Privacy Impact Assessment

Trabalho de Segurança e Privacidade
realizado pelos alunos:

Maximiliano Vítor Phillips e Sá (up202305979),
Rita Maria Pinho Moreira (up202303885)
e Samuel José Sousa Ventura da Silva (up202305647)

0. Índice

1. Introdução

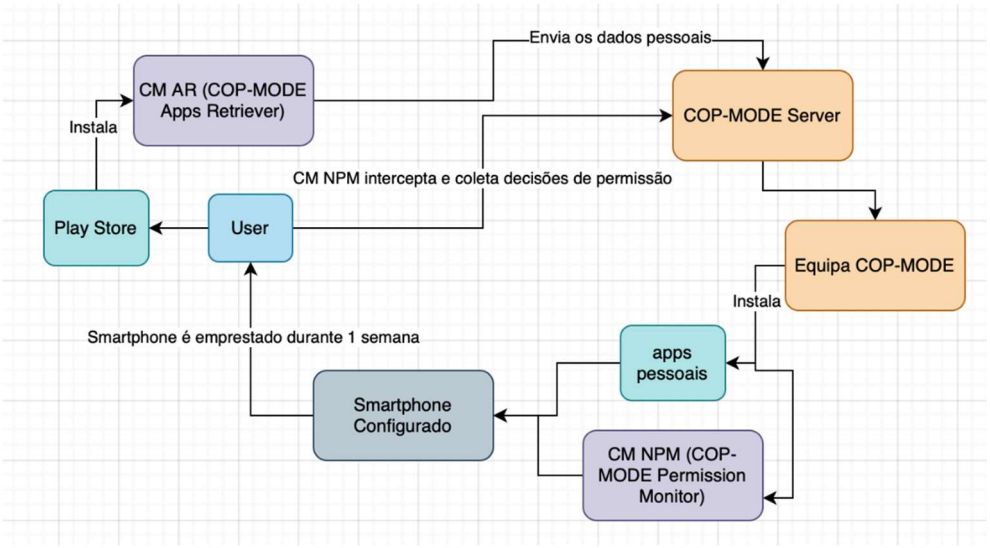
O presente relatório tem como objetivo realizar uma Avaliação de Impacto sobre a Proteção de Dados (PIA) no âmbito do projeto COP-MODE. A PIA é conduzida de acordo com os princípios do Regulamento geral de Proteção de Dados (RGPD)[1], visando identificar riscos, aplicar medidas de mitigação adequadas e garantir o respeito pelos direitos dos titulares dos dados.

2. Descrição do Sistema

Nesta secção, apresenta-se o ambiente técnico e organizacional do COP-MODE, detalhando os seus objetivos, dados capturados e entidades responsáveis, tal como o seu fluxo de dados desde a recolha até à eliminação. Para a avaliação inicial de riscos, assumimos um *plain setup* – ou seja, um ambiente sem qualquer medida de proteção (dados em texto claro, sem TLS, sem autenticação forte e sem cifragem em repouso).

2.1. Visão Geral do Projeto COP-MODE

O projeto COP-MODE visa realizar campanhas de recolha de dados em smartphones, no contexto de investigação científica, par analisar o comportamento dos utilizadores e desenvolver soluções *context-aware*. Durante uma semana, os participantes utilizam dispositivos com uma aplicação instalada, que regista continuamente diversos tipos de dados. Estes dados são posteriormente analisados para identificar padrões e otimizar o uso de recursos como a bateria, o processador e a conectividade dos dispositivos.



[1] O Regulamento Geral de Proteção de Dados (RGPD), é um diploma Europeu (EU 2016/679) que determina as regras relativas à proteção, ao tratamento e à livre circulação dos dados pessoais das pessoas nos países da União Europeia.

2.2. Dados coletados

Os dados recolhidos durante a campanha incluem tanto **dados pessoais identificáveis (PII)**[2], especificamente o endereço de e-mail e identificador de sessão (*SessionID*), como **dados técnicos de sensores**, tais como *timestamp*, nome das aplicações em uso, coordenadas GPS, estado da bateria, uso de CPU e tipo de rede.

2.3. Papéis envolvidos

- **Titulares dos Dados (*Data Subjects/PII Principals*)**: Utilizadores que participam voluntariamente na campanha.
- **Controlador (PII *controller*):** A instituição responsável pelo projeto, que define as finalidades e os meios de tratamento dos dados.
- **Processador (PII *processor*)**: Equipa técnica responsável por operar os servidores e realizar o processamento dos dados, seguindo as instruções do controlador.
- **Terceiros (*Third Parties*)**: Potenciais parceiros de investigação que poderão aceder apenas a dados agregados ou pseudonimizados.

2.4. Arquitetura e Processos

O sistema segue uma arquitetura composta pelas seguintes fases:

1. **Coleta**: A app COP-MODE recolhe dados localmente no smartphone durante uma semana.
2. **Transmissão**: Os dados são enviados periodicamente, de forma segura (TLS 1.3 [3]ou VPN[4]), para o servidor COP-MODE.
3. **Armazenamento e Processamento**: Os dados são armazenados em bases de dados cifradas ("at rest") e processados pela equipa técnica para gerar modelos de comportamento e estatísticas agregadas.
4. **Acesso e Divulgação**: Investigadores internos têm acesso a dados pseudonimizados com controlo de permissões (RBAC[5]), e terceiros apenas recebem dados anonimizados ou agregados.
5. **Eliminação**: Após o fim da campanha e a devolução do dispositivo, os dados PII são eliminados. Apenas os dados anonimizados podem ser retidos para fins científicos.

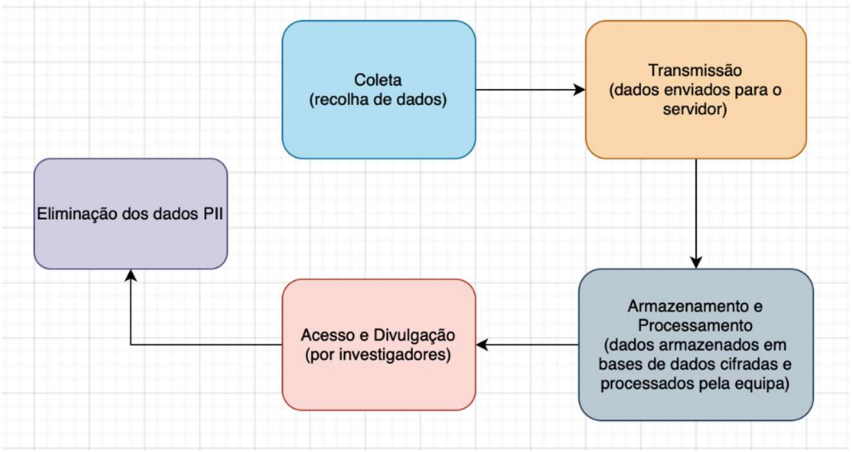
---

[2] Informações que permitem identificação pessoal (PII) são quaisquer dados que possam ser usados para identificar alguém.

[3] TLS significa *Transport Layer Security* e é o sucessor do SSL (*Secure Sockets Layer*). O TLS proporciona uma comunicação segura entre os navegadores web e os servidores.

[4] VPN significa "*Virtual Private Network*" (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas.

[5] O controle de acesso baseado em função (RBAC) é um método para controlar o que os usuários podem fazer nos sistemas de TI de uma empresa. O RBAC faz isso atribuindo uma ou mais "funções" a cada usuário e concedendo permissões diferentes a cada função.



3. Avaliação Inicial de Riscos

Neste capítulo serão avaliados os ricos à privacidade, de forma generalizada, associados ao projeto COP-MODE, antes da implementação de qualquer medida corretiva. Nesta avaliação, serão medidas a probabilidade (*Likelihood*) e a severidade/gravidade (*Severity*) dos três "riscos-base" associados a um *setup plain* (sem cifragem, sem autenticação forte, sem controlo de acesso, etc.). Esta avaliação ajuda na identificação de vulnerabilidades e no entendimento do impacto potencial para os titulares dos dados.

3.1. Definição de Probabilidade e Gravidade

Na avaliação de riscos são utilizadas duas dimensões padrão do instrumento CNIL PIA: A probabilidade (*Likelihood*) e a gravidade, ou severidade (*Severity*).
A probabilidade mede a chance de o evento de risco ocorrer, num período de curto a médio prazo. A gravidade avalia o impacto que a materialização desse risco terá sobre os titulares de dados e sobre a organização.
Abaixo está a escala numérica de 1 a 4 para ambas as dimensões.

Nível	Probabilidade (Likelihood)	Gravidade (Severity)
4	Máximo (várias ocorrências por ano)	Máximo (exposição massiva de dados)
3	Significativo (pode ocorrer no próximo ano)	Significativo (violação de dados sensíveis)
2	Limitado (pode ocorrer nos próximos 2-3 anos)	Limitado (exposição de dados a grupos limitados)
1	Insignificante (quase nunca ocorre)	Insignificante (dados irrelevantes ou já públicos)

3.2. Análise de Riscos Sem Medidas de Correção

3.2.1. Risco I – Acesso ilegítimo dos dados (Confidencialidade)

Este risco traduz-se na possibilidade de acesso, leitura ou extração não autorizada de dados pessoais armazenados ou transmitidos pelo sistema, comprometendo a confidencialidade da informação.

Os impactos nos titulares podem ser diversos. Entre eles destacam-se:

- A violação da privacidade individual;
- A exposição de hábitos de utilização, como apps usadas ou horários, e localização;
- A perda de confiança na entidade responsável pelo tratamento dos dados;
- A potencial perfilização[6] indevida, definida pelo processo automatizado de analisar dados pessoais para avaliar ou prever comportamentos, interesses e características de uma pessoa. Este último impacto é sensível no contexto do RGPD, que o reconhece como uma operação que pode afetar significativamente os titulares dos dados, podendo ser usada para criar perfis detalhados sem o consentimento ou o conhecimento adequado da pessoa.

Este risco pode materializar-se a partir de ameaças, tais como:

- Ciberataques, como o MITM (*Man-in-the-Middle*)[7], onde o atacante interceta comunicações entre o utilizador e o servidor;
- Utilizadores internos com permissões excessivas, como desenvolvedores ou técnicos com acesso desnecessário a dados;
- Vazamento (acidental) de credenciais;
- APIs sem autenticação ou encriptação adequadas.

Essas ameaças são facilitadas por fontes de risco, tais como:

- Infraestrutura mal configurada;
- Ausência de cifragem (encriptação) de dados durante a comunicação e em repouso, quando estão armazenados;
- Falta de mecanismos de autenticação forte.

Com base neste contexto, define-se probabilidade com o nível 4 (**Máximo**), dado o cenário sem medidas corretivas como TLS ou autenticação robusta, e gravidade com o nível 4 (**Máximo**), devido ao tipo de dados envolvidos (como identificadores únicos ou hábitos sensíveis) e ao potencial de reidentificação ou uso abusivo.

[6] Traçar o perfil de.

[7] forma de ataque em que os dados trocados entre duas partes (por exemplo, você e o seu banco) são de alguma forma intercetados, registados e, possivelmente, alterados pelo atacante sem que as vítimas se apercebam.

3.2.2. Risco IN - Modificação indesejada dos dados (Integridade)

Refere-se à alteração não autorizada, maliciosa ou acidental, dos dados armazenados, comprometendo a integridade da informação do sistema. Essa modificação pode ocorrer sem mecanismos adequados de controlo ou verificação, afetando diretamente a fiabilidade dos dados.

Os principais impactos potenciais para os titulares e para o projeto incluem:

- Análises incorretas, baseadas em dados manipulados ou alterados;
- Decisões enviesadas ou injustas, como interpretações erradas de padrões de uso;
- Resultados científicos inválidos, especialmente em contextos de investigação baseada nos dados recolhidos;
- Perda de confiança por parte dos participantes e da sociedade científica.

O risco pode ser concretizado por ameaças, como:

- Ataques internos ou externos com capacidade de manipular dados diretamente, como o acesso à base de dados ou APIs de escrita;
- *Bugs* no armazenamento ou nas interfaces de escrita de dados, que podem introduzir alterações não detetadas.

As ameaças acima são agravadas por fontes de risco, tendo como exemplo:

- Falta de controlo de versões nos dados armazenados;
- Falta de registo (*logging*) de alterações, dificultando a rastreabilidade de modificações;
- Ausência de validações dos dados no momento da inserção ou atualização.

Com base nesta análise, determina-se que a probabilidade deste risco é de nível 2 (**Limitado**), considerando a ausência de validação e de mecanismos de auditoria como o *logging*. Já a gravidade é de nível 3 (**Significativo**), pois as alterações impactam a qualidade da informação e pode prejudicar os titulares, mesmo sem exposição pública dos dados.

3.2.3. Risco D – Desaparecimento dos dados (Disponibilidade)

Por último, este risco diz respeito à perda definitiva ou temporária de dados pessoais, decorrente de falhas técnicas, humanas ou ações maliciosas, comprometendo a disponibilidade da informação do sistema. Este risco afeta a capacidade de acesso contínuo e fiável aos dados pelos titulares e pelos responsáveis pelo tratamento.

Os principais impactos identificados incluem:

- Impossibilidade de exercer direitos, como o direito à portabilidade dos dados;
- Perda de dados recolhidos, que podem ter um determinado valor;
- Atrasos em serviços, realização de análises ou cumprimento de obrigações legais.

O desaparecimento dos dados pode resultar de ameaças como:

- Ataques de *ransomware*[8];
- Falhas em servidores, como falhas de disco ou crashes não recuperáveis;
- Corrupção de base de dados, por bugs ou falhas lógicas;
- Erro humano, como exclusão acidental sem possibilidade de recuperação.

Estas ameaças estão associadas a fontes de risco, como por exemplo:

- Ausência de *backups* regulares, automáticos e testados;
- Infraestrutura sem redundância, como discos ou servidores únicos sem *failover*[9];
- Falta de plano de recuperação de desastres, dificultando a resposta a falhas graves.

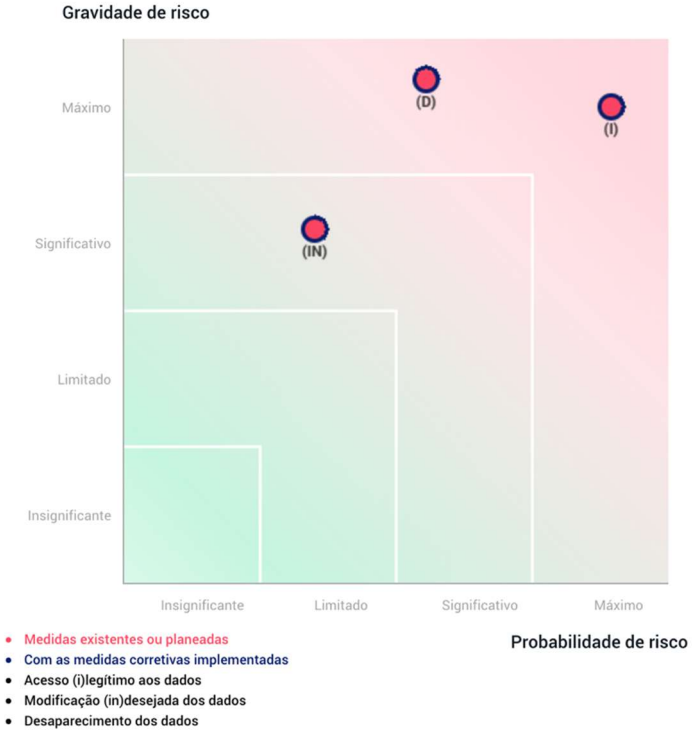
Com esta análise, conclui-se que a probabilidade é de nível 3 (**Significativo**), devido à inexistência de políticas eficazes de backups e tolerância a falhas, e a gravidade é de nível 4 (**Máximo**), pois a perda de dados pode ser irreversível, afetando a continuidade das operações e os direitos dos titulares.

3.3. Matriz de Riscos

Para resumir visualmente a avaliação dos três riscos-base (I, IN e D) no cenário de configuração básica (sem medidas corretivas), é apresentado abaixo a matriz de riscos[10], que cruza as dimensões Probabilidade (eixo horizontal) e Gravidade (eixo vertical).
Uma matriz de riscos tem quatro zonas: **Verde (Baixo), Amarelo (Moderado), Laranja (Alto) e Vermelho (Crítico)**. Desta forma, a matriz fornece um mapa imediato de onde cada risco se encontra no espectro de probabilidade vs. Gravidade.

O **risco I** está no quadrante mais elevado, o **vermelho (Crítico)**, com Probabilidade 4 e Gravidade 4.
O **risco IN** situa-se entre o quadrante **laranja (Alto)** e **amarelo (Moderado)**, com Probabilidade 2 e Gravidade 3.
Por último, o **risco D** encontra-se entre o **laranja (Alto)** e o **vermelho (Crítico)**, com Probabilidade 3 e Gravidade 4.

[8] Malware utilizado para bloquear o acesso (encriptação), destruir ou publicar os dados críticos de uma pessoa, e que exige pagamento para os restaurar
[9] Failover em computação significa tolerância a falhas. Quando um sistema, servidor ou outro componente de hardware ou software fica indisponível, um componente secundário assume operações sem que haja interrupção nos serviços.
[10] A Matriz de Riscos ou Matriz de Probabilidade e Impacto é uma ferramenta de gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção.



4. Medidas Corretivas

Neste capítulo apresentam-se as medidas corretivas destinadas a reduzir os riscos à privacidade identificados descritos anteriormente. Será delineado, em primeiro lugar, um plano de ação detalhado para mitigar cada risco identificado, seguido de uma tabela que associa, de forma clara, os riscos com as respetivas contramedidas. Por fim, serão descritas as técnicas de segurança aplicadas no sistema (desde mecanismos de criptografia e controlo de acesso a processos de recuperação e auditoria), evidenciando como cada uma contribui para diminuir tanto a probabilidade como a gravidade dos riscos analisados.

4.1. Plano de Ação para Mitigação de Riscos

4.1.1. Proteção da Confidencialidade (Risco I)

- Ativar TLS 1.3 em todas as comunicações entre os smartphones e o servidor, para garantir que os dados não podem ser intercetados ou lidos por terceiros;
- Implementar VPN nos canais internos, de modo a assegurar que apenas dispositivos e serviços autenticados mutuamente conseguem trocar informação entre si;
- Usar autenticação multi-fator (MFA) para todos os acessos administrativos ao sistema, reduzindo o risco de credenciais comprometidas permitirem acesso indevido ao sistema;

- Aplicar criptografia AES-256 com as chaves armazenadas em HSM (*Hardware Security Module*)[11] para proteger os dados armazenados no servidor contra acesso não autorizado.

4.1.2. Garantia da Integridade (Risco IN)

- Assinar cada registo de dados com HMAC-SHA-256[12], de forma a permitir a deteção imediata de qualquer modificação não autorizada no conteúdo dos ficheiros;
- Manter *logs* de auditoria *append-only*, onde cada entrada fica imutável e identificada com *timestamp* e utilizador, assegurando que alterações no sistema ficam sempre registadas de forma rastreável;
- Introduzir validações automáticas na API de escrita (como *geofencing* [13]e verificação de plausibilidade de valores) para impedir a inserção de dados que não façam sentido ou se encontrem fora dos intervalos aceitáveis;
- Definir papéis e permissões via RBAC no servidor de aplicações.

4.1.3. Asseguramento da Disponibilidade (Risco D)

- Configurar *backups* automáticos diários, com testes de restauração trimestrais, para garantir que, em caso de falha ou ataque, os dados podem ser recuperados rapidamente sem perda significativa;
- Criar redundância geográfica (um *cluster* secundário noutro *data center*/região), assegurando continuidade de serviço mesmo diante de falhas críticas num determinado local;
- Elaborar e ensaiar um Plano de Recuperação de Desastres (DRP) com SLAs (*Service Level Agreements*), definidos para tempo de restabelecimento, garantindo que a equipa conhece os procedimentos e prazos a cumprir em situações de crise.

4.1.4. Processos de Gestão de Disputas (Todos os Riscos)

Estes mecanismos mitigam riscos jurídicos e regulatórios, além de fortalecer a confiança dos titulares nos processos de proteção de dados.

- Automatizar o modo *'freeze'* quando um titular contesta os seus dados, para impedir o uso desses registos até à resolução da disputa;

---

[11] Os módulos de segurança de hardware (HSM) são dispositivos de hardware reforçados e resistentes a adulteração que protegem processos criptográficos gerando, protegendo e gerenciando chaves usadas para criptografar e descriptografar dados e criar assinaturas e certificados digitais.

[12] o código de autenticação de mensagem com chave hash é um tipo específico de código de autenticação de mensagem (MAC) que usa uma função hash criptográfica e uma chave criptográfica secreta; que pode ser usado para verificar simultaneamente a integridade dos dados e a autenticidade de uma mensagem.

[13] *Geofencing* permite criar uma "cerca virtual" em torno de uma localização específica.

- Definir SLA (*Service Level Agreement*) de 48 horas para o processo de verificação e resposta a pedidos de retificação ou eliminação, assegurando que os direitos dos titulares são efetivamente respeitados num prazo definido.

4.2. Tabela de Riscos e Mitigações

Antes de apresentar a tabela, resumimos que aqui são associados os riscos identificados na análise sem medidas corretivas (subcapítulo 3.2), tal como os outros riscos identificados no enunciado do projeto (COP-MODE), com as contramedidas propostas para cada um. O objetivo é fornecer uma visão clara e concisa de como cada ameaça será mitigada através de técnicas específicas, reduzindo tanto a probabilidade como a severidade dos incidentes de segurança.

Risco	Medidas de Mitigação
Acesso ilegítimo (I)	- Ativar TLS 1.3 em todas as comunicações entre smartphones e servidor para manter uma ligação segura; - Implementar VPN para autenticação mútua de dispositivos; - MFA e RBAC para controlo de acesso; - Criptografia *at-rest* (AES-256) para proteger dados armazenados; - *Firewalls* para filtrar tráfego malicioso.
Modificação indesejada (IN)	- Assinar cada registo com HMAC-SHA-256 para detetar alterações não autorizadas; - *Logs append-only*[14] para rastreabilidade imutável. - Validações na API de escrita (verificação de plausibilidade, geofencing) para evitar inserção de dados inválidos; - Controlo de versões para reverter modificações indevidas.
Desaparecimento de dados (D)	- Backups automáticos diários com testes de restauração periódicos para garantir recuperação rápida; - Redundância geográfica com cluster secundário noutro *data center* para disponibilidade contínua;

[14] Um *log append-only* é um arquivo de log onde apenas novos registos podem ser adicionados no final, nunca alterados ou excluídos.

	- Plano de Recuperação de Desastres[15] (DRP) com procedimentos e SLAs (*Service Level Agreement*)[16] definidos para resposta a falhas graves.
Data leak via eavesdropping	- TLS 1.3 em todos os fluxos de dados e VPN '*site-to-site'* para impedir interceção não autorizada; - Inspeção de tráfego encriptado para identificar padrões suspeitos de intercetação.
***Data leak* via acesso não autorizado ao servidor**	- Firewalls para bloquear acessos indevidos. - *Network segmentation*[17] para isolar componentes críticos; - MFA e RBAC para autenticação forte; - Sessões com *timeout* para minimizar sessões inativas; - Monitorização contínua de *logs* e alertas.
Ligação de dados "*at rest*" a indivíduo	- Pseudonimização de campos PII via *hashing* para impedir reidentificação direta; - Cifragem *at-rest* (AES-256) para proteger dados em repouso; - Gestão de chaves em HSM (*Hardware Security Module*) (UE) para controlo centralizado e seguro das chaves de encriptação.
Divulgação de nomes de aplicações (sensíveis)	- *Hashing* dos nomes de apps no cliente antes do envio para preservar anonimato; - Mapeamento local para análise de padrões sem expor diretamente os nomes; - Remoção de meta-dados identificadores que possam revelar aplicações sensíveis.

4.3. Técnicas de Segurança Aplicadas

Para implementar o plano de ação acima e mitigar os riscos de forma eficaz, recorre-se às seguintes técnicas de segurança:

- Criptografia em trânsito e em repouso: TLS 1.3, VPN, AES-256 com chaves em HSM;
- Autenticação e controlo de acesso: MFA, RBAC e segregação de princípios de menor privilégio;
- Assinaturas e *logging* imutável: HMAC-SHA-256 em cada ficheiro/registo e *logs 'append-only'*;

[15] A recuperação de desastres (DR) é a capacidade de uma organização de restaurar o acesso e a funcionalidade da infraestrutura de TI após um evento de desastre, seja natural ou causado por ação humana (ou erro).

[16] SLA é um acordo de nível de serviço, um contrato entre um prestador de serviços e um cliente, que define detalhes do serviço a ser fornecido.

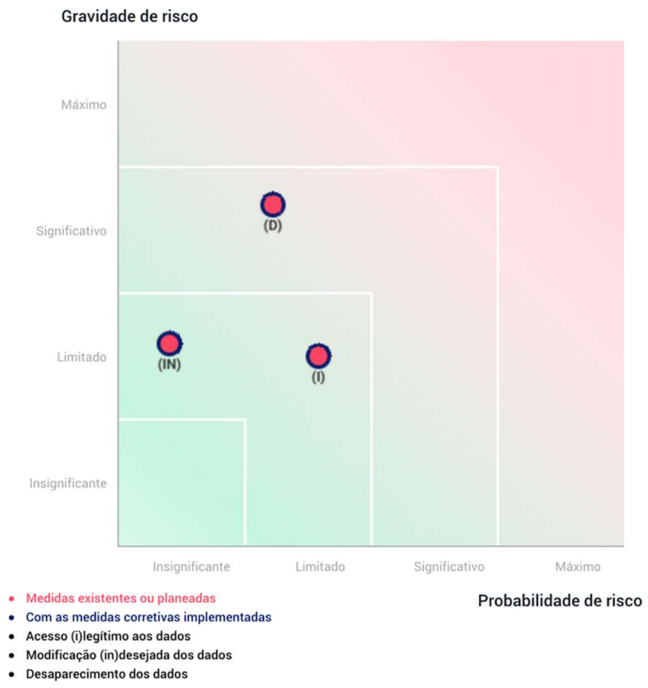
[17] Abordagem de arquitetura que divide uma rede em vários segmentos ou sub-redes, cada um atuando como sua própria pequena rede.

- Validações de entrada: Expressões regulares, plausibilidade de GPS e *geofencing* na API;
- *Backup* e recuperação: Políticas automatizadas de *backup* diário, restauração periódica testada e redundância geográfica;
- Gestão de disputas: Mecanismo de *'freeze'* automático e processos internos com SLA definido, garantindo direitos de retificação.

5. Avaliação de Riscos após Plano de Ação

5.1. Nova Matriz de Riscos

A matriz de riscos apresentada a seguir, mostra os resultados obtidos após a implementação do plano de ação, em comparação com a avaliação inicial. Como é possível observar, houve uma redução significativa tanto na probabilidade quanto na gravidade dos riscos identificados anteriormente. Vamos reavaliar os riscos novamente, de forma a compreender melhor a eficácia das medidas de mitigação impostas.



5.2 Reavaliação dos Riscos

5.2.1. Risco I - Acesso ilegítimo dos dados (Confidencialidade)

Situação inicial: Na avaliação inicial, este risco apresentava nível **máximo** tanto para probabilidade quanto para gravidade, posicionando-se no quadrante **vermelho (crítico)** da matriz de riscos. A ausência de mecanismos de proteção como TLS, autenticação forte e cifragem de dados tornava este risco extremamente elevado.

Situação atual: Com a implementação das medidas corretivas, este risco deslocou-se para o quadrante de risco **limitado** quer em termos de probabilidade quer em termos de gravidade.

5.2.2. Risco IN - Modificação indesejada dos dados (Integridade)

Situação inicial: Este risco estava classificado como **limitado** para probabilidade de risco e **significativo** para gravidade, situando-se no quadrante **laranja (Alto)** da matriz inicial. A falta de controle de versões, validação adequada e registos de auditoria contribuía para esta classificação.

Situação atual: Após as melhorias, o risco foi reduzido para o quadrante de risco **insignificante** em termos de probabilidade, mantendo-se como **limitado** no que toca a gravidade.

5.2.3. Risco D - Desaparecimento dos dados (Disponibilidade)

Situação inicial: A perda de dados era um risco **significativo** para probabilidade de risco e era considerado um risco **máximo** no que toca a gravidade, encontrando-se entre os quadrantes **laranja** e **vermelho** da matriz inicial. A ausência de políticas eficazes de *backup* e tolerância a falhas era particularmente preocupante.

Situação atual: Com as medidas implementadas, o risco foi reduzido para **significativo** em termos de gravidade e manteve-se como **limitado** em termos de probabilidade. Embora ainda represente um nível considerável de risco, houve uma melhoria significativa devido às medidas corretivas.

5.2.4. Conclusão da Reavaliação de Riscos:

Esta reavaliação de riscos demonstra que as medidas de mitigação implementadas foram eficazes na redução dos riscos para níveis aceitáveis, seguindo as normas do RGPD e as melhores práticas internacionais de segurança da informação. O projeto COP-MODE encontra-se assim, numa posição mais robusta para proteger os direitos dos titulares dos dados, mantendo a confidencialidade, integridade e disponibilidade das informações ao longo de todo o ciclo de vida dos dados. No entanto, a gestão de riscos deve sim, permanecer dinâmica, com monitorização e revisão periódica, de forma a garantir que novos riscos, sejam rapidamente identificados e mitigados.

6. Conclusão

O presente Privacy Impact Assessment demonstrou a maturidade e a robustez do processo de tratamento de dados do COP-MODE, garantindo que as preocupações de **confidencialidade**, **integridade** e **disponibilidade** são rigorosamente avaliadas e mitigadas ao longo de todo o ciclo de vida da informação.
Conclui-se assim que o COP-MODE cumpre os requisitos de um PIA sólido, estruturado e alinhado às melhores práticas internacionais. As contramedidas implementadas transformam um cenário de risco elevado num ambiente operacional de baixo risco, permitindo avançar com confiança na exploração científica dos dados de utilização de smartphones, sem comprometer os direitos dos participantes nem a integridade dos seus dados pessoais.

7. Referências

[1] Cloudflare.com. (2025). O que é o controle de acesso baseado em função (RBAC)? [online] Available at: *https://www.cloudflare.com/pt-br/learning/access-management/role-based-access-control-rbac/*.

[2] Cloudflare.com. (2025). O que são PII (informações que permitem identificação pessoal)? | Significado de PII. [online] Available at*:* *https://www.cloudflare.com/pt-br/learning/privacy/what-is-pii/*.

[3] dos, C. (2011). Ataque man-in-the-middle. [online] Wikipedia.org. Available at: *https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle*.

[4] dos, C. (2012). HMAC. [online] Wikipedia.org. Available at: *https://pt.wikipedia.org/wiki/HMAC*.

[5] Entrust.com. (2025). What is a Hardware Security Module (HSM) & its Services? | Entrust. [online] Available at: *https://www.entrust.com/pt/resources/learn/what-are-hardware-security-modules*.

[6] Google Cloud. (n.d.). O que é a recuperação de desastres e por que ela é importante? [online] Available at*:* *https://cloud.google.com/learn/what-is-disaster-recovery?hl=pt-br*.

[7] IGFEJ. (n.d.). Regulamento Geral de Proteção de Dados (RGPD). [online] Available at: *https://igfej.justica.gov.pt/Sobre-o-IGFEJ/Regulamento-Geral-de-Protecao-de-Dados-RGPD*.

[8] Jackson, B. (2020). Visão Geral do TLS 1.3 - Mais rápido e Seguro. [online] Kinsta®. Available at*:* *https://kinsta.com/pt/blog/tls-1-3/*.

[9] Leitura, 5min D. (2023). O que é segmentação de rede? [online] Palo Alto Networks. Available at*:* *https://www.paloaltonetworks.com.br/cyberpedia/what-is-network-segmentation*.

[10] O que é Failover e como funciona. (n.d.). O que é Failover e como funciona. [online] Available at: *https://www.controle.net/faq/o-que-e-failover*.

[11] [PIAF11] PIAFProject. A Privacy Impact Assessment Framework for Data Protection and Privacy Rights. Prepared for the Eurpean Commissiom Directorate General Justice. 21 September 2011. *https://piafproject.wordpress.com/*

[12] S.A, P.I. (n.d.). Dicionário Priberam, Dicionário Online de Português Contemporâneo. [online] Dicionário Priberam. Available at: *https://dicionario.priberam.org*.

[13] [SGTF18] E.U. Smart Grid Task Force. Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems. September 2018. *https://ec.europa.eu/energy/content/data-protectionimpact-assessment-template-smart-grid-and-smart-metering-systems_en*

[14] [SNZ12] Statistics New Zealand. Privacy Impact Assessment for the Integrated Data Infrastructure. 2012. *https://www.stats.govt.nz/assets/Uploads/Retirement-of-archive-website-project-files/Privacy-Impact-Assessment/Privacy-impact-assessment-for-the-Integrated-Data-Infrastructure/idi-privacyimpact-assessment.pdf*

[15] William Stallings, “Information Privacy Engineering and Privacy by Design”, Pearson Addison-Wesley, 2020

[16] www.cnil.fr. (n.d.). The open source PIA software helps to carry out data protection impact assessment. [online] Available at: *https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment.*

[17] www.ibm.com. (n.d.). O que é um acordo de nível de serviço (SLA)? | IBM. [online] Available at*: https://www.ibm.com/br-pt/topics/service-level-agreement*.

[18] www.kaspersky.com.br. (2022). O que é uma VPN e como funciona? [online] Available at*: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn.*