Privacy Impact Assessment

Leonor Oliveira Rodrigues, up202304869
Paulo Diogo Lopes Pinto, up202306412
Rui Filipe Rocha Alvarilhão, up202209989

FCUP - Faculdade de Ciências, Universidade do Porto

1 Introdução

No atual cenário tecnológico, onde a recolha e processamento de dados pessoais se tornaram algo comum além de serem uma mercadoria valiosa, a proteção e privacidade dos nossos dados passaram a ser um requisito legal e ético.

O presente relatório tem como objetivo realizar uma avaliação de Impacto sobre a Privacidade (PIA) no âmbito do projeto de investigação COP-MODE, realizado em parceria pela Universidade de Coimbra, Universidade do Porto, Universidade de Cambridge e INESC TEC. Esta avaliação será realizada com recurso à ferramenta CNIL PIA, com o propósito de identificar riscos, mitigar vulnerabilidades e promover o tratamento adequado da informação pessoal identificável (PII).

Neste trabalho, pretende-se estudar os potenciais riscos associados ao tratamento de dados pessoais, propor medidas eficazes de mitigação e avaliar o impacto dessas medidas através de, por exemplo, uma risk matrix. Deste modo, reforça-se a ideia de que a proteção da privacidade deve ser uma prioridade em qualquer projeto que lide com informações sensíveis.

2 COP-MODE

2.1 Visão geral e fluxo da campanha

O projeto tem como objetivo investigar um grande problema nos dias de hoje, sendo ele a recolha e manuseamento da informação pessoal de um utilizador. Tudo que fazemos através dos nossos telemóveis e computadores é analisado por grandes empresas e muitas vezes partilhado com outras entidades. Por mais que não queiramos aceitar, esses dados, apesar de conterem informações privadas e sensíveis sobre o utilizador, passam a pertencer à empresa, logo que obtenham o nosso consentimento.

O COP-MODE (Context-aware Privacy protection for Mobile Devices) é um projeto de investigação que pretende criar um gestor de privacidade com as 3 propostas seguintes:

1. **Automação:** Prevenir as frequentes notificações ou solicitações de permissão.

2. **Ciente do contexto:** É capaz de respeitar as preferências pessoais de privacidade em função do contexto.
3. **Personalização:** Ajusta as definições de privacidade conforme as preferências pessoais.

Para conseguir criar este gestor de privacidade foi realizada uma campanha, onde foram recolhidos e analisados dados de uso de aplicações em telemóveis, por meio de um servidor e uma equipa organizada. Com o objetivo de analisar decisões de privacidade do utilizador durante uma semana.

As decisões de privacidade consistem em aceitar ou recusar que uma determinada aplicação tenha acesso a um recurso. Já em relação ao contexto, foi capturado o estado atual do dispositivo, por exemplo, aplicações que estão ativas tanto em primeiro e segundo plano. Além disso, informações que descrevam o ambiente e a situação do mesmo, também foram recolhidas, como por exemplo localização e com quem estava.

A campanha realizada pela equipa pode ser resumida em 5 etapas:

- A **1ª etapa** foi o recrutamento. Foram enviados vários e-mails para potenciais participantes. Caso estes desejem participar, terão de instalar a aplicação COP-MODE Apps Retriever (CM-AR).
- A **2ª etapa** consiste em executar a aplicação CM-AR. Esta aplicação manda um e-mail com a data de consentimento e a lista de aplicações e respetivas permissões ,do telemóvel pessoal, para o servidor. Vale ressaltar que nenhum dado que pertença à aplicação foi coletado.
- A **3ª etapa** consistiu na configuração e entrega dos telemóveis. A equipa do COP-MODE, instalou em cada um dos dispositivos da campanha as respetivas aplicações. Este dispositivo vem com COP-MODE Naive Permission Manager (CM-NPM), um gestor de permissões que tratará de pedir permissões de acesso a aplicações, tal como a recolha dos dados.
- A **4ª etapa** durou uma semana e o participante deverá usar o telemóvel da campanha como se fosse o seu telemóvel pessoal. Nesse período de tempo, o gestor CM-NPM irá recolher as respostas do utilizador, bem como o contexto em que elas são dadas.
- Na **5ª etapa** é informado ao utilizador o fim da campanha e este tem de devolver o dispositivo.

No final da campanha os dados recolhidos foram anonimizados, garantindo a privacidade de cada um dos participantes.

2.2 Identificação das entidades e fluxo de dados pessoais

A descrição de **como os dados pessoais (PII - Personally identifiable information)** entram, circulam e saem do sistema, incluindo **as entidades envolvidas e os seus papéis** no tratamento da informação, é um elemento essencial de uma Avaliação de Impacto sobre a Privacidade (PIA).

No caso do projeto COP-MODE, os papéis fundamentais são:

- **Titular dos dados (PII principal / data subject):** Os participantes da campanha COP-MODE. São indivíduos cujos dados pessoais (como localização, decisões de permissão, etc.) são recolhidos durante o estudo.
- **Responsável pelo tratamento dos dados (PII controller):** A equipa COP-MODE, que define as finalidades e os meios do tratamento dos dados pessoais no âmbito do projeto. Inclui investigadores da Universidade de Coimbra, Universidade do Porto, INESC TEC e Universidade de Cambridge.
- **Subcontratante (PII processor):** A própria equipa COP-MODE também desempenha o papel de processador, pois trata os dados com base nas finalidades definidas. O sistema de backend (MongoDB, etc.) processa os dados sob a sua gestão.
- **Terceiros autorizados (third parties):** Apenas parceiros académicos previamente autorizados e que assinem um termo de responsabilidade podem ter acesso a subconjuntos anonimizados dos dados, exclusivamente para fins de investigação.

2.3 Componentes técnicas e design do sistema

Para o projeto COP-MODE conseguir recolher e analisar os dados, tal como a decisão de conceder ou negar uma permissão, foram implementadas no projeto várias ferramentas:

- **COP-MODE Apps Retriever (CM-AR)**
  É a aplicação usada na 2ª etapa da campanha. Ao obter o consentimento do utilizador, as aplicações e as suas respetivas permissões são guardadas num servidor onde são analisadas posteriormente.
- **COP-MODE Naive Permission Manager (CM-NPM)**
  Uma das ferramentas mais importantes em toda a campanha, principalmente na 4ª etapa. Funciona em segundo plano no sistema android, através da tecnologia Xposed/EdXposed, para interceptar sempre que uma aplicação pede uma permissão sensível. Esta ferramenta tem um prompt próprio, que além de gravar a resposta (aceitar/negar), também guarda informação de contexto, por exemplo onde estava, se havia rede, etc. Todas as informações recolhidas são então enviadas para o mesmo servidor usado na aplicação CM-AR.
- **Backend de coleta e análise dos dados**
  É um servidor com uma base de dados, neste caso MongoDB, que recebe e guarda todos os registos enviados pelas duas ferramentas citadas anteriormente. Contém scripts ou notebooks (Python/Jupyter) que processam os dados para gerar determinadas configurações de privacidade, como por exemplo em que situações um utilizador tende a negar ou

aceitar determinada permissão.

Estas 3 ferramentas foram então cruciais para conseguir completar o objetivo do projeto, pois foram elas que permitiram entender o comportamento real dos utilizadores, o que levou à criação do gestor automático de permissões.

2.4 Recolha e Manuseamento dos dados

Os estudos realizados nesta investigação foram aprovados pelo comitê do departamento de Ciência e Tecnologia da Computação da Universidade de Cambridge e pela comissão de ética da Faculdade de Ciências da Universidade do Porto.

Todos os dados guardados durante a campanha e o seu respetivo tratamento tiveram de seguir certas normas, tal como:

- **Proteção e Privacidade dos Dados**
  Nunca foi acedido aos dados pessoais dos participantes, tal como podemos verificar na 1ª etapa, apenas o e-mail e aplicações instaladas foram recolhidas, sem nunca aceder a dados das aplicações. Além disso, a informação recolhida foi usada apenas para os propósitos da campanha, como por exemplo, configuração dos telemóveis, e não para outros fins.
- **Segurança dos dados**
  É assegurado aos participantes que os dados enviados ao servidor, são transmitidos e armazenados de forma segura. Sem que ocorram acessos não autorizados, perda ou destruição dos mesmos.
- **Anonimização e Eliminação dos Dados**
  É garantido aos participantes que os dados não são armazenados por mais tempo do que o necessário. Além de serem removidos identificadores, como por exemplo o e-mail, garantindo a anonimização dos dados.
- **Consentimento Informado**
  É necessário que os participantes autorizem a recolha dos dados, que é feito ao assinar o Acordo De Coleta de Dados COP-MODE, bem como quais são os dados a serem coletados e como vão ser tratados.
- **Transparência e Acesso**
  É necessário informar os participantes de como podem aceder e como solicitar a sua eliminação, bem como quais dados serão armazenados.
- **Assistência Técnica**
  Por último a equipa COP-MODE, deve providenciar qualquer assistência técnica que seja necessária durante a campanha

Segundo o **Acordo de Coleta de Dados COP-MODE**, todos os dados guardados serão utilizados exclusivamente para investigação e tratados apenas pela equipa do COP-MODE na Universidade de Coimbra, a qual se comprometeu às melhores práticas de privacidade e segurança. Vale ressaltar que caso o

participante, assim o desejar, todos os seus dados podem ser removidos da base de dados.

Os seguintes tipos de dados pessoais foram tratados e recolhidos pela equipa:

1. **Dados de contacto**
   Foi recolhido o e-mail, com a finalidade de manter o contacto com o participante. Este dado será apagado assim que for devolvido o telemóvel da campanha.
2. **Dados dos dispositivos**
   Estes dados referem-se às aplicações instaladas e as suas configurações de permissões, tipo de conexão e contexto do dispositivo (nativo, em uso, em chamada, entre outros). Através destes dados a equipa queria analisar o dispositivo e contexto para o projeto. Estes dados foram mantidos até a conclusão da análise dos mesmos, e logo após este processo foram anonimizados ou apagados, caso o utilizador assim o desejasse.
3. **Localização**
   É recolhida a localização geográfica do utilizador, deste modo é possível encontrar padrões no comportamento do utilizador, algo bastante útil para análise dos dados de contexto. Os dados foram mantidos segundo o mesmo conceito dos dados no ponto 2.
4. **Dados de proximidade**
   Quais são os dispositivos próximos. Estes dados são recolhidos através do bluetooth e wi-fi. Tal como os dados do ponto 3 são úteis para análise dos dados de contexto. Os dados foram mantidos segundo o mesmo conceito dos dados no ponto 2.
5. **Dados de pedido de permissão**
   Neste tipo de dados são armazenadas as aplicações que estão a correr em segundo plano e as decisões do participante. Neste caso não são recolhidas quaisquer outras informações sobre dados internos da aplicação. Estes dados são úteis para entender as decisões do utilizador e foram mantidos segundo o mesmo conceito dos dados no ponto 2.

No que diz respeito à partilha dos dados, a equipa do COP-MODE poderá apenas partilhar um conjunto limitado dos dados recolhidos com parceiros académicos e apenas para investigação. Todos os dados foram **sanitizados** e **anonimizados**, de forma a respeitar a privacidade dos participantes.

O dataSet que é partilhado terá apenas os dados nos pontos 2 e 5. Além disso, para obter uma cópia dos dados anonimizados é necessário assinar um acordo, que proíbe a pessoa de partilhar os dados, vendê-los ou usá-los de forma maliciosa. Deve-se guardar os dados de acordo com as melhores práticas de privacidade e segurança. Por fim, caso algum participante queira que os seus dados sejam apagados, a cópia deve ser também alterada atendendo ao pedido do utilizador.

3 Likelihood e Severity

Como o objetivo é identificar quais os principais riscos de privacidade associados ao processamento de dados, com base em dois fatores: **probabilidade de ocorrência** (Likelihood) e **gravidade do impacto** (Severity), vamos começar por explicar esses fatores.

3.1 Likelihood

A **Likelihood** representa a **probabilidade estimada de que uma ação de ameaça ocorra** e gere um impacto negativo para um indivíduo representativo ou típico cujas PII são processadas pelo sistema. De acordo com a NISTIR 8062, esta probabilidade é fruto de quatro fatores:

- A probabilidade de que uma ação de ameaça seja tentada, intencionalmente ou não intencionalmente.
- A capacidade do agente de ameaça de executar o evento de ameaça.
- As vulnerabilidades do sistema, que correspondem a falhas que tornam possível o sucesso da ameaça.
- A redução da probabilidade devido à eficácia dos controles de segurança e privacidade existentes ou planeados.

A avaliação é qualitativa, baseada numa escala de cinco níveis:

- **Muito baixo:** A ocorrência é altamente improvável. Só aconteceria em circunstâncias muito raras ou com múltiplas falhas simultâneas.
- **Baixo:** Pouco provável de ocorrer. Pode requerer condições específicas ou falhas pontuais no sistema.
- **Moderado:** Pode ocorrer ocasionalmente. A ameaça é real, mas depende de certas condições ou vulnerabilidades serem exploradas.
- **Alta:** Provável de ocorrer. Há vulnerabilidades conhecidas ou ausência de controlos, tornando o sistema exposto.
- **Muito Alta:** Altamente provável. O evento pode acontecer em condições normais, especialmente se não houver medidas de segurança implementadas.

Riscos com probabilidade **alta ou muito alta** devem ser tratados com prioridade, aplicando medidas preventivas, corretivas ou de contenção conforme necessário e reduzindo-se a exposição.

3.2 Severity

A **Severity** representa o **potencial de dano que a materialização de uma ameaça pode causar** à organização e aos titulares dos dados. Essa avaliação é baseada em dois fatores principais:

- **Potencial prejudicial**, que corresponde ao grau de dano que pode ser causado, por exemplo, prejuízo financeiro, psicológico ou reputacional;
- **Nível de identificação**, isto é, a facilidade com que uma pessoa pode ser reidentificada com os dados disponíveis.

A avaliação é baseada numa escala qualitativa de cinco níveis:

- **Muito baixo:** Impacto quase impercetível para os titulares ou a organização.
- **Baixo:** Pequeno desconforto ou prejuízo leve e temporário.
- **Moderado:** Prejuízo recuperável, como danos menores à reputação ou perda limitada de dados.
- **Alta:** Dano significativo, como exposição de dados sensíveis ou infrações legais.
- **Muito Alta:** Prejuízo severo e irreversível, com alto impacto legal, financeiro ou psicológico.

4 Medidas de mitigação de risco

1. **Controlos de Acesso**
   Objetivo: Limitar o acesso aos dados pessoais apenas a quem realmente necessita.
   - Implementar controlo de acesso baseado em funções (RBAC), garantindo que cada utilizador apenas acede aos dados estritamente necessários para o seu trabalho.
   - Criar perfis de acesso diferenciados (administrador, técnico, utilizador comum).
   - Incluir revisões periódicas de permissões, evitando acessos excessivos ou desnecessários com o tempo.
   - Automatizar a revogação de acessos quando um utilizador muda de função ou abandona o projeto.
2. **Autenticação e Segurança de Rede**
   Objetivo: Impedir acessos não autorizados e proteger a infraestrutura.
   - Exigir autenticação multifator (MFA) para todos os utilizadores com acesso ao backend ou servidor.
   - Proteger os sistemas com firewalls, segmentação de rede, e utilizar proxies reversos para isolar o servidor da Internet pública.
   - Limitar o acesso remoto via VPN com autenticação segura.
   - Utilizar listas brancas de IP para restringir o acesso ao servidor apenas a localizações autorizadas.
3. **Encriptação e Pseudonimização**
   Objetivo: Garantir a confidencialidade dos dados, mesmo em caso de violação.
   - Encriptar dados em repouso com algoritmos fortes (ex: AES-256).

- Encriptar dados em trânsito usando HTTPS/TLS, com certificados válidos e atualizados.
- Aplicar pseudonimização aos dados identificáveis, como emails, para reduzir o risco de reidentificação.
- Gerir chaves de encriptação com uma plataforma segura de gestão de chaves (ex: AWS KMS, Azure Key Vault).
- Usar encriptação de base de dados a nível de coluna para proteger apenas campos sensíveis, aumentando o desempenho.

4. **Hashing e Tokenização de Dados**
   Objetivo: Proteger identificadores únicos e dados que não devem ser reversíveis.
   - Utilizar algoritmos de hashing seguro (ex: SHA-256) ou tokenização para dados como nomes de aplicações.
   - Adicionar um salt único por registo para impedir ataques por dicionário ou rainbow tables.
   - Avaliar se determinados dados podem ser irreversivelmente hashed para eliminar a necessidade de reversibilidade.
5. **Backup e Recuperação de Desastres**
   Objetivo: Garantir disponibilidade e integridade dos dados.
   - Estabelecer políticas de backup regulares e automatizadas.
   - Armazenar backups em locais físicos ou lógicos separados do sistema principal.
   - Testar periodicamente os procedimentos de recuperação, garantindo que os dados podem ser restaurados rapidamente.
   - Implementar backups incrementais diários e completos semanais, com retenção de versões.
6. **Segurança das Comunicações**
   Objetivo: Proteger os dados durante a transmissão.
   - Utilizar HTTPS com TLS (Transport Layer Security) em todas as comunicações entre cliente (app) e servidor.
   - Ativar HSTS (HTTP Strict Transport Security) para evitar downgrades para HTTP.
   - Implementar VPN para acesso remoto seguro a dados internos.
   - Usar *certificate pinning* na aplicação móvel para assegurar que a aplicação comunique apenas com o servidor identificado por um certificado específico.
   - Revalidar certificados regularmente e configurar alertas de expiração.
7. **Monitorização, Registo de Acessos e Atividades**
   Objetivo: Garantir a rastreabilidade e resposta rápida a incidentes.
   - Registar todas as operações sensíveis (leitura, modificação, criação e eliminação de dados), anotando o utilizador, data-hora e propósito da operação.

- Guardar os logs com segurança (num repositório isolado) e protegê-los contra alterações, sendo acessíveis apenas a administradores autorizados.
- Usar ferramentas de SIEM (Security Information and Event Management) para monitorização e alertas automáticos.
- Definir prazos de retenção de logs com base em requisitos legais e de auditoria, eliminando registos antigos de forma segura quando expirados.
- Analisar periodicamente os logs com ferramentas de deteção de padrões anómalos ou acessos fora de horas.

É importante compreender de que forma as principais medidas de segurança reduzem tanto a Likelihood quanto a Severity dos incidentes de privacidade no COP-MODE.

- **Controlos de Acesso**
  Likelihood: cai drasticamente, dado que apenas utilizadores com permissões adequadas podem chegar aos dados.

  Severity: diminui, já que qualquer tentativa de acesso não autorizado será bloqueada ou limitada a dados de baixo impacto.

- **Autenticação e Segurança de Rede**
  Likelihood: diminui substancialmente, porque o MFA e a segmentação de rede impedem que atacantes consigam contornar a barreira de acesso.

  Severity: reduz ligeiramente, já que mesmo em caso de ataque externo, este fica muito mais contido e detectável antes que cause danos massivos.

- **Encriptação e Pseudonimização**
  Likelihood: torna-se quase irrelevante, uma vez que os atacantes não dispõem das chaves.

  Severity: reduz-se fortemente, pois mesmo dados que seja acedidos de forma ilegal permanecem indecifráveis.

- **Hashing**
  Likelihood: a chance de acesso não é afetada diretamente, contudo reforça a proteção dos identificadores.

  Severity: baixa, porque qualquer modificação ou tentativa de reversão é detetada com facilidade.

- **Backup e Recuperação**
  Likelihood: não impede diretamente alterações indevidas, mas garante que não haja perda permanente de dados.

  Severity: torna-se insignificante, pois podemos restaurar o estado original rapidamente.

- **Segurança das Comunicações (HTTPS/TLS e VPN)**
  Likelihood: reduz-se consideravelmente, prevenindo intercepções e acessos não autorizados em trânsito.

  Severity: mesmo em caso de captura, os dados mantêm-se cifrados e protegidos.

- **Monitorização, Registo de Acessos e Atividades**
  Likelihood: reduz-se significativamente, uma vez que qualquer ação suspeita é imediatamente registada e gera alertas que desencadeiam investigação ou bloqueio.

  Severity: atenua-se, visto que a deteção precoce permite corrigir ou isolar o incidente antes que se propaguem.

Com estas salvaguardas em vigor, espera-se que os riscos caiam de níveis "muito elevados" para "moderados" ou mesmo "baixos". A seguir, apresentamos a tabela de riscos versus mitigações.

Table 1: Riscos e respetivas mitigações

Risco	**Mitigações**
Fuga de dados por interceção das comunicações entre os smartphones e o servidor do projeto	**Segurança das Comunicações:** 1. **HTTPS:** Assegurar que toda a comunicação entre as aplicações nos smartphones e os servidores se faz exclusivamente por HTTPS, utilizando versões atuais do TLS para proteger os dados enquanto circulam na rede. 2. **VPN:** Configurar uma ligação em túnel VPN para todas as trocas de informação, oferecendo uma camada extra de encriptação e evitando a exposição direta dos dados à Internet pública. 3. **Certificate Pinning:** Incorporar na app móvel um mecanismo de certificate pinning SSL/TLS, de modo a que apenas o certificado pré-aprovado do servidor seja aceite, bloqueando tentativas de falsificação ou interceptação.

Risco	Mitigações
Fuga de dados devido a acesso não autorizado ao servidor/dados	**Controles de Acesso:** Estabelecer perfis com permissões específicas, garantindo que apenas utilizadores devidamente autorizados possam consultar ou manipular determinados conjuntos de dados. **Autenticação e Segurança de Rede:** 1. **Autenticação Multifator (MFA):** Exigir a combinação de pelo menos dois fatores (por exemplo, senha e código temporário) para qualquer acesso ao servidor, fortalecendo a verificação de identidade. 2. **Proteção da Infraestrutura:** Colocar o servidor atrás de firewalls robustas, evitando a exposição direta à Internet. Implementar Zonas Desmilitarizadas (DMZ) e proxies reversos para segregar e filtrar o tráfego de entrada, reduzindo a superfície de ataque e dificultando acessos não autorizados.

Risco	Mitigações
Ligação de dados em repouso	**Encriptação e Pseudonimização:** 1. **Encriptação de Dados em Repouso:** Utilizar algoritmos de encriptação avançados para proteger dados sensíveis armazenados. Assim, mesmo que o meio de armazenamento seja indevidamente acedido, a informação permanece indecifrável. 2. **Pseudonimização de Identificadores:** Transformar dados pessoais identificáveis (como endereços de email) em pseudónimos não reversíveis sem uma chave de correspondência. Manter o mapeamento seguro num sistema de gestão de chaves, garantindo que apenas processos autorizados possam recuperar o identificador original. **Monitorização e Registo de Atividades (Logging):** 1. **Logging:** Capturar e registar todas as operações críticas (leitura, escrita, modificação ou eliminação de dados) incluindo o utilizador responsável, timestamp e tipo de ação. 2. **Monitorização:** Implementar ferramentas de auditoria e alertas em tempo real para detetar acessos ou ações suspeitas, permitindo uma resposta imediata a incidentes de segurança.

Risco	Mitigações
Fuga de informações sensíveis, em particular os nomes das aplicações que são recolhidas	**Hashing e Tokenização:** 1. **Substituição de Identificadores:** Em vez de armazenar diretamente nomes de aplicações, aplicar uma função de hash segura ou tokenização que gera identificadores únicos irreversíveis sem acesso à chave. 2. **Acesso Restrito às Chaves:** Limitar estritamente o acesso às chaves de detokenização a componentes ou serviços internos autorizados para cumprir apenas as necessidades de processamento legítimo. 3. **Gestão Segura de Chaves:** Utilizar uma solução dedicada de gestão de chaves criptográficas para armazenar e proteger as chaves usadas no hashing ou tokenização, assegurando rotação periódica e controlo de acessos.

5 Impacto das mitigações dos riscos na Likelihood e Severity

1. **Fuga de dados por interceção das comunicações entre os smartphones e o servidor do projeto**

   - **Likelihood: Baixa**
     Qualquer tentativa de interceção por terceiros é dificultada por protocolos como HTTPS/TLS, VPN e certificate pinning, que asseguram canais de comunicação autenticados e encriptados.
   - **Severity: Alta**
     Uma interceção bem-sucedida poderia expor dados sensíveis, mesmo com baixa probabilidade, comprometendo a integridade do sistema e a privacidade dos utilizadores.

2. **Fuga de dados devido a acesso não autorizado ao servidor/dados**

    - **Likelihood: Moderada**
      A implementação de controlos de acesso baseados em funções (RBAC), autenticação multifator, segmentação da rede e proxies reversos reduz de forma eficaz a possibilidade de acesso indevido.
    - **Severity: Alta**
      Caso ocorra uma violação, a exposição de grandes volumes de dados pessoais pode ter um impacto elevado, tanto em termos de privacidade como de reputação e conformidade legal.

3. **Ligação de dados em repouso**

    - **Likelihood: Moderada**
      A encriptação e pseudonimização de dados armazenados, aliadas ao registo de acessos e monitorização contínua, reduzem substancialmente a possibilidade de exploração dos dados por atacantes.
    - **Severity: Alta**
      Mesmo com proteção ativa, uma eventual exposição de dados em claro ou reidentificáveis pode gerar sérias consequências para o projeto e para os titulares.

4. **Fuga de informações sensíveis, em particular os nomes das aplicações recolhidas**

    - **Likelihood: Baixa**
      A anonimização e encriptação dos nomes das aplicações, associadas a mecanismos de rastreabilidade e controlo de acessos, tornam a fuga desse tipo de dado altamente improvável.
    - **Severity: Moderada**
      Caso ocorra, o impacto seria moderado, já que os dados estão anonimizados e podem ser rapidamente rastreados e a ameaça neutralizada com base nos logs de acesso.

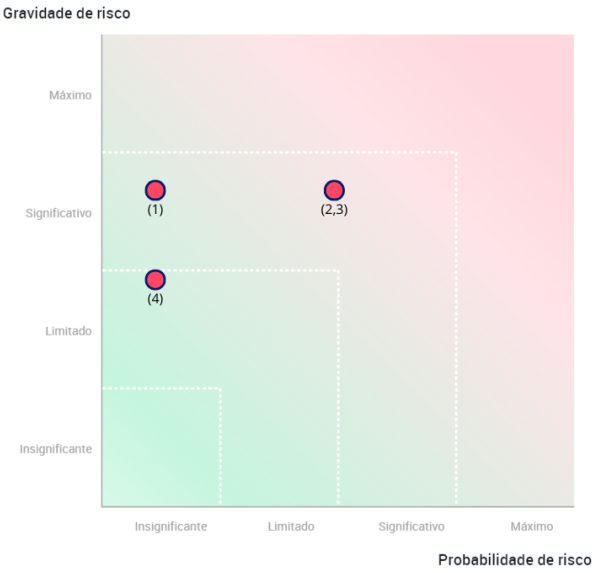

Fig. 1. Matriz de Risco

6 Riscos PIA sem medidas de mitigação

Os riscos associados à segurança dos dados, no âmbito do projeto COP-MODE, tornam-se altamente prováveis e com impacto significativo, na ausência de medidas de mitigação. A seguir, apresentam-se as avaliações detalhadas para cada risco identificado:

1. **Acesso Ilegítimo de Dados**

    - **Likelihood: Muito alta**
      Sem mecanismos de autenticação forte, controlo de acessos e encriptação de dados, os sistemas tornam-se extremamente vulneráveis a acessos indevidos, tanto internos como externos. A inexistência de restrições aumenta substancialmente a exposição dos dados a atores mal-intencionados.
    - **Severity: Muito alta**
      A obtenção não autorizada de dados pessoais sensíveis compromete a privacidade dos participantes, podendo resultar em violações legais, sanções regulatórias e perda de credibilidade científica. O impacto reputacional e a quebra de confiança por parte dos utilizadores e parceiros seriam críticos.

2. **Modificação Indesejada dos Dados**

- **Likelihood: Muito alta**
  Sem mecanismos de verificação de integridade (como registos de auditoria, controlo de versões ou assinaturas digitais), torna-se extremamente provável que os dados sejam alterados (intencionalmente ou por erro humano) sem possibilidade de rastreio ou reversão.
- **Severity: Muito alta**
  Dados corrompidos ou adulterados comprometem a validade dos resultados da pesquisa, o que leva a conclusões equivocadas e reduz o valor científico e acadêmico do estudo. A posterior correção de inconsistências implica: custos adicionais e consumo de tempo precioso.

3. **Desaparecimento dos Dados**

- **Likelihood: Muito alta**
  Sem políticas de backup regulares e redundância de dados, qualquer falha de hardware, erro humano ou evento catastrófico pode culminar na eliminação total dos dados. Confiar num único local de armazenamento, sem planos de contingência, amplia esse risco.
- **Severity: Alta**
  A perda de dados pode, no pior dos casos, significar a necessidade de reiniciar toda a recolha de informações, atrasando ou até mesmo impossibilitando o projeto. Em situações extremas, falhas em recuperar os dados podem levar a consequências legais severas, particularmente se houver incumprimento de compromissos contratuais.

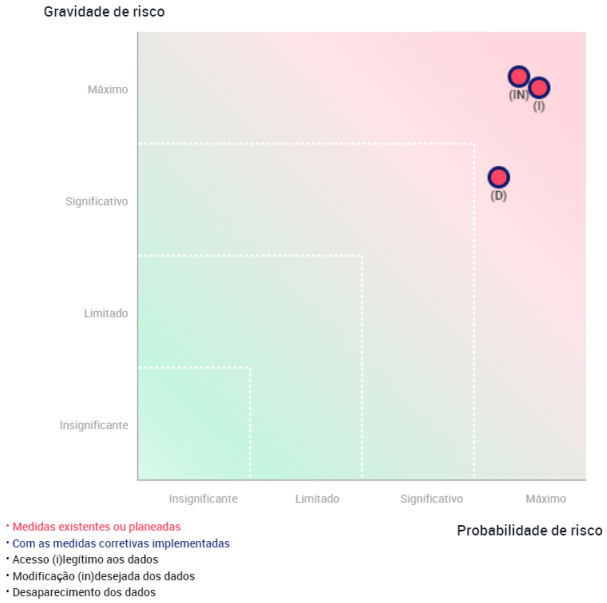

Fig. 2. Matriz de Risco PIA sem Medidas

7 Riscos PIA com medidas de mitigação

- **Controlo de Acesso**

    1. **Redução da Likelihood:**
    Ao restringir o acesso apenas a perfis validados, ataques por credenciais roubadas ou tentativas não autorizadas tornam-se muito menos prováveis.
    2. **Redução da Severity:**
    Mesmo que alguém tente invadir, as barreiras de autenticação e autorização impedem o acesso a dados sensíveis, limitando o dano potencial

- **Encriptação**

    1. **Redução da Likelihood:**
    Reduz significativamente, já que os dados ficam inacessíveis sem as chaves de criptografia adequadas.
    2. **Redução da Severity:**
    Caso os dados encriptados sejam capturados, permanecem incompreensíveis, tornando inócuas tentativas de exploração das

informações.

- **Hashing**

    1. **Redução da Likelihood:**
    Não impede o acesso, mas faz com que qualquer adulteração produza um resumo diferente, denunciando alterações não autorizadas.
    2. **Redução da Severity:**
    Ao detetar imediatamente discrepâncias entre hash original e hash atual, evita-se o uso de dados corrompidos ou manipulados.

- **HTTPS**

    1. **Redução da Likelihood:**
    Reduz a probabilidade de intercepção de dados durante a transmissão
    2. **Redução da Severity:**
    Mesmo que os dados sejam capturados, continuam encriptados, sem possibilidade de leitura.

- **VPN**

    1. **Redução da Likelihood:**
    Reduz a probabilidade ao estabelecer um canal seguro de comunicação para dados transmitidos entre redes diferentes.
    2. **Redução da Severity:**
    Protege os dados contra acessos em redes inseguras.

- **Backup e Recuperação**

    1. **Redução da Likelihood:**
    Embora não impeça modificações indevidas ou desaparecimento dos dados, garante que uma cópia íntegra esteja disponível para restauração após falhas ou ataques.
    2. **Redução da Severity:**
    A existência de backups atualizados e confiáveis reduz muito o impacto causado por alterações indesejadas, pois permite que o projeto restabeleça rapidamente sua base de dados.

- **Monitorização e Registo de Atividades**

    1. **Redução da Likelihood:**
    Saber que cada ação fica registada desencoraja mudanças não

autorizadas e facilita a deteção precoce de comportamentos anómalos.

2. **Redução da Severity:**
   Com alertas em tempo real, incidentes são identificados e contidos rapidamente, limitando significativamente o alcance dos danos.

Após a implementação destas medidas a Likelihood passa a níveis moderados ou baixos. O controlo de acesso dos dados, a monitorização contínua e o registo de atividades contribuem para a redução da Likelihood, uma vez que as barreiras e alertas antecipados tornam muito improvável que ações maliciosas passem despercebidas. O mesmo se aplica na Severity que passa para níveis moderados ou baixos. Mesmo que ocorra alguma modificação não autorizada, a combinação de registos detalhados, deteção em tempo real e estratégias de backup testadas asseguram que o impacto é reduzido, pois é possível reverter rapidamente para um estado íntegro dos dados.

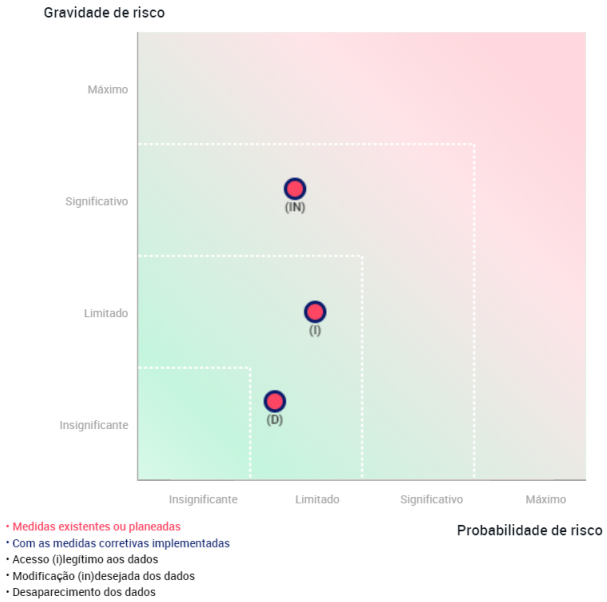

Fig. 3. Matriz de Risco PIA com Medidas

8 Conclusão

A presente Avaliação de Impacto sobre a Privacidade (PIA) permitiu identificar e avaliar os principais riscos associados ao tratamento de dados pessoais no

âmbito do projeto COP-MODE, cuja natureza envolve a recolha e processamento de informações sensíveis provenientes de dispositivos móveis.

A análise demonstrou que, na ausência de medidas de segurança, os riscos de acesso não autorizado, alteração, perda ou intercepção de dados são elevados, podendo comprometer seriamente os direitos dos titulares dos dados, a conformidade legal do projeto e a sua integridade científica.

No entanto, a implementação articulada de um conjunto robusto de medidas técnicas e organizativas – incluindo controlo de acessos baseado em funções, autenticação multifator, encriptação de dados em trânsito e em repouso, pseudonimização, hashing, backup, monitorização contínua e registo de atividades permite mitigar eficazmente esses riscos. Tais salvaguardas reduzem substancialmente tanto a **probabilidade (Likelihood)** quanto a **gravidade (Severity)** dos incidentes de privacidade.

Com as medidas descritas, o projeto apresenta um nível de risco residual **baixo a moderado**, considerado aceitável face à natureza e finalidade do tratamento de dados. O COP-MODE está, assim, em condições de avançar com garantias sólidas de segurança e respeito pelos princípios da proteção de dados, assegurando a confiança dos participantes, parceiros e entidades reguladoras.

References

[1] CNIL: Cnil - privacy impact assessment (pia) - youtube. https://www.youtube.com/watch?v=5J3h9zIFVDo (2017)
[2] CNIL: Open source pia software helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (nd)
[3] CNIL: Privacy impact assessment (pia). https://www.cnil.fr/en/privacy-impact-assessment-pia (nd)
[4] COP-MODE Project: Cop-mode: Collaborative open platform for modeling and design of ethical ai. https://cop-mode.dei.uc.pt/ (nd)
[5] Segurança e Privacidade (Moodle Slides): Semana 07 - t7: Regulations and privacy impact assessment (2025)
[6] Stallings, W.: Information Privacy Engineering and Privacy by Design. Pearson Addison-Wesley (2020)