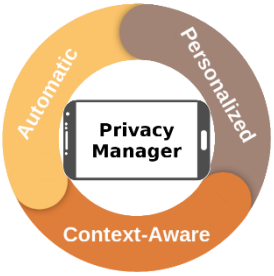
U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Relatório de Avaliação de Impacto sobre a Privacidade (PIA)

Projeto COP-MODE



Elaborado por Rui Coelho e Sérgio Coelho
UC: Segurança e Privacidade

11 de maio de 2025

Índice

Contexto 3

Visão geral 3

Qual é a finalidade de tratamento considerada no âmbito da análise? 3

Quais são as responsabilidades inerentes ao tratamento de dados pessoais? 3

Quais são as normas aplicáveis à finalidade de tratamento? 4

Dados, processos e ativos de suporte 5

Quais são os dados pessoais tratados? 5

Como funciona o ciclo de vida dos dados pessoais e dos processos inerentes? 5

Quais são os ativos de informação utilizados na finalidade de tratamento? 7

Princípios fundamentais 9

Proporcionalidade e necessidade 9

A finalidade de tratamento é específica, explícita e legítima? 9

Qual é o fundamento para tratamento de dados pessoais? 9

Os dados pessoais recolhidos são adequados, relevantes e limitados para o propósito de tratamento realizado (princípio da minimização de dados)? 10

Os dados pessoais estão atualizados e são fidedignos? 10

Qual é o prazo da conservação dos dados? 10

Controlos para proteger os direitos pessoais dos titulares dos dados 11

Como é que os titulares dos dados são informados sobre o tratamento dos seus dados? 11

Como é obtido o consentimento dos titulares de dados? 11

Como é garantido o acesso e portabilidade de dados pessoais? 11

Como é garantida a atualização/retificação e apagamento dos dados pessoais pedida pelo titular dos mesmos? 12

Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos? 12

As obrigações dos subcontratantes são claramente identificadas e reguladas por contrato ou outro ato normativo? 13

No caso de transferência de dados fora da União Europeia, os dados são adequadamente protegidos? 13

Riscos 14

Acesso ilegítimo dos dados 14

Quais poderiam ser os principais impactos nos dados dos titulares se o risco ocorrer? 14

Quais são os principais ameaças que poderiam levar ao risco? 14

Quais são as fontes de risco? 14

Quais são os controlos identificados que contribuem para abordar o risco? 14
Modificação indesejada dos dados 15
Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer? 15
Quais são as principais ameaças que poderiam levar ao risco? 15
Quais são as fontes de risco? 15
Quais são os controlos identificados que contribuem para abordar o risco? 15
Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados? 15
Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados? 15
Desaparecimento de dados 16
Quais são os principais impactos nos dados dos titulares se o risco ocorrer? 16
Quais são as principais ameaças que poderiam levar ao risco 16
Quais são as fontes de risco? 16
Quais são os controlos identificados que contribuem para abordar o risco? 16
Visão Geral dos Riscos 17
Mapeamento dos riscos sem medidas 18
Medidas planeadas ou existentes 19
Anonimização dos Dados 19
Recolha Mínima de Dados (Princípio da Minimização de Dados) 19
Consentimento Informado 19
Monitorização e Registo de Atividades 19
Controlo de Acesso 19
Hashing 20
Auditorias e Revisões Regulares 20
VPNs 20
Backups e Recuperação 20
Mapeamento dos Riscos com as medidas referidas 21
Riscos e Mitigações adicionais 24
Conclusão 26

Contexto

Visão geral

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

A finalidade do tratamento de dados pessoais no âmbito do projeto COP-MODE consiste no desenvolvimento de um mecanismo automatizado, personalizado e consciente do contexto para a gestão de permissões em dispositivos móveis. Este mecanismo visa melhorar a proteção da privacidade dos utilizadores, permitindo uma gestão mais eficiente e adaptativa dos pedidos de acesso feitos pelas aplicações instaladas.

Para este efeito, os dados recolhidos durante as campanhas são utilizados exclusivamente para fins de investigação científica, no contexto da criação de um gestor de permissões que seja capaz de aprender e adaptar-se às preferências individuais de privacidade dos utilizadores, tendo em conta o seu contexto situacional (como localização, pessoas próximas e estado do dispositivo). A recolha de dados permite também compreender melhor os padrões de decisão dos utilizadores face a pedidos de acesso a recursos sensíveis, como localização, contactos, câmara, entre outros.

A recolha do endereço de correio eletrónico tem como única finalidade servir de meio de contacto durante a campanha, sendo eliminado no final da mesma, de forma a garantir a anonimização dos dados e respeitar os princípios de minimização e limitação da conservação previstos no RGPD.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

No âmbito do projeto COP-MODE, a entidade promotora do projeto representada pelas instituições de ensino e investigação envolvidas (Universidade de Coimbra, Universidade do Porto, Universidade de Cambridge e INESC TEC) assume a responsabilidade pelo tratamento dos dados pessoais. Esta entidade atua como responsável pelo tratamento, na medida em que determina as finalidades e os meios de tratamento dos dados recolhidos durante as campanhas.

As responsabilidades do responsável pelo tratamento incluem:

- Garantir que os dados pessoais são recolhidos e tratados exclusivamente para fins legítimos e previamente determinados (investigação científica);
- Implementar medidas técnicas e organizativas adequadas para assegurar a confidencialidade, integridade e segurança dos dados;
- Assegurar a informação clara aos titulares dos dados sobre o tratamento, mediante a assinatura de um acordo de recolha de dados (ponto B), que define de forma transparente o tipo de dados recolhidos, a sua finalidade e os direitos dos participantes;
- Eliminar os dados identificáveis (como o endereço de email) assim que estes deixem de ser necessários, promovendo a anonimização dos dados restantes;
- Garantir o cumprimento das obrigações previstas no Regulamento Geral sobre a Proteção de Dados (RGPD), nomeadamente no que respeita à transparência, legalidade, minimização de dados, e direitos dos titulares.

Caso existam subcontratantes ou terceiros autorizados envolvidos no tratamento (por exemplo, no alojamento dos dados ou suporte técnico da aplicação), estes atuam unicamente segundo instruções do responsável pelo tratamento, estando vinculados contratualmente ao cumprimento das exigências legais em matéria de proteção de dados.

Quais são as normas aplicáveis à finalidade de tratamento?

A finalidade de tratamento de dados pessoais no âmbito do projeto COP-MODE encontra-se enquadrada pelo Regulamento Geral sobre a Proteção de Dados (RGPD). Esta norma europeia é expressamente mencionada nos documentos fornecidos como o principal instrumento legal aplicável ao tratamento de dados realizado no contexto do projeto.

O RGPD estabelece os princípios e as obrigações legais a que os responsáveis pelo tratamento estão sujeitos, incluindo a definição clara das finalidades, a obtenção de consentimento informado dos titulares dos dados, e a implementação de medidas adequadas para garantir a segurança, confidencialidade e minimização dos dados recolhidos.

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Durante a realização das campanhas do projeto COP-MODE, são tratados os seguintes dados pessoais dos participantes:

- Endereço de correio eletrónico: utilizado exclusivamente como meio de contacto durante a campanha. Este dado é eliminado após o fim da participação, contribuindo para a anonimização dos dados remanescentes.
- Lista de aplicações instaladas no smartphone pessoal do participante: inclui os nomes das aplicações e as permissões associadas a cada uma. Não são recolhidos dados internos às aplicações (ex.: mensagens, conteúdos ou contactos).
- Decisões de permissões de acesso: registo das respostas dos participantes a pedidos de acesso feitos pelas aplicações (ex.: aceitar ou recusar acesso à localização).
- Informação contextual associada ao uso do dispositivo:
    - Aplicações em execução em primeiro e segundo plano;
    - Localização do participante;
    - Presença de outras pessoas (com quem se encontra).

Estes dados são recolhidos com o objetivo exclusivo de apoiar a investigação e desenvolvimento de um sistema inteligente de gestão de permissões, sensível ao contexto e adaptado às preferências de privacidade dos utilizadores.

Todos os dados recolhidos são especificados no acordo de recolha de dados, o qual é lido e assinado pelo participante no momento da entrega do smartphone da campanha.

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

O ciclo de vida dos dados pessoais no âmbito do projeto COP-MODE decorre em diferentes fases, desde a recolha inicial até à eliminação ou anonimização, conforme descrito a seguir. O processo é realizado em conformidade com as finalidades científicas do projeto e com o consentimento informado dos participantes.

1. Recolha Inicial (via CM-AR)

A recolha de dados tem início quando o participante instala e executa a aplicação COP-MODE Apps Retriever (CM-AR) no seu smartphone pessoal. Nessa fase são recolhidos:

- O endereço de correio eletrónico, utilizado apenas como meio de contacto durante a campanha;
- A data de consentimento;
- A lista de aplicações instaladas, incluindo os nomes e respetivas permissões.

Estes dados são enviados para o servidor do projeto para configurar o smartphone que será utilizado durante a campanha.

2. Entrega do Dispositivo e Recolha de Consentimento

Antes do início da recolha principal, o participante recebe um smartphone da campanha, previamente configurado com:

- As aplicações pessoais do utilizador;
- A aplicação COP-MODE Naïve Permission Manager (CM-NPM), responsável por recolher os dados durante a utilização.

O participante assina um acordo de recolha de dados, onde são especificados os dados recolhidos e a finalidade do tratamento.

3. Recolha de Dados Durante a Campanha (via CM-NPM)

Durante uma semana, o participante utiliza o smartphone da campanha como dispositivo principal. O CM-NPM atua como gestor de permissões e ferramenta de recolha de dados, intercetando pedidos de permissões por parte das aplicações. Nessa altura, são recolhidos:

- Aplicação solicitante: nome e categoria da Play Store;
- Permissão: nome, grupo e resultado (permitido/negado);
- Estado do telefone: geolocalização, estado de ligação (carregador, dock), estado da chamada, estado do ecrã, tipo de rede, e aplicações em segundo plano;
- Contexto do utilizador: hora, localização semântica e presença em eventos do calendário;

- Expectativa: resposta do utilizador à pergunta *"Pelo que estavas a fazer com o telefone, este pedido era esperado?"*

O sistema apenas intercepta permissões perigosas, conforme definidas pelo Android, e ignora pedidos de aplicações do sistema operativo para preservar a funcionalidade base. Para evitar fadiga do utilizador, a resposta a cada pedido é armazenada durante 30 minutos.

4. Armazenamento e Anonimização

Os dados recolhidos são enviados e armazenados nos servidores do projeto COP-MODE. O endereço de correio eletrónico é eliminado após o fim da campanha, garantindo a anonimização dos dados para futura análise. Os restantes dados permanecem de forma anonimizada para serem utilizados exclusivamente para fins de investigação.

5. Utilização e Disponibilização Científica

A versão anonimizada do conjunto de dados recolhido é posteriormente disponibilizada para investigadores que desejem estudar ou desenvolver soluções na área da privacidade digital. O acesso é condicionado e regulamentado pela equipa do projeto, mediante pedido direto.

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

No contexto do projeto COP-MODE, os ativos de informação dizem respeito a todos os elementos (dados, sistemas, aplicações e infraestruturas) essenciais para a recolha, processamento, armazenamento e análise dos dados pessoais dos participantes. Estes ativos suportam diretamente a finalidade de tratamento — desenvolvimento de um sistema inteligente e sensível ao contexto para gestão de permissões em dispositivos móveis.

Os principais ativos de informação utilizados são:

Dados Pessoais Recolhidos

- Endereço de correio eletrónico (durante a campanha);
- Lista de aplicações instaladas e permissões associadas;

- Decisões de permissões (permitir/recusar);
- Dados contextuais do dispositivo e do utilizador (localização, estado do telefone, presença em eventos, entre outros);
- Informação sobre expectativas de permissões (“pedido esperado”).

Aplicações Desenvolvidas no Âmbito do Projeto

- CM-AR (COP-MODE Apps Retriever): ferramenta responsável pela recolha inicial do email e da lista de aplicações do dispositivo pessoal do participante.
- CM-NPM (COP-MODE Naïve Permission Manager): gestor de permissões avançado e ferramenta de recolha contínua de dados durante a campanha. Implementado como módulo EdXposed, permite interceptar chamadas às permissões perigosas e recolher contexto sem alterar a funcionalidade original das aplicações.

Infraestrutura de Armazenamento e Processamento

- Servidores do projeto COP-MODE, onde os dados recolhidos são armazenados de forma segura. Os servidores gerem o envio inicial de dados via CM-AR, a receção contínua de dados do CM-NPM, e a eliminação ou anonimização dos dados identificáveis ao final da campanha.

Base de Dados Anonimizada para Investigação

- Conjunto de dados processados e anonimizados, armazenados com vista a serem partilhados com a comunidade científica, mediante pedido, para promover investigação em privacidade digital.

Dispositivos da Campanha

- Smartphones emprestados aos participantes para utilização durante uma semana, contendo as aplicações necessárias para a recolha de dados e simulação de uso real.

Estes ativos são geridos exclusivamente pela equipa do projeto COP-MODE, e a sua utilização está limitada aos fins de investigação previamente definidos e comunicados aos

participantes. Medidas de segurança técnica e organizativa são aplicadas para proteger os ativos contra acesso não autorizado ou perda de integridade.

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

Sim, a finalidade de tratamento definida no âmbito do projeto COP-MODE é específica, explícita e legítima.

O objetivo do tratamento é o desenvolvimento de um sistema inteligente de gestão de permissões em dispositivos móveis, baseado na recolha de decisões de privacidade e dados contextuais dos utilizadores. Esta finalidade é claramente comunicada aos participantes no momento da inscrição na campanha, através da aplicação e do acordo de recolha de dados que deve ser assinado no ato da entrega do smartphone.

O tratamento é realizado exclusivamente para fins de investigação científica, no âmbito de um projeto financiado pela União Europeia (Horizon 2020 – NGI_TRUST), sendo obtido o consentimento informado dos participantes e assegurada a eliminação dos dados identificáveis após a campanha. Assim, a finalidade do tratamento está bem definida, é transparente para os titulares dos dados, e cumpre os critérios de legalidade, necessidade e proporcionalidade estabelecidos pelo RGPD.

Qual é o fundamento para tratamento de dados pessoais?

O fundamento para o tratamento de dados pessoais no âmbito do projeto COP-MODE é o consentimento explícito dos participantes. De acordo com o processo descrito, os dados pessoais são coletados apenas após o consentimento informado dos participantes, que é dado de forma explícita no momento da inscrição e assinatura do acordo de coleta de dados.

Os participantes têm conhecimento claro das finalidades da coleta de dados, que se destinam ao desenvolvimento de um gestor de privacidade automatizado e personalizado, consciente do contexto. O consentimento abrange a coleta de dados como o e-mail, a lista de aplicativos instalados no smartphone e as permissões de acesso concedidas a esses aplicativos.

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

Sim, os dados pessoais recolhidos no projeto COP-MODE são adequados, relevantes e limitados ao propósito específico. Apenas são coletados os dados essenciais para o desenvolvimento do gestor de privacidade, como o e-mail (para comunicação), a lista de aplicações instaladas (sem dados sensíveis) e dados contextuais (como localização e estado do dispositivo), em conformidade com o princípio da minimização de dados.

Os dados pessoais estão atualizados e são fidedignos?

Os dados pessoais recolhidos no projeto COP-MODE são atualizados e fidedignos no momento da coleta, pois são fornecidos diretamente pelos participantes durante o processo de inscrição e no uso da aplicação.

A lista de aplicações e permissões é baseada nas configurações atuais do dispositivo do participante, e o e-mail é coletado para comunicação durante a campanha. No entanto, após a conclusão da campanha, os dados, como o e-mail, são anonimizados, garantindo a sua precisão e conformidade com o objetivo do projeto.

Qual é o prazo da conservação dos dados?

Os dados recolhidos serão conservados apenas pelo tempo necessário para cumprir a finalidade do tratamento. Após a conclusão da campanha, dados pessoais como o e-mail serão anonimizados.

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 titulares dos dados são informados sobre o tratamento dos seus dados através de um acordo de coleta de dados que deve ser lido, compreendido e assinado antes da participação no projeto COP-MODE. Este acordo descreve claramente as finalidades da coleta de dados, os tipos de dados pessoais a serem recolhidos, como serão usados e os direitos dos participantes em relação aos seus dados.

Como é obtido o consentimento dos titulares de dados?

O consentimento dos titulares dos dados é obtido de forma explícita e informada durante o processo de inscrição no projeto COP-MODE. Os participantes devem ler e assinar um acordo de coleta de dados antes de fornecer qualquer informação. Este acordo detalha claramente as finalidades da coleta de dados, os tipos de dados recolhidos e como serão utilizados. O consentimento é obtido no momento em que o participante instala e utiliza a aplicação COP-MODE Apps Retriever (CM-AR), após o qual os dados são coletados conforme o descrito no acordo. O consentimento é dado de forma voluntária e pode ser revogado a qualquer momento, conforme as disposições do RGPD.

Como é garantido o acesso e portabilidade de dados pessoais?

O acesso e a portabilidade dos dados pessoais são garantidos através do direito de acesso previsto pelo Regulamento Geral de Proteção de Dados (RGPD). Os titulares dos dados têm o direito de solicitar, a qualquer momento, informações sobre os dados pessoais que foram recolhidos, bem como o direito de os obter em um formato estruturado, de uso comum e legível por máquina, para os transferir a outro responsável pelo tratamento, se desejado.

No contexto do projeto COP-MODE, os participantes podem solicitar o acesso aos dados recolhidos durante a campanha, e a equipe do projeto assegura que esses dados sejam

fornecidos de forma clara e transparente, respeitando os direitos dos participantes. Embora a portabilidade dos dados seja mais relevante para dados pessoais estruturados, a possibilidade de acesso aos dados de maneira detalhada é garantida por meio do acordo de coleta de dados, permitindo que os titulares tomem decisões informadas sobre o tratamento de seus dados.

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

A atualização, retificação e apagamento dos dados pessoais são garantidos em conformidade com os direitos dos titulares previstos no Regulamento Geral de Proteção de Dados (RGPD).

- **Atualização e retificação:** Caso um titular dos dados solicite a atualização ou retificação das suas informações, o projeto COP-MODE assegura que tais alterações sejam feitas de forma rápida e eficaz. O titular pode contactar a equipa do projeto para solicitar a correção de qualquer dado impreciso ou incompleto.
- **Apagamento dos dados:** Os dados pessoais serão apagados quando já não forem necessários para a finalidade para a qual foram recolhidos, ou quando o titular revogar o consentimento e não houver outro fundamento legal para o tratamento. No caso do projeto COP-MODE, o e-mail do participante é apagado no fim da campanha, garantindo a anonimização dos dados pessoais. Se solicitado, o participante pode pedir o apagamento de outros dados recolhidos, desde que não haja outra base legal para a retenção desses dados.

O projeto assegura que os titulares podem exercer esses direitos, através de um contacto direto com a equipa responsável pelo tratamento dos dados, garantindo que os pedidos sejam atendidos de acordo com as regulamentações aplicáveis.

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

A limitação do tratamento dos dados pessoais é garantida em conformidade com o Regulamento Geral de Proteção de Dados (RGPD), que concede aos titulares o direito de

restringir o tratamento dos seus dados em determinadas situações. No projeto COP-MODE, a limitação do tratamento pode ser solicitada pelos titulares dos dados nas seguintes condições:

1. **Correção de dados imprecisos:** Enquanto os dados são corrigidos, o tratamento pode ser temporariamente limitado.
2. **Oposição ao tratamento:** Caso o titular dos dados se oponha ao tratamento dos seus dados pessoais, o projeto COP-MODE deve suspender temporariamente o tratamento até que a equipe verifique a legitimidade da oposição.
3. **Dados tratados ilegalmente:** Se os dados forem tratados de forma ilegal, o titular pode pedir para restringir o tratamento em vez de os apagar, desde que o tratamento seja necessário para cumprir com obrigações legais.
4. **Período de verificação:** Se o titular contestar a exatidão dos dados, o tratamento pode ser limitado até a confirmação da precisão dos mesmos.

Durante o processo de coleta de dados no COP-MODE, qualquer solicitação de limitação de tratamento será tratada com base nos direitos do titular e conforme a legislação aplicável, garantindo que os dados não sejam processados enquanto a limitação estiver em vigor. A equipa do projeto assegura que os pedidos de limitação sejam atendidos de forma eficiente e dentro dos prazos estabelecidos pelo RGPD.

As obrigações dos subcontratantes são claramente identificadas e reguladas por contrato ou outro ato normativo?

Sim, as obrigações dos subcontratantes no âmbito do projeto COP-MODE são claramente identificadas e reguladas por contrato ou outro ato normativo. De acordo com o Regulamento Geral de Proteção de Dados (RGPD), qualquer subcontratante que trate dados pessoais em nome do controlador (no caso, a equipa do COP-MODE) deve estar vinculado a um contrato de subcontratação.

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

Sim, no caso de transferência de dados pessoais para fora da União Europeia (UE), o projeto COP-MODE garante que os dados são adequadamente protegidos, em

conformidade com o Regulamento Geral de Proteção de Dados (RGPD). As transferências internacionais de dados são permitidas, desde que sejam cumpridas as condições estabelecidas pelo RGPD para garantir a proteção dos dados dos titulares.

Riscos

Acesso ilegítimo dos dados

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

Violação da privacidade, Perda dos dados, Uso indevido dos dados, Manipulação não autorizada dos dados, Risco de fraude

Quais são os principais ameaças que poderiam levar ao risco?

Acesso não autorizado, Roubo de dispositivos móveis, Erros humanos, Leaks de informação acidentais, Malware

Quais são as fontes de risco?

Erro Humano, Software Bugs, Acessos não autorizados, Desastres físicos, Ameaças internas

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

Anonimização dos Dados, Recolha Mínima de Dados (Princípio da Minimização de Dados), Consentimento Informado, Monitorização e Registo de Atividades, Controlo de Acesso, Hashing, Auditorias e Revisões Regulares, VPNs, Backups e Recuperação

Modificação indesejada dos dados

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

Perda dos dados, Manipulação não autorizada dos dados, Risco de fraude, Uso indevido dos dados, Violação da privacidade

Quais são as principais ameaças que poderiam levar ao risco?

Leaks de informação acidentais, Malware, Erros humanos

Quais são as fontes de risco?

Acessos não autorizados, Erro Humano, Ameaças internas

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

Anonimização dos Dados, Consentimento Informado, VPNs, Recolha Mínima de Dados (Princípio da Minimização de Dados), Monitorização e Registo de Atividades, Controlo de Acesso, Hashing, Auditorias e Revisões Regulares, Backups e Recuperação

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

Significante

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

Limitado

Desaparecimento de dados

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

Perda dos dados, Uso indevido dos dados, Risco de fraude, Manipulação não autorizada dos dados

Quais são as principais ameaças que poderiam levar ao risco

Erros humanos, Leaks de informação acidentais, Malware

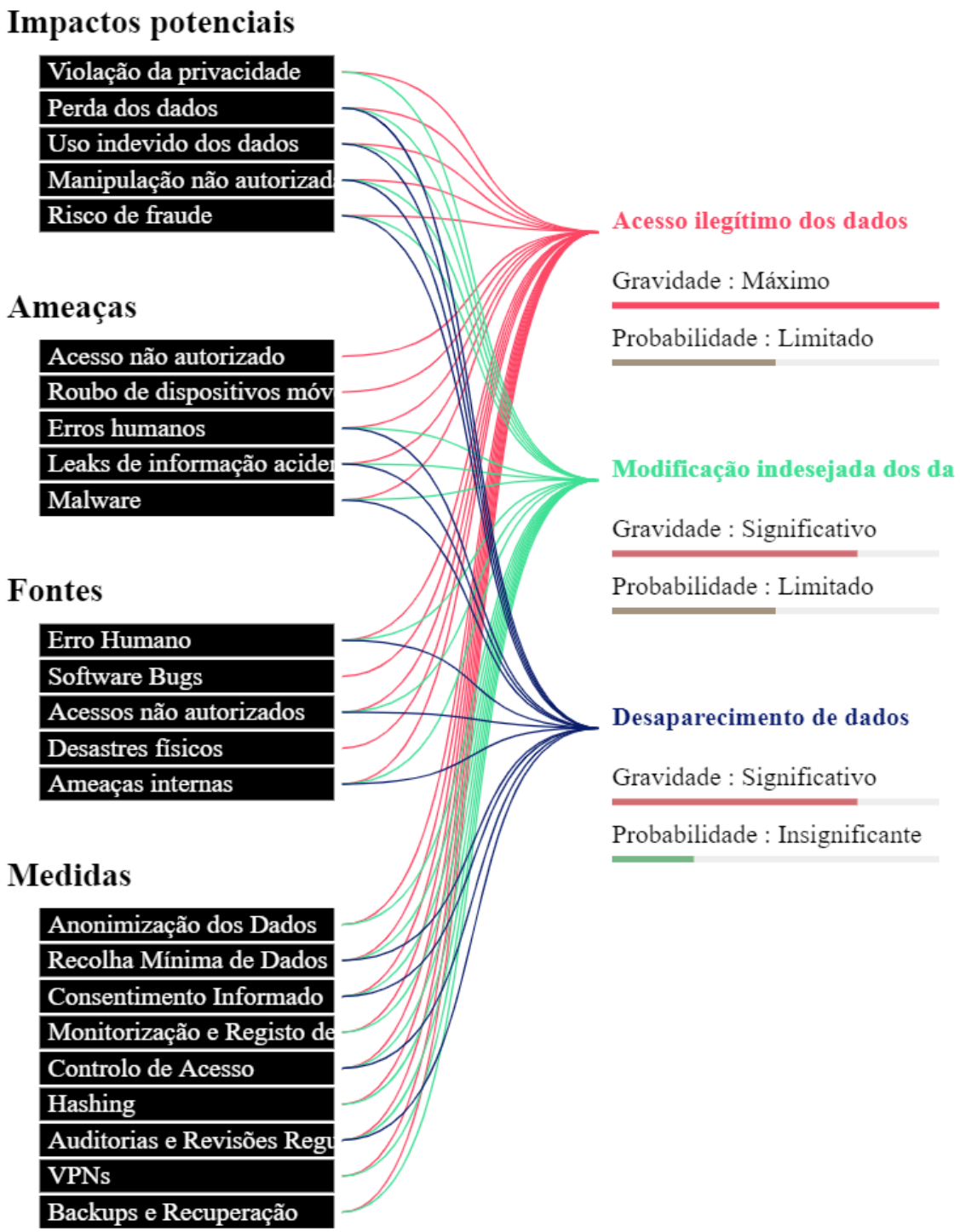
Quais são as fontes de risco?

Erro Humano, Acessos não autorizados, Ameaças internas

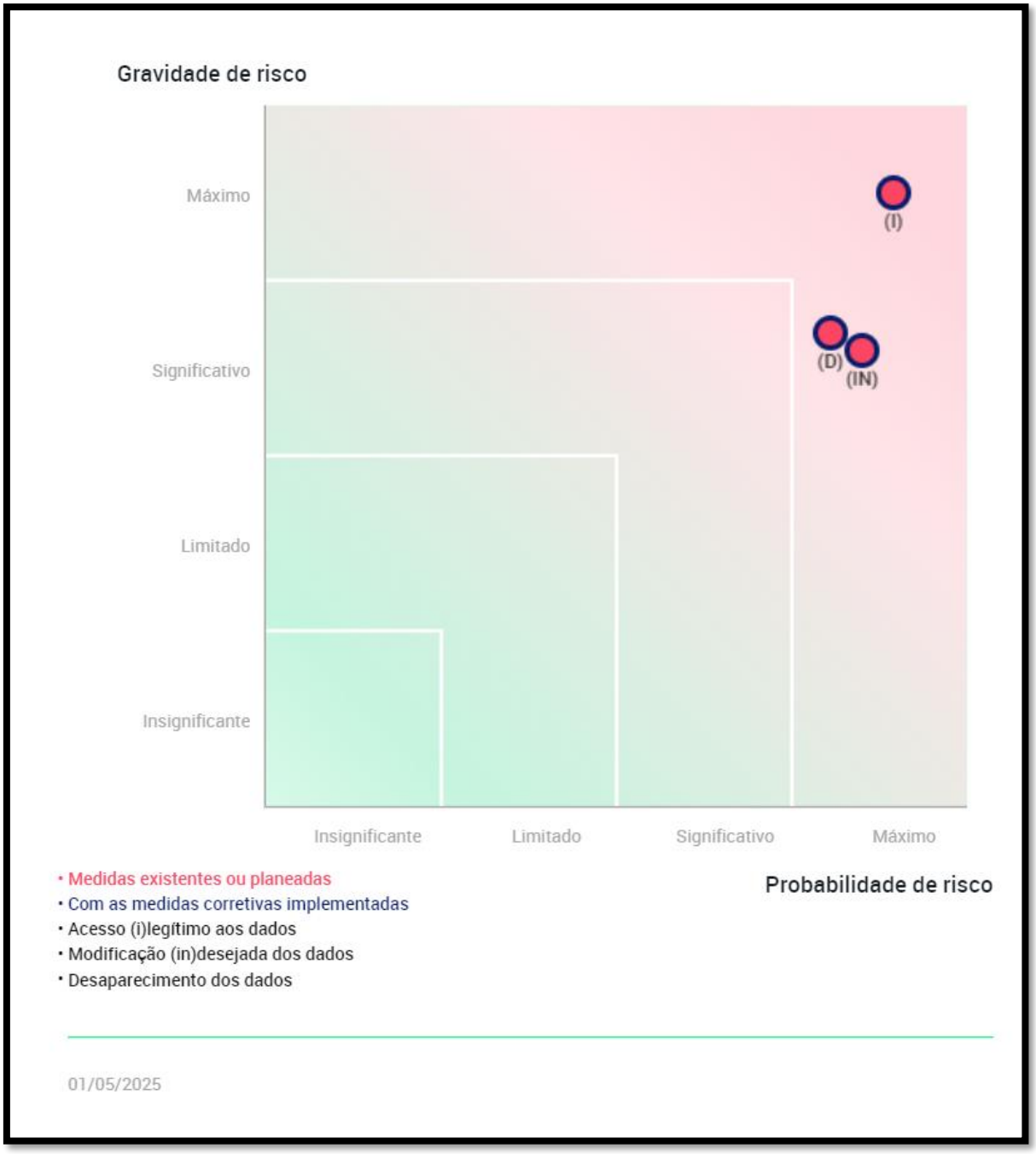
Quais são os controlos identificados que contribuem para abordar o risco?

Recolha Mínima de Dados (Princípio da Minimização de Dados), Controlo de Acesso, Consentimento Informado, Auditorias e Revisões Regulares

Visão Geral dos Riscos



Mapeamento dos riscos sem medidas



Medidas planeadas ou existentes

Anonimização dos Dados

Os dados pessoais recolhidos, como o email e a lista de aplicações, são anonimizados após a conclusão da campanha. Isso ajuda a garantir que as informações pessoais não possam ser associadas a um titular específico sem informações adicionais.

Recolha Mínima de Dados (Princípio da Minimização de Dados)

O projeto coleta apenas os dados estritamente necessários para o desenvolvimento do gestor de privacidade, como a lista de aplicações instaladas e as permissões solicitadas, sem aceder ou coletar dados sensíveis ou confidenciais das aplicações.

Consentimento Informado

O consentimento explícito dos participantes é obtido antes da coleta de qualquer dado, e os participantes são informados de maneira clara sobre os dados que serão coletados e como serão utilizados (via acordo de coleta de dados).

Monitorização e Registo de Atividades

Manter registos detalhados de todas as atividades de acesso e modificação dos dados. Estes registos devem incluir o User, a data, a hora, e a natureza da modificação.

Implementar ferramentas de monitorização que alertam os administradores sobre atividades suspeitas ou não autorizadas em tempo real.

Controlo de Acesso

O acesso aos dados pessoais é restrito apenas às pessoas e sistemas autorizados, com o uso de controlos de acesso rigorosos (e.g., autenticação de dois fatores para usuários).

Hashing

Como medida planeada, a implementação de um sistema de hashing traz mais simplicidade e ao mesmo tempo mais segurança. Em vez de armazenar diretamente o nome das aplicações, estes são substituídos por um identificador único.

Auditorias e Revisões Regulares

O projeto realiza auditorias de privacidade e revisões periódicas para garantir que o tratamento de dados pessoais esteja conforme o regulamento e as práticas de segurança sejam eficazes.

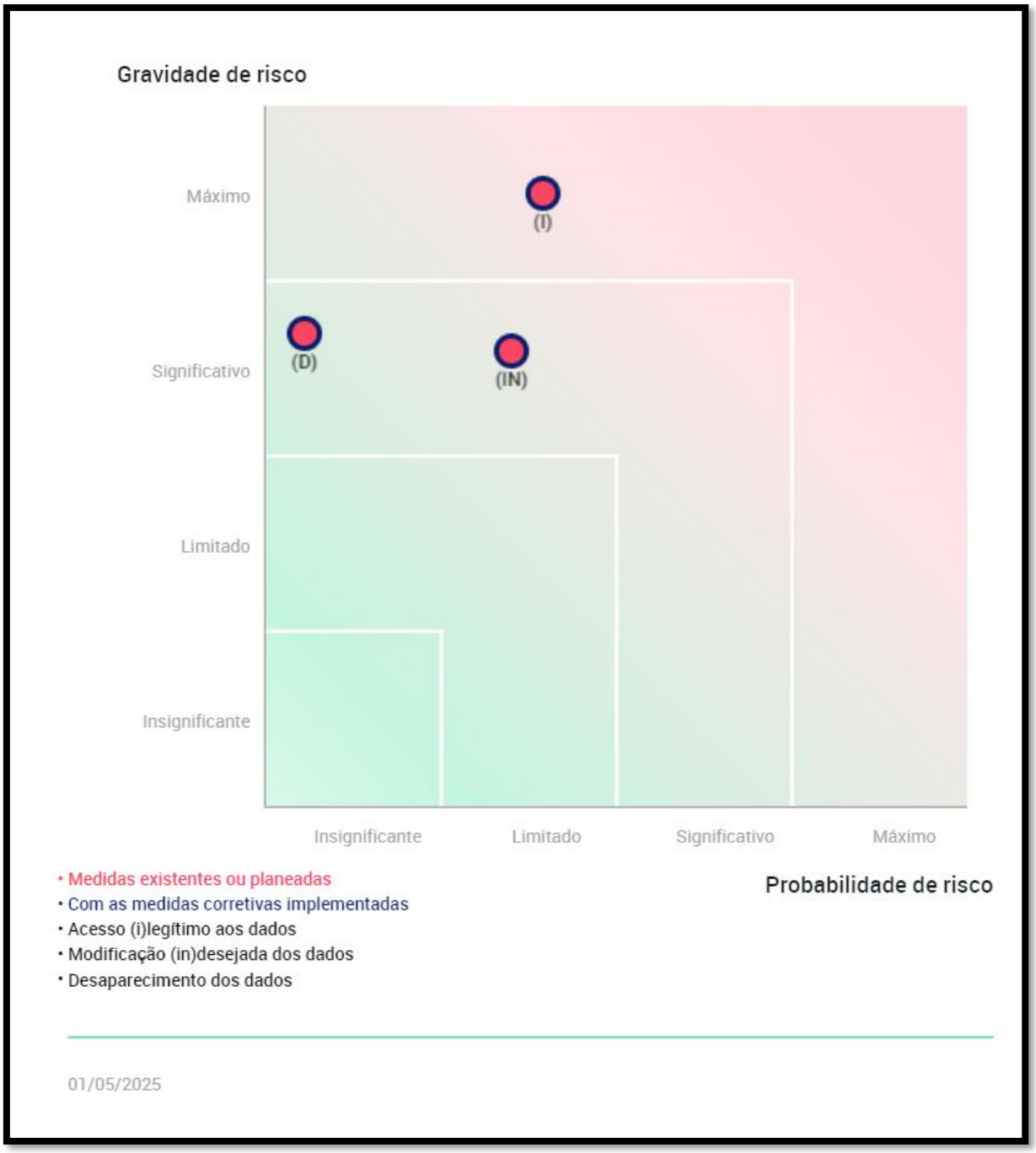
VPNs

A implementação de uma VPN (Virtual Private Network) para transmissões de dados e informações adiciona uma camada extra de encriptação e segurança.

Backups e Recuperação

Foram implementadas políticas de cópias de segurança regulares e seguras, garantindo a possibilidade de recuperação dos dados em caso de perda, alteração acidental ou ataque malicioso. Além disso, são realizados testes periódicos aos procedimentos de recuperação de desastres, assegurando a sua eficácia e a capacidade de restaurar os dados de forma rápida e fiável perante qualquer incidente.

Mapeamento dos Riscos com as medidas referidas



Com a implementação das medidas de mitigação referidas, a probabilidade de haver risco, bem como a gravidade do mesmo associados ao acesso ilegítimo de dados pessoais, podem ser significativamente reduzidos. Abaixo seguem-se algumas medidas, e como a sua implementação teve influência na gravidade e probabilidade de ocorrência de risco.

Consentimento Informado

Impacto na Probabilidade - O risco de tratamento indevido ou não autorizado de dados pessoais diminui, pois, os participantes estão plenamente informados e concordam conscientemente com a recolha e uso dos seus dados.

Impacto na Gravidade - A gravidade do impacto caso o risco ocorra (ex: vazamento de dados) não se altera significativamente, pois os danos aos titulares ainda podem ser elevados. No entanto, a transparência do processo e o respeito pelo direito à informação podem atenuar parcialmente as consequências legais para os responsáveis pelo tratamento.

Hashing

Impacto na Probabilidade - A substituição dos nomes das aplicações por identificadores únicos através de hashing dificulta a identificação direta das aplicações por terceiros não autorizados. Reduz o risco de exposição direta de informação sensível, como nomes de apps que podem indicar comportamentos ou preferências pessoais. A eficácia depende da robustez do algoritmo de hash e da ausência de reversibilidade.

Impacto na Gravidade - Se a técnica for bem implementada (sem armazenamento de tabelas de reversão ou hashes fracos), a gravidade dos impactos em caso de violação pode ser atenuada.

Controlo de Acesso

Impacto na Probabilidade - A aplicação de controlos de acesso rigorosos, como a autenticação de dois fatores, reduz substancialmente a probabilidade de acessos não autorizados.

Impacto na Gravidade - A existência de logs e restrições de acesso pode facilitar a deteção e resposta rápida, reduzindo o tempo de exposição do risco.

Anonimização dos Dados

Impacto na Probabilidade - Ao anonimizar os dados após a campanha, torna-se muito mais difícil que qualquer entidade (interna ou externa) associe a informação recolhida a um indivíduo específico.

Impacto na Gravidade - Mesmo que os dados anonimizados sejam acedidos de forma indevida, a ausência de ligação direta a uma identidade reduz fortemente os danos potenciais (como discriminação, vigilância, ou violação de privacidade). A severidade de impacto em caso de violação passa a estar associada apenas a dados genéricos, sem consequência direta para os titulares.

Recolha Mínima de Dados

Impacto na Probabilidade - Ao limitar a recolha apenas aos dados estritamente necessários, reduz-se a superfície de ataque e o número de pontos vulneráveis que podem ser explorados.

Impacto na Gravidade - Mesmo que haja um acesso não autorizado, o impacto será mais limitado, dado que os dados recolhidos não são sensíveis nem confidenciais. A ausência de dados excessivos ou altamente identificáveis faz com que o dano potencial para os titulares seja muito menor.

Backups e Recuperação

Impacto na Probabilidade - A existência de backups regulares e seguros não impede um ataque, mas mitiga a probabilidade de perda irreversível de dados.

Impacto na Gravidade – Caso ocorra uma falha ou ataque, a capacidade de recuperar os dados rapidamente diminui significativamente o impacto sobre os titulares.

Riscos e Mitigações adicionais

Risco	Mitigação
Fuga de dados por escuta das comunicações entre smartphones e o servidor do projeto.	- Utilização de protocolos de comunicação seguros como HTTPS/TLS. - Implementação de VPN para comunicação entre dispositivos e o servidor. - Encriptação de ponta-a-ponta dos dados transmitidos.
Fuga de dados por acesso não autorizado ao servidor ou aos dados.	- Restrição de acesso aos dados apenas a utilizadores autorizados. - Configuração segura do servidor para não estar diretamente acessível a partir do exterior. - Autenticação forte (e.g., autenticação multifator) para acesso ao sistema.
Ligação dos dados em repouso a indivíduos.	- Encriptação de dados sensíveis, incluindo endereços de e-mail. - Utilização de identificadores pseudónimos que só possam ser revertidos pelo responsável pelo tratamento. - Mecanismo de correspondência interna para garantir a possibilidade de apagar dados a pedido do participante.
Fuga de informação sensível, em particular os nomes das aplicações recolhidas.	- Anonimização ou hashing dos nomes das aplicações antes de serem armazenados. - Utilização de identificadores simbólicos em vez de nomes reais das aplicações. - Separação lógica entre dados identificáveis e nomes das aplicações durante o armazenamento.

Impactos das Mitigações nos Riscos Adicionais

Risco	Probabilidade De Ocorrência	Gravidade Do Risco
Fuga de dados por escuta das comunicações entre smartphones e o servidor do projeto.	Baixa – As comunicações são protegidas por HTTPS, VPN e pinning de certificados, tornando a interceção altamente improvável.	Alta – Se ocorrer, pode expor dados sensíveis, comprometendo a privacidade dos participantes.
Fuga de dados por acesso não autorizado ao servidor ou aos dados.	Baixa – Medidas como controlo de acesso, autenticação multifator e isolamento do servidor reduzem significativamente o risco.	Alta – O acesso não autorizado pode expor grandes volumes de dados pessoais.
Ligação dos dados em repouso a indivíduos	Baixa – Os dados são anonimizados e pseudonimizados após a recolha, impedindo a ligação direta.	Média – Se os dados forem reidentificados, pode haver violação de privacidade individual.
Fuga de informações sensíveis, como nomes das aplicações	Muito baixa – É aplicada uma técnica de hashing para ocultar os nomes das aplicações.	Baixa – Mesmo que os dados sejam acedidos, a informação não estará em formato legível.

Conclusão

A realização desta Avaliação de Impacto sobre a Privacidade (PIA) permitiu analisar, de forma sistemática e fundamentada, os riscos associados ao tratamento de dados pessoais no âmbito do projeto COP-MODE. Ao longo do relatório, identificámos os tipos de dados recolhidos, os processos envolvidos no seu tratamento, os riscos potenciais para os titulares dos dados e as medidas de controlo técnicas e organizativas que foram, ou poderão ser, implementadas para mitigar esses riscos.

O projeto demonstrou uma forte preocupação com a proteção da privacidade dos participantes, adotando práticas alinhadas com os princípios do Regulamento Geral sobre a Proteção de Dados (RGPD), nomeadamente a minimização de dados, a anonimização, o consentimento informado e a limitação da conservação. A aplicação de controlos como o hashing, o controlo de acesso, a monitorização de atividades e as políticas de backup e recuperação reforça a resiliência do sistema e contribui para a redução tanto da probabilidade como da gravidade dos riscos identificados.

Conclui-se que, com as medidas de mitigação implementadas e planeadas, o tratamento de dados no projeto COP-MODE apresenta um risco residual aceitável, desde que haja um acompanhamento contínuo, auditorias regulares e manutenção das boas práticas descritas. O PIA constitui assim não só um exercício de conformidade legal, mas também uma ferramenta valiosa de gestão de riscos e de reforço da confiança dos titulares de dados.