# PIA information

### PIA
Aplicação de testes para alunos

### Author's name
Daniel, Maia

### Assessor's name
Diogo, Costa

### Validator's name
Mafalda, Nunes

### Creation date
30/03/2019

### DPO's name
Grupo5

### DPO's opinion
O Grupo5 acha que os componentes mencionados neste documento podem ser implementados, uma vez que existem projetos anteriores onde foi implementado as técnicas criptográficas associadas.

### Search of concerned people opinion
Concerned people opinion wasn't requested.

### Reason why concerned people opinion wasn't requested
Dada a dimensão do projeto e a dificuldade dos mecanismos de segurança utilizados não se achou necessário.

# Context

## Overview

### Which is the processing under consideration?

O projeto que se pretende desenvolver consiste numa aplicação educativa para crianças, que permite a disponibilização de informações e testes relacionados com temas de carácter pedagógico, bem como estatísticas de acerto para o utilizador corrente. Para além disso, esta aplicação deverá permitir que professores consultem o desenvolvimento dos seus alunos.

As credenciais de acesso dos alunos e professores são disponibilizadas pela escola. Cada aluno terá associado ao seu perfil os seguintes dados: número de aluno, nome completo, nome de utilizador, password, escola, ano e turma. Cada professor será caracterizado por: nome completo, nome de utilizador, password e escola.

Após a autenticação, os professores podem disponibilizar informações e testes para os alunos de um ano e turma, num determinado ano letivo. Posteriormente, os alunos realizam os testes, que são automaticamente corrigidos e acrescentados ao respetivo histórico. Este, por sua vez, apenas
é acessível pelo próprio aluno. Mais ainda, o professor tem acesso às estatísticas dos testes por si efetuados, para os vários alunos.

A escola tem a possibilidade de apagar a conta de um aluno ou professor. Nesse caso, são removidos todos os dados associados ao utilizador, exceto o respetivo histórico (anonimizado), que é mantido para fins estatísticos.

### What are the responsibilities linked to the processing?

Os *data controllers* têm como objetivo garantir que os dados pessoais recolhidos apenas são utilizados no contexto da aplicação, ou seja, para fins escolares. Mais ainda, este deve assegurar que terceiros não têm acesso aos dados e que os utilizadores só conseguem aceder aos dados para os quais têm permissão. Por fim, deve garantir que eliminar um dado aluno não implica a remoção do seu histórico.

Desta forma, os *data processors* deverão cifrar os dados armazenados/comunicados e permitir a anonimização do histórico.

No contexto desta aplicação não se considera necessário a existência de um *joint controller.*

### Are there standards applicable to the processing?

Para cifrar os dados sugere-se a utilização do standard AES para armazenamento e TLS para a comunicação.

No contexto da anonimização sugere-se o uso da técnica de *hashing with key or salt, encryption as a pseudonymisation technique* ou *tokenisation.*

Para a primeira teécnica sugere-se o uso do *standard* HMAC com SHA-2 ou SHA-3.

Para a segunda sugere-se o uso do *standard* AES.

**Evaluation : Acceptable**
**Evaluation comment :**
Falta acabar

## Data, processes and supporting assets

### What are the data processed?

Os dados pessoais do aluno são:
- Nome de utilizador

- Password
- Número do aluno
- Nome completo
- Escola
- Ano
- Turma

Além destes dados o aluno deverá ter um histórico a si associado.

Os dados dos professores são:
- Nome de utilizador
- Password
- Nome completo
- Escola

Além destes dados o professor deverá estar associado aos histórico de testes por si efetuados.

Os dados do administrador são:
- Nome de utilizador
- Password

Todos estes dados são persistentes, sendo que os dados pessoais dos alunos e dos professores têm um tempo de vida limitado, na medida em que são eliminados pelo administrador quando saem da escola em questão.

### How does the life cycle of data and processes work?

Os dados são inseridos na aplicação pelo administrador (dados pessoais de alunos e professores), professores (testes e correção dos mesmos) e alunos (as respostas aos testes). Os primeiros são utilizados para permitir que os vários utilizadores se possam autenticar e identificar dentro da aplicação. Por sua vez, os testes são utilizados para que os alunos os possam realizar. Por fim, as respostas dadas pelos alunos são corrigidas pelos professores. Estas são utilizadas para manter o histórico dos alunos, assim como na elaboração de estatísticas. Todos os dados referidos anteriormente são armazenados numa base de dados única, sendo que é garantida, ao administrador, a possibilidade de anonimização do histórico dos alunos e dos professores (remoção dos dados pessoais). Além disso, os dados não serão partilhados com terceiros. O processamento com maior risco está relacionado com a inserção e armazenamento dos dados pessoais do alunos (crianças), bem como a manutenção do histórico das mesmas.

### What are the data supporting assets?

Sistemas operativos: todos
Aplicações: Vue.js + Spring + Hibernate
DBMS: PostgreSQL

**Evaluation : Acceptable**

# Fundamental principles

## Proportionality and necessity

### Are the processing purposes specified, explicit and legitimate?

O armazenamento dos dados tem como objetivo permitir extrair estatísticas a partir dos testes realizados pelos alunos para conseguir aprimorar o método de ensino. Além disso, permite aos professores, alunos e encarregados de educação (através da conta do aluno) o acompanhamento do histórico escolar do aluno em questão. Por fim, através da aplicação torna-se possível automatizar a correção de algumas questões dos testes.

**Evaluation : Acceptable**

### What are the legal basis making the processing lawful?

Existe uma autorização explícita por parte dos encarregados de educação para o processamento dos dados efetuado pela aplicação.

**Evaluation : Acceptable**

### Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Todos os dados recolhidos têm um propósito objetivo:

**Alunos**:
- Nome de utilizador - Autenticação
- Password - Autenticação
- Número do aluno - Identificação por parte dos professores/administradores
- Nome completo - Identificação por parte dos professores/administradores
- Escola - Organização dos dados por diferentes escolas
- Ano - Organização dos dados por diferentes anos
- Turma - Organização dos dados por diferentes turmas
- Histórico - Recolha de estatísticas

**Professores**:
- Nome de utilizador - Autenticação
- Password - Autenticação
- Nome completo - Identificação por parte dos alunos/administradores
- Escola - Organização dos dados por diferentes escolas
- Histórico de testes - Consulta dos testes efetuados assim como resoluções dos alunos

**Administrador**:
- Nome de utilizador - Autenticação
- Password - Autenticação

**Evaluation : Acceptable**

### Are the data accurate and kept up to date?

Os dados pessoais dos utilizadores são passíveis de ser alterados mediante um pedido realizado à escola e, consequente, administração da aplicação.

**Evaluation : Acceptable**

### What are the storage duration of the data?

Os dados pessoais dos alunos e dos professores têm um tempo de vida limitado pela sua saída do estabelecimento de ensino. Isto acontece porque quando o aluno/professor deixa de frequentar a escola, a avaliação já foi efetuada, pelo que não é necessária a manutenção da ligação entre utilizador e histórico.

Os restantes dados são permanentes para manutenção de estatísticas (histórico).

Os dados do administrador são permanentes devido à necessidade de uma constante administração da aplicação.

**Evaluation : Acceptable**

## Controls to protect the personal rights of data subjects

### How are the data subjects informed on the processing?

Os utilizadores da aplicação estão cientes do uso que é feito dos dados presentes na mesma. Este aspeto é alcançado através de um comunicado que é enviado a todos os encarregados de educação / professores antes de estes serem inscritos na aplicação.

**Evaluation : Acceptable**

### If applicable, how is the consent of data subjects obtained?

A inscrição dos utilizadores na aplicação só é realizada após receber autorização (no comunicado previamente especificado) por parte dos individuos.

**Evaluation : Acceptable**

### How can data subjects exercise their rights of access and to data portability?

Os utilizadores conseguem aceder aos seus dados na página de perfil da aplicação.

A portabilidade dos dados não se aplica.

**Evaluation : Acceptable**

### How can data subjects exercise their rights to rectification and erasure?

Qualquer alteração/remoção dos dados deve ser solicitada à administração.

**Evaluation : Acceptable**

### How can data subjects exercise their rights to restriction and to object?

Não se aplica.

**Evaluation : Acceptable**

### Are the obligations of the processors clearly identified and governed by a contract?

Não se aplica.

**Evaluation : Acceptable**

### In the case of data transfer outside the European Union, are the data adequately protected?

Não existe intenção em transmitir dados da aplicação para fora da União Europeia.

**Evaluation : Acceptable**

# Risks

## Planned or existing measures

### Cifrar os dados

Uma possível medida de segurança passa por cifrar os dados armazenados, com validação de integridade. Desta forma apenas os professores e o próprio aluno têm acesso aos seus resultados escolares.

**Evaluation : Acceptable**

### Anonimização dos dados

Quando professores ou alunos forem removidos da aplicação, então o respetivo histórico deve ser mantido anonimizado.

**Evaluation : Acceptable**

### Sistema de backup

A base de dados deve ser replicada numa unidade de armazenamento externa ao sistema principal.

**Evaluation : Acceptable**

### Autenticação e validação de permissões

Deve existir uma constante autenticação / validação de permissões no que toca ao acesso à BD.

**Evaluation : Acceptable**

## Illegitimate access to data

### What could be the main impacts on the data subjects if the risk were to occur?

Comprometimento da identidade dos alunos/professores., Associar o histórico a um dado utilizador

### What are the main threats that could lead to the risk?

Acesso indevido às passwords dos utilizadores, Ausência das medidas de segurança enunciadas neste PIA

### What are the risk sources?

Recursos humanos internos, Recursos humanos externos

### Which of the identified controls contribute to addressing the risk?

Cifrar os dados, Autenticação e validação de permissões

### How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Como a aplicação armazena dados de individuos vulneráveis (crianças), considera-se que o acesso aos dados por terceiros pode levar a situações de discriminação ou contacto direto com os utilizadores.

### How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, Havendo um cuidado por parte dos utilizadores em seguir à risca as diretivas indicadas na aplicação (e.g. password forte), bem como por parte dos desenvolvedores na implementação das medidas de segurança apresentadas, considera-se que a probabilidade do risco não será muito elevada. Contudo, como se está a lidar com crianças, alguns dos aspetos mencionados anteriormente podem não ser totalmente cumpridos e, como tal, o risco pode aumentar.

**Evaluation : Acceptable**

## Unwanted modification of data

### What could be the main impacts on the data subjects if the risk were to occur?

Modificação das qualificações dos testes

### What are the main threats that could lead to the risk?

Acesso individo à correção dos testes

### What are the risk sources?

Recursos humanos externos, Recursos humanos internos

### Which of the identified controls contribute to addressing the risk?

Cifrar os dados, Autenticação e validação de permissões

### How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Atribuição incorreta de notas a crianças pode levar à reprovação no respetivo ano letivo.

### How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, Seguindo as medidas de segurança, os dados da aplicação serão dificilmente manipulados.

**Evaluation : Acceptable**

## Data disappearance

### What could be the main impacts on the data subjects if the risk were to occur?

Desaparecimento das avaliações dos alunos, Desaparecimento de testes realizados

### What are the main threats that could lead to the risk?

Inexistência de um backup na ocorrência de uma falha, Acesso indevido à BD

### What are the risk sources?

Fontes não humanas, Recursos humanos internos, Recursos humanos externos

### Which of the identified controls contribute to addressing the risk?

Sistema de backup, Autenticação e validação de permissões

### How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Pode levar a situações em que as avaliações realizadas são irrecuperáveis

### How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, Se se cumprir o mecanismos de segurança a probabilidade de o risco acontecer deve ser diminuta.

**Evaluation : Acceptable**

# Action plan

## Overview

### Fundamental principles

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Information for the data subjects
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

### Planned or existing measures

Cifrar os dados
Anonimização dos dados
Sistema de backup
Autenticação e validação de permissões

### Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

## Fundamental principles

No action plan recorded.

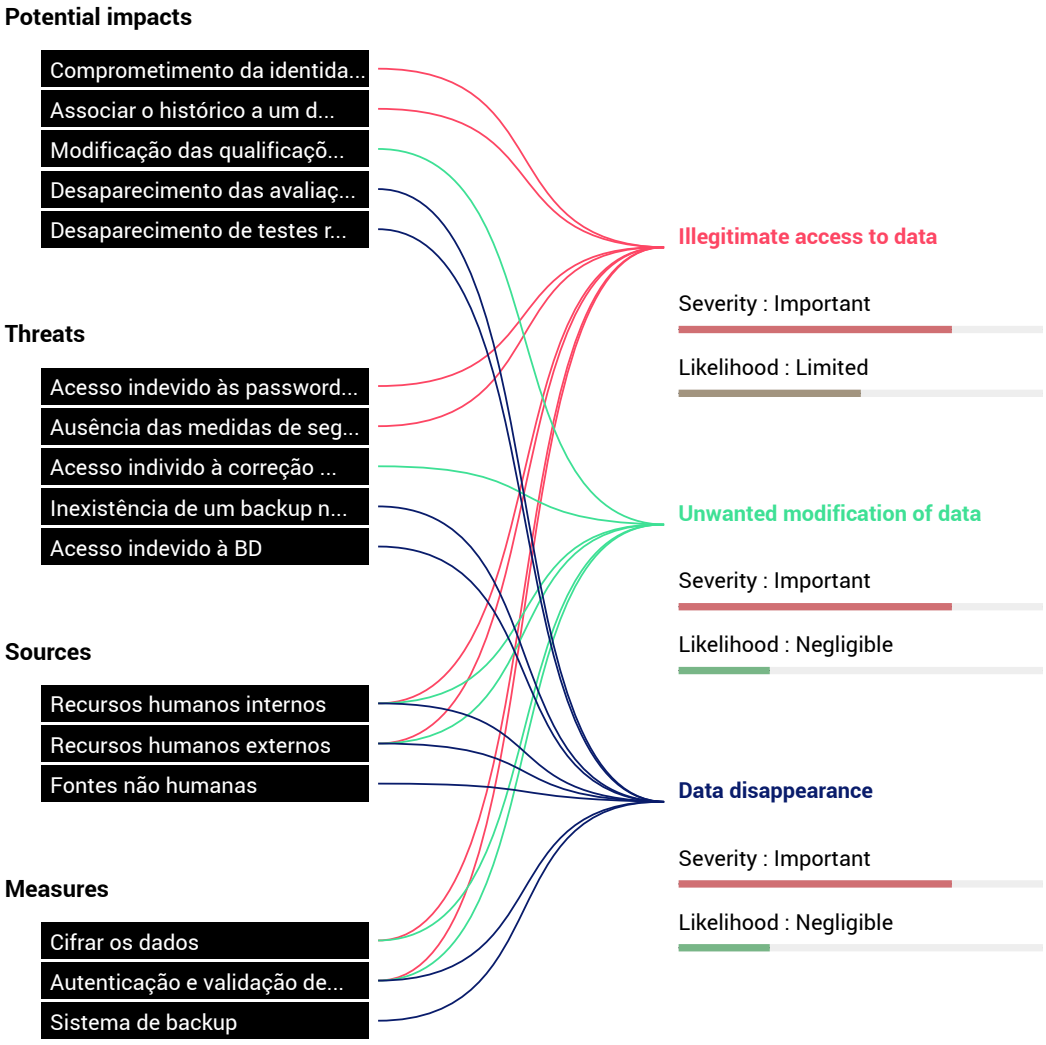
## Existing or planned measures

No action plan recorded.

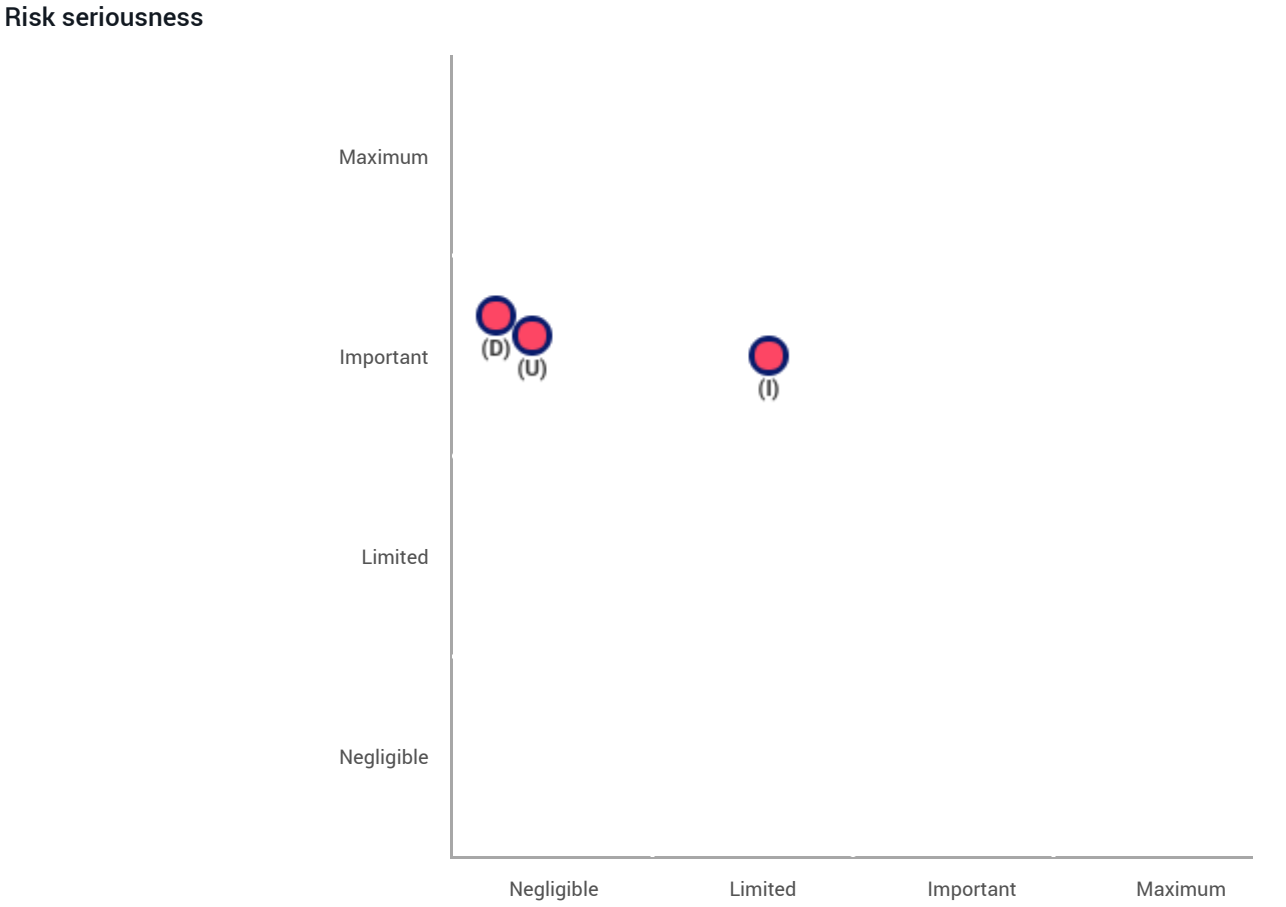
## Risks

No action plan recorded.

# Risks overview



# Risk mapping




- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

30/03/2019