



ORIENTAÇÕES PARA A UTILIZAÇÃO DE UMA ESTRATÉGIA TRAGA O SEU PRÓPRIO DISPOSITIVO (BYOD) NA DIGITALIZAÇÃO DE CAMPANHAS DE MOSQUITEIROS TRATADOS COM INSETICIDA (MTI)

JUNHO DE 2026

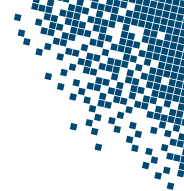


ÍNDICE

Glossário	4
1. Contexto	5
1.1 O que representa BYOD em campanhas de MTI?	5
1.2 Planeamento da estratégia BYOD	6
1.3 Modelos de estratégia de dispositivos	7
1.4 Vantagens e riscos	8
1.5 Considerações para a escolha de uma estratégia de dispositivos	10
2. Âmbito e casos de utilização do modelo BYOD em campanhas de MTI	13
2.1 Em que situações o modelo BYOD é adequado ou não	13
2.2 Avaliar a viabilidade e a prontidão do modelo BYOD	15
3. Política, privacidade e segurança	25
3.1 Elaboração da política de BYOD	25
3.2 Definir a utilização aceitável e as responsabilidades	25
3.3 Definir controlos mínimos de segurança e de acesso	26
3.4 Estabelecer regras de governação e armazenamento de dados	26
3.5 Resposta a incidentes relacionados com dispositivos perdidos, partilhados ou comprometidos	27
4. Implementação do modelo BYOD	28
4.1 Medidas alternativas	28
4.2 Formação	28
4.3 Apoio e supervisão durante a implementação	29
4.4 Controlos operacionais diários	29
4.5 Procedimento de encerramento de equipamentos após a campanha	30
5. Conclusão	31
Anexo 1: Lista de verificação para a avaliação da preparação para o modelo BYOD	32
Anexo 2: Registo no modelo BYOD, verificação de dispositivos e formulário de consentimento	35
Anexo 3: Modelo de inventário de dispositivos	38
Anexo 4: Exemplo de política de BYOD e termos de utilização para campanhas de MTI	39

GLOSSÁRIO

Termo	Definição
IPA	Interface de Programação de Aplicações (interface Android entre a aplicação e o servidor). Identifica que funções e funcionalidades estão disponíveis numa versão específica do sistema operativo.
Traga o seu próprio dispositivo (BYOD)	Uma política que permite que os indivíduos utilizem os respetivos dispositivos pessoais para tarefas aprovadas da campanha, ao abrigo de disposições definidas em matéria de governação, consentimento e apoio.
Aplicações (apps) da campanha	Ferramentas digitais aprovadas utilizadas nas tarefas da campanha de MTI, tais como o registo de agregados familiares, o registo da distribuição, as listas de verificação de supervisão ou a gestão de stocks.
Avaliação do impacto na proteção de dados (DPIA)	Um processo utilizado para identificar e minimizar os riscos relacionados com a proteção de dados associados a um projeto, a um sistema ou a uma atividade de tratamento de dados.
GPS	Sistema de posicionamento global
BYOD híbrido	Um modelo no qual a implementação da campanha utiliza uma combinação de dispositivos pessoais e dispositivos pertencentes ao programa.
Gestão de dispositivos móveis (MDM)	Software que permite a um programa gerir, monitorizar e controlar remotamente funcionalidades dos dispositivos registados para utilização na campanha. Em contextos BYOD, isto limita-se geralmente a controlos ao nível das aplicações.
Offline primeiro	Uma arquitetura de aplicação na qual as principais funções e a introdução de dados funcionam sem uma ligação ativa à Internet, sendo os dados sincronizados quando a ligação estiver disponível.
Dispositivo pertencente ao programa (POD)	Um dispositivo adquirido e detido pelo programa, por outro órgão do Ministério da Saúde ou por outra entidade governamental ou por um parceiro de implementação, configurado e entregue aos colaboradores para utilização na campanha.
BYOD puro	Um modelo no qual os colaboradores da campanha utilizam os seus próprios telemóveis e cartões SIM em fases e funções digitalizadas selecionadas da campanha.
Eliminação remota	A capacidade de eliminar remotamente de um dispositivo os dados de uma campanha.
Root (Android) e jailbreak (iOS)	Processos que eliminam as restrições impostas pelo fabricante ou pela operadora, concedendo aos utilizadores acesso de nível “root” ou de administrador ao sistema operativo.
Acesso baseado em funções	Uma abordagem de segurança na qual os utilizadores só podem aceder aos dados e funções relevantes para a(s) função(ões) que lhes foi(foram) atribuída(s).
Sincronização (sync)	Processo de transferência de dados armazenados localmente de um dispositivo para um servidor central.
Dados zero rating	Acesso a dados móveis para uma aplicação específica que não consome dados móveis do tarifário pessoal do utilizador.



1. CONTEXTO

A malária continua a constituir um desafio crítico para a saúde pública em muitos países endêmicos. Os mosquiteiros tratados com inseticida (MTI) continuam a ser uma das intervenções mais eficazes para a redução da transmissão da malária e para a prevenção da morbilidade e da mortalidade. Na maioria dos países onde a malária é endêmica, as campanhas de distribuição em massa de MTI são geralmente implementadas em grande escala e com calendários apertados, com o objetivo de aumentar rapidamente o acesso dos agregados familiares aos MTI e a proteção contra a malária a nível comunitário.

As exigências operacionais destas campanhas requerem dados atuais, precisos e completos. Os prazos de implementação apertados, o grande número de colaboradores temporários e a complexa logística de último quilómetro;

todos estes dependem de informações fiáveis para apoiar o planeamento, a supervisão e as medidas corretivas. A qualidade e a pontualidade dos dados são, por isso, fundamentais para o desempenho da campanha.

A digitalização de determinadas funções da campanha pode dar resposta a muitos destes desafios. No entanto, a aquisição e a gestão de grandes quantidades de dispositivos móveis padronizados são dispendiosas, demoradas e exigentes do ponto de vista operacional. Em muitos contextos, estas restrições podem limitar a viabilidade ou a escalabilidade de campanhas totalmente digitalizadas. Uma alternativa prática é a utilização de dispositivos móveis pessoais por parte dos colaboradores da campanha, sendo esta estratégia geralmente designada de Traga o seu próprio dispositivo (BYOD).

1.1 O que representa BYOD em campanhas de MTI?

BYOD é uma estratégia que permite que os colaboradores da campanha utilizem os respetivos dispositivos pessoais, geralmente smartphones, para tarefas aprovadas da campanha. No âmbito da estratégia BYOD, os dispositivos pessoais que tenham sido submetidos a uma verificação (ver abaixo) são temporariamente registados para executar aplicações aprovadas da campanha. Os colaboradores da campanha acedem a ferramentas e aplicações de recolha de dados nos dispositivos que já detêm e que sabem utilizar.

Esta abordagem revela-se particularmente valiosa nos casos em que os orçamentos das campanhas tornam difícil a nível operacional a aquisição e a gestão de grandes quantidades de dispositivos pertencentes ao programa. Para além das poupanças financeiras, ficou

demonstrado que a estratégia BYOD aumenta a produtividade e a satisfação dos utilizadores, uma vez que os colaboradores no terreno podem realizar as respetivas tarefas em dispositivos com os quais estão familiarizados e com os quais se sentem à vontade¹.

Vários países têm aplicado a estratégia BYOD em campanhas de MTI. O Uganda apresentou a sua experiência na utilização da estratégia BYOD para a digitalização das campanhas de cobertura universal de MTI na Reunião de digitalização da campanha da AMP de 2023². O Togo documentou a utilização de dispositivos pessoais nas suas campanhas em massa de MTI de 2020 e 2023, num estudo de caso publicado no sítio Web da AMP³. Estas experiências indicam que a estratégia BYOD pode ser viável do ponto de vista operacional em contextos de

1. <https://www.tandfonline.com/doi/full/10.1080/08874417.2018.1543001>

2. https://allianceformalariaprevention.com/wp-content/uploads/2024/02/2.8-Rukaari-Medard_Uganda.pdf

3. https://allianceformalariaprevention.com/wp-content/uploads/2026/06/Togo_Estudo_de_Caso_Digitalizacao_BYOD_112024_PRT-2.pdf



campanha, contanto que seja apoiada por critérios de elegibilidade claros, uma estratégia abrangente no que diz respeito à utilização, mecanismos de apoio em matéria de dados e um conjunto de dispositivos destinados a empréstimo aos colaboradores que não disponham de um smartphone compatível ou que não pretendam utilizar o seu próprio dispositivo.

Esta orientação apresenta recomendações práticas e considerações operacionais relativas à estratégia BYOD em campanhas de distribuição em massa de MTI. Esta destina-se aos programas nacionais de controlo da malária (PNM), aos respetivos parceiros de implementação e financiamento e aos prestadores de serviços de saúde digitais que apoiam o planeamento e a execução de campanhas de MTI.

As recomendações que se seguem resumem as principais medidas para a implementação segura e eficaz de uma estratégia BYOD e são abordadas de forma mais pormenorizada na orientação:

- **Estabelecer uma estratégia BYOD antes do início de qualquer processo de registo.** Definir a utilização adequada, as responsabilidades dos utilizadores, os requisitos de proteção de dados, as normas de segurança, as compensações, a comunicação de incidentes e a responsabilidade civil. Obter o aval da direção do Ministério da Saúde/programa nacional de controlo da malária (MdS/PNM) e concluir a análise jurídica.
- **Definir e aplicar normas mínimas relativas aos dispositivos e à segurança.** Verificar todos os dispositivos durante o registo. Não registar dispositivos que não cumpram os requisitos.

- **Disponibilizar formação diferenciada e prática, adaptada aos níveis de literacia digital de cada grupo de utilizadores.** Verificar as competências antes da implementação. Assegurar que o apoio técnico se encontra disponível ao longo de todo o processo de implementação.
- **Aplicar controlos de segurança adequados.** No mínimo: início de sessão seguro, acesso baseado em funções, armazenamento encriptado, tempo limite de sessão e possibilidade de terminar remotamente a sessão. Aplicar controlos mais rigorosos aos fluxos de trabalho de maior sensibilidade.
- **Utilizar uma abordagem híbrida.** A estratégia BYOD não é adequada para todas as funções da campanha nem para todos os utilizadores. Reservar os dispositivos pertencentes ao programa para fluxos de trabalho de alto risco. Manter um conjunto de dispositivos destinados a empréstimo e uma solução alternativa ou de contingência comprovada.
- **Assegurar que a estratégia BYOD não acarreta quaisquer custos injustos para os colaboradores.** Definir medidas de apoio aos pacotes de dados e acordos de compensação antes do início da campanha e comunicá-las de forma clara durante a formação.
- **Monitorizar a implementação utilizando os indicadores definidos, desde a fase-piloto em diante.** Ajustar o âmbito, as salvaguardas ou o modelo de implementação com base em dados evidências. Não alargar a escala de uma abordagem que não cumpra os objetivos da fase-piloto.

1.2 Planeamento da estratégia BYOD

A estratégia BYOD deve ser planeada com antecedência, para assegurar que é adequada e que os resultados pretendidos são alcançados. O planeamento requer que os PNM sigam, por ordem, as seguintes etapas, sobre as quais são disponibilizados mais pormenores nas secções

seguintes da orientação:

1. **Realizar uma avaliação de viabilidade relativa à estratégia BYOD e documentar as decisões:** Isto deverá permitir confirmar se a estratégia BYOD é

adequada, em que contextos pode ser utilizada e qual a abordagem a adotar (Secção 2.2).

2. Definir os requisitos mínimos dos dispositivos para utilização na campanha: Estes devem refletir as necessidades de aplicação da campanha e as normas mínimas de segurança exigidas (Secção 2.2.1).

3. Realizar o recenseamento dos dispositivos e classificar os utilizadores por nível de preparação: Isto ajuda a determinar quantos colaboradores dispõem de dispositivos adequados, onde existem lacunas e a dimensão provável de um conjunto de dispositivos destinados a empréstimo para os colaboradores que não dispõem dos seus próprios dispositivos (2.2.1).

4. Confirmar e verificar se a plataforma selecionada é adequada para a estratégia BYOD: A plataforma deve funcionar nos tipos de dispositivos pessoais previstos na campanha, especialmente nos telemóveis Android mais comuns. Os testes devem incluir uma amostra representativa dos dispositivos reais, incluindo modelos de gama baixa, e devem confirmar a funcionalidade offline, o desempenho da sincronização e a possibilidade de utilização nas áreas-alvo (2.2.4).

5. Elaborar e validar a política de BYOD e os formulários de utilizador relacionados: Isto inclui formulários de reconhecimento ou consentimento do utilizador

nos principais idiomas locais, conforme exigido (Secção 3 e Anexos 2 e 4).

6. Calcular as necessidades orçamentais e obter aprovação: A estratégia BYOD reduz os custos de aquisição de dispositivos, mas outros custos operacionais mantêm-se, independentemente de serem utilizados dispositivos pertencentes ao programa ou dispositivos pessoais, pelo que estes devem ser orçamentados antes da implementação. Os custos podem incluir o fornecimento de pacotes de dados, tempo de antena, dispositivos destinados a empréstimo, cartões SIM, power banks, formação e assistência técnica (2.2.6).

7. Adquirir e configurar o conjunto de dispositivos destinados a empréstimo e outros itens de apoio necessários: Isto deve ser realizado com antecedência suficiente para facilitar o registo, permitir medidas alternativas e assegurar a plena inclusão dos colaboradores.

8. Realizar um projeto-piloto em distritos representativos e analisar os resultados antes da implementação: O projeto-piloto deve testar a abordagem em condições realistas e avaliar o desempenho em função dos critérios de expansão acordados. Caso o desempenho não cumpra os critérios acordados, o âmbito, as salvaguardas ou o modelo de implementação devem ser revistos antes da implementação (2.2.8).

1.3 Modelos de estratégia de dispositivos

As campanhas de MTI podem recorrer a diferentes estratégias de dispositivos consoante o contexto. Embora alguns contextos possam ser adequados para a implementação da estratégia BYOD pura ou apenas com dispositivos pertencentes ao programa (POD), é provável

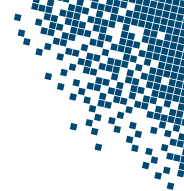
que a maioria das campanhas beneficie de uma abordagem híbrida que combine dispositivos pessoais com um conjunto específico de dispositivos adquiridos no âmbito do programa (Quadro 1).

Quadro 1: Modelos de estratégia de dispositivos para a digitalização de campanhas de MTI

Modelo BYOD	Descrição	Mais adequado para
BYOD puro	Os colaboradores da campanha utilizam os seus próprios telemóveis e cartões SIM em fases e funções selecionadas da campanha.	Contextos caracterizados por uma elevada penetração de smartphones, redes de implementadores bem estabelecidas, conectividade fiável e requisitos menos exigentes em termos de normalização e controlo dos dispositivos.
POD	É adquirido, configurado e entregue um dispositivo padronizado a todos os colaboradores da campanha que necessitem de utilizar a ferramenta digital. Todos os dispositivos são pertencentes ao programa e são geridos pelo mesmo ao longo de todo o ciclo de vida, incluindo a distribuição, a logística inversa, o armazenamento e a manutenção entre campanhas.	Campanhas nas quais a posse de smartphones entre os colaboradores-alvo da campanha é baixa, nas quais os requisitos nacionais de proteção de dados restringem a utilização de dispositivos pessoais, nas quais todas as funções da campanha exigem controlos de segurança completos ao nível do dispositivo, ou nas quais está prevista a reutilização dos dispositivos em vários ciclos e intervenções da campanha.
BYOD híbrido	A implementação da campanha utiliza uma combinação de dispositivos pessoais e dispositivos adquiridos no âmbito do programa. Os dispositivos adquiridos no âmbito do programa são distribuídos em locais nos quais a posse de smartphones é reduzida ou nos quais é necessária uma maior padronização, fiabilidade ou segurança.	A maioria das campanhas. Ideal para programas que procuram tirar partido das vantagens em termos de custos e de familiaridade do modelo BYOD, reduzindo simultaneamente os riscos de implementação e assegurando a cobertura para os colaboradores ou a utilização de funções que não podem depender exclusivamente de dispositivos pessoais.

Os PNM que utilizam o modelo BYOD devem prever um pequeno conjunto de dispositivos destinados a empréstimo, por exemplo, cerca de 5 a 10% da força de trabalho que se prevê que adote o modelo BYOD, para promover a inclusão e assegurar a continuidade operacional dos colaboradores cujos dispositivos não cumpram os requisitos mínimos ou que optem por não utilizar o respetivo dispositivo pessoal para o trabalho da campanha. Sempre que possível, este

conjunto de dispositivos destinados a empréstimo pode ser complementado através da coordenação com outros programas de saúde e parceiros, com vista a requisitar temporariamente ou reatribuir equipamentos já existentes.



1.4 Vantagens e riscos

O modelo BYOD pode proporcionar importantes vantagens operacionais e em termos de custos, mas apenas nos casos em que for adequado ao contexto e nos casos em que os riscos associados são geridos de forma ativa. O equilíbrio entre vantagens e riscos irá variar em função do contexto da campanha, pelo que os gestores do programa devem avaliar ambos antes de decidirem se e de que forma o modelo BYOD deve ser utilizado.

As potenciais vantagens incluem:

- Redução dos custos relativos a aquisição, armazenamento e distribuição de dispositivos.
- Implementação mais rápida, sem necessidade de aquisição e configuração de dispositivos em grande escala.
- Os colaboradores utilizam dispositivos com os quais já estão familiarizados, o que poderá permitir uma redução da curva de aprendizagem e do tempo de formação.
- Permite uma rápida expansão sem uma complexa logística de dispositivos.
- A posse pessoal pode incentivar um maior cuidado no manuseamento e na utilização do dispositivo.
- A exposição a aplicações da campanha pode contribuir para o desenvolvimento de familiaridade com o mundo digital, com vista a uma utilização futura de programas de saúde.
- Evita a necessidade de recolha, armazenamento e manutenção de dispositivos após a campanha, bem como o fardo dos resíduos eletrónicos.
- Os materiais de formação e os materiais de apoio ao trabalho podem ser pré-carregados nos dispositivos dos colaboradores, sendo possível partilhar facilmente atualizações e orientações de reciclagem durante a implementação, conforme necessário. Isto pode incluir breves lembretes de formação ou notificações para a resolução de problemas quando surgem dificuldades, podendo todos estes ser

transmitidos através de canais simples, tais como ligações para o YouTube ou para outras plataformas digitais de uso comum.

- Pode reduzir as despesas do programa com dispositivos de substituição e acessórios em alguns contextos.

No entanto, as vantagens devem ser ponderadas em relação aos potenciais riscos, que podem incluir:

- Variações na qualidade dos dispositivos e na compatibilidade com a aplicação da campanha.
- Questões relacionadas com a equidade, incluindo questões de género e exclusão digital em sentido mais lato, devido às quais alguns colaboradores não dispõem de smartphones adequados nem têm acesso equitativo às ferramentas digitais.
- Riscos para a proteção de dados devido ao facto de os dados pessoais e os dados de campanha coexistirem no mesmo dispositivo.
- Responsabilidade pouco clara em caso de perda, danos ou comprometimento de um dispositivo pessoal.
- Limitações de conectividade e falhas na sincronização offline.
- Aumento das necessidades de assistência e eventuais problemas de qualidade dos dados nos casos em que a literacia digital é limitada.
- Risco de acesso não autorizado no caso de os dispositivos serem partilhados ou de não estarem devidamente protegidos.
- Litígios relativos a incentivos ou reembolsos, caso as condições não estejam claramente definidas.
- As diferenças entre sistemas operativos e configurações dos dispositivos podem complicar a assistência técnica.

Poderá consultar outros riscos e medidas para a respetiva mitigação na [Secção 2.2.9](#).

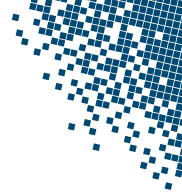
1.5 Considerações para a escolha de uma estratégia de dispositivos

Antes de se comprometer com uma única estratégia de dispositivo, os gestores dos programas de controlo da malária e o pessoal de assistência nas áreas de dados, M&A e TIC devem avaliar de que forma o modelo BYOD puro, o modelo apenas POD e o modelo BYOD híbrido se comparam nas principais dimensões operacionais e políticas relevantes para a respetiva

campanha. Conforme indicado no Quadro 1, o modelo BYOD híbrido é a opção predefinida recomendada para a maioria das campanhas. O quadro abaixo (Quadro 2) destina-se a ajudar os gestores do programa a confirmar ou ajustar esse valor predefinido, tendo em consideração o respetivo contexto específico.

Quadro 2: Orientações de decisão para a seleção de uma estratégia de dispositivos

Dimensão da decisão	Favorece o modelo BYOD	Favorece a estratégia apenas POD	BYOD híbrido
Custo inicial	Inferior, uma vez que a aquisição de dispositivos é dispendiosa e, muitas vezes, o tempo disponível para a aquisição é limitado.	Reduzido ao longo do tempo, à medida que os dispositivos forem sendo reutilizados ao longo de vários ciclos de campanha e intervenções.	Reduz o custo total de aquisição, limitando as compras no âmbito do programa a um subconjunto definido de dispositivos que devem ser planeados para reutilização em diferentes intervenções e atividades.
Prazo de aquisição	Mais rápido: não requer qualquer procedimento de aquisição de dispositivos pessoais.	Requer o estabelecimento de um prazo para a aquisição, configuração e distribuição de todos os dispositivos.	Mais curto do que numa estratégia apenas POD, uma vez que é necessário adquirir e configurar menos dispositivos. Os programas devem continuar a prever tempo para a aquisição do conjunto de dispositivos destinados a empréstimo.



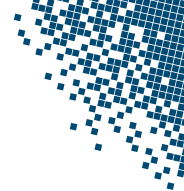
Dimensão da decisão	Favorece o modelo BYOD	Favorece a estratégia apenas POD	BYOD híbrido
Disponibilidade dos dispositivos	Só será viável se a penetração dos smartphones for suficientemente elevada entre os grupos-alvo de colaboradores em todas as zonas da campanha.	Assegura que todos os colaboradores registados dispõem de um dispositivo compatível, independentemente de serem detentores de um dispositivo a título pessoal.	Expande a cobertura através da utilização de dispositivos pessoais cuja taxa de posse é elevada e da atribuição de dispositivos adquiridos no âmbito do programa a quadros, zonas ou funções cuja posse de smartphones é baixa ou nas quais é necessária a padronização dos dispositivos
Familiaridade do colaborador	Os colaboradores estão familiarizados com os seus próprios dispositivos; isto traduz-se numa adoção mais rápida por parte dos utilizadores e num menor número de erros relacionados com os dispositivos durante as tarefas de rotina.	Requer tempo de formação adicional para a utilização de um dispositivo e de um sistema operativo com os quais não se está familiarizado.	Mantém a vantagem da familiaridade para os colaboradores que utilizam os respetivos dispositivos pessoais, ao mesmo tempo que disponibiliza dispositivos padronizados e formação para funções e áreas geográficas específicas.
Controlo da segurança dos dados	Limitado: o programa não pode controlar completamente um dispositivo pessoal. Os controlos ao nível da aplicação são a abordagem mais viável.	Permite a gestão total de dispositivos móveis (MDM), a encriptação e a configuração dos dispositivos sob o controlo do programa.	Aplica controlos completos ao nível do dispositivo aos dispositivos adquiridos no âmbito do programa e utilizados em fluxos de trabalho de maior risco, tais como pagamentos e administração do sistema. Os dispositivos pessoais utilizados para outras funções funcionam sob controlos ao nível das aplicações.



Dimensão da decisão	Favorece o modelo BYOD	Favorece a estratégia apenas POD	BYOD híbrido
Responsabilidade por perdas e danos	Ambíguo, a menos que a política BYOD defina claramente a responsabilidade antes do registo.	O programa assume a totalidade dos custos decorrentes de perdas e danos em todos os dispositivos.	A responsabilidade recai sobre o proprietário do dispositivo. Os dispositivos adquiridos no âmbito do programa estão cobertos pelo programa; os dispositivos pessoais regem-se pelos termos definidos na política BYOD.
Gestão pós-campanha	Não é necessária a devolução do dispositivo, mas é necessário proceder à remoção remota da aplicação e à eliminação dos dados, o que deve ser verificado.	Todos os dispositivos devem ser recolhidos após cada campanha, armazenados de forma segura, sujeitos a manutenção e reutilizados em campanhas subsequentes, sempre que aplicável.	Mais simples do que se verifica na estratégia apenas POD, uma vez que apenas os dispositivos pertencentes ao programa requerem recolha, armazenamento e manutenção. É necessário proceder à remoção remota da aplicação e à eliminação dos dados nos dispositivos pessoais.
Equidade e inclusão	Risco de exclusão nos casos em que alguns colaboradores, nomeadamente mulheres e colaboradores mais velhos, não disponham de smartphones compatíveis.	Assegura a igualdade de acesso, independentemente da posse de dispositivos pessoais.	Aborda diretamente o risco de desigualdade, atribuindo os dispositivos adquiridos no âmbito do programa aos colaboradores que não dispõem de um smartphone compatível ou que optam por não aderir ao modelo BYOD.

Não existe nenhum modelo que se adeque a todas as campanhas. A escolha deve basear-se nos resultados do recenseamento de

dispositivos ([Secção 2.2.1](#)), na análise de custos ([Secção 2.2.6](#)) e na avaliação da prontidão da força de trabalho, da sensibilidade dos dados e



do risco operacional. Na maioria dos contextos, o modelo BYOD híbrido proporciona o melhor equilíbrio entre eficiência de custos, inclusão e gestão de riscos. O modelo BYOD puro pode ser adequado nos casos em que a taxa de posse de smartphones é muito elevada e nenhuma das funções da campanha requer controlos de segurança reforçados. O modelo apenas POD

deve ser considerado em situações nas quais a posse de smartphones entre a força de trabalho-alvo é baixa, nas quais os requisitos nacionais de proteção de dados restringem a utilização de dispositivos pessoais ou nas quais está prevista a reutilização dos dispositivos em vários ciclos ou em diferentes atividades/intervenções.

2. ÂMBITO E CASOS DE UTILIZAÇÃO DO MODELO BYOD EM CAMPANHAS DE MTI

2.1 Em que situações o modelo BYOD é adequado ou não

O modelo BYOD não é adequado para todas as campanhas, funções ou locais. A utilização deste modelo depende do contexto operacional, do perfil da força de trabalho, dos requisitos dos sistemas digitais, da capacidade da gestão do programa para gerir riscos e do alinhamento com as políticas governamentais em matéria de dados. As consequências da implementação do modelo BYOD em condições inadequadas vão além da perturbação operacional: se a recolha de dados falhar devido à incompatibilidade dos dispositivos ou à incapacidade dos colaboradores de os utilizarem de forma eficaz, os agregados familiares podem ficar por registar e as famílias podem não receber os MTI de que necessitam.

Na maioria das campanhas de MTI, o modelo BYOD é mais adequado para funções operacionais de menor risco, tais como o registo de agregados familiares, o registo de distribuições e as atividades de supervisão e monitorização, especialmente nos casos em que o acesso a smartphones é elevado e a conectividade é adequada. No entanto, o modelo BYOD também pode ser utilizado em atividades que envolvam dados pessoais ou sensíveis, contanto que sejam implementadas medidas de salvaguarda adequadas para assegurar a proteção dos dados, a segurança e a responsabilização. O aspeto fundamental a ter em consideração

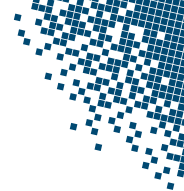
não é a possibilidade de haver dados pessoais envolvidos, mas sim a possibilidade de aplicar controlos suficientes sobre a forma como os dados são acedidos, armazenados e transmitidos. Nos casos em que seja mais difícil assegurar tais controlos ou em que sejam necessários níveis mais elevados de garantia e supervisão, os dispositivos pertencentes ao programa poderão revelar-se mais adequados.

A adequação pode também variar em função da área geográfica. O modelo BYOD é, em geral, mais viável em áreas urbanas e periurbanas com ligação à Internet fiável, acesso a pontos de carregamento e utilização generalizada de smartphones. Em zonas rurais, remotas ou afetadas por conflitos, com fraca cobertura de Internet, possibilidades limitadas de carregamento ou baixa penetração dos smartphones, os dispositivos pertencentes ao programa ou uma abordagem híbrida poderão revelar-se mais adequados. Nos casos em que nem todos os critérios e condições de adequação definidos possam ser cumpridos, um modelo híbrido é geralmente a opção mais prática

Antes de adotar o modelo BYOD, os programas devem avaliar se estão reunidas as condições mínimas a nível técnico, de políticas e de implementação. O Quadro 3 apresenta um enquadramento simples para essa avaliação.

Quadro 3: Quadro de adequação para a adoção do modelo BYOD

Utilizar o modelo BYOD nas situações em que:	Limitar ou evitar o modelo BYOD nas situações em que:	Não utilizar o modelo BYOD nas situações em que:
A taxa de posse de smartphones entre os colaboradores da campanha é suficientemente elevada para cobrir a maioria das funções necessárias.	O acesso a dispositivos adequados é extremamente desigual e muitos dos quadros de colaboradores necessários não dispõem de smartphones que cumpram os requisitos mínimos.	O dispositivo não cumpre os requisitos mínimos de segurança (root, jailbreak, sem suporte para encriptação, sem bloqueio de ecrã).
Os colaboradores já utilizam smartphones noutros programas de saúde digital.	É provável que as lacunas em matéria de literacia digital afetem significativamente a qualidade da implementação e a fiabilidade dos dados.	A política nacional ou a autoridade de proteção de dados proíbem explicitamente o tratamento de dados pessoais em dispositivos pessoais no que diz respeito à categoria de dados em questão.
A funcionalidade offline e a sincronização foram testadas e confirmadas.	É provável que os desafios relacionados com a conectividade e a sincronização comprometam a integralidade ou a pontualidade dos dados.	As tarefas requerem o armazenamento ou o processamento de grandes volumes de credenciais financeiras ou dados bancários; utilizar dispositivos pertencentes ao programa para todos os fluxos de trabalho de pagamentos.
É possível prestar assistência técnica para uma vasta gama de dispositivos.	A capacidade de assistência técnica é demasiado limitada para gerir eficazmente a diversidade de dispositivos.	O programa não é capaz de disponibilizar uma alternativa de exclusão ou uma compensação razoável pela utilização de dispositivos pessoais.
Os prazos ou os orçamentos tornam impraticável a aquisição em grande escala de dispositivos pertencentes ao programa.	Os riscos de segurança não podem ser mitigados a um nível aceitável com os recursos disponíveis.	
As medidas mínimas de segurança e de proteção de dados podem ser aplicadas de forma consistente.	Os dados altamente sensíveis não podem ser suficientemente minimizados, protegidos ou isolados em dispositivos pessoais.	
Existe um quadro claro de incentivos, compensação e responsabilização.	Os requisitos políticos, jurídicos ou de governação continuam por resolver.	



2.2 Avaliar a viabilidade e a prontidão do modelo BYOD

O modelo BYOD não deve ser adotado por predefinição. Antes de optarem pelo modelo BYOD como modalidade de campanha, os PNM devem avaliar o panorama dos dispositivos, a prontidão da aplicação, as restrições de conectividade, os requisitos legais e de proteção de dados, as implicações em termos de inclusão da força de trabalho, a capacidade de assistência técnica e o risco global de implementação. Sempre que sejam identificadas lacunas significativas, estas devem ser colmatadas antes da implementação ou, em alternativa, deve ser utilizada uma abordagem híbrida ou baseada em dispositivos pertencentes ao programa.

Na prática, a avaliação deve começar durante a fase de macroplaneamento, e não depois de a plataforma da campanha já ter sido selecionada. O Anexo 1 apresenta uma lista de verificação para a avaliação da prontidão para o modelo BYOD, abrangendo os principais domínios a analisar durante o macroplaneamento.

2.2.1 Panorama dos dispositivos e requisitos mínimos dos dispositivos

Uma avaliação do modelo BYOD deve começar por uma análise sobre que dispositivos os colaboradores da campanha possuem e se estes

dispositivos são compatíveis com a aplicação da campanha. Não basta ter um smartphone. Os PNM devem utilizar o formulário de registo e consentimento do modelo BYOD (Anexo 2) para recolher informações básicas sobre o tipo de dispositivo, modelo, sistema operativo, capacidade de armazenamento, bateria, GPS, câmara e estado do bloqueio do ecrã, e, em seguida, classificar os utilizadores por zona e função como totalmente compatíveis, compatíveis com condições ou não compatíveis. O [Anexo 2, parte 2](#) (inventário de dispositivos e verificação das especificações) é um exemplo de inventário de utilizadores e de confirmação de compatibilidade.

Os utilizadores que não cumpram os requisitos mínimos devem receber apoio através de um conjunto de dispositivos destinados a empréstimo ou de uma solução alternativa. O Quadro 4 apresenta os requisitos mínimos indicativos dos dispositivos para a participação no modelo BYOD, com base nos requisitos funcionais comuns observados nas ferramentas de recolha de dados de campanhas digitais e nas especificações típicas necessárias para assegurar a compatibilidade, a possibilidade de utilização e a segurança dos dados nas operações no terreno. Os limiares finais devem ser confirmados durante o planeamento da campanha, com base na aplicação selecionada.

Quadro 4: Exemplo de requisitos mínimos dos dispositivos para a participação no modelo BYOD

Especificação	Requisito mínimo	Notas
Sistema operativo	Android 8.0 ou posterior (nível de API 26 ou superior) ou iOS 13 ou posterior	Confirmar o nível exato da API junto do programador da aplicação.
RAM	2 GB	Os dispositivos com 1 GB podem abrir a aplicação, mas é provável que deixem de funcionar em condições reais de utilização.
Armazenamento interno gratuito	Mínimo de 2 GB antes da instalação da aplicação	Deve cobrir a aplicação, a cache de dados offline para 2–3 dias e os anexos multimédia.
Desempenho da bateria	Suficiente para um dia de trabalho completo (mínimo de 6–8 horas)	Avaliar o estado real da bateria, e não apenas a capacidade original indicada.



Especificação	Requisito mínimo	Notas
Tamanho do ecrã	Pelo menos 5,0 polegadas	Os ecrãs mais pequenos aumentam a dificuldade de navegação e os erros na introdução de dados.
GPS	Obrigatório quando a aplicação recolhe dados de localização	Confirmar o limiar de precisão aceitável do GPS, geralmente dentro de 20 metros.
Câmara	Obrigatório quando a aplicação utiliza a leitura de códigos QR/códigos de barras	Realizar testes em modelos de dispositivos comuns de gama baixa na área da campanha.
Encriptação	O dispositivo suporta encriptação ao nível da aplicação ou de todo o disco	A encriptação de todo o disco está ativada por predefinição no Android 6.0 ou posterior e no iOS 8 ou posterior.
Segurança	Bloqueio do ecrã ativado	A ausência de um bloqueio do ecrã constitui um critério de exclusão absoluto.
Segurança	Dispositivo sem root ou jailbreak	Os dispositivos com root ou jailbreak constituem um critério de exclusão absoluto.

2.2.2 Viabilidade jurídica, política e em matéria de proteção de dados

A viabilidade jurídica e política deve ser analisada numa fase inicial. Se a legislação nacional, a política ministerial ou as regras do programa não permitirem que os dados relevantes sejam tratados em dispositivos pessoais, o modelo BYOD não deve ser utilizado.

Os gestores do programa devem:

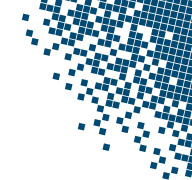
- Analisar as regras nacionais em matéria de proteção de dados e de dados de saúde.
- Confirmar se o tratamento em dispositivos pessoais é permitido.
- Identificar quaisquer requisitos relativos à localização de dados ou à hospedagem.
- Classificar os dados da campanha por nível de confidencialidade.
- Realizar uma avaliação do impacto sobre a proteção de dados sempre que existam dados de risco elevado envolvidos.

Nos casos em que os dados de GPS possam representar um risco, especialmente em contextos afetados por conflitos ou sensíveis, os programas devem reduzir a precisão, restringir o acesso, evitar a localização ao nível do agregado familiar ou seguir outras políticas nacionais ou subnacionais, conforme adequado.

2.2.3 Equidade, inclusão e mecanismos de exclusão

O modelo BYOD não deve criar nem reforçar desigualdades na participação na campanha. A prontidão deve ser avaliada de forma desagregada por género, faixa etária, quadro e área geográfica. Em muitos contextos, as mulheres voluntárias e os colaboradores mais velhos apresentam taxas mais baixas de posse de smartphones e de literacia digital.

- A participação no modelo BYOD deve ser verdadeiramente voluntária; os colaboradores não devem ser penalizados por se recusarem a utilizar um dispositivo pessoal.
- Deve existir sempre uma alternativa viável, como um dispositivo destinado a empréstimo pertencente ao programa ou uma função que não envolva o modelo BYOD no âmbito da campanha.



- As estruturas de incentivos não devem ser concebidas de forma a obrigar à participação; a participação no modelo BYOD deve ser dissociada da elegibilidade para pagamento.
- Deve ser previsto no orçamento e previamente preparado um conjunto de dispositivos destinados a empréstimo que cubra, pelo menos, cinco a dez por cento da força de trabalho que se pretende que adote o modelo BYOD.

2.2.4 Conectividade, prontidão para funcionamento offline e adequação à plataforma

O planeamento deve basear-se nas condições de campo mais desfavoráveis previsíveis, e não na cobertura média da rede.

- Mapear a conectividade por zona de campanha e testar o desempenho da sincronização em áreas representativas com fraca conectividade.
- A aplicação deve funcionar de forma totalmente offline para todos os fluxos de trabalho essenciais. O armazenamento local deve ter uma capacidade suficiente para, pelo menos, dois a três dias de registos sem sincronização.
- Definir pontos de sincronização (unidades de saúde, escolas, serviços distritais) e a frequência prevista para a sincronização, que deve ser, pelo menos, diariamente durante a distribuição ativa.
- Confirmar se a lógica de prevenção de duplicados funciona no modo offline, e não apenas quando ligado à Internet.
- Os supervisores devem ser capazes de identificar que dispositivos não se sincronizaram no período previsto; esta é uma funcionalidade obrigatória para o painel de monitorização.

A plataforma deve ser testada nos tipos de dispositivos que os colaboradores da campanha efetivamente detêm, incluindo modelos Android de gama baixa, comuns em muitos contextos.

2.2.5 Disposições de segurança e apoio

Na maioria dos contextos de campanhas de MTI, os controlos de segurança ao nível das aplicações, incluindo encriptação, autenticação e cancelamento da autenticação remoto, combinados com uma supervisão operacional rigorosa, constituem a abordagem mais viável.

No mínimo:

- Os dispositivos que tenham sido modificados para contornar os controlos de segurança padrão do sistema operativo (dispositivos Android com root, iPhones com jailbreak) não devem ser autorizados.
- Os dados da campanha não devem ser exportados para aplicações pessoais. Devem ser implementados controlos técnicos adequados para impedir ou restringir tais exportações, sempre que tal seja viável.
- Os dispositivos devem ter o bloqueio do ecrã ativado.
- O acesso deve ser baseado em funções.
- As sessões dos utilizadores devem expirar automaticamente após um período de inatividade.

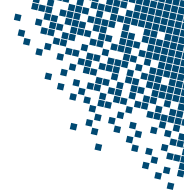
Uma frota heterogénea de dispositivos pessoais coloca maiores exigências ao apoio técnico do que uma frota de POD padronizada. Deve existir uma estrutura de apoio em vários níveis antes da implementação.

2.2.6 Considerações sobre os custos

O modelo BYOD pode reduzir os custos de aquisição de dispositivos, mas não elimina os custos do programa. Os programas devem comparar o custo total do modelo BYOD com o custo dos dispositivos pertencentes ao programa, em vez de se concentrarem apenas nos custos de aquisição dos telemóveis. O Quadro 5 apresenta uma comparação de custos entre as duas abordagens.

Quadro 5: Comparação de custos entre o modelo BYOD e o modelo com dispositivos pertencentes ao programa (POD)

Categoria de custos	Abordagem BYOD	Abordagem POD	Nível de alteração dos recursos (BYOD vs. POD)
Aquisição de dispositivos	Não há custos diretos para o programa.	A totalidade dos custos é suportada pelo programa.	Inferior
Pacotes de dados/tempo de antena	Subsídio, ajuda de custo ou reembolso para fins de campanha.	O programa adquire cartões SIM e planos de dados para todos os dispositivos.	Igual
Apoio técnico	Superior, devido à variação nos tipos e configurações dos dispositivos.	Inferior, uma vez que os dispositivos são padronizados e pré-configurados.	Superior
Formação	Ligeiramente superior, uma vez que a variedade de dispositivos aumenta os requisitos de formação.	Mais padronizado, uma vez que todos os dispositivos são iguais.	Superior
Perda/danos no dispositivo	Responsabilidade definida pela política; as compensações são geralmente limitadas.	A totalidade dos custos de substituição é suportada pelo programa.	Inferior
Recuperação pós-campanha	Não é necessária qualquer recolha de dispositivos; é necessário remover o acesso à campanha e os dados.	Os dispositivos são recolhidos após cada campanha, armazenados, sujeitos a manutenção e reutilizados em outras campanhas, sempre que aplicável.	Inferior
Gestão de dispositivos/licenciamento	Geralmente limitados a controlos ao nível da aplicação, com um custo mais baixo.	Poderá ser necessária uma gestão completa dos dispositivos, o que implica custos mais elevados.	Inferior
Conjunto de dispositivos destinados a empréstimo	Normalmente, é necessário para 5 a 10% da força de trabalho.	Embora geralmente não seja obrigatório, é necessário dispor de um stock de contingência para a implementação.	Inferior
Gestão de resíduos eletrónicos	Não aplicável ao programa.	Obrigatório no final da vida útil dos dispositivos.	Inferior



2.2.7 Reembolso e compensação

Os colaboradores não devem arcar com os custos da digitalização da campanha a partir dos respetivos recursos pessoais. As medidas de compensação devem ser definidas antes do início da implementação:

- Cartões SIM com pacote de dados pré-pago, emitidos durante a formação.
- Um subsídio diário fixo para dados ou um montante estipulado com base no trabalho, pago juntamente com outros subsídios da campanha.
- Acesso a dados com zero rating para a plataforma da campanha, o que requer negociação com a operadora de telecomunicações nacional e é viável em alguns países.

2.2.8 Decisão relativa à fase piloto e à expansão

- O modelo BYOD deve ser testado numa fase piloto antes de ser implementado de forma mais abrangente, especialmente nos casos em que está a ser utilizado pela primeira vez ou nos quais a conectividade e a qualidade dos dispositivos variam de local para local. Os locais-piloto devem refletir as principais condições de implementação previstas para a campanha. O programa só deve ser expandido quando o projeto-piloto demonstrar que:
- A maioria dos utilizadores do modelo BYOD registados consegue enviar registos válidos.
- A sincronização decorre dentro dos prazos previstos.
- A integralidade dos dados é aceitável.
- Os problemas técnicos podem ser resolvidos rapidamente.
- O recurso ao papel ou aos dispositivos pertencentes ao programa mantém-se limitado.

Nos casos em que os resultados da fase-piloto revelem lacunas significativas, estas devem ser corrigidas antes de se proceder à implementação em maior escala ou de se reduzir o âmbito do modelo BYOD.

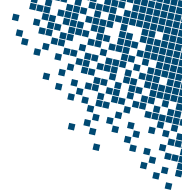
2.2.9 Plano de avaliação e mitigação de riscos

A utilização de dispositivos pessoais acarreta riscos operacionais, técnicos e relacionados com a proteção de dados, os quais devem ser identificados e geridos atempadamente. Estes riscos devem ser avaliados durante a fase de planeamento e devem ser implementadas medidas práticas de mitigação antes da implementação. O quadro 6 abaixo resume os riscos comuns associados ao modelo BYOD e as medidas de mitigação sugeridas.

NOTA: O quadro relativo aos riscos e às medidas de mitigação encontra-se também reproduzido em Excel, sob a forma de uma ferramenta adaptável anexada ao documento. Esta ferramenta pode ser descarregada e adaptada pelos PNM que estejam a considerar a adoção de uma estratégia BYOD, a fim de servir de base ao respetivo *Plano de avaliação e mitigação de riscos*.

Quadro 6: Principais áreas de risco do modelo BYOD, prioridades e medidas de mitigação *(também disponível sob a forma de uma ferramenta adaptável em Excel)*

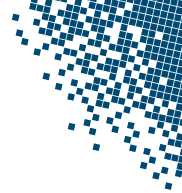
Categoria	Área de risco	Exemplo de risco	Medidas de mitigação
Técnica	Compatibilidade dos dispositivos	Os dispositivos pessoais não cumprem os requisitos mínimos das aplicações	Definir as especificações mínimas dos dispositivos; realizar um recenseamento e uma verificação dos dispositivos antes da implementação; manter um conjunto de dispositivos destinados a empréstimo
Técnica	Desempenho dos dispositivos	Baixa autonomia da bateria, capacidade de armazenamento limitada, falhas nas aplicações ou baixa precisão do GPS	Testar a aplicação em tipos de dispositivos comuns; exigir requisitos mínimos de RAM e armazenamento; disponibilizar orientações sobre o carregamento ou a utilização de power banks, sempre que possível
Técnica	Apoio técnico	A coexistência de diferentes tipos de dispositivos resulta num aumento das necessidades de apoio em relação ao esperado	Estabelecer um sistema de apoio por níveis; elaborar orientações para a resolução de problemas; formar os supervisores para a resolução de problemas básicos
Técnica	Estabilidade da plataforma	Uma falha na aplicação ou na plataforma perturba a implementação da campanha	Testar a plataforma antes da implementação; definir procedimentos de expansão; assegurar o apoio do fornecedor e estabelecer medidas alternativas



Categoria	Área de risco	Exemplo de risco	Medidas de mitigação
Operacional	Conectividade e sincronização	A fraca cobertura de rede atrasa a sincronização e afeta a monitorização em tempo real	Utilizar aplicações que privilegiem o modo offline; definir pontos e horários de sincronização; assegurar a monitorização dos dispositivos não sincronizados por parte de um supervisor; elaborar um plano alternativo com recurso a papel ou POD, sempre que necessário
Operacional	Qualidade dos dados	As taxas de literacia digital inconsistentes ou a falta de familiaridade com os fluxos de trabalho podem resultar em registos incompletos ou imprecisos	Ministrar formação prática e orientada para as funções; simplificar os formulários; utilizar a validação na aplicação e a lógica de exclusão; reforçar a revisão por parte dos supervisores
Operacional	Duplicação e fraude	Vários registos relativos ao mesmo agregado familiar ou registos não autorizados	Utilizar identificadores únicos, verificações de duplicados, registos de auditoria e revisão por parte de um supervisor; aplicar validação do lado do servidor sempre que possível
Operacional	Comunicação de incidentes	A perda de dispositivos, a utilização indevida ou os problemas técnicos não são comunicados com a rapidez necessária	Estabelecer um processo claro de comunicação de incidentes; ministrar formação aos utilizadores e supervisores sobre os passos a seguir em caso de escalada; divulgar amplamente os contactos de apoio



Categoria	Área de risco	Exemplo de risco	Medidas de mitigação
Segurança	Proteção de dados e privacidade	Os dados pessoais e os dados de campanha coexistem no mesmo dispositivo, o que aumenta o risco de acesso ou partilha não autorizados	Utilizar um sistema de início de sessão seguro, acesso baseado em funções e encriptação; restringir a exportação de dados; exigir o bloqueio do ecrã; disponibilizar orientações claras sobre a utilização aceitável
Segurança	Perda ou roubo de dispositivos	Um dispositivo que contém dados da campanha é perdido, roubado ou substituído durante a implementação	Exigir a comunicação imediata de incidentes; permitir a desativação remota ou a eliminação de dados, sempre que possível; limitar o armazenamento local dos dados; verificar os dispositivos de substituição antes da utilização dos mesmos
Segurança	Utilização partilhada de dispositivos	Os membros do agregado familiar ou outros utilizadores acedem à aplicação da campanha ou aos dados num telemóvel partilhado	Exigir contas de utilizador individuais; proibir a partilha de contas; avaliar se o modelo BYOD é adequado nos casos em que não seja possível assegurar a utilização de dispositivos privados
Segurança	Configuração insegura do dispositivo	Os dispositivos com root ou jailbreak contornam os controlos de segurança	Excluir dispositivos com root ou jailbreak da participação no modelo BYOD; verificar o estado do dispositivo durante o registo
Segurança	Dados que permanecem pós-campanha	Os dados da campanha permanecem nos dispositivos pessoais após o término da campanha	Aplicar um procedimento de encerramento; desativar contas; apagar os dados locais sempre que necessário; realizar verificações aleatórias sempre que possível



Categoria	Área de risco	Exemplo de risco	Medidas de mitigação
Segurança	Dados de localização sensíveis	Os dados de GPS revelam a localização de agregados familiares em zonas afetadas por conflitos ou politicamente sensíveis	Reduzir a precisão do GPS sempre que necessário; restringir a exportação de dados de localização; avaliar o risco por zona antes da implementação
Jurídica/governança	Governança e responsabilização	Responsabilidade pouco clara por incidentes relacionados com dispositivos, violações de políticas ou incumprimento	Definir as responsabilidades dos utilizadores, os procedimentos de comunicação de incidentes e as consequências do incumprimento numa política simples relativa ao modelo BYOD
Jurídica/governança	Conformidade regulamentar	O tratamento de dados do agregado familiar em dispositivos pessoais está sujeito a restrições impostas pela legislação nacional ou pelas autoridades nacionais	Analisar atempadamente os requisitos legais; realizar uma Avaliação do impacto na proteção de dados (DPIA), sempre que adequado; colaborar com as autoridades competentes; limitar a recolha de dados pessoais ao mínimo operacional
Jurídica/governança	Funções de alto risco	As atividades sensíveis, tais como pagamentos em massa ou administração do sistema, são realizadas em dispositivos pessoais	Restringir as funções de alto risco aos dispositivos pertencentes ao programa e controlados pelo mesmo
Equidade/RH	Equidade e inclusão	Alguns colaboradores não têm smartphones adequados ou preferem não utilizar os respetivos dispositivos pessoais	Tornar o modelo BYOD voluntário; disponibilizar dispositivos pertencentes ao programa ou destinados a empréstimo; recorrer a uma implementação híbrida sempre que necessário



Categoria	Área de risco	Exemplo de risco	Medidas de mitigação
Equidade/RH	Coação ou pressão injusta para participar	Os colaboradores sentem-se obrigados a utilizar dispositivos pessoais para continuarem a ter direito ao emprego ou ao pagamento	Distinguir a participação no modelo BYOD da elegibilidade para pagamento; disponibilizar opções de exclusão; comunicar a política de forma clara durante a formação
Equidade/RH	Compreensão da política	Os colaboradores não compreendem totalmente as condições e responsabilidades relacionadas decorrentes do modelo BYOD	Utilizar uma linguagem simples e expressões típicas do idioma local; disponibilizar explicações orais e verificar a compreensão durante a formação
Financeira/sustentabilidade	Incentivos e reembolso	Os colaboradores têm de suportar custos relacionados com dados ou com carregamentos e sentem-se tratados de forma injusta	Definir condições de compensação claras antes da implementação; disponibilizar pacotes de dados, subsídios ou outro tipo de apoio
Financeira/sustentabilidade	Expectativas relativas à substituição de dispositivos	Os colaboradores esperam que o programa substitua os dispositivos pessoais danificados ou perdidos	Definir e comunicar uma política clara sobre substituição, reparação e indemnização antes da implementação
Financeira/sustentabilidade	Acessibilidade financeira a longo prazo	Os subsídios destinados ao modelo BYOD utilizados numa campanha não são sustentáveis em campanhas futuras	Definir níveis de apoio realistas; documentar as estimativas de custos; alinhar com a orçamentação do programa a longo prazo
Reputação	Confiança da comunidade	As comunidades manifestam preocupação quanto à utilização indevida de dados quando os colaboradores das campanhas utilizam os seus telemóveis pessoais	Realizar ações de sensibilização da comunidade; utilizar modelos de consentimento claros e mensagens sobre privacidade; monitorizar e responder rapidamente aos rumores

3. POLÍTICA, PRIVACIDADE E SEGURANÇA

Esta secção define o enquadramento de governação para a utilização de dispositivos pessoais nas campanhas de MTI. Esta abrange a elaboração de políticas de BYOD, idealmente alinhadas com as políticas do Ministério da Saúde, sempre que estas existam, e adaptadas conforme necessário aos requisitos específicos

de cada programa ou campanha. Isto inclui regras de utilização aceitável, normas de segurança, governação de dados e resposta a incidentes. Uma governação clara protege os dados da campanha, os colaboradores e as comunidades a que a campanha se destina.

3.1 Elaboração da política de BYOD

Uma política de BYOD define as condições mediante as quais os dispositivos pessoais podem ser utilizados no âmbito do trabalho da campanha. Esta deve ser redigida, aprovada pela direcção do PNM, submetida a revisão jurídica sempre que necessário e disponibilizada nos principais idiomas utilizados na área da campanha antes do início da implementação. No [Anexo 4](#), é apresentado um modelo de Política e Termos de Utilização.

No mínimo, a política deve definir:

- Quem pode participar e que dispositivos e funcionalidades da campanha estão abrangidos.
- O que os utilizadores podem e não podem fazer nos dispositivos pessoais utilizados para o trabalho da campanha.

- Requisitos mínimos relativos aos dispositivos e à segurança.
- Requisitos relativos ao tratamento de dados, incluindo o armazenamento, a transmissão, a conservação e a eliminação.
- Disposições relativas ao apoio, à compensação e à responsabilidade.
- Procedimentos de comunicação e resposta a incidentes.
- Consequências do incumprimento.

A política deve ser explicada oralmente durante a formação, e não apenas apresentada por escrito para assinatura. Os colaboradores devem compreender as regras e as implicações do modelo BYOD antes de concluírem o registo.

3.2 Definir a utilização aceitável e as responsabilidades

Os utilizadores só podem utilizar os respetivos dispositivos pessoais para trabalhos aprovados das campanhas. Isto inclui a utilização de aplicações aprovadas pelo programa para as tarefas atribuídas, a comunicação com os supervisores através dos canais aprovados e o acesso a materiais de formação ou de referência aprovados. A fotografia para fins de campanha não é recomendada e só deve ser permitida nos casos em que seja explicitamente aprovada e em que existam procedimentos de consentimento em vigor.

Os utilizadores não devem copiar, exportar ou partilhar dados de campanhas fora dos canais aprovados, inclusive através de e-mail pessoal, armazenamento pessoal na nuvem ou aplicações de mensagens pessoais. Estes não devem fazer capturas de ecrã dos dados de nenhum membro da comunidade, partilhar credenciais de acesso nem permitir que pessoas não autorizadas acedam às aplicações da campanha.



Durante a formação, deve ser fornecido aos colaboradores um modelo padrão de consentimento oral, e estes devem ser capazes de explicar, por palavras próprias, aos membros dos agregados familiares que informações estão a ser recolhidas, por que razão são necessárias e quem terá acesso às mesmas. Ao participarem no modelo BYOD, os utilizadores aceitam as seguintes responsabilidades: manter o seu dispositivo seguro e atualizado; tratar os dados da campanha de acordo com as regras do programa; comunicar imediatamente quaisquer incidentes; cooperar com a supervisão do programa; tratar os dados dos membros da

comunidade com respeito. A participação no modelo BYOD deve ser voluntária. Os colaboradores que optem por ser excluídos do modelo não devem ser penalizados e devem ter acesso a uma solução alternativa.

A gestão do programa também tem as suas responsabilidades. Esta deve comunicar claramente as regras relativas ao modelo BYOD, proporcionar orientação e apoio, aplicar a política de forma consistente e proteger a privacidade dos colaboradores, na medida do possível, mantendo simultaneamente a segurança dos dados da campanha.

3.3 Definir controlos mínimos de segurança e de acesso

Todos os dispositivos utilizados no âmbito do modelo BYOD devem cumprir os requisitos mínimos de segurança. No mínimo, os dispositivos devem ter o bloqueio do ecrã ativado, não devem ter sido submetidos a root ou jailbreak, devem cumprir os requisitos mínimos do sistema operativo aprovado e devem instalar a aplicação da campanha apenas a partir de uma fonte aprovada. A encriptação deve ser ativada sempre que for suportada. Consulte a lista de verificação das especificações e da verificação do dispositivo no [Anexo 2](#).

Deverão também ser aplicados controlos de acesso mínimos. Estas medidas devem incluir a autenticação dos utilizadores na aplicação da campanha, o acesso baseado em funções para

que os utilizadores vejam apenas os dados e as funções de que necessitam, o tempo limite automático da sessão após um período de inatividade e a desativação imediata do acesso quando um utilizador sai da campanha ou quando um dispositivo é comprometido.

As contas de campanha não devem ser partilhadas entre utilizadores. Nos casos em que um dispositivo seja partilhado no seio de um agregado familiar, o modelo BYOD só deverá ser utilizado se a aplicação da campanha e a conta permanecerem acessíveis exclusivamente ao utilizador registado. Caso tal não possa ser assegurado, deverá ser encontrada uma solução alternativa.

3.4 Estabelecer regras de governação e armazenamento de dados

Os PNM devem recolher apenas os dados necessários para as operações da campanha. Para cada campo de formulário proposto, deve ser ponderado que decisão ou ação específica do programa requer estes dados. Eliminar quaisquer campos para os quais não exista uma resposta operacional clara ou cujos dados sejam utilizados apenas para efeitos de elaboração de relatórios.

Os PNM devem definir que dados são recolhidos; durante quanto tempo os dados perma-

necem no dispositivo antes da sincronização; em que momento os dados locais devem ser apagados; e quem pode exportar ou aceder aos conjuntos de dados após a campanha.

Os dados da campanha incluem todos os dados pessoais, sensíveis e operacionais recolhidos durante as atividades do programa. Os dados devem ser armazenados no contentor encriptado da aplicação e sincronizados automaticamente com o servidor assim que se veri-

fique uma ligação à Internet. Os dados não devem ser mantidos no dispositivo para além do necessário do ponto de vista operacional — o máximo recomendado é de 72 horas após a última sincronização bem-sucedida. Os colaboradores não devem fazer cópias de segurança dos dados da campanha em contas pessoais na nuvem, e as definições das aplicações devem impedir esta ação sempre que possível. Quanto menos dados estiverem armazenados no dispositivo num determinado momento, menor será o risco em caso de perda, partilha ou comprometimento do dispositivo.

Sempre que tal for possível, deve ser definida uma abordagem de desativação remota ou de eliminação remota dos dados da campanha. Isto deve aplicar-se em casos de perda ou roubo de dispositivos, violação confirmada da política, incidente de segurança grave ou encerramento da campanha. Nos casos em que não se recorra a uma MDM completa, a política deve deixar claro que a eliminação remota se aplica apenas aos dados da campanha e não ao conteúdo pessoal do colaborador.

3.5 Resposta a incidentes relacionados com dispositivos perdidos, partilhados ou comprometidos

Os PNM devem estabelecer um processo simples de comunicação e resposta a incidentes antes do início da implementação. Este deve abranger:

- Dispositivos perdidos ou roubados
- Tentativas falhadas de início de sessão ou suspeitas de utilização indevida da conta
- Partilha accidental de dados
- Substituição do dispositivo durante a campanha

- Mau funcionamento da aplicação que afeta a integridade dos dados
- Suspeita de violação de dados ou acesso não autorizado

Todos os utilizadores devem comunicar qualquer incidente de segurança, incluindo a perda ou roubo de dispositivos, suspeitas de violações de dados ou acesso não autorizado, ao respetivo superior hierárquico direto ou ao canal de apoio de TIC designado, dentro de um prazo definido, e devem cooperar plenamente com os procedimentos de resposta a incidentes.

*Inquérito sobre a penetração
e a utilização dos telemóveis
© Togo CDM 2014*





No mínimo, o acesso à campanha deve ser prontamente desativado sempre que necessário, os dispositivos de substituição devem ser novamente verificados antes da utilização e todos os incidentes devem ser registados e analisados.

Nos casos em que a partilha de dispositivos é comum, os programas devem avaliar se o modelo BYOD é adequado para este quadro ou se é necessário implementar medidas de segurança adicionais ou soluções alternativas.

4. IMPLEMENTAÇÃO DO MODELO BYOD

Esta secção descreve os passos práticos para a implementação do modelo BYOD numa campanha de MTI. Antes da implementação, os PNM devem confirmar se a plataforma é adequada, se a política está em vigor, se a pronti-

dão dos dispositivos foi avaliada e se o orçamento necessário foi aprovado. Os passos descritos na Secção 1.2 devem ser concluídos antes do início da implementação.

4.1 Medidas alternativas

O modelo BYOD nunca deve ser a única opção operacional. Devem ser elaboradas medidas alternativas (de contingência) no âmbito do planeamento da digitalização da campanha durante a fase de macroplaneamento, e não como solução improvisada.

As medidas alternativas devem ser ativadas quando:

- Um dispositivo não passa na verificação ou é perdido, roubado ou danificado
- A aplicação não funciona de forma fiável ou a falta de conectividade impede a sua utilização operacional

- O utilizador opta por excluir-se do modelo BYOD

As medidas alternativas podem incluir:

- Dispositivos destinados a empréstimo ou dispositivos pertencentes ao programa
- Realocação do utilizador para uma função que não seja BYOD
- Registo temporário em papel, com introdução posterior dos dados
- Envio com a assistência do supervisor, sempre que apropriado

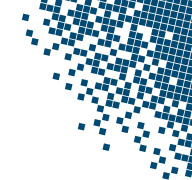
4.2 Formação

Certificar-se de que todos os proprietários de dispositivos participam nas sessões de formação com os respetivos dispositivos registados. A formação deve ser prática e específica para cada função. Esta deve abranger tanto a utilização da aplicação como as regras operacionais relativas ao modelo BYOD.

No mínimo, os utilizadores devem receber formação sobre:

- Como iniciar sessão e aceder aos formulários corretos

- Como trabalhar offline e quando sincronizar
- Como proteger os dados do dispositivo e da campanha
- O que fazer e quem contactar se a aplicação deixar de funcionar, se o dispositivo for perdido ou se a sincronização não funcionar
- A quem recorrer para obter apoio técnico
- Procedimentos operacionais normalizados (PON) da campanha



Os supervisores devem receber formação adicional sobre a verificação de dispositivos, a monitorização da sincronização, a escalada de problemas e a ativação de medidas alternativas.

Para além dos procedimentos operacionais normalizados (PON) da campanha, a formação dos colaboradores no terreno deve abranger:

- Visão geral da política de BYOD: o que está a ser aceite pelos colaboradores, o que será disponibilizado através do programa e quais são os respetivos direitos, incluindo o direito de exclusão
- Procedimento de escalada: a quem ligar para cada tipo de problema; números de contacto do apoio informático, etc.
- Prática de modelos de consentimento: exercício de simulação no qual os colaboradores praticam o ato de explicar aos membros do agregado familiar por que razão os dados estão a ser recolhidos utilizando as suas próprias palavras

4.3 Apoio e supervisão durante a implementação

O modelo BYOD requer um apoio ativo durante a implementação, especialmente quando os dispositivos variam em termos de idade, qualidade e configuração. Os PNM devem estabelecer uma estrutura de apoio em vários níveis, abrangendo os níveis local, distrital e nacional, tal como:

- Apoio a nível local para a configuração, o início de sessão e a resolução de problemas básicos
 - Apoio a nível distrital para a resolução de problemas relacionados com contas, sincronização e aplicações
 - Apoio a nível nacional ou dos parceiros em caso de falhas da plataforma, problemas com os dados e incidentes de segurança
- Os supervisores devem monitorizar regularmente:
- Se os utilizadores registados estão ativos
 - Se os dispositivos estão a ser sincronizados atempadamente
 - Se os problemas relacionados com a qualidade dos dados estão a aumentar
 - Se algum utilizador precisa de recorrer a medidas alternativas

4.4 Controlos operacionais diários

Durante a implementação, devem ser aplicados os seguintes controlos operacionais, conforme apropriado para o quadro de colaboradores, para as respetivas responsabilidades e para o nível de acesso aos sistemas e dados da campanha.

- Os utilizadores devem efetuar a sincronização de acordo com o calendário definido
 - Os supervisores devem verificar diariamente os utilizadores cujos dados não estão sincronizados
 - As verificações de duplicados e os relatórios de exceções devem ser monitorizados
 - Os dados relativos ao stock, à distribuição e à supervisão devem ser analisados para verificar se estão completos
 - Os problemas técnicos não resolvidos devem ser escalados rapidamente
- Os programas devem assegurar que estes controlos são simples e estão alinhados com os processos de gestão de campanhas existentes.

4.5 Procedimento de encerramento de equipamentos após a campanha

No final da campanha, os programas devem assegurar que o acesso no âmbito do modelo BYOD é devidamente cancelado. O procedimento de encerramento do dispositivo deve ser executado de forma sistemática e documentada, conforme apresentado no Quadro 7.

Quadro 7: Procedimento de encerramento de equipamentos após a campanha

Etapa	Ação	Verificação
Terminar remotamente a sessão	O responsável de TI termina remotamente a sessão de todas as contas registadas na consola de administração da plataforma.	A consola de administração da plataforma mostra todas as contas como não tendo sessão iniciada.
Confirmação da remoção da aplicação	O supervisor confirma que a aplicação foi removida do dispositivo durante a visita final ao local ou através de uma videochamada.	O supervisor é responsável por concluir o procedimento de encerramento do dispositivo.
Verificação da eliminação dos dados	O colaborador confirma que não restam dados da campanha em qualquer aplicação, ficheiro ou cópia de segurança na nuvem no seu dispositivo.	A conclusão deve ser confirmada mediante assinatura da lista de verificação do procedimento de encerramento.
Verificação aleatória após a campanha	O responsável de TI seleciona 10% dos colaboradores para uma verificação aleatória adicional no prazo de 14 dias.	Manutenção de um registo de verificações aleatórias.
Encerramento do inventário de dispositivos	Os equipamentos destinados a empréstimo devem ser devolvidos após cada campanha, registados no inventário, armazenados de forma segura e mantidos para reutilização em futuras campanhas ou noutras atividades do programa, com uma gestão de inventário contínua.	Inventário final assinado pelo responsável de TI do distrito.

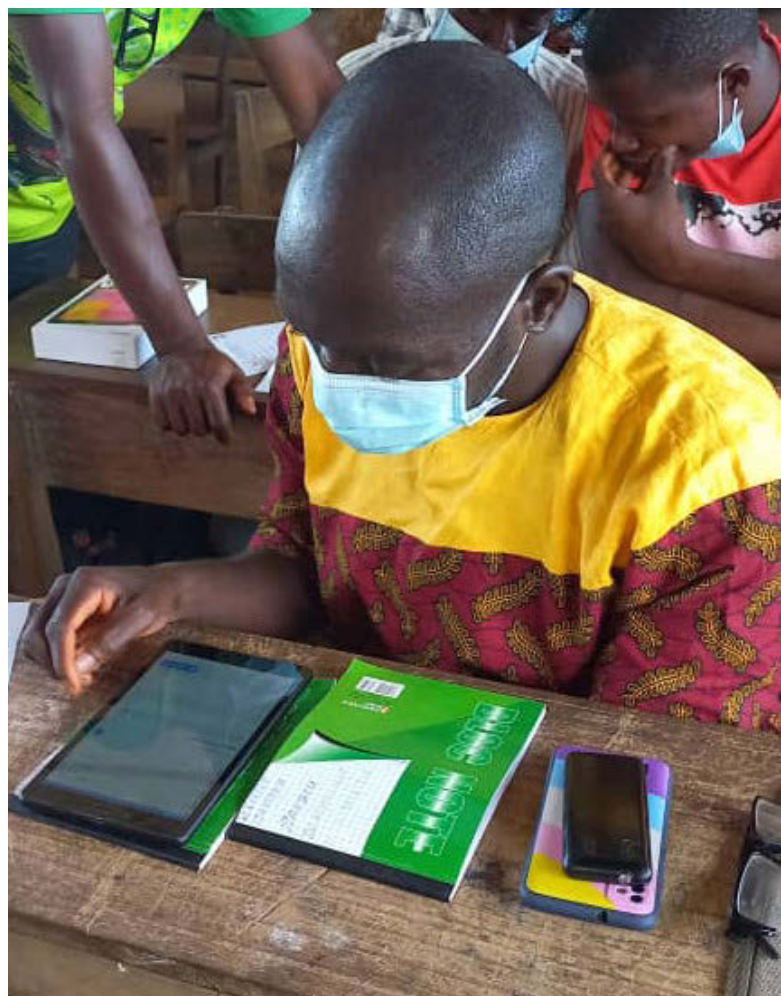
5. CONCLUSÃO

Os programas que estejam a considerar ou a expandir a implementação do modelo BYOD para a digitalização de campanhas de MTI devem adotar uma abordagem ponderada e faseada. O modelo BYOD só deve ser utilizado quando estiverem reunidas as condições políticas, técnicas, operacionais e de equidade mínimas. Este não deve ser adotado como solução por defeito nem escalado apenas por uma questão de conveniência.

O modelo BYOD pode proporcionar vantagens importantes em termos operacionais e de custos para a digitalização da campanha da MTI, mas apenas se este for implementado com uma política clara, uma avaliação realista da prontidão, medidas de salvaguarda adequadas e um acompanhamento ativo. Uma abordagem estruturada e baseada em dados concretos ajudará os PNM a utilizar o modelo BYOD nos casos em que este acrescenta valor, ao mesmo tempo que protege os dados, apoia os colaboradores e mantém a qualidade da implementação.

Referências

Doargajudhur, M. S., & Dell, P. (2020). The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation. *Journal of Computer Information Systems*, 60(6), 518–529. <https://doi.org/10.1080/08874417.2018.1543001>



Campanha na Guiné 2022

ANEXO 1: LISTA DE VERIFICAÇÃO PARA A AVALIAÇÃO DA PREPARAÇÃO PARA O MODELO BYOD

(Também disponível sob a forma de uma ferramenta adaptável em MS Word)

Preencher esta lista de verificação durante a concepção da campanha, antes da seleção da plataforma e da elaboração do orçamento.

#	Questão	Resposta	Notas/comentários
Questões jurídicas, políticas e de proteção de dados			
1	A legislação nacional ou a autoridade de proteção de dados permite o tratamento das categorias de dados relevantes em dispositivos pessoais?	☐ Sim ☐ Não ☐ Em curso	
2	Foi realizada uma avaliação do impacto sobre a proteção de dados nos casos em que existem dados de risco elevado envolvidos?	☐ Sim ☐ Não ☐ Em curso	
3	A política de BYOD já foi elaborada, submetida a revisão jurídica e aprovada pelo PNM e pelos parceiros de implementação?	☐ Sim ☐ Não ☐ Em curso	
4	A política foi traduzida para os principais idiomas da campanha?	☐ Sim ☐ Não ☐ Em curso	
Panorama dos dispositivos e requisitos			
5	Foi realizado um recenseamento de dispositivos que abrangesse, pelo menos, 80% dos colaboradores-alvo da campanha?	☐ Sim ☐ Não ☐ Em curso	
6	Pelo menos 85% dos dispositivos do recenseamento cumprem as especificações mínimas?	☐ Sim ☐ Não ☐ Em curso	
7	A aplicação foi testada em, pelo menos, três modelos representativos de dispositivos de gama baixa?	☐ Sim ☐ Não ☐ Em curso	

#	Questão	Resposta	Notas/comentários
Equidade, inclusão e opção de exclusão			
8	Foi realizada uma avaliação da literacia digital dos colaboradores-alvo da campanha?	☐ Sim ☐ Não ☐ Em curso	
9	A prontidão foi avaliada de forma desagregada por género, idade, quadro e área geográfica?	☐ Sim ☐ Não ☐ Em curso	
10	Foi elaborado um orçamento relativo a um conjunto de dispositivos destinados a empréstimo correspondente a, pelo menos, 5% da força de trabalho do modelo BYOD?	☐ Sim ☐ Não ☐ Em curso	
11	As alternativas de exclusão voluntária estão documentadas e foram comunicadas a todos os colaboradores?	☐ Sim ☐ Não ☐ Em curso	
Conectividade, segurança e plataforma			
12	A aplicação funciona de forma totalmente offline para todos os fluxos de trabalho essenciais, com 2 a 3 dias de armazenamento local?	☐ Sim ☐ Não ☐ Em curso	
13	Os controlos ao nível da aplicação estão confirmados — encriptação, autenticação, acesso baseado em funções e tempo limite de sessão?	☐ Sim ☐ Não ☐ Em curso	
14	É possível confirmar o encerramento da sessão/ cancelamento da autenticação remoto para todos os tipos de dispositivos registados?	☐ Sim ☐ Não ☐ Em curso	
Custo e compensação			
15	Foi realizada uma comparação completa dos custos entre o modelo BYOD e o modelo com dispositivos pertencentes ao programa?	☐ Sim ☐ Não ☐ Em curso	
16	Existe um modelo de reembolso ou compensação definido e comunicado antes da implementação?	☐ Sim ☐ Não ☐ Em curso	

#	Questão	Resposta	Notas/comentários
Risco e prontidão para a implementação			
17	Os riscos associados ao modelo BYOD foram avaliados, tendo os riscos residuais elevados ou críticos sido resolvidos ou formalmente aceites?	☐ Sim ☐ Não ☐ Em curso	
18	O modelo BYOD vai ser testado numa fase piloto com critérios definidos para a respetiva expansão antes da implementação total?	☐ Sim ☐ Não ☐ Em curso	

Resumo	
Comentários	
Nível de prontidão	☐ Pronto ☐ Pronto com lacunas ☐ Não pronto
Lacunas críticas a colmatar antes de prosseguir	
Realizado por	
Data	
Revisto por (PNM ou ponto focal do IP)	

ANEXO 2: Registo no modelo BYOD, verificação de dispositivos e formulário de consentimento

(Também disponível sob a forma de uma ferramenta adaptável em Excel)

Preencher um formulário por cada utilizador registado. Recolher os dados durante a formação, antes da instalação da aplicação ou, sempre que possível, antes da formação. Guardar cópias assinadas junto do coordenador distrital e do responsável pela digitalização do PNM.

Secção 1 — Informações do colaborador			
Nome completo			
Género	☐ Feminino ☐ Masculino ☐ Outro		
Cargo/função na campanha de MTI			
Organização (se aplicável)			
Distrito/ instalações/ comunidade	Distrito	Instalações	Comunidade
Número de telefone (principal)			
E-mail (se aplicável)			
Secção 2 — Identificação do dispositivo e verificação das especificações (a preencher pelo responsável de TI/supervisor)			
Item	Detalhes registados	Requisito mínimo	Resultado
Tipo de dispositivo		Smartphone ou tablet	☐ Aprovado ☐ Reprovado
Marca e modelo		Registo para o inventário	—
Sistema operativo e versão		Android 8.0 ou posterior (IPA 26 ou superior) ou iOS 13 ou posterior	☐ Aprovado ☐ Reprovado
RAM		2 GB, no mínimo	☐ Aprovado ☐ Reprovado
Armazenamento interno gratuito		2 GB antes da instalação da aplicação	☐ Aprovado ☐ Reprovado

Bateria (dia de trabalho completo)		Mínimo de 6 a 8 horas; avaliar o estado real	☐ Aprovado ☐ Cond. ☐ Reprovado
Tamanho do ecrã		Pelo menos 5,0 polegadas	☐ Aprovado ☐ Reprovado
Rede móvel		2G, no mínimo; 3G recomendado	☐ Aprovado ☐ Reprovado
GPS/serviços de localização		Funcionalidade com a qual a aplicação deteta a localização	☐ Aprovado ☐ N/A
Câmara		Funcionalidade com a qual a aplicação lê um código QR/código de barras	☐ Aprovado ☐ N/A
IMEI/número de série		Opcional	—

Registar os dados reais na coluna do meio e anotar o resultado. Um dispositivo tem de ser aprovado em todos os requisitos aplicáveis para ser aprovado como um todo.

Secção 3 — Segurança, exclusão e verificações funcionais (a preencher pelo responsável de TI/supervisor)

Verificação	Requisito	Resultado
Bloqueio do ecrã ativado	PIN, palavra-passe, padrão ou dados biométricos confirmados como ativos	☐ Aprovado ☐ Reprovado
Dispositivo SEM root ou jailbreak	Sem indícios de SuperSU, Magisk ou jailbreak. Critério de exclusão absoluto.	☐ Aprovado ☐ Reprovado
Sistema operativo atualizado	Versão mais recente disponível, sempre que possível	☐ Yes ☐ No
Encriptação ativa	Encriptação confirmada de todo o disco ou ao nível da aplicação	☐ Aprovado ☐ Reprovado
A aplicação da campanha é instalada e pode ser executada	A aplicação abre corretamente o formulário e efetua um envio de teste	☐ Aprovado ☐ Reprovado
Cancelamento remoto da autenticação confirmado	O responsável de TI confirma que o encerramento remoto da sessão funciona para esta conta	☐ Aprovado ☐ Reprovado

Um dispositivo com root ou jailbreak constitui um critério de exclusão absoluto e não pode ser registado, independentemente dos restantes resultados

Secção 4 — Declaração e consentimento do colaborador (a preencher pelo colaborador)

O dispositivo acima descrito é da minha propriedade ou está sob o meu controlo.	☐ Confirmado
Li, compreendi e concordo com o cumprimento da política de BYOD e dos Termos de Utilização (Anexo 4).	☐ Confirmado
Compreendo que as aplicações e os dados da campanha podem ser desativados ou removidos remotamente pelo programa.	☐ Confirmado
Comunicarei prontamente qualquer perda, roubo ou suspeita de utilização indevida do meu dispositivo ou dos dados da campanha.	☐ Confirmado
Compreendo que a participação no modelo BYOD é voluntária e que a decisão de não participar não afeta a minha participação na campanha nem a minha compensação.	☐ Confirmado
Ao assinar abaixo, confirmo as declarações constantes acima. Esta assinatura atesta também que tomei conhecimento da Política BYOD e dos Termos de Utilização.	
Assinatura do colaborador	Data

Secção 5 — Aprovação do programa e decisão de registo (apenas para uso interno)

O dispositivo cumpre os requisitos técnicos e de segurança mínimos	☐ Sim ☐ Não — Motivo:
Registado por (nome do responsável de TI ou do representante do programa)	
Data de registo	
ID de utilizador BYOD/ID do dispositivo atribuído no sistema	
Assinatura do responsável pela aprovação	

ANEXO 3: Modelo de inventário de dispositivos

(também disponível sob a forma de uma ferramenta adaptável em Excel)

Manter sob a forma de uma folha de cálculo partilhada, acessível aos responsáveis de TI do distrito e ao responsável pela digitalização do PNM. Atualizações em tempo real ao longo de toda a campanha.

ID de utilizador BYOD	Nome completo	Função	Distrito	Marca/modelo do dispositivo	OS e versão	Cumpre os requisitos mínimos	Data de registo	Data de cancelamento do registo	Notas
BYOD-0001	Nome de exemplo	Pessoal de registo de agregados familiares	[Distrito]	Samsung A10	Android 11	Sim	DD-MM-AAAA		
BYOD-0002									
BYOD-0003									

ANEXO 4: Exemplo de política de BYOD e termos de utilização para campanhas de MTI

(Também disponível sob a forma de uma ferramenta adaptável em MS Word)

Substituir todo o texto entre [parênteses] por informações específicas do país ou do programa antes de utilizar. É obrigatório submeter a

uma revisão jurídica antes da finalização e divulgação desta política. Traduzir para todos os idiomas utilizados na área da campanha.

1. Propósito

A presente política Traga o seu próprio dispositivo (BYOD) estabelece as condições mediante as quais os dispositivos móveis de propriedade pessoal podem ser utilizados para apoiar a campanha de MTI de [país] de [ano], coordenada pelo [Ministério da Saúde/programa nacio-

nal de controlo da malária] ("o programa"). O objetivo é permitir a utilização segura e eficaz de dispositivos pessoais em atividades de campanha aprovadas, protegendo simultaneamente os dados do programa, os colaboradores e os beneficiários dos MTI.

2. Âmbito

A presente política aplica-se a:

- Todo o pessoal, voluntários e prestadores de serviços ("utilizadores") que participem na campanha de MTI de [país] de [ano] e que utilizem dispositivos pessoais para o trabalho da campanha
- Todos os smartphones, tablets ou computadores portáteis pessoais registados para aceder a aplicações ou dados da campanha

A presente política não abrange servidores de back-end, infraestrutura de alojamento ou dispositivos pertencentes ao programa, os quais são regidos por políticas distintas em matéria de TIC e proteção de dados.

3. Definições

Termo	Definição
BYOD	A utilização de dispositivos pessoais para trabalhos de campanha aprovados ao abrigo da presente política.
Dispositivo pessoal	Um smartphone, tablet ou computador portátil que é propriedade do utilizador, e não do programa.
Aplicação da campanha	Uma ferramenta digital aprovada utilizadas nas atividades da campanha, tais como o registo de agregados familiares, o registo da distribuição, a supervisão ou a elaboração de relatórios de stock.
Dispositivo pertencente ao programa	Um dispositivo adquirido e gerido no âmbito do programa ou por um parceiro de implementação.

4. Elegibilidade

Um utilizador só pode participar no modelo BYOD se todas as condições que se seguem estiverem cumpridas:

- O utilizador está formalmente envolvido na campanha
- O dispositivo cumpre os requisitos técnicos e de segurança mínimos estabelecidos no [Anexo 2](#)
- O utilizador concluiu a formação ou orientação obrigatória sobre BYOD, conforme comprovado pelo teste final online

- O utilizador assinou a presente política e o formulário de registo e consentimento relativo ao modelo BYOD, constante no [Anexo 2](#)

A participação no modelo BYOD é voluntária. Os trabalhadores que se recusarem a utilizar um dispositivo pessoal não devem ser penalizados e devem ter acesso a uma solução alternativa. O programa pode recusar, suspender ou revogar a participação no modelo BYOD a qualquer momento por motivos de segurança, legais ou operacionais.

5. Utilização aceitável

Os utilizadores só podem utilizar os respetivos dispositivos pessoais para tarefas aprovadas das campanhas. Estas incluem (por exemplo):

- Registo de agregados familiares
- Registo de distribuição de MTI
- Listas de verificação para supervisão e garantia da qualidade
- Atualizações relacionadas com o stock e a logística
- Materiais de formação e de referência aprovados

Os utilizadores podem também recorrer aos canais de comunicação aprovados para coordenar as campanhas com superiores e colegas.

Os utilizadores não devem utilizar dispositivos pessoais registados no âmbito do modelo BYOD para:

- Partilhar dados da campanha através de aplicações ou canais não aprovados

- Copiar, exportar ou armazenar dados de campanhas fora das aplicações aprovadas
- Fazer capturas de ecrã de listas de destinatários, de dados relativos aos agregados familiares ou de qualquer informação que contenha identificadores pessoais
- Permitir que pessoas não autorizadas tenham acesso às aplicações ou aos dados da campanha
- Assediar, maltratar ou discriminar destinatários, colegas ou membros da comunidade
- Aceder a conteúdos ilegais, prejudiciais ou inadequados utilizando dados financiados pelo programa

A utilização das redes sociais, de serviços de streaming e de outros serviços não relacionados com o trabalho durante as atividades da campanha deve ser restringida nos casos em que sejam fornecidos dados financiados pelo programa.

6. Requisitos de segurança

Os utilizadores devem garantir que:

- O dispositivo está protegido por um PIN, uma palavra-passe, um padrão ou um bloqueio biométrico
- O dispositivo bloqueia automaticamente após, no máximo, cinco minutos de inatividade
- O sistema operativo e as aplicações da campanha são mantidos atualizados
- O dispositivo não foi submetido a qualquer root ou jailbreak
- Apenas as aplicações de campanha aprova-

das são utilizadas para a realização de trabalhos da campanha

- Os dados da campanha não são copiados, exportados nem partilhados fora dos canais aprovados

Sempre que possível, o programa poderá aplicar controlos técnicos, tais como definições de segurança ao nível das aplicações, perfis de trabalho ou ferramentas de gestão de dispositivos móveis.

7. Proteção de dados e privacidade

Os utilizadores devem recolher e tratar apenas os dados necessários para as atividades da campanha, em conformidade com os procedimentos do programa e com a legislação aplicável em matéria de proteção de dados de [país].

Os utilizadores não devem guardar dados de campanhas em serviços de armazenamento em nuvem pessoais, no e-mail pessoal, em aplicações de mensagens pessoais ou em outros locais não autorizados.

O programa irá:

- Aplicar os princípios de minimização de dados e recolher apenas os dados necessários para as operações da campanha

- Utilizar os controlos técnicos menos intrusivos que forem necessários para proteger os dados da campanha
- Evitar o acesso a conteúdos pessoais no dispositivo, exceto nos casos em que tal seja permitido por lei e estritamente necessário para investigar um incidente grave de segurança

Será fornecido aos colaboradores um guião de consentimento oral aprovado para que possam comunicar aos agregados familiares que dados estão a ser recolhidos, por que razão são necessários e quem terá acesso aos mesmos.

8. Apoio, reembolso e equipamento

O programa irá:

- Ministrando formação e disponibilizar apoio técnico básico relativamente às aplicações de campanha aprovadas
- Fornecer dados, tempo de antena ou um subsídio definido, para a utilização razoável relacionada com a campanha, em conformidade com os procedimentos da campanha
- Manter um conjunto limitado de dispositivos pertencentes ao programa e destinados a empréstimo para utilizadores que não disponham de dispositivos pessoais adequados ou para situações de contingência

(Dependendo das decisões políticas) não é garantida a substituição total de um dispositivo pessoal perdido, roubado ou danificado. Qualquer apoio prestado dependerá das regras do programa, dos recursos disponíveis e das circunstâncias documentadas do incidente.

9. Responsabilidades do utilizador

Ao participarem no modelo BYOD, os utilizadores concordam em:

- Cumprir a presente política e os procedimentos do programa a ela associados
- Manter os respetivos dispositivos seguros, atualizados e em bom estado de funcionamento
- Comunicar imediatamente a perda ou roubo de dispositivos, suspeitas de violações de dados e violações das políticas
- Permitir que o programa elimine as aplicações e os dados da campanha no final da campanha ou do período de envolvimento
- Permitir que o programa desative o acesso ou elimine remotamente os dados da campanha em caso de perda, roubo ou incidente de segurança grave

Os utilizadores não devem permitir que pessoas não autorizadas utilizem os respetivos dispositivos para aceder a aplicações ou dados da campanha.

10. Responsabilidades do programa

O programa irá:

- Comunicar as regras, os riscos e as responsabilidades relacionadas com o modelo BYOD de forma clara e numa linguagem que os colaboradores compreendam
- Fornecer materiais de formação e contactos de apoio antes do início da campanha
- Aplicar a presente política de forma consistente e justa a todos os utilizadores e quadros
- Tomar medidas razoáveis para proteger tanto os dados da campanha como a privacidade do conteúdo dos dispositivos pessoais dos colaboradores

11. Não conformidade

O incumprimento da presente política pode resultar em:

- Suspensão ou revogação do acesso ao modelo BYOD
- Desativação de contas de aplicações da campanha
- Ações disciplinares em conformidade com os procedimentos aplicáveis ao pessoal ou aos voluntários
- Comunicação às autoridades competentes, sempre que exigido por lei

12. Reconhecimento do utilizador

Este formulário deve ser assinado antes da conclusão do registo do dispositivo e antes da concessão de acesso às aplicações da campanha.

Campo	Response
Eu, [nome], confirmo que li e compreendi a política de BYOD e os termos de utilização da campanha de MTI de [país] de [ano]. Concordo em cumprir estes requisitos e compreendo as responsabilidades associadas à utilização do meu dispositivo pessoal para o trabalho da campanha.	
Nome completo	
Cargo/função	
Organização (se aplicável)	
Número de telefone	
Marca e modelo do dispositivo	

Campo	Response
IMEI/número de série (opcional)	
Assinatura	
Data	



AMP CONTACTOS

Para se juntar à conferência semanal AMP todas as quartas-feiras às 10:00 horas hora de Leste (16:00 PM CET) utilize a linha de reunião Zoom seguinte:

<https://us06web.zoom.us/j/88935481892?pwd=h3cuJ3x5LOsR58YXcEaub8ULqu5LMj.1>

Pode encontrar o seu número local para aderir à chamada semanal:

<https://zoom.us/j/acyOjklJj4>

Para ser adicionado à lista de correio da AMP, visite:

<https://allianceformalariaprevention.com/join-us>

Para contactar a AMP ou juntar-se a um grupo de trabalho da AMP, envie um e-mail para:

info@allianceformalariaprevention.com

Para mais informações, consulte o site da AMP:

<https://allianceformalariaprevention.com>