avaliação : Aceitável

Sistema de backup

A base de dados deve ser replicada num dispositivo de armazenamento externo ao sistema.

Avaliação : Aceitável

Regular a autenticação e validação de permissões

É benéfico existir um contaste controlo, tanto de autenticação como de validação de permissões, especialmente no que diz respeito à base de dados.

Avaliação : Aceitável

Acesso ilegítimo dos dados

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

- Perda de informações capazes de serem utilizadas por entidades terceiras para identificar direta ou indiretamente os titulares das mesma, como nome, endereço de email, entre outras. Uma vez descoberta a escola que o aluno frequenta,

facilmente um indivíduo consegue ir ao seu encontro., - Perigo inerente ao facto de um dado histórico ser associado a um alino, o que pode conduzir, por exemplo, a situações em que o mesmo possa ser persuadido a não ir para determinada escola ou universidade, por entidades que beneficiem com tal escolha.

Quais são os principaisameaçasque poderiam levar ao risco?

- Acesso às passwords dos utilizadores;, - Falta de medidas de segurança já mencionadas.

Quais são as fontesde risco?

Entidades internas e externas

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

DPO, Cifragem de dados, Minimizar, Proteção de dados, Sistema de backup, Regular a autenticação e validação de permissões

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

Significante, Serão armazenados dados de individuos vulneráveis (menores de idade), o que pode conduzir ás situações de perigo já aqui mencionadas.

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

Limitado, Caso os utiluzadores utilizem *passwords* fortes e caso a implementação elaborada pelos desenvolvedores da aplicação respeite as medidas de segurança exigidas, então a gravidade do risco não será elevada. No entanto, o facto de os utilizadores poderem ser vulneráveis implica um cuidado acrescido.

Avaliação : Aceitável

Modificação indesejada dos dados

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

Alteração dos testes vocacionais

Quais são as principais ameaças que poderiam levar ao risco?

Mau acesso às análises elaboradas durante o processo de avaliação de vocação.

Quais são as fontesde risco?

Entidades externas e internas

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

DPO, Cifragem de dados, Minimizar, Sistema de backup, Proteção de dados, Regular a autenticação e validação de permissões

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

Máximo, A análise inadequada aos alunos pode conduzir a que estes se direccionem para uma vocação que não lhes seja a mais apropriada, podendo este factor condicionar toda uma vida.

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

Limitado, A manipulação de dados será dificilmente concebida, caso as medidas de segurança sejam consideradas.

Avaliação : Aceitável

Desaparecimento de dados

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

- Desaparecimentos de análises já feitas;, - Desaparecimento de dados pessoais;, - Desaparecimento do histórico, factor indispensável para o bom funcionamento da avaliação vocacional.

Quais são as principais ameaças que poderiam levar ao risco

- Acesso ilegal à base de dados;

Quais são as fontesde risco?

Entidades externas e internas

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

Sistema de backup, DPO, Regular a autenticação e validação de permissões

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

Máximo, O desaparecimento de dados pode originar que todo o processo seja apagado e consequentemente um remomeçar da avaliação vocacional seria um factor custoso a nível de tempo, pois os alunos que recorrem a esta aplicação estarão, à partida, com um termpo contado para a tomada de decisão.

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

Insignificante, A probabilidade deste risco acontecer é tanto menor quanto maior for o cuidado a ter com a segurança.

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

DPO
Cifragem de dados
Minimizar
Proteção de dados
Sistema de backup
Regular a autenticação e validação de permissões

Riscos

Acesso ilegítimo de dados
Modificação indesejada de dados
Desaparecimento de dados

Medidas Improváveis
Medidas Aceitáveis

Princípios fundamentais

Nenhum plano de ação registado.

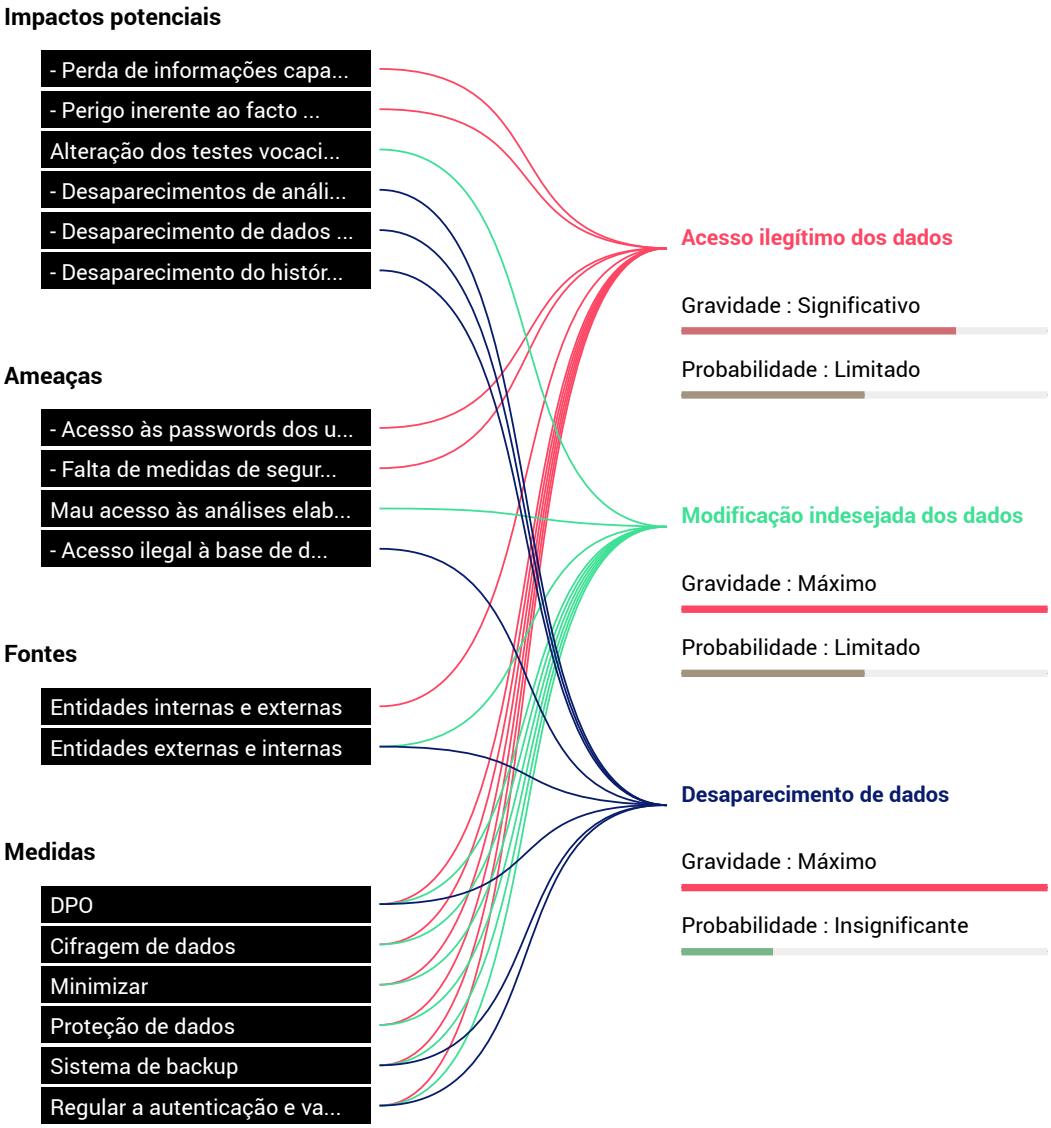
Medidas existentes e planeadas

Nenhum plano de ação registado.

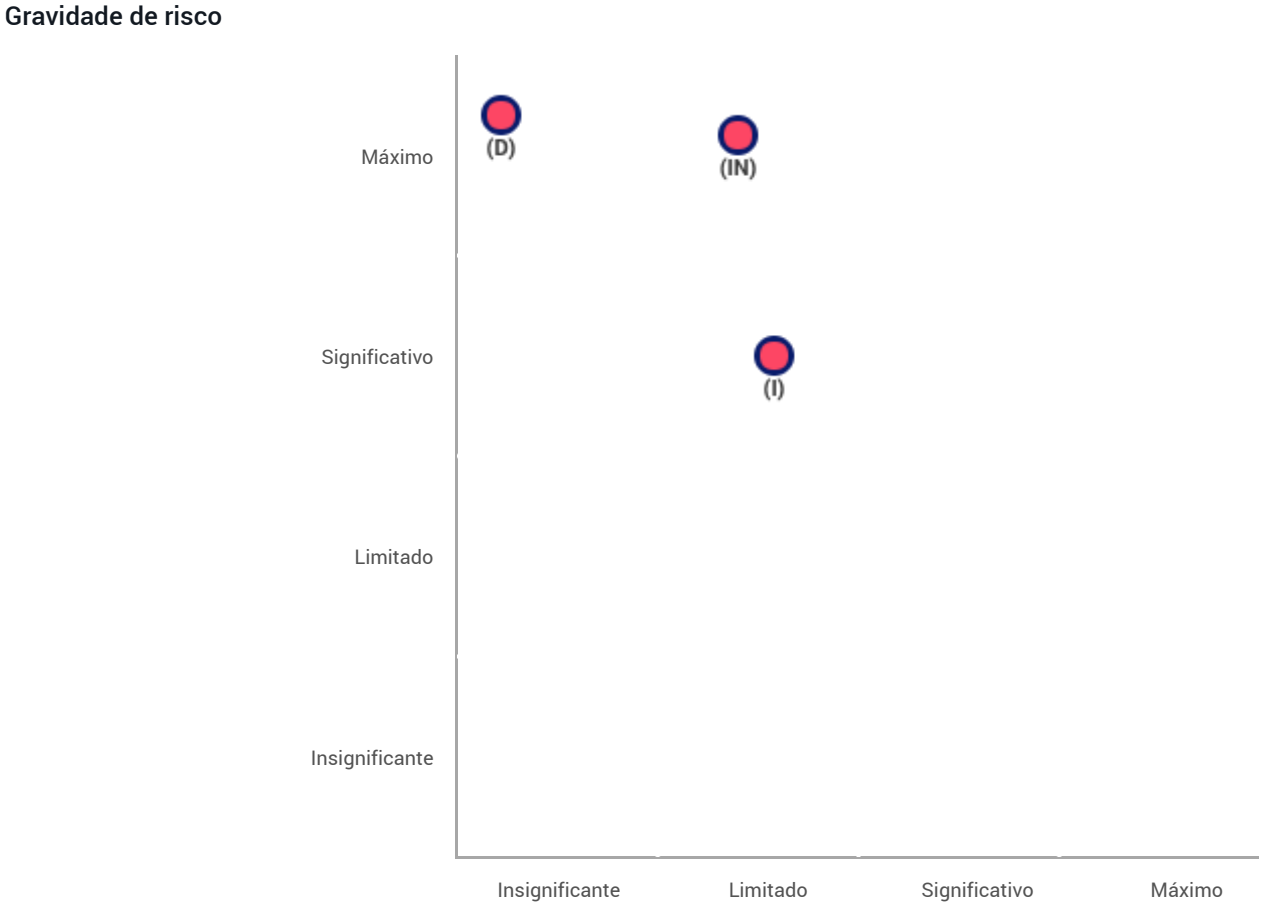
Riscos

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

17/04/2019