COP- MODE SETUP

Guilherme Jesus Oliveira , 202204987
Mário João Reis Minhava, 202206190
.

1. Contexto e Análise do projeto COP-MODE

Visão geral

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

O projeto COP-MODE envolve a recolha e análise de dados de uso de aplicações em smartphones por meio de um servidor e uma equipa organizada . O objetivo é avaliar as decisões de privacidade individuais do usuário durante uma semana de testes, utilizando a aplicação Retriever (CM- AR) para enviar os dados ao servidor COP-MODE. No contexto de um smartphone e de forma geral, as decisões de privacidade resumem-se à escolha de ou aceitar ou recusar o acesso por parte de uma aplicação a um determinado recurso, como a localização, por exemplo. Para isso, os participantes devem instalar a aplicação COP-MODE, que enviará aos servidor informações como e-mail, data de consentimento e uma lista das aplicações instaladas no dispositivo do participante, incluindo suas permissões, mas não dados pessoais das aplicações.

Após o envio dessas informações, a equipa COP-MODE prepara um smartphone da campanha, instalando as mesmas aplicações do usuário e o COP-MODE Naive Permission Manager (CM-NPM), que gerencia permissões e coleta dados necessários. O participante é então notificado para retirar o dispositivo e assinar um acordo de coleta de dados. Durante uma semana, o participante usa o smartphone fornecido, com o CM-NPM que monitoriza e solicita autorizações para acesso às aplicações, registando as respostas. Ao final da semana, o participante é informado sobre o término da campanha por e-mail e os dados são anonimizados, garantindo a privacidade dos participantes.

Visão Geral e Design do Sistema

O Projeto COP-MODE é concebido para monitorizar e analisar a utilização de aplicações móveis e as suas permissões, focando-se em como as permissões são concedidas e utilizadas por várias aplicações num smartphone. O projeto implementa vários sistemas e ferramentas, incluindo:

COP-MODE Apps Retriever (CM-AR): Uma aplicação que os participantes instalam nos seus smartphones para recolher dados sobre as aplicações instaladas e as suas permissões.

COP-MODE Naive Permission Manager (CM-NPM): Este sistema gere os pedidos de permissão e regista as respostas dos participantes sobre se as permissões devem ser concedidas.

Sistema de Coleta e Análise de Dados: Sistemas de backend que armazenam, processam e analisam os dados recolhidos das aplicações CM-AR e CM-NPM.

Responsabilidades inerentes ao tratamento de dados pessoais

As responsabilidades inerentes ao tratamento de dados pessoais incluem:

- Proteção e Privacidade dos Dados:

Apenas são recolhidos dados essenciais, como e-mail, data de consentimento e a lista de aplicações instaladas, sem que nunca seja acedido dados pessoais contidos nas aplicações.

Garantir que a informação recolhida é usada apenas para os propósitos definidos (como configurar os smartphones da campanha) e não para outros fins.

- Consentimento Informado:

Assegurar que os participantes são plenamente informados sobre o que será coletado e como será usado antes de consentirem com a participação.

Obter consentimento explícito para a coleta e uso dos dados, o que é feito através do acordo de coleta de dados que os participantes assinam ao retirar o smartphone.

- Segurança dos Dados:

Implementar medidas adequadas para proteger os dados dos participantes de acessos não autorizados, perda ou destruição.

Assegurar que os dados enviados ao servidor são transmitidos e armazenados de forma segura.

- Anonimização e Eliminação dos Dados:

Remover identificadores pessoais (como o e-mail) no final da campanha para anonimizar os dados restantes.

Garantir que os dados pessoais não são mantidos por mais tempo do que o necessário para os propósitos da pesquisa.

- Transparência e Acesso:

Informar os participantes sobre como seus dados serão usados, como podem acessá-los e como podem requerer a sua eliminação.

Permitir que os participantes tenham acesso às informações sobre quais dados são coletados e como são processados.

É também necessário que a equipa do COP-MODE se comprometa a providenciar qualquer assistência técnica que seja necessária durante a campanha.

Normas aplicáveis à finalidade de tratamento

Esta campanha foi aprovada pelo comité de ética do departamento de Ciência de Tecnologia da Computação da Universidade de Cambridge e pela comissão de ética da Faculdade de Ciências da Universidade do Porto.
A partilha de dados pela equipa do COP-MODE é restrita a parceiros académicos e destinada exclusivamente para fins de pesquisa. Os dados compartilhados serão previamente sanitizados e anonimizados para garantir a privacidade dos usuários.

Somente tipos específicos de dados, não sensíveis, como o tipo de conectividade, o contexto do dispositivo e os dispositivos em proximidade serão incluídos no conjunto de dados partilhados. Investigadores interessados em acessar este conjunto de dados devem assinar um acordo que inclui termos rigorosos de não compartilhamento, proibição de venda ou uso malicioso dos dados. Além disso, os dados devem ser armazenados e manuseados conforme as melhores práticas de segurança e privacidade. Importante ressaltar que um participante pode solicitar a qualquer momento a eliminação de seus dados, e essa solicitação deve ser atendida por todos os detentores dos dados, que são obrigados a apagar as informações conforme requerido.

Dados, processos e ativos de suporte

Tipos de dados pessoais tratados

1.Dados de Contacto

Tipo de Dado: Endereço de e-mail.
Finalidade: Comunicação principal com os participantes.
Prazo de Conservação: Até ao "retorno" do smartphone em causa, após o qual deve ser apagado, a menos que haja consentimento para mantê-lo por mais tempo para futuras comunicações ou se aplicações legais exigirem a sua retenção por um período mais longo.

2. Dados do Dispositivo

Tipo de Dados:

Aplicações instaladas e as suas configurações de permissão.
Tipo de conexão (WiFi, etc.).
Contexto do dispositivo (inativo, em uso, em chamada, etc.).

Finalidade: Análise do uso do dispositivo e contexto para a pesquisa.

Prazo de Conservação: até a conclusão da análise dos dados para os fins do projeto, após o qual deve ser anonimizado ou apagado, a menos que regulamentações específicas exijam uma retenção mais longa.

3. Dados de Localização

Tipo de Dado: Localização geográfica.
Finalidade: Rastrear movimentos e padrões para análise no âmbito do projeto.
Prazo de Conservação: até a conclusão das análises relevantes, seguido de anonimização ou exclusão.

4. Dados de Proximidade

Tipo de Dado: Dispositivos próximos.
Finalidade: Entender interações sociais ou ambientais.
Prazo de Conservação: deverá ser limitado ao período necessário para análise dos dados coletados.

5. Dados de Interação com Aplicações

Tipo de Dados:
Informações das aplicações no momento dos prompts de permissão.
Decisões do usuário sobre permissões.
Localização semântica (entrada do usuário).

Finalidade: Entender comportamentos do usuário e as suas decisões sobre privacidade.

Não serão recolhidas qualquer tipo de dados internos às aplicações.

Prazo de Conservação: até a conclusão da avaliação do comportamento do usuário e, posteriormente, anonimizar ou eliminar

Ciclo de vida dos dados pessoais e dos processos inerentes

Todos os dados coletados pelo COP-MODE serão utilizados exclusivamente para investigação e serão guardados e tratados apenas pela equipa do COP-MODE na UC, a qual se comprometerá às melhoras práticas de privacidade e segurança.

O email do participante (bem como todos os dados descritos acima) será guardado durante o período da campanha. Isto é necessário para contactar o participante durante a campanha e será, portanto, apagado no fim da mesma.

A qualquer momento o participante poderá contactar a equipa do COP-MODE para apagar todos os seus dados.

Ativos de informação utilizados na finalidade de tratamento

Os ativos de informação utilizados foram o smartphone pessoal e de teste, o email do participante, o servidor COP-MODE e as duas aplicações, CM-AR e CM-NPM.

Os meios de tratamento automatizados utilizados foram as duas aplicações já que estes operam como meios tecnológicos para a recolha, processamento e gerenciamento dos dados pessoais dos participantes. Por sua vez os meios de tratamento não automatizados envolvem operações manuais como a gestão de e-mails pelos membros da equipa COP-MODE, especialmente durante a comunicação com os participantes. Além disso, pode haver a necessidade de manusear os documentos em papel para a assinatura do acordo de coleta de dados pelos participantes.

Os ativos de informação são transmitidos através de e-mails, transferências de dados entre dispositivos e, potencialmente, de forma física. A equipa COP-MODE é responsável por gerir e controlar esses ativos durante a campanha.

Proporcionalidade e necessidade

A finalidade de tratamento é específica já que a recolha de dados está restrita às informações necessárias para atingir os objetivos da análise. A finalidade de tratamento é comunicada de forma transparente aos participantes, permitindo a estes que compreendam com clareza como os seus dados serão utilizados durante a campanha. Por fim, é legítima pois esta foi aprovada pelo comité de ética do departamento de Ciência e Tecnologia da Computação da Universidade de Cambridge.

O fundamento para o tratamento de dados pessoais na campanha COP-MODE é o consentimento dos participantes, que concordam voluntariamente com o tratamento dos seus dados para os fins específicos da pesquisa. Este consentimento é obtido de forma transparente e explícita, através da assinatura do participante no documento do Acordo De Coleta de Dados COP-MODE, disponibilizado no site do projeto.

Os dados pessoais recolhidos são adequados, relevantes e limitados para o propósito de tratamento. O e-mail, por exemplo, é necessário para a comunicação, entre a equipa e o participante, durante a campanha. Já a lista de aplicações é essencial para a análise da privacidade e segurança das mesmas. Os dados de consentimento são cruciais para garantir a conformidade com as regulamentações de proteção de dados. Além disso, também são recolhidos dados pessoais relacionados com cada pedido de permissão por parte das aplicações como a informação da aplicação pedinte, a aplicação em primeiro plano, a aplicação em segundo plano e a decisão do participante. Estes são importantes para analisar o comportamento das aplicações em interação com os participantes

Prazo da conservação dos dados

Os dados recolhidos, serão conservados durante a campanha sendo estes apagados quer no fim da mesma, quer quando o participante o deseje

Riscos

Medidas planeadas ou existentes

Controlos de Acesso

Implementar sistemas rigorosos de controlo de acesso baseado em funções para garantir que apenas pessoal autorizado tenha acesso a tipos específicos de dados.

Autenticação e Segurança de Rede

Usar mecanismos de autenticação multifatorial (MFA) fortes para utilizadores que acedem aos dados do servidor.

Assegurar que o servidor está protegido por firewalls e não está diretamente exposto à Internet. Usar Zonas Desmilitarizadas (DMZ) e proxies reversos para isolar o servidor de acessos externos diretos.

Encriptação

Encriptar dados sensíveis em repouso usando algoritmos de encriptação fortes, garantindo que, mesmo em caso de acesso indevido, a informação permaneça protegida.

Aplicar pseudonimização aos dados armazenados, especialmente endereços de email, para garantir que não estão em texto claro e não são diretamente ligáveis a indivíduos. Usar um sistema de gestão de chaves seguro para lidar com os pseudónimos e a sua correspondência com dados reais.

Hashing

Em vez de armazenar diretamente os nomes das aplicações, usar um sistema de hashing onde os nomes das aplicações são substituídos por um identificador único . Garantir que esse processo não possa ser facilmente revertida sem acesso à chave .

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.

Utilização de HTTPS

Garantir que todos os dados transmitidos entre os smartphones e o servidor sejam encriptados usando HTTPS, que emprega TLS (Transport Layer Security) para proteger os dados em trânsito.

Utilização de VPN´s

Implementar uma Rede Privada Virtual (VPN) para todas as transmissões de dados, adicionando uma camada adicional de encriptação e segurança.

Pinning de Certificado

Utilizar pinning de certificados SSL/TLS na aplicação móvel para prevenir ataques de intermediários, assegurando que a aplicação comunique apenas com o servidor identificado por um certificado específico.

Registos de acesso

Implementar um sistema detalhado de registo para acessos e modificações dos dados, assegurando que qualquer acesso não autorizado ou ligação inapropriada possa ser rapidamente detetada e tratada

Backup e Recuperação

Políticas de Backup Regular: Garantir que os backups dos dados sejam realizados regularmente e de forma segura. Isso permite a recuperação de dados no caso de modificação maliciosa ou acidental.

Testes de Recuperação de Desastres: Realizar testes regulares das políticas e procedimentos de recuperação para garantir que eles sejam eficazes e possam restaurar os dados rapidamente após uma alteração indesejada.

Riscos

Acesso ilegítimo dos dados

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

Violação de privacidade, Roubo de identidade, Prejuízo à integridade dos Dados

Quais são os principais ameaças que poderiam levar ao risco?

Leak de credenciais, Fraude de Identidade, Acesso Não Autorizado ao Servidor/Dados, Interceção das Comunicações Entre os Smartphones e o Servidor do Projeto, Malware

Quais são as fontes de risco?

Colaboradores e parceiros externos, vulnerabilidades dos dispositivos moveis, Falhas nas políticas de privacidade

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

Controlos de Acesso, Encriptação, Hashing, Utilização de HTTPS, Utilização de VPN´s

Modificação indesejada dos dados

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

Integridade de Dados comprometida, Risco de fraude, Distorção da informação

Quais são as principais ameaças que poderiam levar ao risco?

Acesso Não Autorizado ao Servidor/Dados, Interceção das Comunicações Entre os Smartphones e o Servidor do Projeto, Leak de credenciais, Fraude de Identidade

Quais são as fontes de risco?

Colaboradores e parceiros externos, vulnerabilidades dos dispositivos moveis, Falhas nas políticas de privacidade

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

Backup e Recuperação, Monitorização e Registo de Atividades, Controlos de Acesso

Desaparecimento de dados

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

Integridade de Dados comprometida, Risco de exposição e uso indevido de dados pessoais, Perda de controle sobre os dados

Quais são as principais ameaças que poderiam levar ao risco

Acesso Não Autorizado ao Servidor/Dados, Leak de credenciais, Interceção das Comunicações Entre os Smartphones e o Servidor do Projeto, Malware

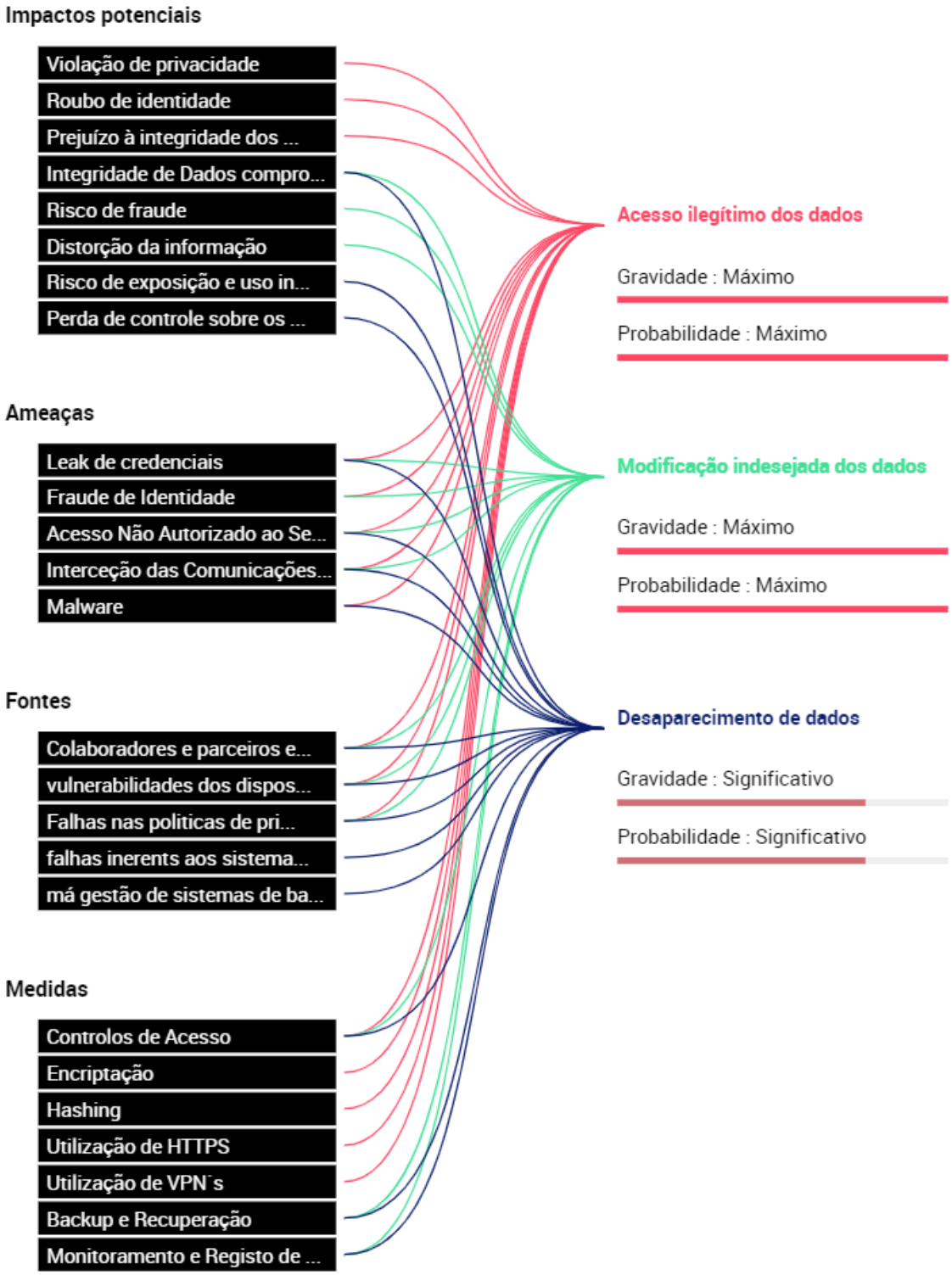
Quais são as fontes de risco?

Falhas nas políticas de privacidade, Colaboradores e parceiros externos, vulnerabilidades dos dispositivos moveis, falhas inerentes ao sistema de armazenamento de dados, más gestões dos sistemas de backup.

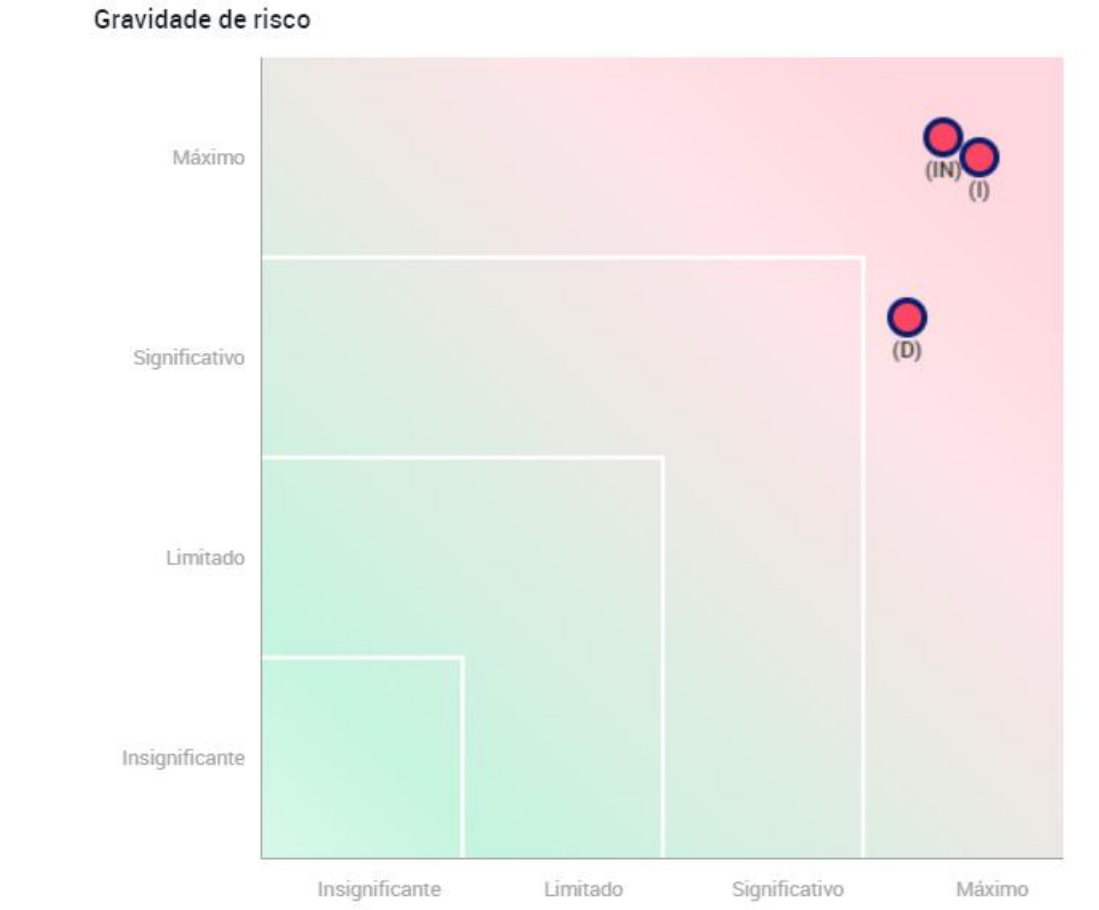
Quais são os controlos identificados que contribuem para abordar o risco?

Backup e Recuperação, Monitorização e Registo de Atividades, Controlos de Acesso

Visão Geral dos Riscos sem medidas de segurança



Mapeamento dos Riscos sem os processos de mitigação referidos



- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

Na ausência de medidas de mitigação, os riscos associados à segurança dos dados em um projeto como o COP-MODE podem tornar-se extremamente prováveis e graves. Aqui estão avaliações detalhadas para cada risco mencionado:

1. Acesso Ilegítimo de Dados

Probabilidade: Muito Alta

Sem medidas de segurança apropriadas, como encriptação de dados, autenticação forte e controle de acesso, os dados ficam vulneráveis a ataques externos e internos. A facilidade de acesso aumenta drasticamente a probabilidade de ocorrência de acessos não autorizados.

Gravidade: Muito Alta

O acesso ilegítimo pode resultar na exposição de informações pessoais sensíveis dos participantes, levando a violações de privacidade e possíveis consequências legais. Além disso, a perda de confiança dos participantes e danos à reputação da organização podem ser significativos.

2. Modificação Indesejada dos Dados

Probabilidade: Muito Alta

Na ausência de controles de integridade, como trilhas de auditoria, assinaturas digitais e mecanismos de verificação, a modificação indesejada de dados (seja maliciosa ou acidental) é muito provável. Sem esses controles, não há como garantir que os dados não sejam alterados de forma inapropriada.

Gravidade: Alta

A modificação dos dados pode comprometer a validade e a fidelidade dos resultados da pesquisa. Isso poderia resultar em conclusões errôneas, impactando negativamente o valor científico e académico do estudo. Adicionalmente, correções e verificações posteriores podem resultar em custos adicionais e perda de tempo valioso.

3. Desaparecimento dos Dados

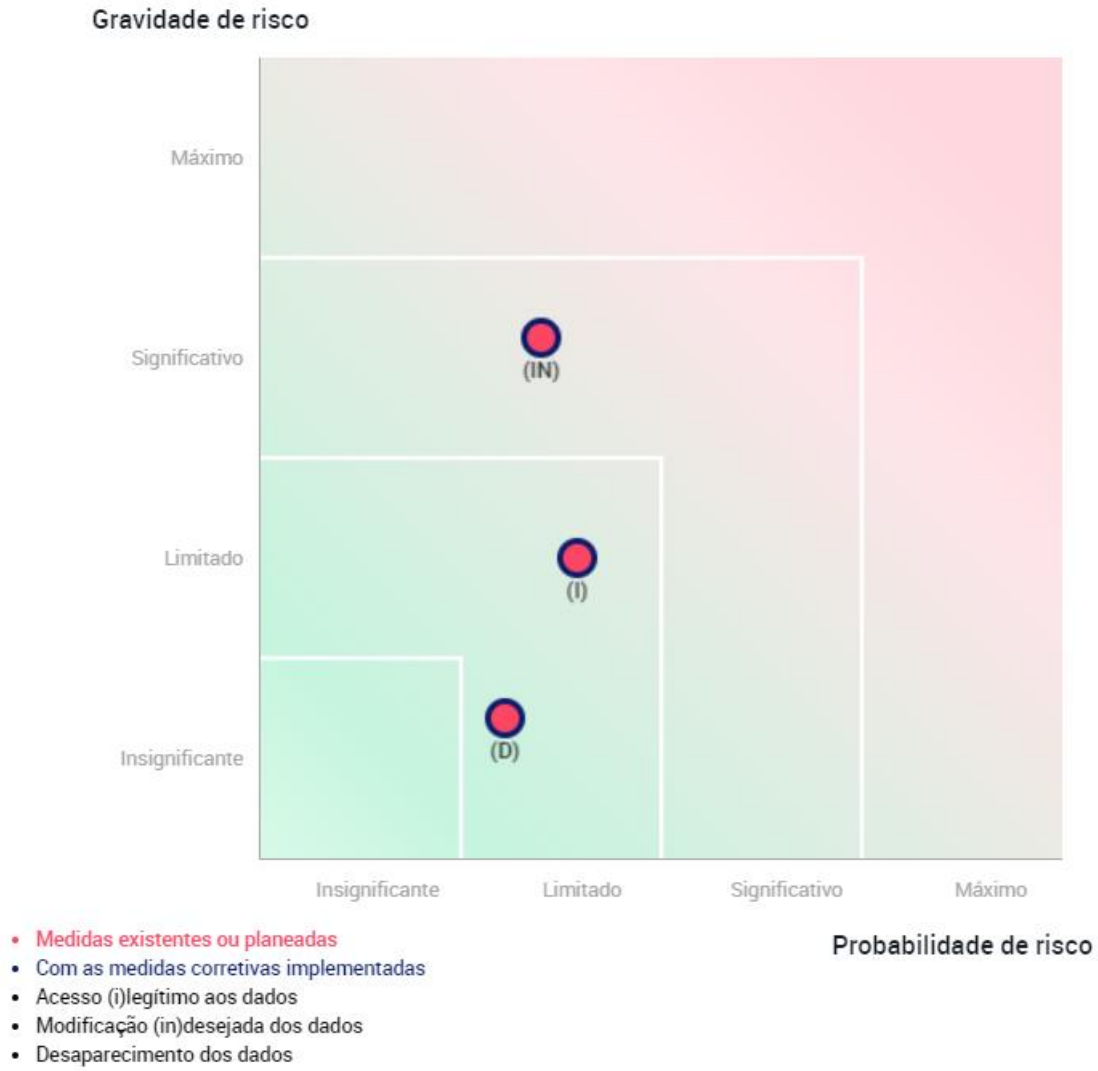
Probabilidade: Muito Alta

Sem backups regulares e redundância de dados, qualquer falha técnica, erro humano ou desastre natural poderia resultar na perda total dos dados. A dependência de um único local ou sistema para armazenamento de dados sem planos de contingência aumenta significativamente essa probabilidade.

Gravidade: Alta (ou muito alto consoante a dimensão da perda)

A perda de dados pode significar a perda (possivelmente total) do trabalho realizado, a necessidade de repetir a recolha de dados e, em casos extremos, o fim do projeto. Para além disso a incapacidade de recuperar os dados pode levar a implicações legais graves, especialmente se houver violação de compromissos contratuais

Mapeamento dos Riscos com medidas de mitigação



Com a implementação de medidas de mitigação eficazes como Controles de Acesso, Encriptação, Hashing, Utilização de HTTPS e VPNs, **a probabilidade e a gravidade do risco de acesso**

ilegítimo de dados no projeto COP-MODE podem ser significativamente reduzidas. Vamos analisar como cada uma dessas medidas impacta o risco:

Controles de Acesso

Impacto na Probabilidade: Reduz consideravelmente a probabilidade, uma vez que limita o acesso a dados apenas para indivíduos autorizados.

Impacto na Gravidade: Minimiza a gravidade pois, mesmo que haja uma tentativa de acesso, será bloqueada ou restrita a dados não críticos.

Encriptação

Impacto na Probabilidade: Reduz significativamente, já que os dados ficam inacessíveis sem as chaves de criptografia adequadas.

Impacto na Gravidade: Reduz a gravidade, pois mesmo que os dados sejam acedidos ilegalmente, eles não poderão ser lidos ou usados.

Hashing

Impacto na Probabilidade: Não afeta diretamente a probabilidade de acesso, mas ajuda a proteger a integridade dos dados

Impacto na Gravidade: Reduz a gravidade ao garantir que qualquer alteração nos dados seja facilmente detetável

Utilização de HTTPS

Impacto na Probabilidade : Reduz a probabilidade de interceção de dados durante a transmissão

Impacto na Gravidade : Diminui a gravidade, pois os dados eventualmente capturados durante a transmissão permanecem encriptados e , portanto, ilegíveis

Utilização de VPNs

Impacto na Probabilidade: Reduz a probabilidade ao estabelecer um canal seguro de comunicação para dados transmitidos entre redes diferentes.

Impacto na Gravidade: Ajuda a reduzir a gravidade, protegendo os dados contra acessos em redes inseguras.

Quando se trata **de mitigar o risco de modificação indesejada e desaparecimento dos dados no projeto COP-MODE,** as medidas como Backup e Recuperação, Monitorização e Registo de Atividades, e Controlos de Acesso, desempenham um papel crucial em reduzir tanto a probabilidade quanto a gravidade deste risco:

Backup e Recuperação

Impacto na Probabilidade: Indireto

Enquanto o backup e a recuperação por si só não previnem a modificação ou desaparecimento, garantem que os dados podem ser restaurados ao seu estado original após uma alteração indesejada.

Impacto na Gravidade: Alto

A capacidade de restaurar dados a partir de backups seguros e atualizados minimiza significativamente a gravidade do impacto de uma modificação indesejada, permitindo que o projeto recupere rapidamente sua linha de base de dados.

Monitorização e Registo de Atividades

Impacto na Probabilidade: Alto.

Monitorizar, registar todas as atividades de acesso e modificação de dados cria um ambiente em que é difícil para os agentes mal-intencionados alterar dados sem serem detetados.

Impacto na Gravidade: Moderado a Alto

A rápida deteção de alterações indesejadas por meio de logs detalhados permite intervenções rápidas, o que limita o escopo do dano.

Controlos de Acesso

Impacto na Probabilidade: Alto

Restringir o acesso aos dados apenas a usuários autorizados e com a necessidade de conhecer a base diminui drasticamente a probabilidade de que os dados sejam modificados de forma inapropriada.

Impacto na Gravidade: Moderado a Alto

A modificação indesejada se torna menos provável de causar danos significativos, pois o número de pessoas capazes de fazer tais alterações é limitado e bem regulado.

Avaliação Final com Mitigações

Probabilidade: Baixa a Moderada. Com o monitorização contínuo e o controle rigoroso de quem pode aceder e modificar os dados, a chance de modificações indesejadas é significativamente reduzida.

Gravidade: Baixa a Moderada

Mesmo no caso de modificações ocorrerem, a capacidade de rapidamente detetar, registar e reverter essas mudanças limita seu impacto.

Riscos adicionais

Risco	Mitigações
Fuga de Dados por Interceção das Comunicações Entre os Smartphones e o Servidor do Projeto	Utilização de HTTPS: Garantir que todos os dados transmitidos entre os smartphones e o servidor sejam encriptados usando HTTPS, que emprega TLS (Transport Layer Security) para proteger os dados em trânsito. VPN: Implementar uma Rede Privada Virtual (VPN) para todas as transmissões de dados, adicionando uma camada adicional de encriptação e segurança. Pinning de Certificado: Utilizar pinning de certificados SSL/TLS na aplicação móvel para prevenir ataques de intermediário, assegurando que a aplicação comunique apenas com o servidor identificado por um certificado específico.
Fuga de Dados devido a Acesso Não Autorizado ao Servidor/Dados	Controlos de Acesso: Implementar sistemas rigorosos de controlo de acesso baseado em funções para garantir que apenas pessoal autorizado tenha acesso a tipos específicos de dados. As medidas de segurança robustas como autenticação multifatorial, controlos de acesso baseados em funções e isolamento de servidor através de DMZ e proxies reversos reduzem significativamente o risco de acessos não autorizados. Autenticação: Usar mecanismos de autenticação multifatorial (MFA) fortes

	para utilizadores que acedem aos dados do servidor. Segurança da Rede: Assegurar que o servidor está protegido por firewalls e não está diretamente exposto à Internet. Usar Zonas Desmilitarizadas (DMZ) e proxies reversos para isolar o servidor de acessos externos diretos.
Ligação de Dados em Repouso	Encriptação: Encriptar dados sensíveis em repouso usando algoritmos de encriptação fortes, garantindo que, mesmo em caso de acesso indevido, a informação permaneça protegida. Pseudonimização: Aplicar pseudonimização aos dados armazenados, especialmente endereços de email, para garantir que não estão em texto claro e não são diretamente ligáveis a indivíduos. Usar um sistema de gestão de chaves seguro para lidar com os pseudónimos e a sua correspondência com dados reais. Registo de Acessos: Implementar um sistema detalhado de registo para acessos e modificações dos dados, assegurando que qualquer acesso não autorizado ou ligação inapropriada possa ser rapidamente detetado e tratado
Fuga de Informação Sensível (Nomes de Aplicações)	Hashing: Em vez de armazenar diretamente os nomes das aplicações, usar um sistema de hashing onde os nomes das aplicações são substituídos por um identificador único . Garantir que esta tokenização não possa ser facilmente revertida sem acesso à chave ou serviço de tokenização. Acesso Limitado: Restringir o acesso às chaves ou métodos de detokenização estritamente às entidades autorizadas dentro do sistema que precisem de ligar as entradas de dados para fins de processamento legítimo. Gestão Segura de Chaves: Usar um sistema de gestão de chaves seguro para

	manejar as chaves criptográficas usadas na hash ou tokenização de forma segura.

IMPACTOS DAS MITIGAÇÕES DOS RISCOS ADICIONAIS NA GRAVIDADE E NA PROBABILIDADE

RISCO	PROBABILIDADE	GRAVIDADE
Fuga de Dados por Interceção das Comunicações Entre os Smartphones e o Servidor do Projeto	INSIGNIFICANTE Com a implementação do HTTPS, VPN e pinning de certificados, a comunicação entre smartphones e servidores fica altamente protegida contra interceções. Estas medidas asseguram que os dados em trânsito estejam encriptados e autenticados, dificultando significativamente a interceção por terceiros.	SIGNIFICATIVA Apesar da baixa probabilidade, se uma interceção ocorresse, os dados intercetados poderiam incluir informações sensíveis ou confidenciais, resultando em graves consequências para a privacidade dos usuários e integridade do projeto.
Fuga de Dados devido a Acesso Não Autorizado ao Servidor/Dados	LIMITADA As medidas de segurança robustas como autenticação multifatorial, controlos de acesso baseados em funções e isolamento de servidor através de DMZ e proxies reversos reduzem significativamente o	SIGNIFICATIVO Acesso não autorizado ao servidor ou aos dados pode levar à exposição de uma grande quantidade de dados sensíveis, tendo um impacto substancial sobre a privacidade dos usuários e a

	risco de acessos não autorizados.	operacionalidade do sistema.
Ligação de Dados em Repouso	LIMITADA A encriptação e pseudonimização de dados em repouso são técnicas eficazes para proteger os dados contra acessos indevidos. O registo de acessos facilita a deteção e resposta a incidentes de segurança.	SIGNIFICATIVO Embora as medidas reduzam a probabilidade de ocorrência, o impacto de uma possível violação permanece significativo, especialmente se os dados desencriptados forem expostos.
Fuga de informações sensíveis, nomeadamente o nome das aplicações coletadas	INSIGNIFICANTE Devido à encriptação dos dados e à anonimização dos mesmos, a probabilidade de acontecer é muito reduzida	LIMITADO Caso haja uma fuga, podemos analisar os diferentes acessos aos dados e identificar rapidamente a ameaça

Conclusão

Neste relatório foi feita uma análise do projeto COP-MODE, projeto este que visa aprimorar a privacidade em dispositivos móveis, promovendo a segurança dos utilizadores em um ambiente digital cada vez mais complexo. Através da coleta e análise de dados pessoais, este projeto busca insights valiosos para melhorar a proteção da privacidade, garantindo ao mesmo tempo a transparência e o consentimento dos participantes. No entanto, é essencial reconhecer e mitigar os diversos riscos associados ao tratamento de dados, incluindo fugas de dados, modificações não autorizadas e acessos ilegítimos. Ao implementar medidas robustas de segurança, como encriptação, uma autenticação com mais etapas e protocolos de comunicação seguros, podemos mitigar efetivamente esses riscos e proteger a integridade e confidencialidade dos dados dos participantes.