UNIVERSIDADE DE CAXIAS DO SUL
ÁREA DO CONHECIMENTO DE CIÊNCIAS EXATAS E ENGENHARIAS

DANIEL ALMEIDA DA COSTA ABREU

ANÁLISE DE FERRAMENTAS PARA GERENCIAMENTO DE DISPOSITIVOS MÓVEIS ANDROID

CAXIAS DO SUL
2022

DANIEL ALMEIDA DA COSTA ABREU

ANÁLISE DE FERRAMENTAS PARA GERENCIAMENTO DE DISPOSITIVOS MÓVEIS ANDROID

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientador Prof. Giovanni Ely Rocco.

CAXIAS DO SUL
2022

DANIEL ALMEIDA DA COSTA ABREU

ANÁLISE DE FERRAMENTAS PARA GERENCIAMENTO DE DISPOSITIVOS MÓVEIS ANDROID

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Aprovado em: __/__/__.

Banca Examinadora

_____

Prof. Giovanni Ely Rocco

Universidade de Caxias do Sul - UCS

_____

Profa. Dra. Maria de Fátima Webber do Prado Lima

Universidade de Caxias do Sul - UCS

_____

Prof. Marcos Eduardo Casa

Universidade de Caxias do Sul - UCS

AGRADECIMENTOS

Agradeço primeiramente ao meu pai Leonardo de Souza Abreu por me proporcionar a oportunidade de estudo no ensino superior, sempre apontando a importância deste alicerce para o crescimento pessoal quanto profissional.

Agradeço a minha namorada Thais Ballico, por sua dedicação, paciência e apoio nesta caminhada em que me acompanha desde o começo e a minha irmã Maria Eduarda pelo empréstimo do dispositivo utilizado para os testes práticos.

Agradeço também ao Prof. Giovanni Ely Rocco por ser responsável na orientação deste trabalho, dando total suporte e apoio na concretização do mesmo, além de partilhar conhecimento fundamental para esta etapa.

Agradeço ainda aos colegas, professores, amigos e demais pessoas que de alguma forma colaboraram para a concretização deste objetivo.

RESUMO

Atualmente, sistemas de gerenciamento de dispositivos móveis são considerados importantes para as empresas devido aos recursos e funcionalidades que possuem, as quais facilitam a gestão e a segurança dos dispositivos móveis da empresa. Nesse campo existe uma variedade de ferramentas disponíveis, o que dificulta a escolha apropriada para aquisição. Portanto, o objetivo deste trabalho consiste em analisar e selecionar ferramentas de gerenciamento de dispositivos móveis, com o intuito de avaliar a adequação para utilização em qualquer tamanho de organização corporativa. Para tal, a fim de promover um processo comparativo equânime, o trabalho propõe o uso das normas ISO/IEC 25010 e ISO/IEC 25040. Neste processo, foram pré-selecionadas as ferramentas Mobile Device Manager Plus, Miradore, Soti MobiControl, IBM MaaS360 e Pulsus, estas ferramentas foram submetidas a avaliação quantitativa em que receberam pontuações de acordo com os requisitos definidos. Aplicado o processo proposto, duas ferramentas foram testadas e avaliadas pelo método avaliativo qualitativo, concluindo-se que as aplicações de MDM ainda não atingiram um estágio de maturidade esperado para essa finalidade.

Palavras-chave: MDM, Gerenciamento de dispositivos móveis, Avaliação de software.

ABSTRACT

Currently, mobile device management systems are considered important for companies due to their features and functionalities that facilitate the management and security of the company's mobile devices. In this field there is a variety of tools available, which makes it difficult to make the appropriate choice for acquisition. Therefore, the objective of this work is to analyze and select mobile device management tools, in order to evaluate their suitability for use in any size of corporate organization. To this end, in order to promote an equitable comparative process, the work proposes the use of the ISO/IEC 25010 and ISO/IEC 25040 standards. In this process, the tools Mobile Device Manager Plus, Miradore, Soti MobiControl, IBM MaaS360 and Pulsus were pre-selected, these tools were submitted to quantitative evaluation in which they received scores according to the defined requirements. After applying the proposed process, two tools were tested and evaluated by the qualitative evaluation method, concluding that the MDM applications have not yet reached a stage of maturity expected for thispurpose.

Keywords: MDM, Mobile Device Management, Software evaluation.

LISTA DE FIGURAS

Figura 1 - Estatísticas de pacotes de instalação maliciosos 15
Figura 2 - Arquitetura MDM 19
Figura 3 - Modelo de qualidade de produto de software conforme ISO/IEC 25010 .. 29
Figura 4 - Dispositivo Samsung A03 Core 44
Figura 5 - Opções de diversos fatores 44
Figura 6 – Mensagem de erro 45
Figura 7 – Dispositivo incompatível 45
Figura 8 – Desabilitando verificação de integridade durante a inscrição 46
Figura 9 – Erro “não é possível adicionar um perfil de trabalho” 46
Figura 10 – Opções de locais de teste 47
Figura 11 – Opções de autenticação de dois fatores 47
Figura 12 – Autenticação recusada 48
Figura 13 – Escolha de sistema operacional para provisionamento 49
Figura 14 – Código QR para provisionamento 49
Figura 15 – Escaneamento do cógido QR 50
Figura 16 – Status cadastrado 50
Figura 17 – Status pendente 50
Figura 18 – Criação de perfil 51
Figura 19 – Controle de recursos e funcionalidades 52
Figura 20 – Status de associação de perfil 52
Figura 21 – Controle Web 53
Figura 22 – Modo quiosque 53
Figura 23 – Observação ao aplicar modo quiosque 54
Figura 24 – Permitindo modo quiosque no dispositivo 54
Figura 25 – Recurso desabilitado 55
Figura 26 – Seleção de plataforma para adicionar aplicativo 56

Figura 27 – Google Play gerenciado 56
Figura 28 – Opções de configuração do Google Play gerenciado 57
Figura 29 – Etapa de configuração sem conta Gsuite 57
Figura 30 – Informações para registro no Google Play gerenciado 57
Figura 31 – Detalhes Google Play gerenciado 58
Figura 32 – Aplicativos Google Play 58
Figura 33 – Detalhes de aplicativos do catalogo 59
Figura 34 – Seleção de dispositivo para distribuição de aplicativo 59
Figura 35 – Seleção de aplicativo para distribuição 60
Figura 36 – *Dashboard* 60
Figura 37 – Acesso remoto 61
Figura 38 – Erro ao iniciar sessão remota 61
Figura 39 – Logs de auditoria 62
Figura 40 – Gerenciamento de conteúdo 62
Figura 41 – Política de gerenciamento de conteúdo 63
Figura 42 – Inventário de dispositivos 63
Figura 43 – Inventário de aplicativos 64
Figura 44 – Dados de localização 64
Figura 45 – Resumo do dispositivo (Rom utilizada, rede e sistema operacional) 65
Figura 46 – Resumo do dispositivo (Segurança e atestado de segurança da rede) . 65
Figura 47 – Aplicativos instalados 66
Figura 48 – Retorno sobre localização do dispositivo testado 66
Figura 49 – Opções de relatórios pré-definidos 67
Figura 50 – Exemplo de filtro para customização de relatório 67
Figura 51 – Configurações de exportação de relatórios 67
Figura 52 – Seleção de limpeza remota 68
Figura 53 – Habilitando modo perdido 69

Figura 54 – Status modo perdido 69
Figura 55 – Dispositivo perdido 70
Figura 56 – Opções de limpeza remota 70
Figura 57 – Confirmação de limpeza remota 71
Figura 58 – Quantidade de dispositivos suportados para gerenciamento 71
Figura 59 – Uso de recursos utilizados no dispositivo 72

LISTA DE QUADROS

Quadro 1 - Etapas do processo de aquisição de software conforme a ISO/IEC 25040.....31

Quadro 2 - Características e subcaracterísticas selecionadas para avaliação.....33

Quadro 3 - Multiplicador de pontuação de acordo com o nível de requerimento.....36

Quadro 4 - Nomenclatura das ferramentas.....36

Quadro 5 - Métrica para avaliação quantitativa.....37

Quadro 6 - Resultado da avaliação quantitativa.....38

Quadro 7 - Critérios de medições de qualidade.....43

LISTA DE ABREVIATURAS E SIGLAS

BYOD	Bring Your Own Device
MDM	Mobile Device Management
TI	Tecnologia da Informação
OTA	Over The Air
S&SC	Software e Serviços Correlatos
VPN	Virtual Private Network
IOT	Internet of Things
RAM	Random Access Memory
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
MWC	Mobile World Conference
ROM	Read Only Memory
RAM	Random Access Memory

SUMÁRIO

1 INTRODUÇÃO 14

1.1 PROBLEMA DE PESQUISA 16

1.2 OBJETIVO 16

1.2.1 OBJETIVOS ESPECÍFICOS 16

1.3 METODOLOGIA 17

1.4 ESTRUTURA DO TRABALHO 17

2 FUNDAMENTAÇÃO TEÓRICA 19

2.1 *OVER THE AIR* 20

2.2 INVENTÁRIO 20

2.3 PROVISIONAMENTO 20

2.4 GERENCIAMENTO E CONTROLE 21

2.5 MONITORAMENTO E SUPORTE 21

2.6 SEGURANÇA 21

2.7 PROTEÇÃO DE DADOS 22

2.8 MULTIPLATAFORMA 22

2.9 CONSIDERAÇÕES FINAIS DO CAPITULO 22

3 PRÉ-SELEÇÃO DE FERRAMENTAS 23

3.1 MOBILE DEVICE MANAGER PLUS 24

3.2 MIRADORE 25

3.3 SOTI MOBICONTROL 26

3.4 IBM MAAS360 26

3.5 PULSUS 27

3.6 CONSIDERAÇÕES FINAIS DO CAPÍTULO 27

4 NORMALIZAÇÃO PARA SELEÇÃO E AQUISIÇÃO DE FERRAMENTAS DE SOFTWARE 28

4.1 ISO/IEC 25010 28

4.2 ISO/IEC 25040 E ISO/IEC 25041 30

4.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO 31

5 PROPOSTA DE SOLUÇÃO 32

5.1 ETAPA 1 32

5.2 ETAPA 2 33

5.3 ETAPA 3 35

5.4 ETAPA 4 37

5.5 CONSIDERAÇÕES FINAIS DO CAPITULO 42

6 AVALIAÇÃO QUALITATIVA 43

6.1 IBM MAAS360 44

6.2 MOBILE DEVICE MANAGER PLUS 47

6.3 ETAPA 5 72

6.4 CONSIDERAÇÕES FINAIS DO CAPITULO 73

7 CONCLUSÃO 74

REFERÊNCIAS 77

1 INTRODUÇÃO

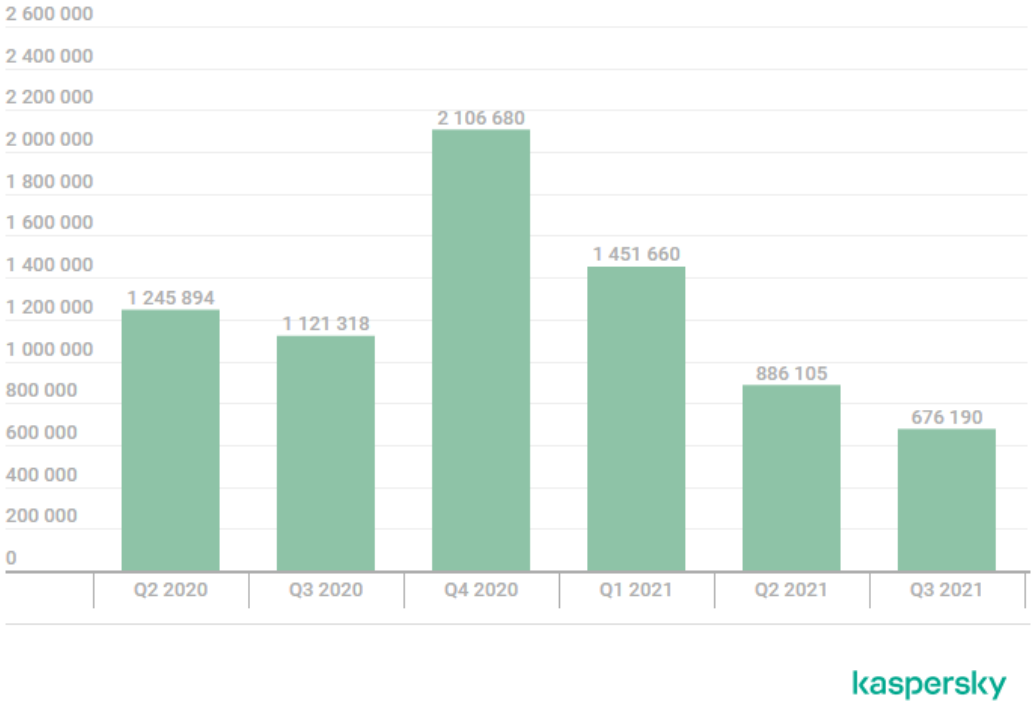
Os recursos de tecnologia da informação estão evoluindo rapidamente, devido à disseminação de dispositivos móveis no âmbito empresarial. Estes dispositivos, como celulares e *tablets*, têm sido destaque como ferramenta de comunicação e produtividade no meio corporativo. Esse fenômeno pode ser chamado de consumerização de TI e se refere a utilização de dispositivos móveis pessoais no ambiente de trabalho para fins corporativos (NIEHAVES; KOFFER; ORBACH, 2012).

Devido ao retorno positivo que podem ter, as organizações optaram por aderir cada vez mais ao uso de soluções envolvendo dispositivos móveis para alavancar a produtividade. Dentre os benefícios, é notável a questão da mobilidade, em que se tem o rápido acesso a informações de qualquer lugar e a qualquer momento, resolvendo urgências mais rapidamente. A economia de recursos, pelo fato de não ser necessário o funcionário estar no local para participar de uma reunião, poupando tempo e recursos de deslocamento. A comunicação com clientes se tornou mais eficiente, o que pode ser visto como um diferencial competitivo (MELO, 2020).

O uso crescente destes dispositivos vem fazendo com que as empresas se tornem cada vez mais expostas a ameaças de segurança e vazamento de dados, o que pode ser catastrófico para uma organização. Conforme aponta o relatório 2021 sobre ameaças móveis emergentes da Check Point, cerca de 46% das organizações sofreram uma ameaça contra sua rede e seus dados, devido a pelo menos um download de aplicativo móvel malicioso feito por um colaborador em 2020 (CHECKPOINT, 2021).

Em contrapartida, a Kaspersky apresentou diminuição nas estatísticas de ameaças destinadas a dispositivos móveis em 2021, no qual houve um volume menor de pacotes de aplicativos maliciosos. Conforme é observado na Figura 1, no terceiro trimestre de 2021, a Kaspersky detectou 676.190 pacotes de instalação maliciosos, cerca 209.915 a menos que no trimestre anterior e 445.128 a menos que no terceiro trimestre de 2020 (SHISHKOVA, 2021). Mas isto não indica que menos dispositivos estão sendo alvos, pois os ataques estão se tornando mais sofisticados em termos de funcionalidade e vetores de *malware*, o que leva estes ataques a terem uma taxa maior de sucesso.

Figura 1 - Estatísticas de pacotes de instalação maliciosos



Fonte: Shishkova *et al*. (2021).

Para minimizar a chance de problemas, é necessário gerenciar os dispositivos que podem acessar os dados da empresa por meio de um sistema que funcione de forma centralizada. No caso de dispositivos móveis, denomina-se este tipo de sistema como MDM (*Mobile Device Management*) que tem como propósito a gestão completa dos dispositivos móveis corporativos e consequentemente a segurança. Essa gestão contempla políticas de bloqueio de uso e instalação de aplicativos indevidos, como jogos, redes sociais e outros que sejam definidos pela organização. Abrange o recurso de inventário online, que facilita a organização e criação de políticas de segurança. Também possui a funcionalidade de rastreador, em que é possível saber onde o aparelho se encontra em tempo real. Destaca-se também o recurso de instalação, atualização e remoção de aplicativos remotamente, entre outras funcionalidades que as ferramentas deste segmento disponibilizam.

É importante ressaltar, antes de tudo, que alguns especialistas fazem uma diferenciação entre consumerização e BYOD (*Bring Your Own Device*, que, em português, significa Traga Seu Próprio Dispositivo). Para eles, a consumerização é quando o dispositivo pertence à empresa, enquanto o termo BYOD, o dispositivo pertence ao profissional. Alguns estudiosos preferem usar apenas a consumerização para se referir ao fenômeno como um todo. Neste estudo o entendimento do termo

consumerização será tratado como o dispositivo sendo de propriedade da empresa (DENER, 2020).

1.1 PROBLEMA DE PESQUISA

Devido a evolução tecnológica houve um aumento significativo de dispositivos utilizados nas organizações, e dependendo da necessidade, as empresas estão adotando dispositivos móveis como celulares e tablets para a execução de algumas tarefas. Desta forma, é necessário que a empresa administre estes dispositivos de forma centralizada para garantir a produtividade do funcionário e a segurança dos dados sensíveis da empresa.

Com isto, atualmente existem diversas soluções disponíveis para este nicho, no qual oferecem várias funcionalidades, o que acaba dificultando a decisão da ferramenta de gerenciamento de dispositivos móveis mais adequada para implantar na organização. Nesse sentido é importante definir um processo base para auxiliar na avaliação das ferramentas que tem potencial para suprir esta demanda.

Questão de pesquisa: Como escolher uma ferramenta adequada para o gerenciamento de dispositivos móveis?

1.2 OBJETIVO

Este trabalho tem como objetivo, avaliar e selecionar ferramentas para o gerenciamento de dispositivos móveis, com ênfase a celulares e *tablets* com sistema operacional *Android* usados no contexto empresarial.

1.2.1 OBJETIVOS ESPECÍFICOS

Os objetivos específicos a serem abordados neste trabalho são:

a) Definir escopo de avaliação de acordo com a ISO/IEC 25040;

b) Definir critérios para a avaliação destes sistemas com base na norma ISO/IEC 25010;

c) Selecionar as ferramentas de MDM e aplicar o processo comparativo entre as ferramentas;

d) Validar a adequação da(s) ferramenta(s) selecionada(s) aplicando-a(s) em um caso de estudo para análise qualitativa.

1.3 METODOLOGIA

A metodologia de desenvolvimento do trabalho consiste na aplicação de um estudo de caso exploratório, que consiste no estudo aprofundado de determinada situação, no qual possivelmente o pesquisador irá elaborar hipóteses para um estudo posterior (WAZLAWICK, 2021). O presente estudo bibliográfico busca detalhar o conhecimento sobre sistemas de gerenciamento de dispositivos móveis e suas funcionalidades, auxiliando a atingir o objetivo previamente proposto. O desenvolvimento da metodologia conta com 5 etapas.

a) 1ª etapa: Estudar e compreender o que abrange sistemas de gerenciamento de dispositivos móveis;
b) 2ª etapa: Realizar uma pré-seleção de quais ferramentas serão utilizadas para análise;
c) 3ª etapa: Definir o escopo e os critérios de avaliação com o embasamento das normas ISO/IEC 25010 e ISO/IEC 25040 que contém requisitos e recomendações para avaliação de softwares;
d) 4ª etapa: Analisar e selecionar as ferramentas de acordo com os critérios definidos;
e) 5ª etapa: Testar e validar a(s) ferramenta(s) selecionada(s) em um estudo de caso experimental.

1.4 ESTRUTURA DO TRABALHO

A organização do trabalho está dividida em 7 capítulos, incluindo esse capítulo de apresentação da motivação, objetivos e metodologia.

O capítulo 2, apresenta um estudo sobre o MDM, descrevendo os recursos presentes neste tipo de sistema.

No capítulo 3, encontram- se as ferramentas pré-selecionadas para análise e um resumo sobre as mesmas.

O capítulo 4, traz um resumo sobre as normas ISO/IEC 25010 e ISO/IEC 25040, que apresenta um modelo de qualidade e uma estrutura a ser seguida para avaliação de produto de software.

O capítulo 5 trata sobre a proposta de solução para o problema abordado no capítulo 1 deste trabalho. Contém as métricas e critérios para a análise quantitativa

das ferramentas pré-selecionadas de gerenciamento de dispositivos móveis e a pontuação atingida por elas.

No capitulo 6 encontra-se a avaliação qualitativa realizada juntamente com a descrição dos testes das ferramentas selecionadas após análise quantitativa das mesmas.

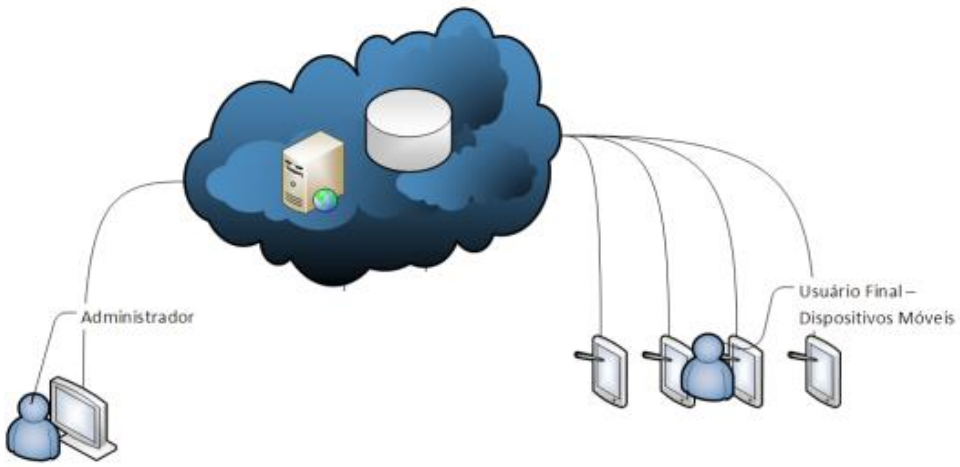
Por fim, o capítulo 7 apresenta a conclusão final deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Um sistema de gerenciamento de dispositivos móveis (MDM) é definido por suas principais características, que consiste em gerenciar smartphones e tablets de forma centralizada. Esse gerenciamento tem como objetivo proteger, monitorar e controlar estes dispositivos remotamente, garantindo ao mesmo tempo a produtividade do funcionário e a segurança dos dados da empresa.

A arquitetura básica do sistema MDM consiste em ter o servidor de aplicação, a console de gerenciamento ou administração e dispositivos clientes, como é mostrado na Figura 2. Atualmente os fornecedores de soluções MDM disponibilizam acesso apenas a console de gerenciamento via navegador *Web*, onde a aplicação é executada na nuvem, ou seja, no servidor do fornecedor. O gerenciamento dos dispositivos que possuem o agente instalado e que tenham comunicação com a console é realizado neste centro de administração.

Figura 2 - Arquitetura MDM



Fonte: Adaptado de Silvestrin (2013).

É de comum entendimento que os recursos gerais de um sistema MDM variam de acordo com a necessidade de cada organização, mas, pode-se citar algumas consideradas essenciais, como *Over The Air* (OTA), inventário, provisionamento, gerenciamento, controle, monitoramento, suporte, segurança, proteção de dados e suporte a diferentes sistemas operacionais (PHIFER, 2013).

2.1 *OVER THE AIR*

Um dos principais recursos que um sistema MDM deve ter, é realizar operações remotamente. A maioria dos dispositivos móveis contam com a tecnologia OTA, que consiste em configurar um ou vários dispositivos móveis, enviando atualizações, bloqueando ou até mesmo limpando estes dispositivos de forma remota.

2.2 INVENTÁRIO

Através do inventário é possível obter a lista de aparelhos que a empresa possui, e que estão sendo gerenciados. O inventário deve trazer informações úteis destes aparelhos, como nome do dispositivo, modelo do aparelho, informações de hardware e de software. Dentre as informações de hardware, pode-se citar o modelo do processador, capacidade total da bateria, quantidade de memória *RAM*, quantidade de armazenamento total. Sobre as informações de software, cita-se, por exemplo, a versão do sistema operacional e a versão do pacote de segurança.

O inventário deve ser capaz de permitir realizar uma classificação ou um agrupamento de acordo com algum filtro, como por exemplo a versão do sistema operacional, a fim de organizar e facilitar a visualização em que a lista será apresentada.

2.3 PROVISIONAMENTO

O gerenciamento de um dispositivo durante seu ciclo de vida começa na ativação e provisionamento do mesmo. O sistema MDM pode ajudar os administradores a registrar os dispositivos portáteis da empresa ou permitir que os usuários registrem seus próprios dispositivos, por meio de portais, por exemplo.

Para realizar a inclusão de um dispositivo no console de gerenciamento do MDM, é necessário instalar no dispositivo o agente que fará a comunicação entre ele e a aplicação. É por meio deste agente que é coletado e enviado informações para aplicação, além de receber instruções de tarefas a serem realizadas ou políticas a serem aplicadas no dispositivo. A instalação do agente depende de como é disponibilizado pelo fornecedor da ferramenta MDM, sendo o mais comum a instalação pelas lojas de aplicativos oficiais.

2.4 GERENCIAMENTO E CONTROLE

Sistemas MDM podem ajudar a TI a automatizar a distribuição de instalação e atualização em massa de aplicativos que a organização utilize.

O objetivo do gerenciamento de aplicativos está associado a funcionalidade de instalação, desinstalação e atualização de aplicativos de forma remota, sem que haja interação por parte do usuário do dispositivo. Já o controle, se refere a permissões que o usuário pode ter em relação à instalação ou desinstalação de aplicativos, também podendo aplicar bloqueios de recursos do aparelho, como câmera ou microfone.

2.5 MONITORAMENTO E SUPORTE

O monitoramento por meio de um sistema MDM auxilia a diagnosticar problemas nos dispositivos, através da coleta de informações em tempo real. Essa coleta abrange informações como lista de aplicativos instalados no dispositivo, armazenamento disponível, tempo de atividade ou status do aparelho, última localização de acordo com o *GPS*, nome da rede *Wifi* em que está conectado, entre muitas outras que são possíveis de obter. As informações mencionadas devem ajudar a tomar decisões sobre uma possível troca de aparelho, suporte ou manutenção do mesmo.

Em alguns momentos é necessário a intervenção do suporte técnico de TI para resolver alguma questão no dispositivo, e isso é realizado por meio de controle remoto. É importante que um sistema MDM inclua recursos de suporte remoto, onde é possível o compartilhamento da tela ou o próprio controle remoto do dispositivo.

2.6 SEGURANÇA

A segurança é imprescindível para qualquer sistema, e para um sistema MDM não poderia ser diferente. Levando em consideração que um dispositivo móvel tem chances maiores de serem roubados ou perdidos, é necessário ter políticas de segurança para evitar transtornos caso o incidente venha a ocorrer. Para isso, essas políticas devem possuir autenticação para acesso a dados e aplicativos da empresa, e meios de remover todos os dados sensíveis do dispositivo em caso de perda ou roubo.

2.7 PROTEÇÃO DE DADOS

Os dados são o ativo mais sensível de uma empresa. Um sistema MDM deve ter o recurso de criptografia destes dados por meio de políticas, implementados via software ou hardware. Além da criptografia, a auditoria destes dados se faz necessária por meio de rastreamento do histórico dos mesmos, englobando informações de transferência ou modificações de arquivos. A proteção de dados também contempla a realização de cópias de segurança e restauração do dispositivo.

2.8 MULTIPLATAFORMA

Devido a diversificação dos sistemas operacionais e suas diferentes versões, um sistema MDM deve ser abrangente nesta questão, sendo compatível com as diferentes plataformas do mercado, como IOS e Android. No entanto, os fabricantes de dispositivos ou versões mais antigas do SO podem causar problemas para uma ferramenta de MDM, devido a compatibilidade de algumas funcionalidades.

2.9 CONSIDERAÇÕES FINAIS DO CAPITULO

Embora cada ferramenta MDM seja diferente uma da outra e contenham recursos diferentes, existem alguns recursos que essas soluções devem disponibilizar, e a falta deles sugere que a ferramenta não seja adequada para atender algumas necessidades da empresa.

Portanto, neste capítulo é abordado os recursos destacados como essenciais para a aquisição de uma solução de gerenciamento de dispositivos móveis, pois normalmente podem ser utilizados como fator decisivo para determinar a aquisição correta da solução.

3 PRÉ-SELEÇÃO DE FERRAMENTAS

Existem diversas soluções para o gerenciamento de dispositivos móveis disponíveis, o que torna a seleção dessas ferramentas demorada e desgastante. Desta forma, com o intuito de afunilar o número de ferramentas, foi realizado uma pré-seleção de acordo com as funcionalidades que as mesmas dispõem. A partir de pesquisas é possível retirar ferramentas de listas comparativas para se basear nas mais indicadas. De acordo com o propósito deste trabalho, foi encontrado 3 listas contendo as melhores ferramentas de MDM, entre elas estão a lista da Iplace (IPLACE, 2018), NaneeDigital (NANEEDIGITAL, 2021) e Comparitech (COOPER, 2022), porém, por ser mais atual e também pela própria análise mais aprofundada que contém de forma clara os critérios utilizados para a formação da lista, optou-se por se basear pela lista da Comparitech.

Definida a fonte base para a seleção prévia das ferramentas a analisar, algumas das ferramentas pré-selecionadas são retiradas da lista comparativa de ferramentas de MDM realizada pela Comparitech, que usou funcionalidades como requisitos para comparação. Estão presentes as funcionalidades de rastreabilidade, bloqueio e limpeza de dispositivos, monitoramento e disparo de tarefas em massa. Avaliação gratuita e preço de aquisição do software referente ao custo benefício, foram usados conjuntamente como requisitos para a formação da lista da Comparitech (COOPER, 2022).

Das 11 ferramentas presentes na lista, ManageEngine Mobile Device Manager Plus, Kandji, VMWare Workspace ONE, BlackBerry Unified Endpoint Management, Citrix Endpoint Management, SOTI MobiControl, IBM MaaS360, Cisco Meraki, Miradore Mobile Device Management, Jamf Now, Simply Secure, foram selecionadas apenas 4 delas de acordo com os prós e contras apresentados, pois demonstraram que se sobressaem perante as demais.

As ferramentas Kandji e Jamf Now foram descartadas devido a possuir compatibilidade somente com dispositivos da Apple, o que acaba indo contra o escopo do trabalho que se refere a dispositivos móveis cujo sistema operacional é o Android. A ferramenta da Cisco chamada Cisco Meraki não foi levada em consideração, devido a um ponto negativo apontado em relação a sua limitação da visualização dos dados. A ferramenta de gerenciamento de endpoints unificados da BlackBerry teve como ponto negativo apontado pela Comparitech poucas opções de segurança móvel e por

este motivo foi desqualificada e não aparece na lista de pré-seleção. A solução da VMWare, também ficou de fora da lista por ter cerca de 7 planos para contratação, o que pode acabar confundindo no momento de contratar a solução e, em particular, na realização deste trabalho comparativo. Já a ferramenta Simply Secure da Beachhead está fora da lista pois é indicada para redes menores, e o propósito do trabalho consiste em atender qualquer tamanho de organização corporativa.

A solução da Citrix para gerenciamento de endpoints aparenta ter maior aderência em ambientes construídos utilizando outras tecnologias da mesma empresa. Outro motivo para não ser utilizada como uma solução a ser levada em consideração é a integração somente com o Active Directory da Azure não podendo ser utilizado a integração do Active Directory local como a maioria das empresas utilizam atualmente, porém, o principal motivo é que não é possível testar a ferramenta por um período de tempo de forma gratuita, somente visualizar uma demonstração realizada com a equipe de vendas da fornecedora.

Para a pré-seleção de ferramentas também foi realizada uma pesquisa por soluções bem posicionadas no mercado brasileiro, no qual foi encontrado a Startup brasileira Pulsus sendo a melhor referência neste segmento. A Pulsus é vista como líder na América latina em gerenciamento de dispositivos móveis (LAM, 2022) e foi uma das expositoras no *Mobile World Conference* Barcelona 2022 (MWC BARCELONA, 2022) e por este motivo complementa a lista.

A seguir é apresentado um breve resumo das ferramentas escolhidas para ser realizada a análise quantitativa, e posteriormente escolher as melhores posicionadas a fim de conduzir uma avaliação qualitativa.

3.1 MOBILE DEVICE MANAGER PLUS

A Mobile Device Manager Plus foi uma das 4 ferramentas selecionadas da lista da Comparitech e tem como pontos positivos a personalização de painéis de monitoramento e relatórios, possibilita a descoberta automatizada de dispositivos, tal como a utilização de alertas inteligentes para reduzir falsos positivos, também é possível automatizar alertas para serem recebidos em e-mails ou SMS.

Foi destacado também a possibilidade de soluções de problemas remotamente com o acesso remoto do dispositivo, a permissão de agendar verificações regulares dos dispositivos a fim de manter as informações atualizadas de acordo com a

frequência desejada e a disponibilidade de um chat para se comunicar com o usuário final do dispositivo, por meio deste chat pode-se emitir comandos de segurança. O único ponto negativo apontado pela Comparitech é a extensão de recursos presente na ferramenta, o que demanda tempo para aprender adequadamente a sua utilização (COOPER, 2022).

A solução de MDM da Manage Engine, propõe uma interface fácil de utilizar por meio de um *dashboard,* garante a solução de problemas remotamente, bem como a aplicação de políticas, distribuição e gerenciamento de aplicativos, gerenciamento de inventário, limpeza remota, entre outras funcionalidades. A ferramenta possui 3 versões, a gratuita que suporta o gerenciamento de até 25 dispositivos, dita como ideal para pequenas empresas, a versão padrão que contempla o gerenciamento básico dos dispositivos móveis e a versão profissional, que possui gerenciamento escalável. É possível utilizar a ferramenta localmente (disponível apenas para Windows) ou por meio da nuvem, em ambas pode-se realizar a avaliação gratuita de 30 dias (MANAGEENGINE, 2022).

3.2 MIRADORE

A solução Miradore permite gerenciar computadores com Windows 10 e MacOs e dispositivos móveis com IOS e Android. As funções de acesso remoto permitem bloquear ou limpar um dispositivo perdido, além de redefinir sua senha ou até mesmo ignorar qualquer senha de hardware definida pelo usuário. O Miradore também possui um mapa no painel de administração que mostra exatamente onde todos os dispositivos gerenciados estão localizados. Foi apontado na avaliação da Comparitech que possui uma ampla gama de recursos que podem levar para serem totalmente explorados (COOPER, 2022).

Os recursos do MDM Miradore, permitem a segurança dos dispositivos e dados, por meio de criptografia e códigos de acesso. Possui modo quiosque, em que é possível configurar perfis com restrições, também realiza o gerenciamento de aplicativos, oferece suporte remoto, visualização de informações por meio do inventário e dashboard, tal como possibilita a criação de relatórios personalizados. A ferramenta possui dois planos, o plano livre, que é gratuito e possui limitações e o plano premium, não possui limitações, mas é cobrado de acordo com o número de

dispositivos gerenciados, é possível testar todos os recursos da versão premium por 14 dias gratuitamente (MIRADORE, 2022).

3.3 SOTI MOBICONTROL

Compatível com dispositivos de mais de 170 fornecedores, a solução Soti MobiControl tem como principais características a visualização remota, controle remoto, algumas integrações com outros sistemas ou aplicações e a possibilidade de usar scripts para executar ações de gerenciamento. Permite a utilização de um bate-papo para que o administrador se comunique com o usuário final do dispositivo, também pode ser usado para gerenciamento de conteúdo móvel para proteger arquivos e conteúdo da web, além de possibilitar por meio de listas brancas e negras adicionar quais aplicativos podem ou não serem utilizados, em que ajuda a garantir que os usuários permaneçam produtivos. Conforme indicado pela Comparitech, esta solução é mais indicada para redes grandes, mas isso não significa que não possa ser usada em redes menores (COOPER, 2022).

Conforme descrito pela fornecedora, a Soti MobiControl oferece visibilidade e controle sobre onde estão os dispositivos móveis, o que estão fazendo e quais riscos de segurança ou conformidade estão enfrentando. Com a solução é possível instalar aplicativos em smartphones, provisionar novos dispositivos e acompanhar a localização dos dispositivos gerenciados. Também é compatível com endpoints de IoT. Nas versões Premium Plus ou Enterprise Plus a tecnologia Soti Xtreme e Soti Xtreme Hub está disponível, com elas é otimizada a comunicação em conexões limitadas e reduzir o tempo necessário para concluir implantações de dados e aplicativos em um grande número de dispositivos *Android* (SOTI MOBICONTROL, 2022).

3.4 IBM MAAS360

De acordo com a Comparitech, a solução IBM MaaS360 tem como seu maior ativo os recursos de segurança dos dispositivos, a plataforma do dispositivo pode detectar e corrigir malware em endpoints, por meio dessa detecção é fornecida uma camada extra de segurança móvel que ajuda a evitar que os terminais sejam comprometidos e coloquem seus dados em risco. Tem como suas principais características o monitoramento de uso de dados em tempo real, login único para

aplicativos da web e nuvem, compatibilidade e monitoramento de dispositivos IoT, além de possuir suporte 24/7. A solução da IBM é mais indicada para redes maiores, mas não há nada que impeça o uso em redes menores.

Os destaques da solução da IBM para gerenciamento de dispositivos móveis, é apontado pela fabricante como uma implementação rápida, dispõe de proteção de informações, gerenciamento remoto de ameaças, acesso seguro aos recursos da empresa sem a necessidade de uma VPN, suporte a políticas para BYOD e dispositivos IoT, entre outras funcionalidades. A solução possui um período de avaliação gratuito de 30 dias (IBM, 2022).

3.5 PULSUS

A Pulsus surge da necessidade de solucionar problemas operacionais e entregar soluções completas de forma ágil e segura, trazendo suporte e recursos automatizados para TI, pessoas, gestão e performance por meio de tecnologia de ponta.

O MDM da Pulsus é uma plataforma completa, com interface simples e intuitiva, que promete controle de aplicativos, arquivos, atualizações, distribuição massiva, acesso remoto, exportação de relatórios, entre outras funcionalidades personalizáveis como o modo motorista. A Pulsus é localizada no Brasil e é referência no setor na américa latina e dispõe de 15 dias de teste da sua solução (PULSUS,2022).

3.6 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Destaca-se que as ferramentas pré-selecionadas têm em comum recursos e funcionalidades como o monitoramento dos dispositivos, geração de relatórios, gerenciamento de aplicativos, inventário, suporte remoto, entre outros, e a disponibilização de avaliação gratuita.

De acordo com o que foi apresentado neste capítulo, realizou-se a pré-seleção das ferramentas que serão utilizadas para a avaliação quantitativa, como também foi justificado a escolha delas, além de apresentar um resumo sobre as mesmas.

4 NORMALIZAÇÃO PARA SELEÇÃO E AQUISIÇÃO DE FERRAMENTAS DE SOFTWARE

Devido a grande quantidade de soluções de software disponíveis no mercado atualmente, independente do nicho que esse recurso se encontra, escolher a melhor solução dentre as várias ferramentas encontradas, torna-se necessário critérios e processos definidos para efetuar uma avaliação, a fim de auxiliar na decisão sobre a mesma. Para realizar a definição da avaliação, é válido contar com o suporte de normas, que tem como objetivo padronizar processos e critérios, a fim de mensurar a qualidade de produtos ou serviços, apoiando desta forma na decisão sobre a aquisição.

Ao decorrer do tempo diversos modelos de aquisição e avaliação de software foram propostos, dentre eles as normas ISO/IEC 9126 (ABNT, 2003), ISO/IEC 14598 (ABNT, 2001) e o Guia de Aquisição do MPS.BR (SOFTEX, 2013). A ISO/IEC 9126 define um conjunto de parâmetros com o objetivo de padronizar a avaliação da qualidade de software. Enquanto a ISO/IEC 14598, descreve o processo de avaliação de produtos de software e possui o modelo definido que distingue três perspectivas de avaliação: desenvolvedor, adquirente e avaliador. Já o Guia de Aquisição do MPS.BR, tem o intuito de servir como um guia para empresas que adquirem Software e Serviços Correlatos (S&SC), detalhando as atividades e tarefas envolvidas, descrevendo os produtos de trabalho e fornecendo exemplos de preenchimento dos principais documentos.

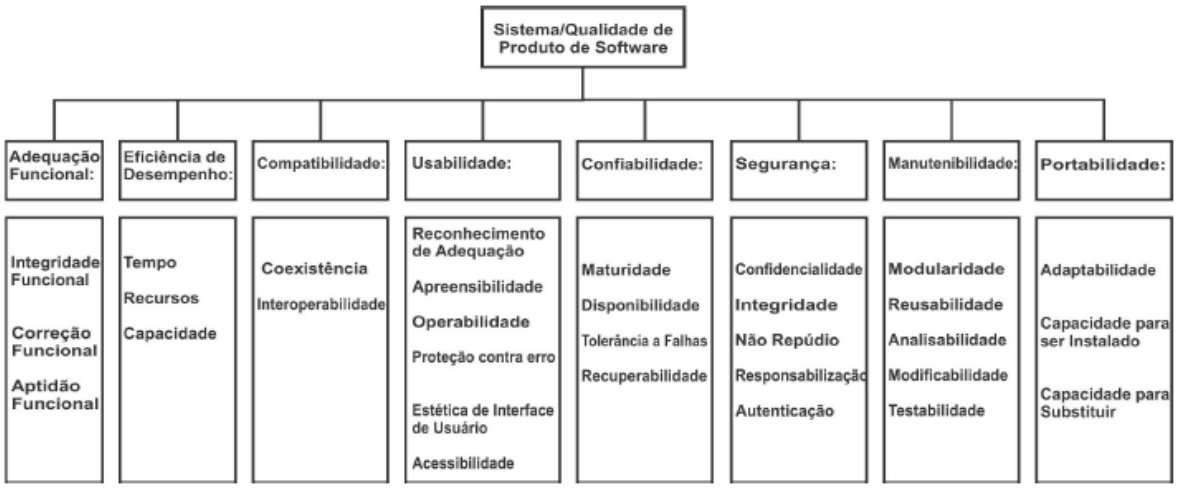
As normas ISO/IEC 9126 e ISO/IEC 14598 foram substituídas pelas normas ISO/IEC 25010 (ISO/IEC; COMMISSION, 2011a) e ISO/IEC 25040 (ISO/IEC; COMMISSION, 2011b), respectivamente.

4.1 ISO/IEC 25010

De acordo com a ISO/IEC 25010, o modelo de qualidade determina quais características de qualidade serão consideradas para avaliar as propriedades de um produto de software. A qualidade de um software ou sistema é medido de acordo com o grau em que ele satisfaz as necessidades implícitas e declaradas de suas várias partes interessadas. Através dessas necessidades se categoriza a qualidade do produto em características e subcaracterísticas. Na figura 3, pode-se visualizar as 8

características e suas 31 subcaracterísticas de qualidade que a ISO/IEC 25010 compreende no modelo de qualidade.

Figura 3 - Modelo de qualidade de produto de software conforme ISO/IEC 25010



Fonte: Adaptado ISO/IEC 25010.

Como é mostrado na Figura 3, cada característica do modelo possui um conjunto de subcaracterísticas que estão relacionadas, a seguir é apresentado um breve resumo de cada característica.

- **Adequação funcional:** Esta característica representa o grau em que um sistema ou produto fornece funções que atendem as necessidades declaradas e implícitas quando usado sob condições especificadas;
- **Eficiência de desempenho:** Representa a quantidade de recursos utilizados nas condições estabelecidas;
- **Compatibilidade:** Compatibilidade é uma das duas características adicionadas na ISO/IEC 25010, se comparada a ISO 9126. É definida pela capacidade do produto, sistema ou componente poder trocar informações com outros produtos, sistemas e/ou componentes, enquanto compartilha do mesmo ambiente de hardware ou software;
- **Usabilidade:** Consiste em o produto ou sistema, poder ser utilizado por usuários específicos para atingir propósitos específicos com eficácia, eficiência e satisfação em um contexto de uso específico;

- **Confiabilidade:** Grau em que um sistema, produto ou componente executa funções especificadas sob condições especificadas por um período de tempo especificado;
- **Segurança:** Segurança é uma das duas características adicionadas na ISO/IEC 25010, em relação a ISO 9126. Essa característica compreende que um produto ou sistema protege as informações e dados, para que pessoas ou outros sistemas ou produtos, tenham o grau de acesso a dados adequado aos seus tipos e níveis de autorização;
- **Manutenibilidade:** Essa característica representa o grau de eficácia e eficiência com que um produto ou sistema pode ser modificado para melhorá-lo, corrigi-lo ou adaptá-lo às mudanças no ambiente e nos requisitos;
- **Portabilidade:** Consiste na eficácia e eficiência com que um sistema, produto ou componente pode ser transferido de um hardware, software ou outro ambiente operacional ou de uso para outro.

4.2 ISO/IEC 25040 E ISO/IEC 25041

A ISO/IEC 25000 possui uma divisão de avaliação de qualidade, a ISO/IEC 2504n. Nesta divisão, são apresentados padrões para requisitos, recomendações e diretrizes para avaliação de produtos de software.

A ISO/IEC 25040 é considerada um modelo e guia de referência de avaliação, nele contém requisitos gerais para especificação e avaliação de qualidade de software. Fornece uma estrutura para avaliar a qualidade do produto de software e estabelece os requisitos para métodos de medição e avaliação do produto de software.

Enquanto a ISO/IEC 25041 é considerada guia de avaliação para desenvolvedores, adquirentes e avaliadores independentes. Na qual é caracterizada por fornecer requisitos, recomendações e diretrizes para desenvolvedores, adquirentes e avaliadores independentes do sistema e produto de software.

O processo de avaliação da qualidade do produto de software de acordo com a ISO/IEC 25040 consiste em 5 etapas: estabelecer os requisitos de avaliação; especificar a avaliação; o projeto da avaliação; executar a avaliação e concluir a avaliação, conforme especificado no quadro 1.

Quadro 1 - Etapas do processo de aquisição de software conforme a ISO/IEC 25040

Etapas	Propósito	Atividades
1° Etapa	Estabelecer os requisitos de Avaliação	Estabelecer o objetivo da avaliação;
		Obter os requisitos de qualidade de produto de software;
		Identificar as partes do produto a serem incluídas na avaliação;
		Definir o rigor da avaliação;
2° Etapa	Especificar a Avaliação	Selecionar medidas de qualidade (módulos de avaliação);
		Definir critérios de decisão para medidas de qualidade;
		Definir critérios de decisão para avaliação;
3° Etapa	Elaborar a Avaliação	Planejar atividades de avaliação;
4° Etapa	Executar a Avaliação	Realizar medições;
		Aplicar critérios de decisão para medidas de qualidade;
		Aplicar critérios de decisão para avaliação;
5° Etapa	Concluir a Avaliação	Revisar o resultado da avaliação;
		Elaborar relatório da Avaliação;
		Revisar a avaliação da qualidade e fornecer feedback à organização;
		Realizar a disposição dos dados de avaliação.

Fonte: ISO/IEC 25040 (2011), tradução próprio autor (2022).

Além de ser uma forma de determinar a aceitação do produto, o processo de avaliação pode ser usado para comparar produtos concorrentes, selecionar alternativas, avaliar os efeitos positivos e negativos de um produto em uso e muito mais.

4.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Ao decorrer deste capítulo foi discorrido de forma geral os principais modelos de aquisição e avaliação de software, que servem como base para a realização da escolha de uma solução de software.

A fundamentação do processo de aquisição e avaliação neste trabalho é apoiado na norma ISO/IEC 25040 que oferece o processo base para a avaliação das ferramentas, enquanto a ISO/IEC 25010 estabelece um conjunto de parâmetros de qualidade de software que serão usados como critérios comparativos.

5 PROPOSTA DE SOLUÇÃO

A proposta de solução deste trabalho baseia-se em analisar ferramentas de MDM, avaliá-los quanto à qualidade de software e a capacidade para auxiliar as organizações a administrarem seus dispositivos móveis. Esta análise permitirá avaliar quais ferramentas realizam o gerenciamento mais adequado conforme os critérios definidos neste capítulo.

5.1 ETAPA 1

De acordo com o processo de aquisição de software demonstrado na ISO/IEC 25040, a primeira etapa tem como propósito estabelecer os requisitos de avaliação. As atividades que fazem parte desta primeira etapa são: determinar o objetivo da avaliação; obter os requisitos de qualidade do produto de software; identificar as partes do produto a serem incluídas na avaliação; determinar o rigor da avaliação.

Conforme evidenciado, o objetivo dessa avaliação de diferentes sistemas de gerenciamento de dispositivos móveis tem como propósito selecionar quais as soluções mais adequadas dentre as alternativas citadas, para posteriormente efetuar a aplicação a um estudo de caso para validação da adequação das ferramentas.

As partes interessadas da avaliação são adquirentes deste tipo de sistema, que buscam uma solução, dentre várias alternativas que possuem disponíveis neste nicho atualmente. Os requisitos de qualidade que serão avaliados, seguem o modelo de qualidade especificado na norma ISO/IEC 25010 apresentada anteriormente.

Fazem parte do escopo de avaliação, requisitos que as ferramentas devem suprir, como os recursos já citados como essenciais, sendo eles *over the air*, inventário, provisionamento, gerenciamento, controle, monitoramento, suporte, segurança, proteção de dados e multiplataforma, além de possuir a utilização do software na nuvem, período de teste gratuito, facilidade em contatar o fornecedor e a funcionalidade de geração de relatórios.

A funcionalidade de geração de relatórios no MDM é desejável para obter informações dos dispositivos móveis, auxiliando desta forma na tomada de uma ação decisiva sobre algum aspecto que precise de atenção.

Existem diversos pontos positivos para a utilização do software na nuvem, como a redução de custos, pois não é preciso alocar recursos internos de infraestrutura para instalação e operação do sistema, além da mobilidade de acesso

e gerenciamento não ser exclusivo de uso interno, proporcionando a possibilidade de escalonamento sem muito esforço caso necessário.

A comunicação com o fornecedor da solução é indispensável para a resolução de eventuais problemas ou dúvidas, por isso ela deve ser facilitada.

Pretende-se por meio do método avaliativo, demonstrar comparações entre as ferramentas, com o intuito de evidenciar qual delas se sobressai como a solução mais apropriada para o cenário proposto anteriormente.

5.2 ETAPA 2

A segunda etapa do processo de aquisição de software tem a finalidade de especificar a avaliação e possui as seguintes atividades: selecionar medidas de qualidade (módulos de avaliação); determinar critérios de decisão para medidas de qualidade; determinar critérios de decisão para avaliação.

Os módulos de avaliação a serem utilizados para avaliação qualitativa das ferramentas selecionadas, têm como base características e subcaracterísticas de qualidade de software descritos na ISO/IEC 25010, conforme apresentado no quadro 2.

Quadro 2 - Características e subcaracterísticas selecionadas para avaliação qualitativa

Característica	**Subcaracterística**
Adequação Funcional	Integridade Funcional
	Aptidão Funcional
Compatibilidade	Interoperabilidade
Confiabilidade	Disponibilidade
	Recuperabilidade
Segurança	Integridade
	Autenticação
Eficiência de Desempenho	Tempo
	Recursos
	Capacidade

Fonte: ISO/IEC 25010, próprio autor (2022).

A característica de adequação funcional é fundamental para validar se o sistema cumpre aquilo que ele propõe com êxito, por isso serão analisadas as subcaracterísticas de integridade funcional e aptidão funcional. A subcaracterística de integridade funcional, também conhecida como completude funcional, é definida sendo a competência no qual o conjunto de funções cobre todas as tarefas especificadas e objetivos do usuário. Destaca-se também a subcaracterística de aptidão funcional, descrita sendo o grau em que as funções do sistema facilitam a realização de tarefas e objetivos especificados. Para uma solução MDM a adequação funcional é utilizada para esclarecer se os recursos e funcionalidades presentes na solução fazem parte do escopo do que compreende o que deve ou não suprir.

A compatibilidade é necessária para determinar se é compatível com outros sistemas, para tal optou-se pela subcaracterística de interoperabilidade, definida pela possibilidade de troca e uso de informações trocadas entre dois ou mais sistemas. Devido a gama de sistemas operacionais, esta característica é utilizada para averiguar quais sistemas operacionais são suportados pela ferramenta de MDM.

A confiabilidade é importante para determinar se o software avaliado possui capacidade de se manter em um bom nível de desempenho, mesmo se utilizado em condições específicas. Entre as subcaracterísticas de confiabilidade escolhidas para serem avaliadas, encontra-se a de disponibilidade, que tem como objetivo medir se o sistema está operacional e acessível quando necessário para utilização, e a de recuperabilidade, no qual se refere que em caso de interrupção ou falha, um sistema pode recuperar os dados diretamente afetados e restabelecer o estado desejado do sistema. Um sistema MDM deve ser confiável para a execução de suas funções tendo disponibilidade sempre que necessário, e em caso de interrupção como a desconexão de internet de algum dispositivo móvel gerenciado, ao restabelecer a conexão, o status do aparelho deve ser atualizado juntamente com suas informações.

A característica de segurança foi selecionada pois é de imprescindível que o ambiente que executa em nuvem, tenha mecanismos que assegurem a seguridade do mesmo. Por isso serão levadas em consideração as subcaracterísticas de integridade e autenticação. Levando em consideração as subcaracterísticas de segurança selecionadas para avaliação, a de integridade se refere ao impedimento de acesso não autorizado ou a modificação de dados do sistema. Enquanto, a autenticação é a identidade de um assunto ou recurso que pode ser comprovada como

aquela reivindicada, ou seja, comprovar que determinado usuário é ele mesmo. A central de administração do sistema MDM possui diversas informações restritas e também possibilita a execução de tarefas de forma remota, portanto a mesma necessita ter mecanismos de verificação de acesso.

A característica eficiência de desempenho foi selecionada pois é essencial entender se o software tem capacidade de manter o desempenho adequado em condições explícitas. Deste modo é utilizado as subcaracterísticas de tempo, que especifica o nível em que os tempos de resposta, processamento e as taxas de rendimento de um sistema ao executar suas funções atendem os requisitos definidos. A subcaracterística de recursos, que representa o grau em que as quantidades e tipos de recursos usados por um sistema ao executar suas funções, e a subcaracterística de capacidade, que corresponde ao grau em que os limites máximos de um parâmetro do sistema atendem os requisitos estipulados. Embora a maioria das soluções de MDM sejam suportadas em nuvem, isso não representa que o desempenho seja melhor por isso. Sendo assim, essa característica deve ser avaliada conforme a necessidade e objetivo proposto.

Conforme apresentado anteriormente, são 8 características de qualidade e 31 subcaracterísticas que contemplam a ISO/IEC 25010, foi selecionado somente as julgadas estarem mais alinhadas com o tipo de sistema a ser avaliado.

5.3 ETAPA 3

Na terceira etapa, conforme apresentado na ISO/IEC 25040, é necessário especificar a avaliação por meio de atividades de planejamento. Desta forma, será realizada a avaliação quantitativa, em que as ferramentas pré-selecionadas serão analisadas e pontuadas de acordo com as informações disponibilizadas pelo fornecedor da solução.

Em conformidade com o que foi destacado anteriormente, leva-se em consideração para a avaliação quantitativa recursos descritos como essenciais para sistemas MDM, sendo eles *over the air*, inventário, provisionamento, gerenciamento e controle, monitoramento e suporte, segurança, proteção de dados, multiplataforma. Também é considerado como requisito a ser avaliado, a presença da funcionalidade de geração de relatórios, além da exigência que a utilização do software seja na

nuvem, assim como a facilidade em contatar à fornecedora para eventuais dúvidas ou suporte.

Através desse conjunto de especificações que as ferramentas devem suprir, é atribuída uma pontuação a cada uma dessas especificações, sendo considerado pontuação “0” quando a especificação não é atendida, pontuação “1” quando a especificação é atendida parcialmente e pontuação “2” quando é a especificação é totalmente atendida.

Para cada recurso e funcionalidade selecionado atribuiu-se um nível de requerimento para ser usado como base para decisão de relevância. Desta forma, cada nível de requerimento possui um multiplicador de nota, sendo atribuído a multiplicação conforme evidenciado no quadro 3. Esse multiplicador é utilizado para que os recursos e funcionalidades mais relevantes tenham um peso maior na pontuação.

Quadro 3 - Multiplicador de pontuação de acordo com o nível de requerimento

Nível de requerimento	**Multiplicador**
Essencial	5X
Importante	2X
Desejável	1X

Fonte: Próprio autor (2022).

Para facilitar a visualização dos nomes das ferramentas no quadro 5, atribuiu-se as seguintes nomenclaturas, conforme apresentado no quadro 4.

Quadro 4 - Nomenclatura das ferramentas

Ferramenta	**Nomenclatura**
Mobile Device Manager Plus	F1
Miradore	F2
Soti MobiControl	F3
IBM MaaS360	F4
Pulsus	F5

Fonte: Próprio autor (2022).

Posteriormente, é preenchido o quadro 5 de acordo com a soma das pontuações atingidas por cada ferramenta e aplica-se o multiplicador para os níveis de requerimento apresentado anteriormente.

Quadro 5 - Métrica para avaliação quantitativa

Recurso	**Requerimento**	**F1**		**F2**		**F3**		**F4**		**F5**	
Over The Air	Essencial (X5)										
Utilização em nuvem	Essencial (X5)										
Gerenciamento e controle	Essencial (X5)										
Monitoramento e suporte	Essencial (X5)										
Provisionamento	Importante (X2)										
Segurança	Importante (X2)										
Proteção de dados	Importante (X2)										
Multiplataforma	Importante (X2)										
Inventário	Importante (X2)										
Facilidade de contato com fornecedor	Desejável (X1)										
Geração de relatórios	Desejável (X1)										
Total			**0**		**0**		**0**		**0**		**0**

Fonte: Próprio autor (2022).

Após obter as pontuações da avaliação comparativa entre as ferramentas, seguindo as etapas definidas para o trabalho, a ferramenta que se destacar das demais deve ser aplicada para uma avaliação qualitativa em relação à adequação de uso, alinhado com o objetivo definido para este estudo.

5.4 ETAPA 4

A próxima etapa estabelecida pela ISO/IEC 25040 expressa sobre a execução da avaliação, em que destaca as atividades de fazer medições, aplicar critérios de medições e aplicar critérios de decisão.

As escalas de medições foram aplicadas de acordo especificado anteriormente, desta forma destaca-se no quadro 6 as pontuações atribuídas para cada uma das ferramentas. Na primeira coluna dentro das colunas de cada ferramenta encontra-se a nota sem a atribuição do multiplicador, enquanto a segunda coluna condiz a nota multiplicada conforme o nível de requerimento.

Quadro 6 - Resultado da avaliação quantitativa

Recurso	**Requerimento**	**F1**		**F2**		**F3**		**F4**		**F5**	
Over The Air	Essencial (X5)	2	10	2	10	2	10	2	10	2	10
Utilização em nuvem	Essencial (X5)	2	10	2	10	2	10	2	10	2	10
Gerenciamento e controle	Essencial (X5)	2	10	2	10	0	0	2	10	1	5
Monitoramento e suporte	Essencial (X5)	1	5	1	5	0	0	1	5	1	5
Provisionamento	Importante (X2)	2	4	2	4	0	0	2	4	1	2
Segurança	Importante (X2)	1	2	1	2	0	0	2	4	0	0
Proteção de dados	Importante (X2)	2	4	1	2	0	0	2	4	0	0
Multiplataforma	Importante (X2)	2	4	2	4	1	2	2	4	1	2
Inventário	Importante (X2)	1	2	1	2	0	0	2	4	2	4
Facilidade de contato com fornecedor	Desejável (X1)	2	2	2	2	1	1	2	2	1	1
Geração de relatórios	Desejável (X1)	2	2	2	2	0	0	2	2	0	0
Total			**55**		**53**		**23**		**59**		**39**

Fonte: Próprio autor (2022).

A busca de informações para o preenchimento do quadro 6 foi realizada através do contato por e-mail e chat com o fornecedor, assim como a ficha de dados quando presente no site de cada fabricante (Mobile Device Manager Plus, Miradore, Soti MobiControl, IBM MaaS360, Pulsus, 2022). Por meio das funcionalidades que cada solução possui, enquadrou-se cada uma delas nos recursos apresentados, e definido quais delas teriam peso maior para a atribuição das notas.

O *Over The Air* é o principal recurso de um sistema gerenciador de dispositivos móveis, em que realiza o envio de comandos ou instruções para dispositivos sem a necessidade de conectá-los por algum cabo, portanto, este recurso é categorizado como essencial. Foi verificado que todas as soluções citadas abrangem este recurso de forma integral, sendo possível realizar diversas funcionalidades sem a obrigatoriedade do uso de algum meio físico de conexão.

A utilização em nuvem é um dos pré-requisitos definidos para a pré-seleção das ferramentas para este trabalho, consequentemente é constatado que todas as ferramentas possuem a utilização em nuvem, não sendo necessário atribuir recursos da infraestrutura local ou de *cloud* pelo adquirente da ferramenta.

Os recursos de gerenciamento e controle são classificados como essenciais devido ao seu objetivo, que consiste em gerenciar diversos aspectos do sistema como aplicativos, tarefas, perfis e aplicações de políticas em relação a permissões e bloqueios. As ferramentas que receberam 1 como nota nesta categoria, possuem como funcionalidade restrições de aplicativos/sites, restrições de recursos (wi fi, câmera, etc…) e disparo de tarefas. Já as que obtiveram a nota 2, contemplam a

mesma gama de funcionalidades das que receberam nota 1, mas que também possuem o modo quiosque, em que possibilita a execução de um único aplicativo na tela do dispositivo, não podendo realizar nenhuma outra ação.

As ferramentas F1, F2 e F4 obtiveram nota 2 pois contemplam as funcionalidades citadas anteriormente para esta nota, enquanto a ferramenta F5 recebeu a nota 1 por não possuir modo quiosque, já ferramenta F3 recebeu nota 0 por não apresentar funcionalidades que pertencessem aos recursos de gerenciamento e controle.

Um dos objetivos do sistema MDM é possibilitar o monitoramento dos dispositivos gerenciados e consequentemente auxiliando a prestar suporte aos mesmos, por este motivo estes dois recursos são categorizados como essenciais. As soluções que receberam nota 1, permitem acesso remoto pela própria plataforma e dispõe de um dashboard com informações de software/hardware, enquanto as que receberam 2 como nota contém as mesmas funcionalidades citadas anteriormente, além de informar a localização em tempo real dos dispositivos e permitir disparo de notificações e alertas.

De acordo com informações obtidas com os fornecedores, cerca de 4 ferramentas alcançaram nota 1 em relação aos recursos de monitoramento e suporte. A ferramenta F1 não cita diretamente o que o *dashboard* apresenta de informações, já a ferramenta F2 não possui acesso remoto diretamente pela ferramenta e também não apresenta quais informações são exibidas no *dashboard*. A ferramenta F4 também não cita quais informações são demonstradas no seu *dashboard*, já a ferramenta F5 não possui a funcionalidade de acessar dispositivos remotamente pela própria solução. Em relação a ferramenta F3, não foi encontrado informações sobre as funcionalidades relacionadas aos recursos de monitoramento ou suporte e em razão disso foi atribuída a nota 0. Destaca-se que mesmo as ferramentas não atendendo totalmente as funcionalidades, as mesmas possuem algumas funcionalidades citadas para atingirem a nota 2, que foi levado em consideração e por este motivo foi aplicado a nota 1 para as mesmas.

Conforme dito anteriormente, o provisionamento é o início do ciclo de vida do dispositivo, por meio deste que é registrado no sistema para realizar o gerenciamento, para este recurso foi catalogado como importante, pois não é a principal função deste tipo de sistema. Foi atribuído a nota 1 as ferramentas que possuem a possibilidade de

provisionamento em massa, ou seja, de vários dispositivos ao mesmo tempo. A nota 2 foi atribuída às ferramentas que além de possuir a funcionalidade de provisionamento em massa, também apresentam ao menos 3 formas de provisionamento citadas, como por exemplo, por meio de código QR, NFC e e-mail.

Dentre as funcionalidades exigidas para as ferramentas atingirem a nota 2, as ferramentas F1, F2 e F4 obtiveram a maior nota para o recurso de provisionamento. Apenas a ferramenta F5 atingiu nota 1, pois apresentou apenas que realiza provisionamento individual e em massa, mas não relatou qual a forma que pode ser realizada, enquanto a ferramenta F3 recebeu nota 0 pois apenas alegou que realiza provisionamento por código de barras e não mencionou se é possível provisionar dispositivos em massa.

A segurança é um dos recursos presentes em sistemas de MDM, portanto não é a especialização deste tipo de sistema, deste modo este recurso é especificado como importante. A atribuição da nota 1 para este critério, tem como base as funcionalidades de limpeza de dispositivo e possuir algum método de autenticação seguro, como suporte a biometria. A nota 2 tem como base as mesmas funcionalidades citadas previamente, além da aplicabilidade de impedir o acesso de dispositivos comprometidos à central de gerenciamento.

Para o recurso de segurança, a ferramenta F4 foi a única que obteve nota máxima, pois somente ela cita que impede o acesso de dispositivos comprometidos à central de gerenciamento, consequentemente a nota 1 foi atribuída às ferramentas F1 e F2 por não possuírem esta funcionalidade. Já as ferramentas F3 e F5 não descrevem sobre funcionalidades de segurança, e por este motivo receberam nota 0.

O acesso a dados por dispositivos móveis é considerado uma brecha de segurança, deste modo se faz necessário a proteção destes dados, mas não é um recurso imprescindível para este tipo de solução, por isto está rotulado como um recurso importante e não essencial. Para a distribuição de notas perante a este recurso, as ferramentas que receberam nota 1 cita ao menos uma funcionalidade, que se refere a criptografia ou auditoria, e a nota 2 possui a menção das duas funcionalidades citadas ou mais.

A respeito do recurso de proteção de dados, as ferramentas F1 e F4 alcançaram nota 2 por possuírem as funcionalidades citadas para a obtenção desta nota, enquanto a F2 recebeu nota 1 por contemplar apenas a funcionalidade de

criptografia de armazenamento. A nota 0 foi atribuída às ferramentas F3 e F5 por não terem sido encontradas informações referentes a este recurso.

Atualmente existe uma gama de sistemas operacionais para dispositivos móveis, assim como as empresas utilizam diversos sistemas voltados para o seu negócio, deste modo, o recurso de multiplataforma é considerado importante para avaliação. Foi levado em consideração para receber nota 1 as soluções que são compatíveis com ao menos 4 sistemas operacionais, sendo eles *Android*, IOS, *Windows* e MacOS, enquanto para nota 2 é utilizado as mesmas funcionalidades citadas para atribuição da nota 1, mas adicionando a possibilidade de integração com outro sistema, como por exemplo o *Active Directory* da Microsoft.

Referente ao recurso de multiplataforma, às ferramentas F1, F2 e F4 conquistaram nota máxima por atenderem aos requisitos definidos para a aplicação da nota 2. Já a ferramentas F3 recebeu nota 1 por não possuir compatibilidade com o sistema operacional MacOS e também por não possibilitar integração com outros sistemas. A ferramenta F5 é compatível somente com sistemas operacionais *Android* e IOS e também não possui possibilidade de integração com outros sistemas.

Através do recurso de inventário obtém-se informações dos dispositivos móveis gerenciados, além de organizar essas informações para visualização, devido a isto é considerado um recurso importante. As ferramentas que obtiveram a nota 1 fornecem informações de *hardware/software*, e os que alcançaram a nota 2 portam funcionalidades de personalização de filtros, exportação de informações, além de apresentar informações de *hardware/software*.

A nota 2 para o recurso de inventário foi concedida as ferramentas F4 e F5, enquanto a nota 1 foi alcançada pelas ferramentas F1 e F2 por que não possuem as funcionalidades de personalização de filtros e exportação de informações. Somente a ferramenta F3 recebeu nota 0 neste quesito pois não disponibilizou informações em sua documentação ou pelo contato realizado com o mesmo.

Outro pré-requisito utilizado é a facilidade de contatar o fornecedor da solução, por não ser um aspecto que atrapalhe na utilização ela é categorizada como desejável. A definição das notas nesta categoria deu-se através de quantos formas de contato é possível utilizar, os que possuem até 2 formas de contato receberam a nota 1, e os que possuem mais de duas formas de contato e disponibilizam material de tutorial da solução ganharam a nota 2. Dentre as ferramentas pré-selecionadas, as ferramentas

F1, F2 e F4 adquiriram a nota 2 por contemplarem o que foi definido para a obtenção desta nota, enquanto as ferramentas F3 e F5 obtiveram a nota 1 por que não possui informações claras do funcionamento de funcionalidades de suas soluções.

O pré-requisito de geração de relatórios é considerado desejável para um MDM, pois não é algo que possa ser considerado essencial ou importante, ou seja, é apenas uma função adicional que facilita a sustentação de uma ação sobre um dispositivo. As soluções que receberam nota 1 possuem relatórios pré-definidos para utilização, enquanto as que receberam nota 2 possuem relatórios pré-definidos, permitem customização de parâmetros para a geração de relatórios e também permitem a exportação dos relatórios. Tiveram a nota 2 as ferramentas F1, F2 e F4 por contemplarem o que estabelecido para a atribuição desta nota, enquanto as ferramentas F3 e F5 receberam a nota 0 por que não possibilitam a customização e exportação de relatórios.

5.5 CONSIDERAÇÕES FINAIS DO CAPITULO

Este capitulo apresentou a realização das etapas definidas para a proposta de solução deste trabalho de acordo com a ISO/IEC 25040, em que foi realizada a definição de critérios de qualidade em conformidade com a ISO/IEC 25010 justificando o uso das características de qualidade selecionadas para sistemas gerenciadores de dispositivos móveis.

Ainda neste capitulo, foi realizada avaliação quantitativa em que foram atribuídas pontuações para as ferramentas pré-selecionadas a serem avaliadas. Vale destacar que a ferramenta F4 se mostrou mais aderente ao que foi avaliado perante as demais, chegando à pontuação de 59, enquanto a ferramenta F3 foi a pior pontuada com 23 pontos por não dispor de documentação suficiente sobre as funcionalidades que a mesma possui em seu site e pelo contato realizado.

Deste modo, a ferramenta F4 e F1 foram selecionadas para a realização da avaliação qualitativa, em que será submetida a testes com o intuito de validar a sua adequação de acordo com o que foi proposto.

6 AVALIAÇÃO QUALITATIVA

A avaliação qualitativa pertence a etapa 4 citada na ISO/IEC 25040, em que foi definido que as ferramentas que se destacaram das demais na avaliação quantitativa são submetidas a teste para validação de critérios de qualidade, os critérios para medição de qualidade selecionados estão presentes no quadro 7.

Quadro 7 - Critérios de medições de qualidade para avaliação qualitativa

Medida de qualidade	Critério de medição de qualidade
Adequação Funcional	Atende aos objetivos definidos pelo usuário (Integridade Funcional); A ferramenta possui funcionalidades fáceis de utilizar (Aptidão Funcional).
Compatibilidade	Realiza troca de informações com dois ou mais sistemas operacionais (Interoperabilidade).
Confiabilidade	A disponibilidade da ferramenta deve ser o tempo todo (Disponibilidade); Em caso de falhas, a recuperação de informações e o estado da ferramenta deve ser o mais breve possível (Recuperabilidade).
Segurança	A ferramenta deve impedir acesso não autorizado (Integridade); A ferramenta deve conter o mecanismo de login adequado para comprovação de acesso (Autenticação).
Eficiência de desempenho	O tempo de resposta de uma ação iniciada pelo usuário do sistema deve ser em menos de 30 segundos (Tempo); O agente de comunicação utilizado nos dispositivos não deve consumir muitos recursos do aparelho (Recursos); A ferramenta deve suportar gerenciar no mínimo 25 dispositivos móveis (Capacidade).

Fonte: Próprio autor (2022).

Os testes foram realizados em um dispositivo físico da Samsung, modelo A03 Core que possui 32GB de memória *rom*, 2GB de memória *ram* e sistema operacional *Android* versão 11, o mesmo é mostrado na Figura 4, vale comentar que este dispositivo é considerado de entrada devido as suas características de hardware. Para a realização dos testes o dispositivo foi restaurado para o padrão de fábrica. Como as ferramentas são todas em nuvem, é necessário apenas possuir acesso à internet e um navegador *web* para acesso ao painel de gerenciamento. Desta forma, foi realizado o cadastro no site da solução para utilizar a versão de avaliação gratuita.

Figura 4 – Dispositivo Samsung A03 Core

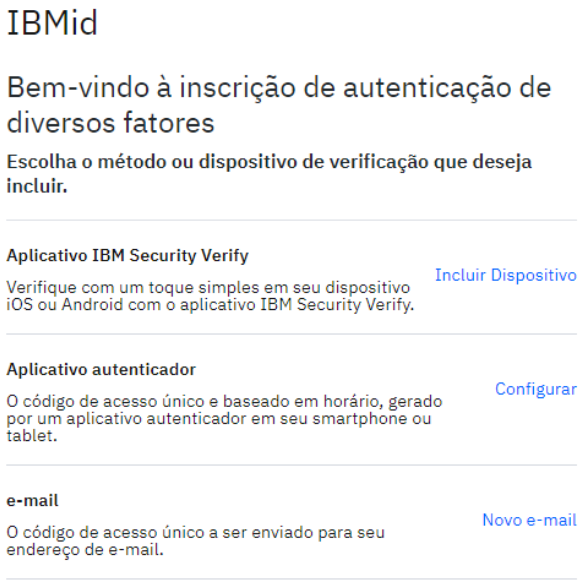
Fonte: Casas Bahia (2022).

As ferramentas IBM MaaS360 e Mobile Device Manager Plus obtiveram pontuações maiores e se destacaram das demais na avaliação quantitativa, e por isso são colocadas para a validação do seu uso de acordo com os critérios de qualidade definidos.

6.1 IBM MAAS360

O acesso para avaliação gratuita foi concedido após realizar o cadastro no site da solução. O primeiro acesso ao painel de gerenciamento foi solicitado para configurar um método adicional para login, conforme mostrado na Figura 5.

Figura 5 – Opções de diversos fatores



Fonte: IBM MaaS360 (2022).

Foi escolhida a opção “aplicativo autenticador” e configurado para utilização no aplicativo *Authenticator* da Google, a configuração foi fácil e rápida, bastou abrir o aplicativo e realizar a leitura do código QR disponibilizado no site.

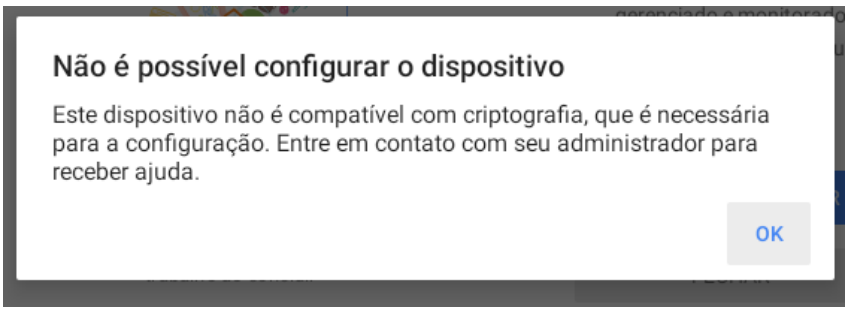
Ao decorrer do uso da solução, navegando sobre os menus e realizando parametrizações de algumas funcionalidades, percebeu-se diversas mensagens retornando erro, que é demonstrado pela Figura 6, estas mensagens acabam atrapalhando o fluxo de aprendizado e descobrimento da ferramenta, assim como o próprio âmbito de salvar as alterações.

Figura 6 – Mensagem de erro

Fonte: IBM MaaS360 (2022).

O primeiro passo realizado para validação foi a de provisionamento, em que foi parametrizado para adicionar o dispositivo por meio de código QR. Em seguida, foi instalado o aplicativo MaaS360 MDM for Android no dispositivo para fazer a leitura do código QR gerado pelo painel de gerenciamento, e assim adicionar o dispositivo para gerenciamento. Entretanto, não foi possível realizar o provisionamento pois sempre que era realizado a leitura do código QR, retornava a mensagem no dispositivo conforme mostra a Figura 7.

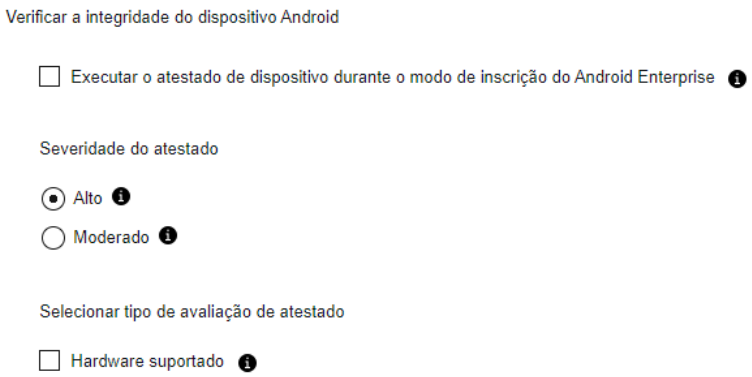
Figura 7 – Dispositivo incompatível



Fonte: IBM MaaS360 (2022).

Essa situação foi contornada desabilitando a verificação de integridade durante o provisionamento do dispositivo, conforme é demonstrado na Figura 8.

Figura 8 – Desabilitando verificação de integridade durante a inscrição



Fonte: IBM MaaS360 (2022).

Posteriormente foi realizado uma nova tentativa de leitura do código para provisionamento do dispositivo, mas outra mensagem de erro foi retornada conforme é mostra na Figura 9.

Figura 9 – Erro “não é possível adicionar um perfil de trabalho”

Fonte: IBM MaaS360 (2022).

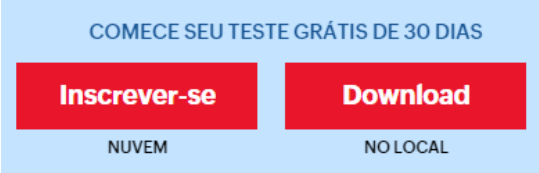
Imediatamente foi consultado a vasta documentação presente no site, onde pouco se achou sobre a mensagem em especifico, então foi acionado o suporte pelo chat da solução em que a conversa era somente em inglês. Houve muita demora de

resposta por parte da IBM no chat e nenhuma solução, pois foi alegado que como a ferramenta estava no período de avaliação, não poderiam prestar treinamento por este meio de comunicação. Devido a isso, não foi possível validar a solução da IBM, pois sem o provisionamento do dispositivo no painel de gerenciamento, é impossível testar as demais funcionalidades e características definidas no escopo do trabalho.

6.2 MOBILE DEVICE MANAGER PLUS

Para ter acesso a avaliação gratuita da ferramenta, foi necessário escolher entre testar na nuvem ou no local como mostra a Figura 10. Vale destacar que apenas esta ferramenta possui estas duas versões, como definido anteriormente para este trabalho foi escolhido a versão em nuvem. Após escolher o local de teste, realizou-se o cadastro no site para ter acesso a plataforma de gerenciamento.

Figura 10 – Opções de locais de teste

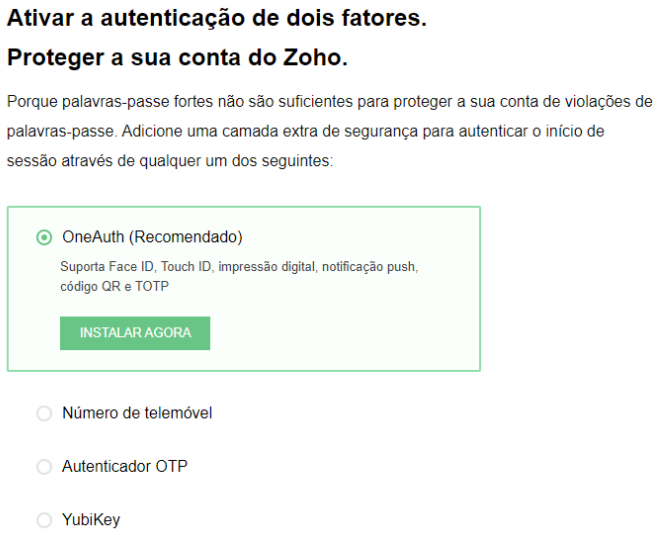


Fonte: Mobile Device Manager Plus (2022).

Após fazer o cadastro, o primeiro acesso ao painel solicita para configurar a autenticação de dois fatores, em que dispõe de 4 opções que são mostradas na Figura 11. Foi selecionado a opção “autenticação OTP” e configurado para utilização no aplicativo *Authenticator* da Google, a configuração foi fácil e rápida, bastou abrir o aplicativo e realizar a leitura do código QR disponibilizado no site. Vale destacar que a configuração de autenticação de dois fatores por OTP pode ser configurado em qualquer aplicativo de gerenciamento de senhas que suporte esse recurso.

A ferramenta impede acesso não autorizado conforme é apontado na Figura 12, porém ao negar a autenticação não envia nenhuma notificação para o e-mail cadastrado relatando que houve uma tentativa de login falha.

Figura 11 – Opções de autenticação de dois fatores



Fonte: Mobile Device Manager Plus (2022).

Figura 12 – Autenticação recusada

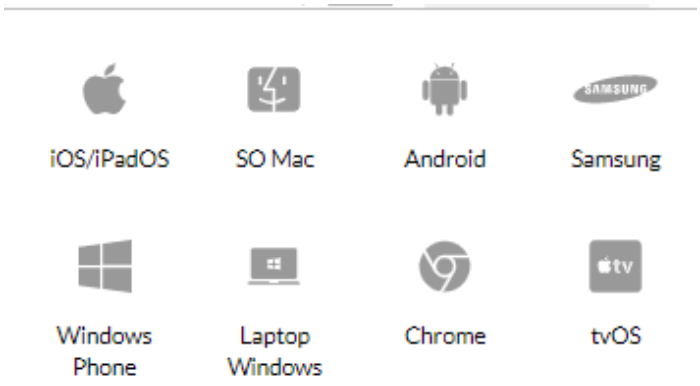
Fonte: Mobile Device Manager Plus (2022).

Para realizar o teste adequação funcional da ferramenta é obrigatório ter pelo menos um dispositivo adicionado no painel, com essa finalidade é necessário provisionar o dispositivo, porém se tem a disponibilidade de apenas um dispositivo para testes, o que impede de realizar o provisionamento em massa.

Com o dispositivo tendo as configurações padrões concluídas, sendo elas a seleção de fuso horário e localidade, rede sem fio a ser conectada e conta google vinculada. Foi instalado o aplicativo ManageEngine MDM pela loja de aplicativos para adicionar o dispositivo ao painel de gerenciamento.

No painel de gerenciamento, o registro de dispositivos é realizado na aba “cadastro”, em que ao clicar em “inscrever dispositivos” deve-se escolher o sistema operacional do dispositivo a ser adicionado, conforme mostra a Figura 13. De acordo com as opções de sistemas operacionais listadas, já demonstra que a solução possui compatibilidade com sistemas operacionais mais utilizados atualmente.

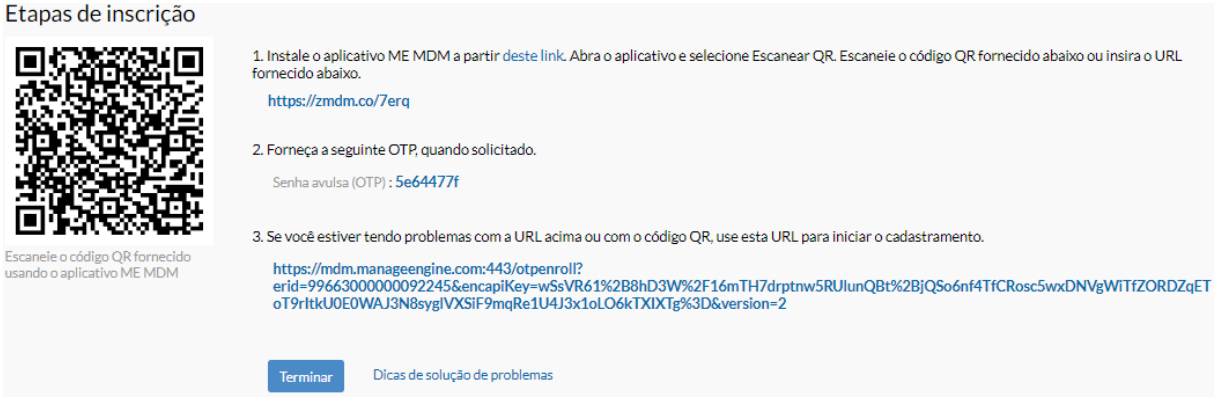
Figura 13 – Escolha de sistema operacional para provisionamento



Fonte: Mobile Device Manager Plus (2022).

Devido ao dispositivo de testes ser da *Samsung*, escolheu-se esta opção e pulou-se para a etapa de provisionamento, que foi através da leitura do código QR gerado no painel da ferramenta demonstrada na Figura 14. A leitura do código QR é realizada pelo aplicativo ManageEngine MDM instalado no dispositivo de acordo com o que a Figura 15 exibe.

Figura 14 – Código QR para provisionamento



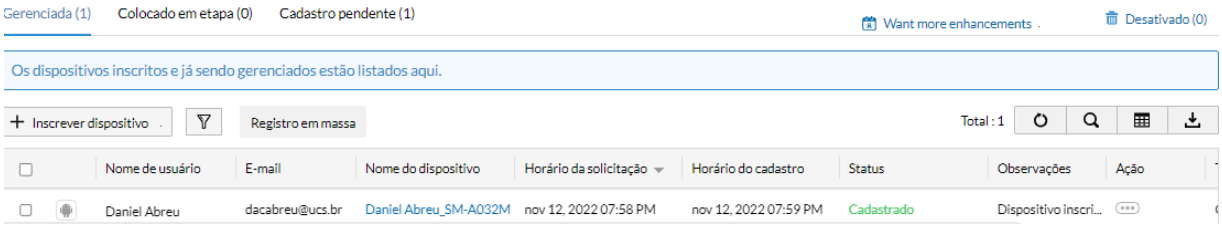
Fonte: Mobile Device Manager Plus (2022).

Figura 15 – Escaneamento do código QR

Fonte: Mobile Device Manager Plus (2022).

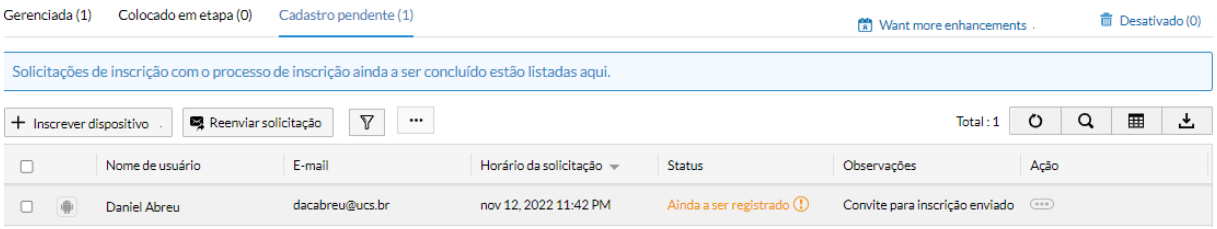
Após a leitura do código QR, se encerra e etapa de inscrição do dispositivo e o mesmo aparece com status “Cadastrado” como exibe a Figura 16, caso não se encerre a etapa de inscrição o status obtido é de “Ainda a ser registrado” é possível terminar o cadastro na aba “Cadastro pendente” como mostra a Figura 17.

Figura 16 – Status cadastrado



Fonte: Mobile Device Manager Plus (2022).

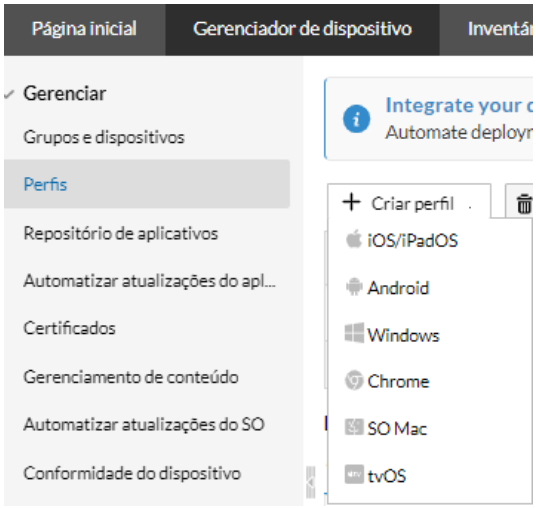
Figura 17 – Status pendente



Fonte: Mobile Device Manager Plus (2022).

Com o dispositivo registrado no painel da solução, é possível realizar o gerenciamento do mesmo conforme a necessidade. A interface do painel de gerenciamento é intuitiva e fácil de manipular, porém contém muitas funcionalidades dependentes de outras o que leva tempo para achar nos menus existentes. Para realizar o gerenciamento e controle, é necessário criar um perfil de acordo com o tipo de sistema operacional desejado conforme é exibido na Figura 18.

Figura 18 – Criação de perfil

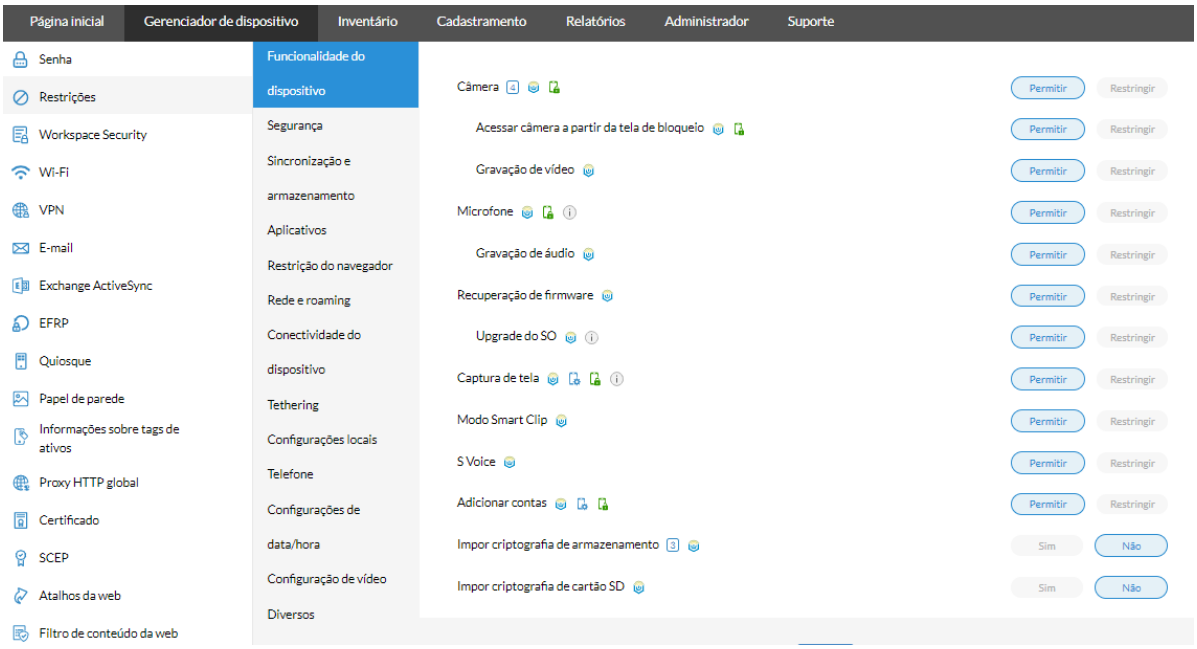


Fonte: Mobile Device Manager Plus (2022).

No perfil é possível atribuir diversas configurações de restrições, permissões e parametrizações conforme destacado nas Figuras 19, 21 e 22. Por ter muitas opções foi destacado apenas as funcionalidades usadas como base para aplicação de pontuação no recurso de gerenciamento e controle na avaliação qualitativa.

Para testar, foi criado um perfil restringindo acesso aos recursos de câmera, microfone e *bluetooth*. Neste mesmo perfil, foi restringido o acesso ao navegador, assim como bloqueado alguns sites para acesso pelo mesmo, além de restringir a permissão do usuário de desinstalar aplicativos e instalar aplicativos não autorizados, por último foi adicionado o papel de parede a partir de uma imagem que foi feito o upload para a ferramenta.

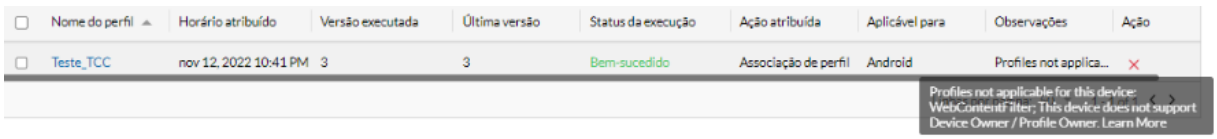
Figura 19 – Controle de recursos e funcionalidades



Fonte: Mobile Device Manager Plus (2022).

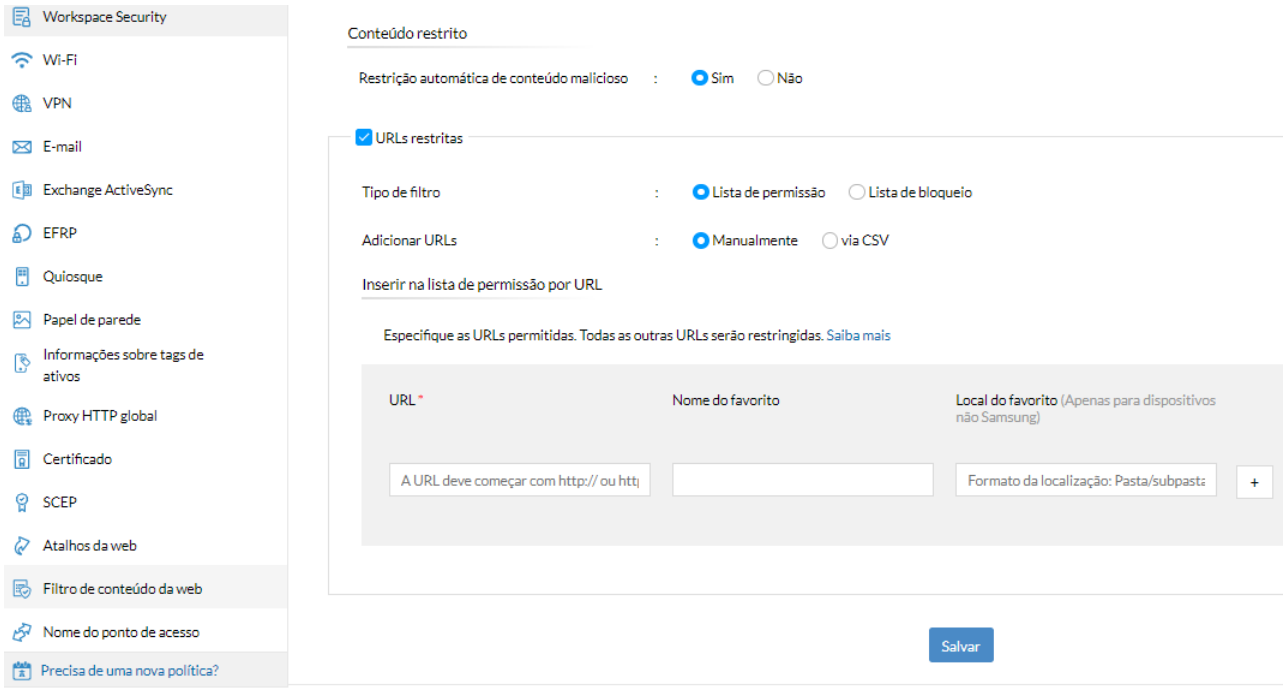
Com as parametrizações efetuadas no perfil que foi criado e associado ao dispositivo para aplicar as regras citadas, o perfil obteve status “bem sucedido” como a Figura 20 mostra, porém apenas o papel de parede foi aplicado corretamente no dispositivo, o restante foi validado e continua funcionando normalmente. Foi encontrado na documentação que era necessário dar permissão de administrador no dispositivo, entretanto mesmo após permitir o aplicativo o problema persiste.

Figura 20 – Status de associação de perfil



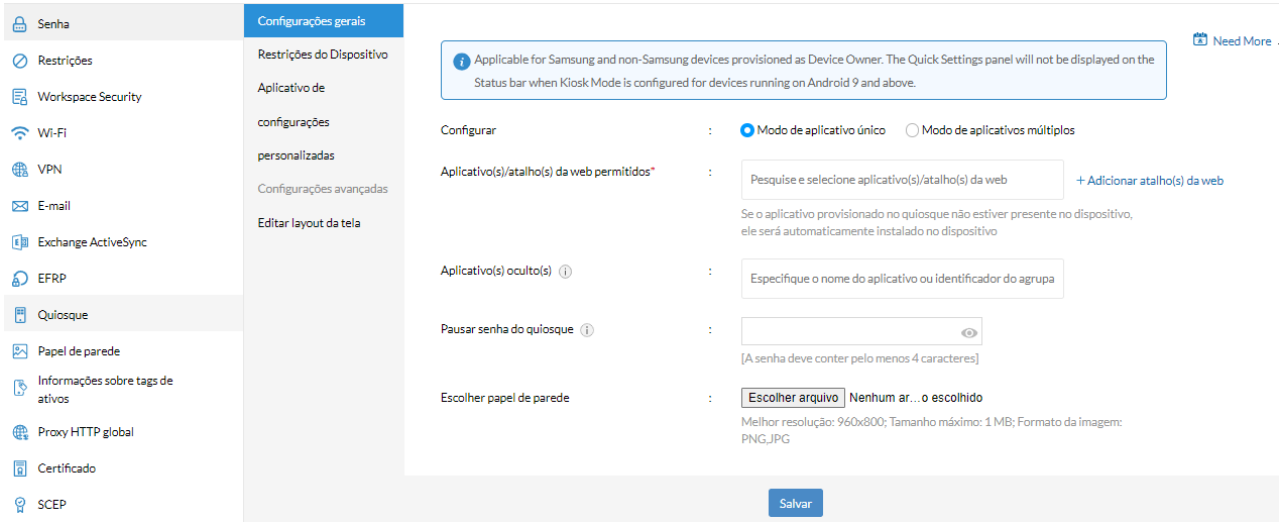
Fonte: Mobile Device Manager Plus (2022).

Figura 21 – Controle *Web*



Fonte: Mobile Device Manager Plus (2022).

Figura 22 – Modo quiosque



Fonte: Mobile Device Manager Plus (2022).

Não foi possível validar o uso de modo quiosque, ao tentar aplicar a política para o dispositivo é retornado que o mesmo foi configurado com a conta de proprietário do perfil, conforme demonstrado na Figura 23.

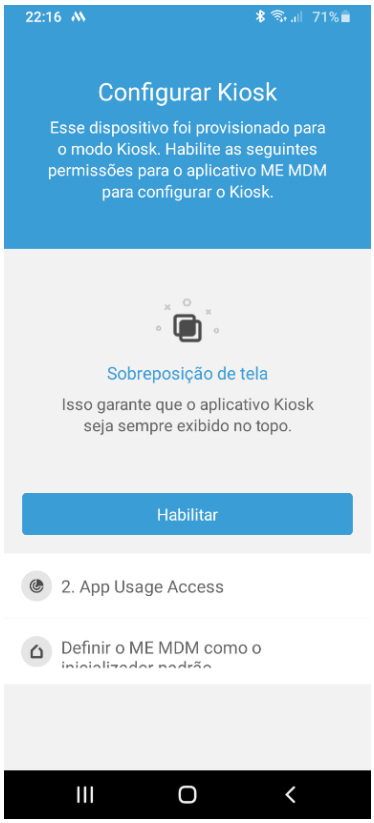
Figura 23 – Observação ao aplicar modo quiosque

Status da execução	Ação atribuída	Aplicável para	Observações
Com falha	Associação de perfil	Android	As informações da tag do ativo não se aplicam aos dispositivos do proprietário do perfil.

Fonte: Mobile Device Manager Plus (2022).

Porém no dispositivo ao sincronizar com o painel de gerenciamento, aparece a opção de configurar o modo quiosque de acordo com a Figura 24. Entretanto, ao prosseguir é apresentado que o recurso não está disponível pois foi desativado por que causa lentidão no *smartphone*, exibido na Figura 25.

Figura 24 – Permitindo modo quiosque no dispositivo



Fonte: Mobile Device Manager Plus (2022).

Figura 25 – Recurso desabilitado

Fonte: Mobile Device Manager Plus (2022).

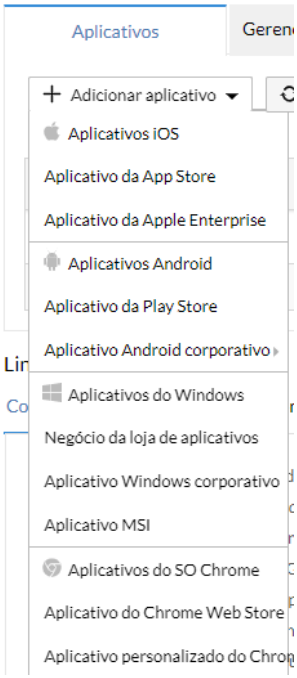
Ainda na parte de gerenciamento e controle, com o intuito de organização tem-se a disposição opções de criação de grupos em que é possível associar perfis, dispositivos, aplicativos e arquivos ao grupo criado.

A solução também permite a distribuição de aplicativos, em que podem ser adicionados ao repositório de aplicativos da ferramenta podendo ser baixados pelo próprio usuário no dispositivo por meio do catalogo, ou realizar a distribuição silenciosa, que não tem a necessidade de interação do usuário para o aplicativo ser instalado. Para adicionar aplicativos ao repositório, deve-se selecionar para qual plataforma quer incorporar conforme é mostrado na Figura 26.

Contudo para realizar as distribuições de aplicativos é necessário configurar o Google Play gerenciado que é demonstrado na Figura 27. Sem esta configuração não é possível instalar e nem gerenciar nenhum aplicativo pela ferramenta.

A configuração do Google Play gerenciado pode ser realizada com ou sem uma conta Gsuite, conforme apresentado na Figura 28.

Figura 26– Seleção de plataforma para adicionar aplicativo



Fonte: Mobile Device Manager Plus (2022).

Figura 27 – Google Play gerenciado

Fonte: Mobile Device Manager Plus (2022).

Como não há disponibilidade da assinatura do serviço Gsuite para a realização deste trabalho, foi realizada a configuração sem uma conta Gsuite, a Figura 29 ilustra a tela de configuração desta etapa.

Para prosseguir com a configuração basta informar o nome da empresa e o nome do provedor de gerenciamento de mobilidade empresarial, de acordo com o que a Figura 30 mostra.

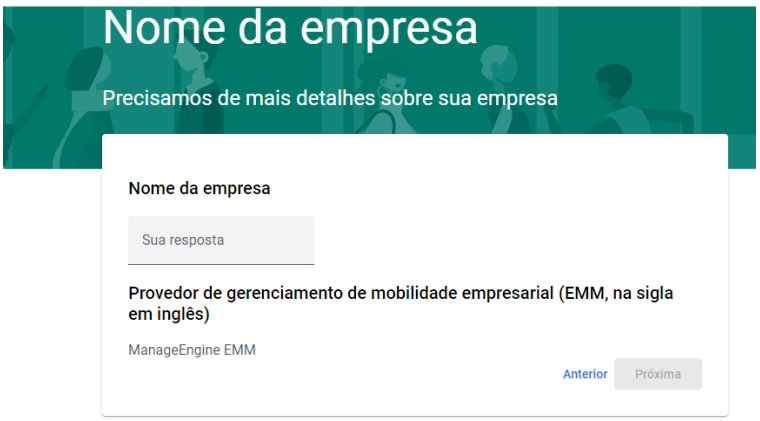
Figura 28 – Opções de configuração do Google Play gerenciado

Fonte: Mobile Device Manager Plus (2022).

Figura 29 – Etapa de configuração sem conta Gsuite

Fonte: Mobile Device Manager Plus (2022).

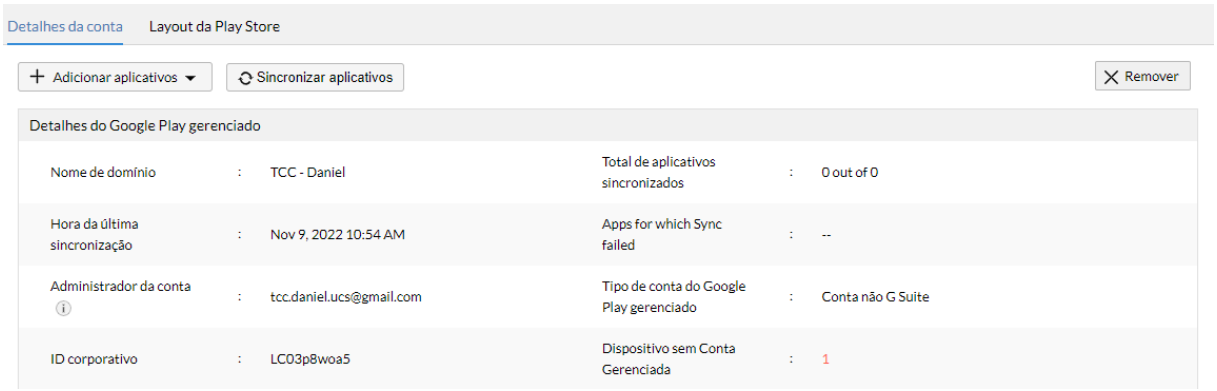
Figura 30 – Informações para registro no Google Play gerenciado



Fonte: Mobile Device Manager Plus (2022).

Após terminar a configuração desta etapa, é possível visualizar os detalhes do Google Play gerenciado, em que informações como total de aplicativos sincronizados, última sincronização, o tipo de conta, entre outras conforme é mostrado na Figura 31.

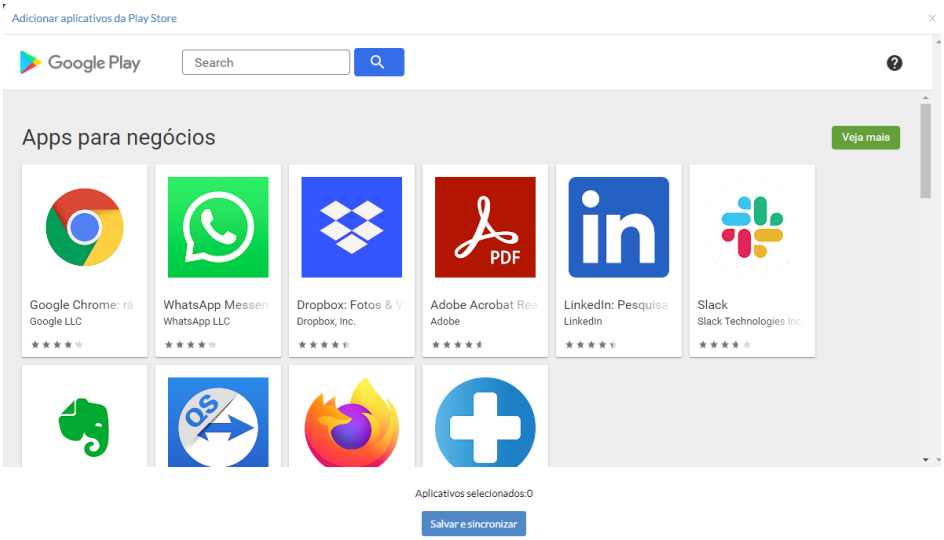
Figura 31 – Detalhes Google Play gerenciado



Fonte: Mobile Device Manager Plus (2022).

Com a conta configurada, é permitido navegar pela Google Play para escolher aplicativos a serem adicionados ao catalogo de aplicativos da ferramenta, conforme demonstra a Figura 32.

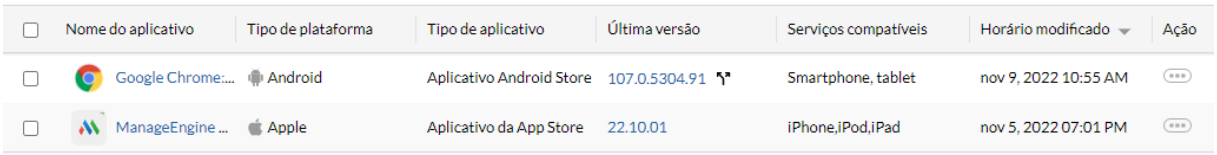
Figura 32 – Aplicativos Google Play



Fonte: Mobile Device Manager Plus (2022).

Após adicionar o aplicativo no catalogo, fica disponível para visualização os detalhes do mesmo, mostrando informações versão, horário de modificação, serviços compatíveis, entre outras que são evidenciadas na Figura 33.

Figura 33 – Detalhes de aplicativos do catalogo



Fonte: Mobile Device Manager Plus (2022).

Para distribuir os aplicativos, basta selecionar o dispositivo, grupo, ou usuário que desejar e clicar na opção “ação” e escolher “distribuir aplicativos”, neste caso foi selecionado por dispositivo conforme mostra a Figura 34.

Figura 34 – Seleção de dispositivo para distribuição de aplicativo

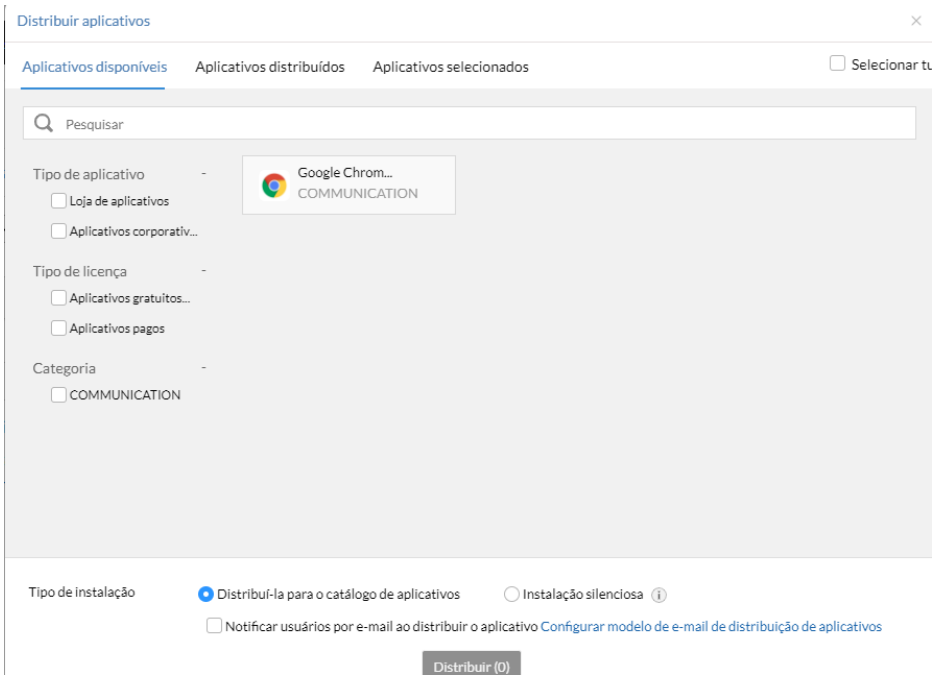
Fonte: Mobile Device Manager Plus (2022).

Ao clicar em distribuir aplicativos, é necessário escolher qual aplicativo do catalogo deseja distribuir, e após isso, definir se deseja distribuir de forma silenciosa em que o mesmo é instalado sem interação pelo usuário, ou apenas se deseja aparecer listado no catalogo de aplicativos no aplicativo ManageEngine MDM para o próprio usuário realizar a instalação, de acordo com o que a Figura 35 mostra.

A respeito do recurso de monitoramento, a página inicial da solução é o dashboard que exibe diversas informações relevantes, como a quantidade de dispositivos registrados, dispositivos inativos, dispositivos com cadastro pendente, dispositivos com aplicativos bloqueados e número de usuários cadastrados. Na página inicial também é encontrado informações por meio de gráficos de pizza, estão presentes referencias sobre tipos de dispositivos, tipos de sistemas operacionais, resumo de aplicativos informando a porcentagem dos permitidos e bloqueados. Também é exibido um gráfico de barras que contém o resumo dos dispositivos gerenciados com base no tempo de último contato. Destaca-se também o feed de log

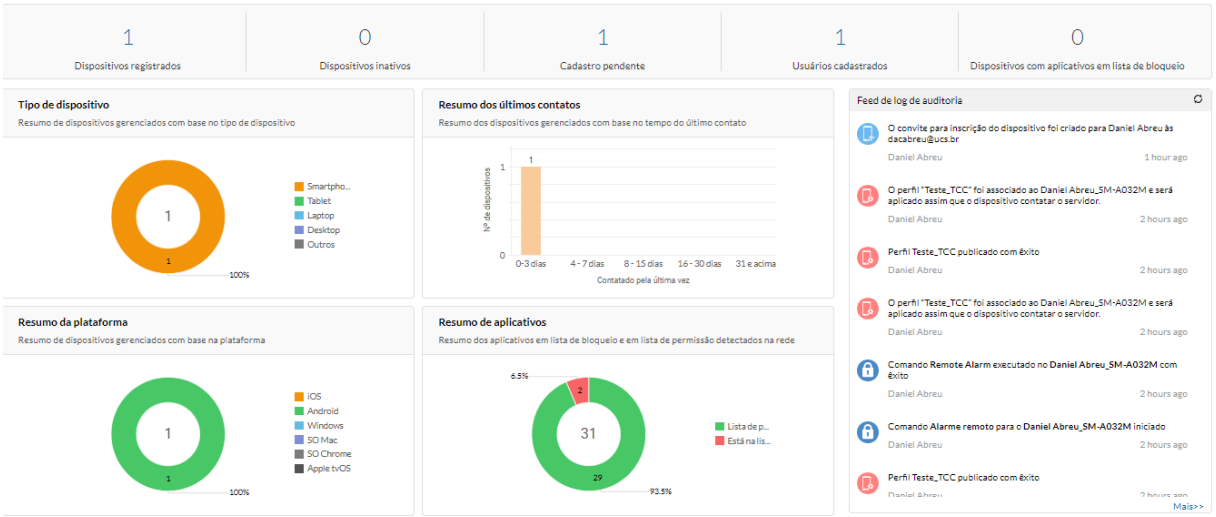
de auditoria, que é encontrado no lado direito da página inicial. Os dados citados anteriormente são demonstrados conforme na Figura 36.

Figura 35 – Seleção de aplicativo para distribuição



Fonte: Mobile Device Manager Plus (2022).

Figura 36 – *Dashboard*



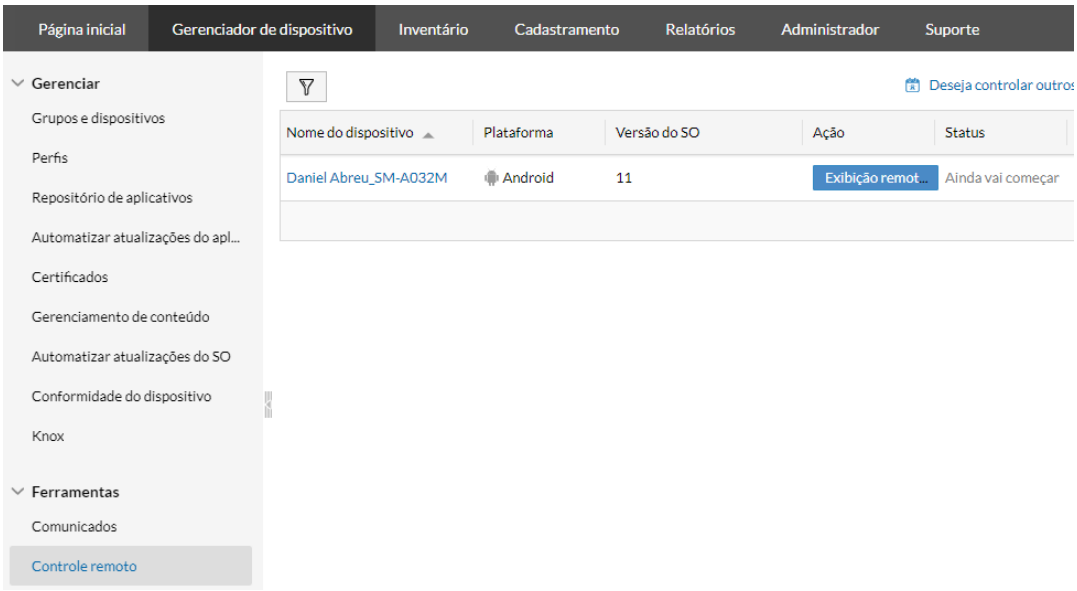
Fonte: Mobile Device Manager Plus (2022).

Para o recurso de suporte a ferramenta dispõe da funcionalidade de acesso remoto pelo próprio painel de gerenciamento de acordo com o que a Figura 37 apresenta. Porém ao tentar realizar o acesso remoto no dispositivo, a seguinte

mensagem é exibida “não é possível iniciar a sessão remota: comando não aplicável para o dispositivo” conforme mostra a Figura 38. Ao clicar em saiba mais, é direcionado para uma página de ajuda, porém foi validado as informações presentes na documentação e não foi encontrado a solução para o não funcionamento desta funcionalidade de acesso remoto.

Referente a proteção de dados, a solução conta com a funcionalidade de auditoria e criptografia de armazenamento. É possível configurar o retorno de logs conforme sua necessidade com as opções disponíveis conforme é demonstrada na Figura 39.

Figura 37 – Acesso remoto

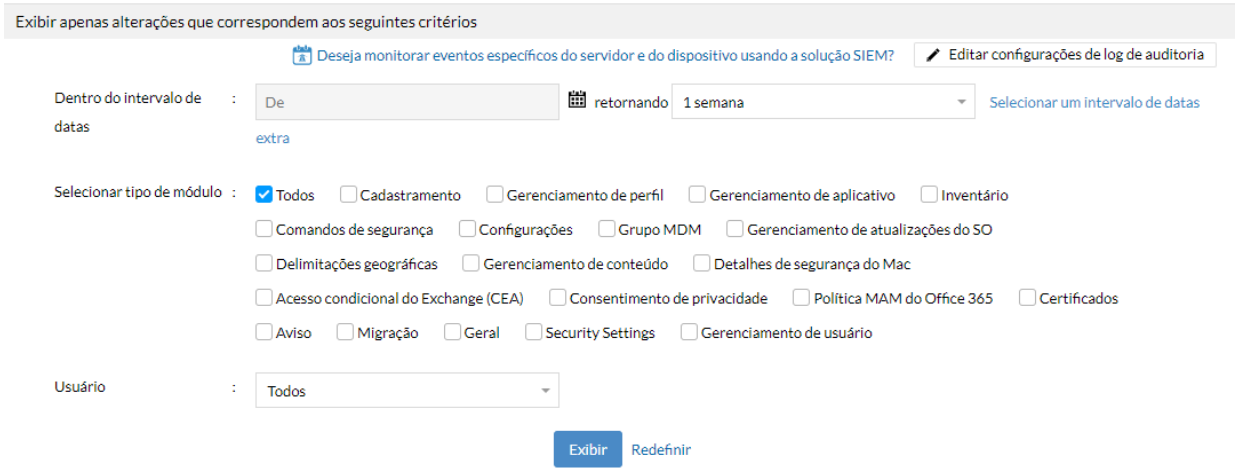


Fonte: Mobile Device Manager Plus (2022).

Figura 38 – Erro ao iniciar sessão remota

Fonte: Mobile Device Manager Plus (2022).

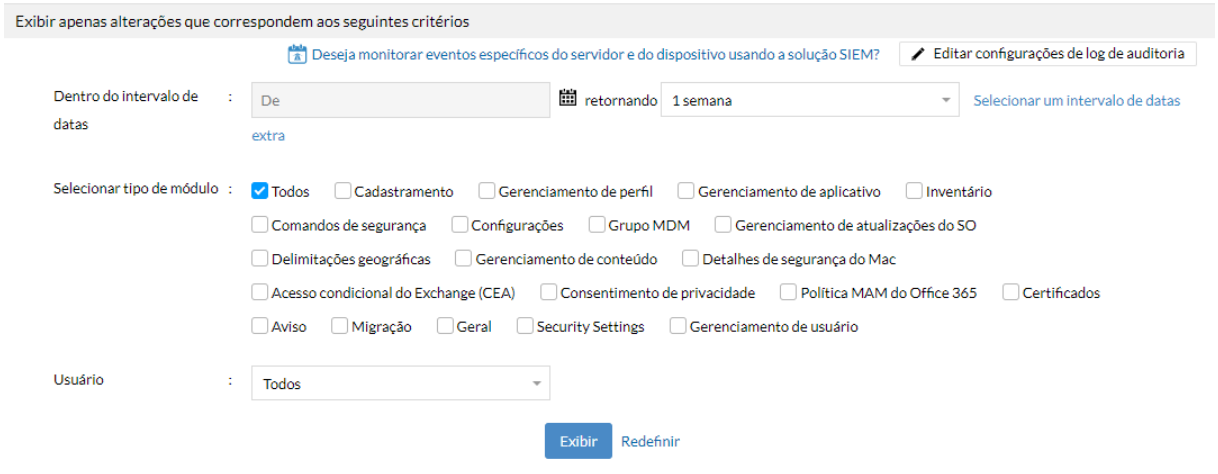
Figura 39 – Logs de auditoria



Fonte: Mobile Device Manager Plus (2022).

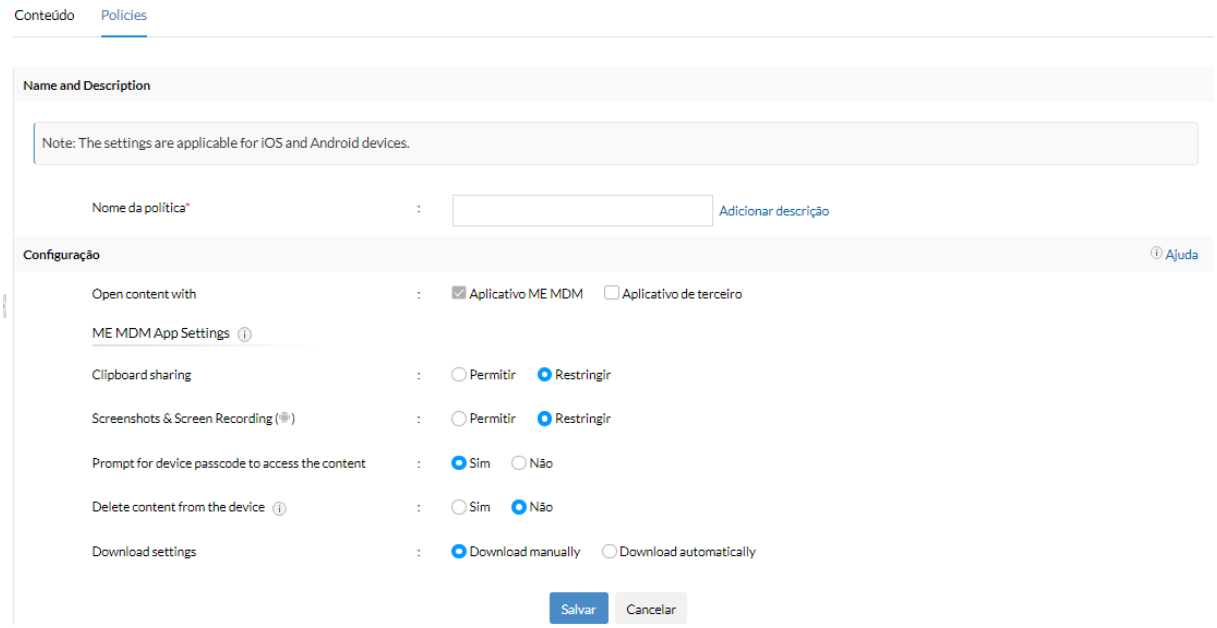
Já a criptografia é referenciada apenas nas documentações que cita criptografia para armazenamento, mas não descreve qual método e tipo de criptografia é utilizado. Vale destacar que para acessar arquivos é necessário fazer o upload no painel de gerenciamento da ferramenta na aba de gerenciamento de conteúdo, de acordo com o que é exibido na Figura 40. Também é possível configurar políticas para cada arquivo conforme mostra a Figura 41. O acesso ao arquivo é realizado pelo aplicativo ManageEngine MDM no dispositivo.

Figura 40 – Gerenciamento de conteúdo



Fonte: Mobile Device Manager Plus (2022).

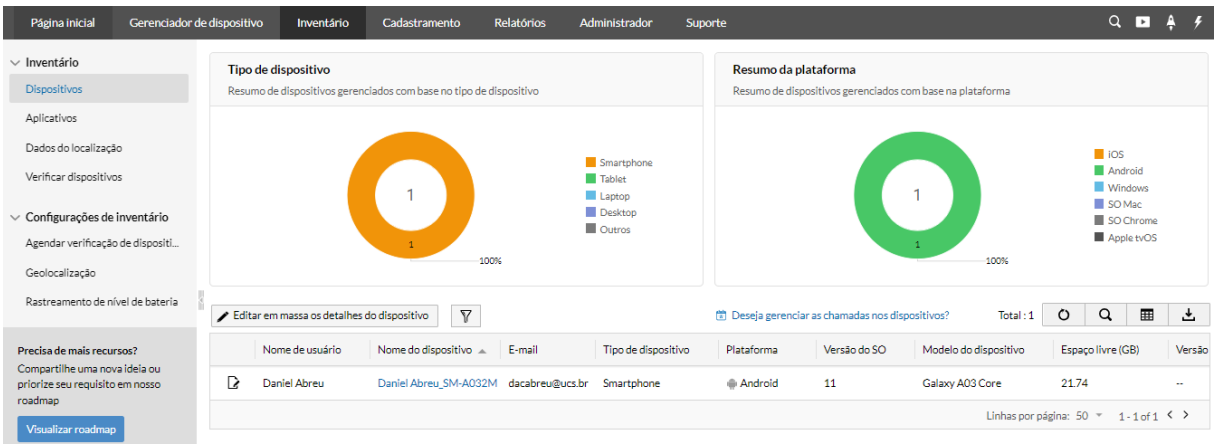
Figura 41 – Política de gerenciamento de conteúdo



Fonte: Mobile Device Manager Plus (2022).

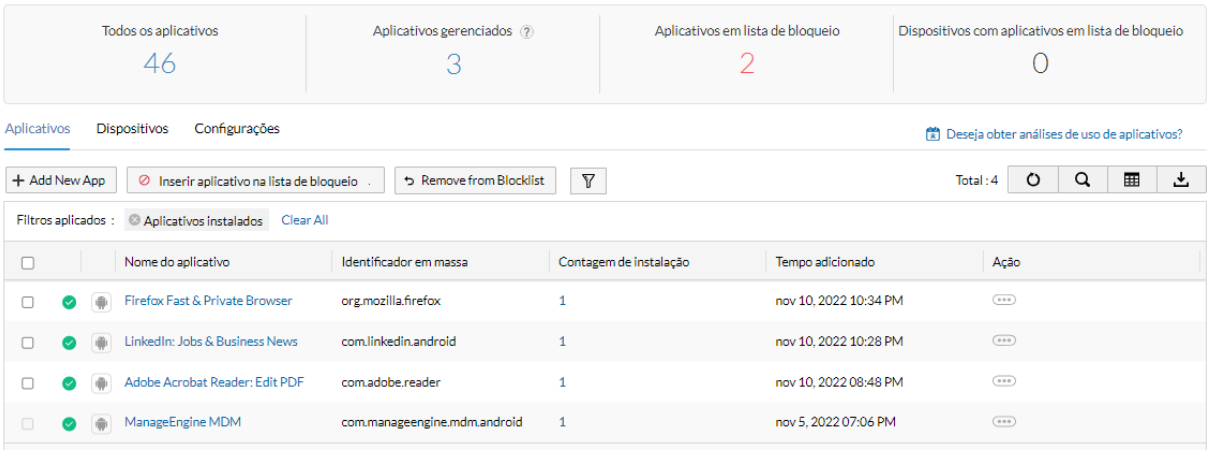
A ferramenta dispõe de recurso de inventário que consiste em trazer informações dos dispositivos, de aplicativos e dados de localização dos mesmos conforme é demonstrado nas Figura 42, 43 e 44. Também pode-se configurar agendamentos de verificação dos dispositivos, assim como definir opções da geolocalização que será imposta aos dispositivos ou grupo de dispositivos definidos. Além disso, é possível parametrizar o rastreamento do nível de bateria dos dispositivos gerenciados para gerar relatórios sobre isso quando necessário.

Figura 42 – Inventário de dispositivos



Fonte: Mobile Device Manager Plus (2022).

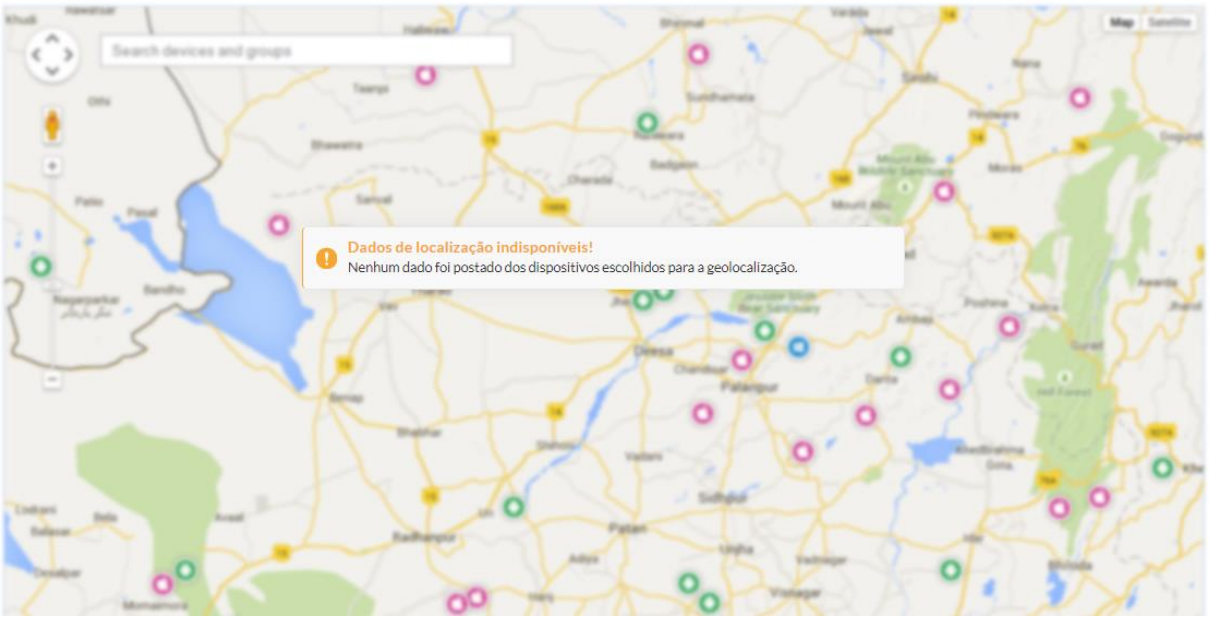
Figura 43 – Inventário de aplicativos



Fonte: Mobile Device Manager Plus (2022).

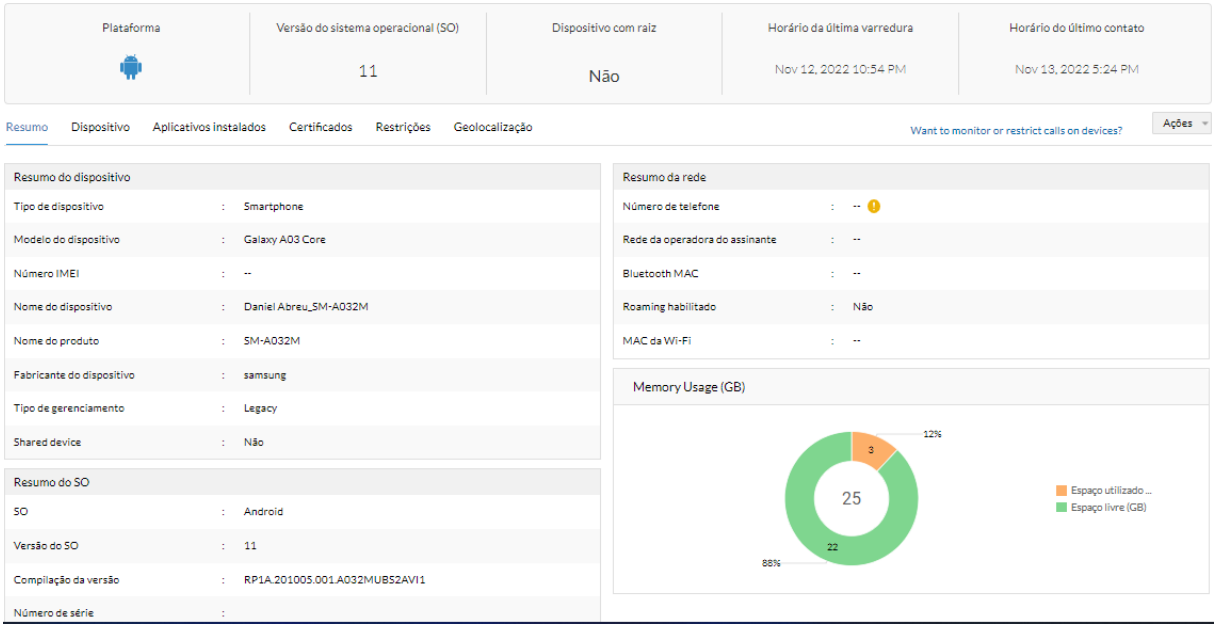
Ao clicar no dispositivo que deseja obter informações no inventário, visualiza-se um resumo de informações sobre o mesmo, com informações de rede, sistema operacional, de segurança, assim como status de atestado de segurança de rede e também sobre a memória *rom* utilizada, demonstrada através de um gráfico de pizza conforme demonstra as Figuras 45 e 46.

Figura 44 – Dados de localização



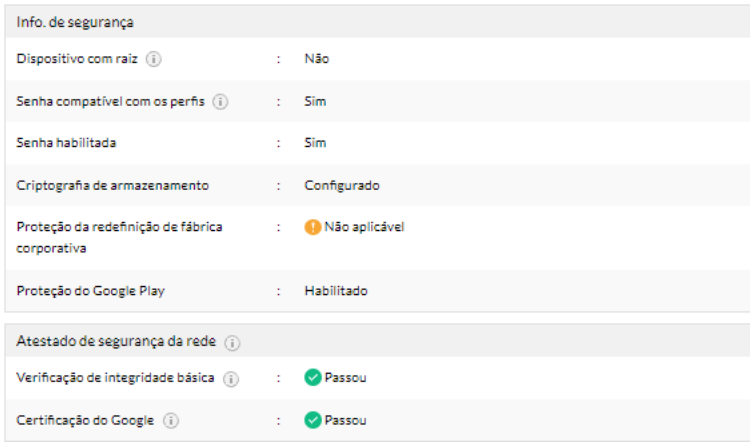
Fonte: Mobile Device Manager Plus (2022).

Figura 45 – Resumo do dispositivo (Rom utilizada, rede e sistema operacional)



Fonte: Mobile Device Manager Plus (2022).

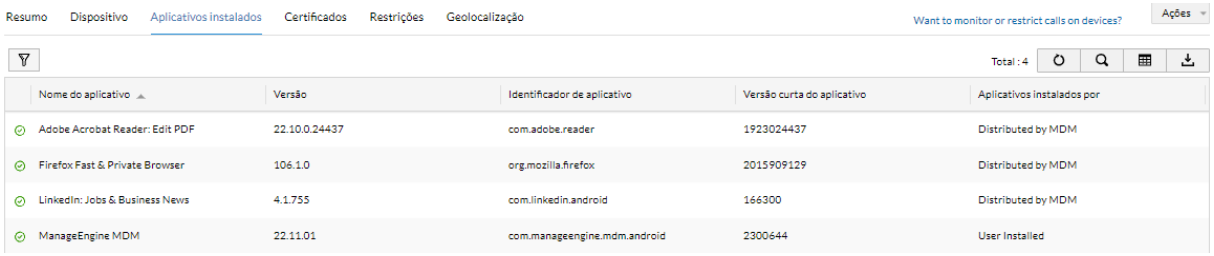
Figura 46 – Resumo do dispositivo (Segurança e atestado de segurança da rede)



Fonte: Mobile Device Manager Plus (2022).

A aba “dispositivo” contém mais informações do dispositivo, rede e do chip de operadora. A aba “aplicativos instalados” inclui a lista dos aplicativos instalados no dispositivo com informações de versão do aplicativo e se ele foi instalado pelo usuário ou pela distribuição pelo painel de gerenciamento, demonstrado na Figura 47. A aba “certificados”, exibe os cerificados presentes no dispositivo informando a identidade, data de expiração e nome do emissor. A aba “restrições” apresenta as restrições que estão impostas no dispositivo por meio de grupos, em que ao lado da funcionalidade possui um status, podendo ser permitido, restrito ou controlado pelo usuário.

Figura 47 – Aplicativos instalados



Fonte: Mobile Device Manager Plus (2022).

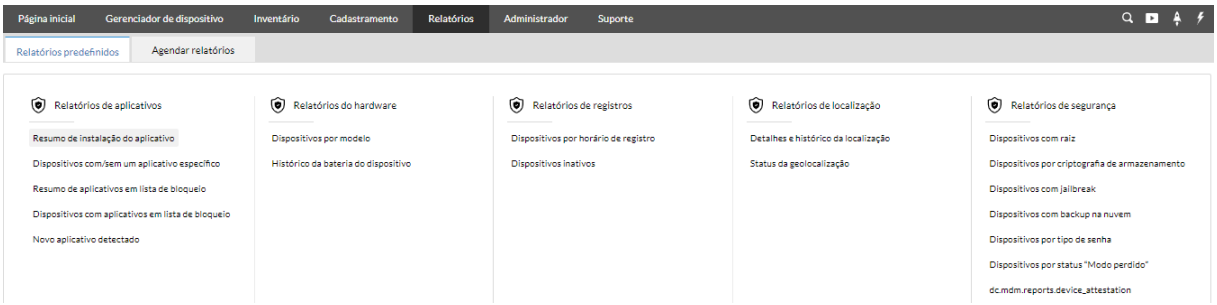
A funcionalidade de localização foi testada e não funcionou, ao tentar verificar no inventário do painel de gerenciamento é obtido o retorno mostrado na Figura 48. A orientação encontrada na documentação foi para permitir o recurso de GPS para o aplicativo ManageEngine MDM no dispositivo e manter o recurso habilitado o tempo todo, foi verificado e as permissões estão concedidas, mas o erro persiste.

Figura 48 – Retorno sobre localização do dispositivo testado

Fonte: Mobile Device Manager Plus (2022).

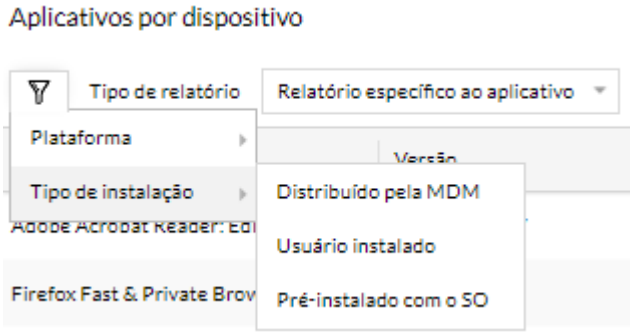
A solução possui relatórios pré-definidos para utilização categorizados por tipo, de acordo com o que a Figura 49 mostra. A customização de relatório é realizada dentro do próprio relatório pré-definido, onde ele permite alterar algumas opções de filtros para a geração do mesmo, conforme é mostrado na Figura 50.

Figura 49 – Opções de relatórios pré-definidos



Fonte: Mobile Device Manager Plus (2022).

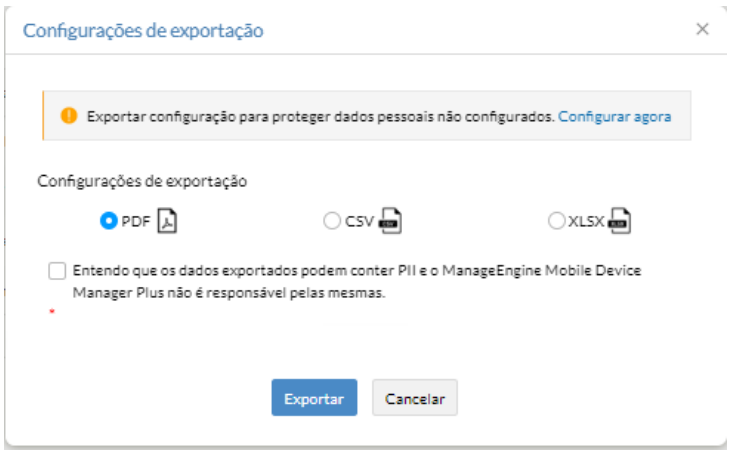
Figura 50 – Exemplo de filtro para customização de relatório



Fonte: Mobile Device Manager Plus (2022).

Existe a possibilidade de exportar os relatórios em três formatos, sendo eles *PDF*, *CSV* e *XLSX*, demonstrado na Figura 51.

Figura 51 – Configurações de exportação de relatórios



Fonte: Mobile Device Manager Plus (2022).

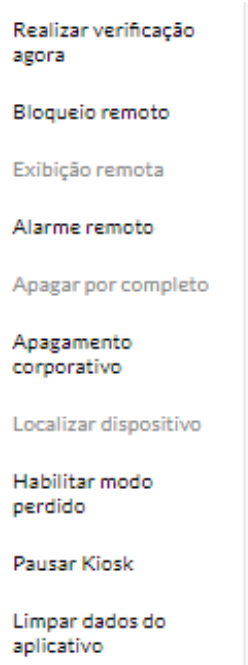
Por último foi validado a funcionalidade de limpeza remota, essa funcionalidade remete a segurança. Neste quesito a ferramenta tem disponível as opções de realizar

apenas a limpeza de aplicativos e de configurações corporativas no dispositivo de propriedade do funcionário, assim como a opção de limpar por completo o dispositivo pertencente a empresa, podendo ser selecionado juntamente o cartão de memória caso o dispositivo possua.

Para iniciar o processo de limpeza do dispositivo, é necessário escolher uma das opções, sendo elas “apagamento corporativo” e “apagamento por completo” de acordo com o que é mostrado na Figura 52.

Um pré-requisito para habilitar a opção “apagar por completo” é marcar o dispositivo em questão como perdido. Desta forma foi configurado o modo perdido, em que é obrigatório informar um telefone para contato e uma mensagem para aparecer na tela do dispositivo, conforme mostrado na Figura 53.

Figura 52 – Seleção de limpeza remota



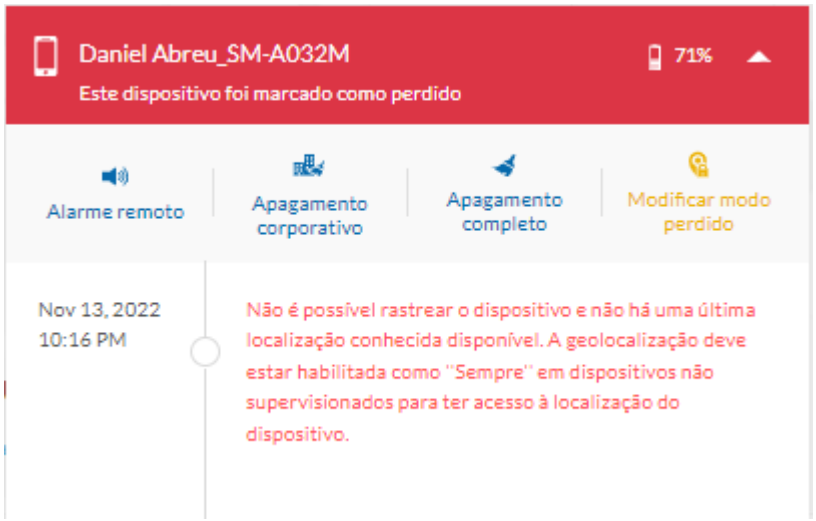
Fonte: Mobile Device Manager Plus (2022).

Figura 53 – Habilitando modo perdido

Fonte: Mobile Device Manager Plus (2022).

Ao concluir esta etapa, o dispositivo é marcado no painel de gerenciamento como perdido, no qual é exibido de acordo com a Figura 54.

Figura 54 – Status modo perdido



Fonte: Mobile Device Manager Plus (2022).

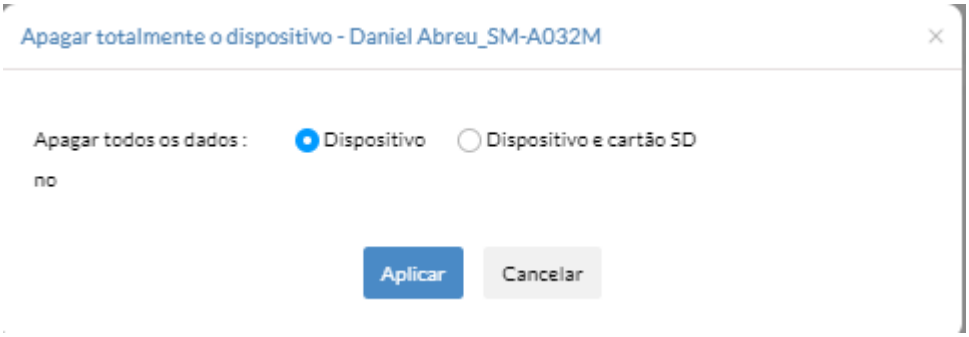
Ao definir o dispositivo como perdido, o mesmo é bloqueado e exibe somente a mensagem e o número para contato definidos anteriormente, possibilitando a ligação pelo próprio aparelho caso o mesmo tenha suporte para tal função. A tela do dispositivo nesse status é demonstrada na Figura 55.

Figura 55 – Dispositivo perdido

Fonte: Mobile Device Manager Plus (2022).

Para validação foi selecionado a opção de “apagamento completo” que direcionou para a próxima tela que solicitava escolher entre apagar somente o dispositivo ou apagar o dispositivo e cartão SD, conforme demonstra a Figura 56.

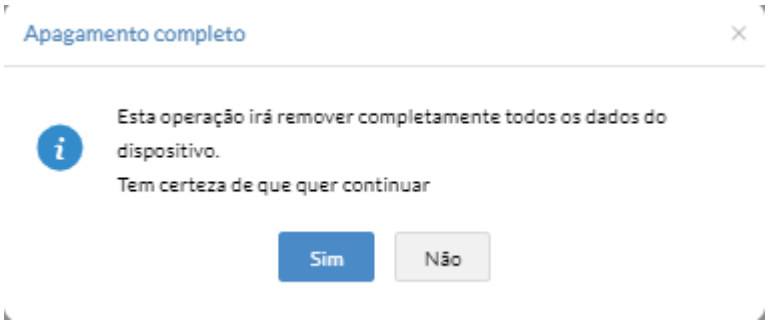
Figura 56 – Opções de limpeza remota



Fonte: Mobile Device Manager Plus (2022).

Ao clicar em aplicar é solicitado uma confirmação para o disparo da tarefa, avisando que o dispositivo será apagado por completo de acordo com o que é demonstrado na Figura 57.

Figura 57 – Confirmação de limpeza remota



Fonte: Mobile Device Manager Plus (2022).

Em relação a disponibilidade da solução a mesma se manteve acessível sempre que requisitada para uso. Devido a ferramenta se manter o tempo todo operacional, não houve incidentes de falhas por parte da mesma.

Referente a eficiência de desempenho, o tempo de resposta para publicar alguma mudança no painel de gerenciamento é adequada, mas em contra partida a sincronização do dispositivo com o painel de gerenciamento por muitas vezes demorava para ocorrer, e dependendo do comando enviado para o dispositivo, o mesmo não concluía.

Foi verificado que a ferramenta pode gerenciar até 10000 dispositivos, conforme é demonstrado na Figura 58, porém a disponibilidade para testes era de apenas um dispositivo.

Figura 58 – Quantidade de dispositivos suportados para gerenciamento

Fonte: Mobile Device Manager Plus (2022).

O uso de recursos pelo aplicativo ManageEngine MDM instalado no dispositivo, responsável por receber comandos e aplica-los ao mesmo, tem uso aceitável referente a memória *ram*, memoria *rom* e bateria. É demonstrado sobre o uso dos recursos na Figura 59.

Figura 59 – Uso de recursos utilizados no dispositivo

Fonte: Mobile Device Manager Plus (2022).

6.3 ETAPA 5

A etapa 5 do processo de aquisição de software de acordo com a ISO/IEC 25040, tem como objetivo concluir a avaliação da qualidade do produto de software. Nesta etapa é revisado o resultado da avaliação, criado um relatório sobre a avaliação, fornecido feedback sobre a avaliação e tratado os dados utilizados para avaliação.

Foi realizada a revisão dos critérios selecionados para avaliação quantitativa e qualitativa, e os mesmos se mostraram viáveis para serem utilizados para avaliação das ferramentas. Foi descrito na etapa 4 como foi realizada a avaliação quantitativa e qualitativa, juntamente com o conjunto de requisitos utilizados para medir a aplicação.

O feedback está esclarecido na conclusão deste trabalho, em que visa apresentar se o processo de avaliação é valido para este avaliar este tipo de solução. Referente ao tratamento dos dados, os mesmos foram levantados de acordo com a documentação presente no site dos fornecedores, desta forma não sendo necessário nenhum tipo de descarte ou devolução por parte do avaliador.

6.4 CONSIDERAÇÕES FINAIS DO CAPITULO

Este capitulo apresentou os critérios selecionados para medição de qualidade utilizados para a realização da avaliação qualitativa das ferramentas IBM MaaS360 e Mobile Device Manager Plus. As duas soluções foram submetidas a validação de seus recursos e funcionalidades, conforme foi descrito ao de decorrer desta etapa.

Vale destacar que não foi possível validar a solução da IBM devido a problemas enfrentados na parte de provisionamento. Como explicado anteriormente, o provisionamento é responsável por adicionar o dispositivo no painel da solução, para que ele possa ser gerenciado pelo mesmo. Portanto, ao não conseguir adicionar o dispositivo, é impossível validar as demais funcionalidades de modo prático.

Cabe comentar que a solução Mobile Device Manager Plus foi validada de acordo com as funcionalidades usadas como base para a obtenção da nota na avaliação quantitativa.

Evidencia-se que ao restringir recursos, aplicativos e sites no dispositivo testado, o mesmo continuou funcionando normalmente mesmo após sincronização do comando enviado. Foi configurado o modo quiosque, mas o mesmo não aplicou corretamente no dispositivo, alegando que o recurso foi desativado por causar lentidão no aparelho, porém não foi encontrado na documentação que o modelo do dispositivo de testes usado em questão não era compatível, ou que as configurações de hardware não eram suficientes para tal função.

O recurso de acesso remoto pela própria plataforma também não funcionou, ao procurar na documentação conforme indicado na mensagem de retorno, não se encontrou qualquer procedimento para correção que fosse claro e funcional para aplicação. Outro recurso que se mostrou disfuncional foi o de localização em tempo real, que consiste em saber por meio do GPS do dispositivo em qual lugar o mesmo se encontra no momento. Ao analisar o retorno apresentado e ser encaminhado para duas documentações especificas sobre o problema enfrentado, seguiu-se as orientações descritas nos procedimentos, contudo continuou não funcionando.

7 CONCLUSÃO

No mundo corporativo, os dispositivos móveis se tornaram uma das principais ferramentas de trabalho para as equipes externas e internas, impactando diretamente na produtividade dos funcionários. A mobilidade corporativa trouxe a possibilidade de aumentar o rendimento dessas equipes, melhorar a agilidade e o cumprimento de metas, facilitar a execução de tarefas e gerar economia para as empresas. Com isso, a procura por soluções completas de gerenciamento móveis dentro das organizações, visando performance e eficiência na gestão é cada vez maior.

Através deste trabalho foi possível compreender a importância de um sistema de gerenciamento de dispositivos móveis e como isso pode afetar diretamente a segurança digital das empresas, além de facilitar a administração de dispositivos portáteis. Entretanto, a decisão da ferramenta mais adequada acaba sendo dificultada devido a gama de soluções disponíveis para esse propósito. O objetivo deste trabalho, portanto, consistiu em analisar, comparar e selecionar uma solução adequada de sistema de gerenciamento de dispositivos móveis para organizações empresariais de qualquer tamanho.

Neste contexto, o trabalho apresentou um estudo sobre a fundamentação de sistemas de gerenciamento de dispositivos móveis e seus recursos tidos como essenciais. A partir desses fundamentos, é possível identificar quais características levar em consideração para análise.

Para a realização de uma avaliação comparativa é necessário determinar um processo com métodos e critérios bem definidos. Para tal, a proposta está fundamentada nas normas da série ISO/IEC 25000, particularmente a ISO/IEC 25010 que estabelece um conjunto de características de qualidade de software para avaliar as propriedades de um produto de software, e a ISO/IEC 25040 que define um conjunto de atividades para avaliação deste processo.

Foi decidido primeiramente realizar uma avaliação quantitativa com algumas ferramentas pré-selecionadas de acordo com requisitos definidos que devem ser atendidos. Com os requisitos definidos, foi aplicado notas para cada um e utilizado um multiplicador de notas de acordo com a importância definida para o requisito em questão, com o intuito que os requisitos mais importantes fossem fator decisivo para a escolha. Pode-se observar que o grau de importância de cada quesito pode ser adequado à realidade de cada organização.

Com a finalização da avaliação quantitativa foi obtido a soma total das notas aplicadas, e realizada a escolha de duas ferramentas, no qual alcançaram a maior pontuação para validação da adequação por meio de uma avaliação qualitativa. Foi definido critérios para medição de qualidade de acordo com a ISO/IEC 25010, em que foram julgados serem mais pertinentes para este tipo de solução a ser testada.

A solução da IBM não se mostrou adequada perante aos testes realizados, apresentou diversas vezes mensagens de erro na sua plataforma ao tentar salvar alterações de configurações, o que acaba impactando de forma negativa a usabilidade. Entretanto, o principal fator negativo foi a dificuldade de provisionar o dispositivo para com o painel de gerenciamento, impedindo de investigar as demais funcionalidades e recursos que a solução dispõe, pois se faz necessário um dispositivo no painel de gerenciamento para enviar comandos e validar o comportamento no dispositivo.

A ferramenta Mobile Device Manager Plus demonstrou ser de fácil uso e possui uma interface intuitiva. O provisionamento foi realizado rapidamente e sem muita dificuldade no dispositivo. Porém, ao realizar os testes, não apresentou total aptidão funcional do que se dispõe a realizar, deixando a desejar em alguns quesitos considerados importantes para este tipo de solução.

Fica entendido que as ferramentas de gerenciamento de dispositivos moveis precisam melhorar em relação a adequação funcional, assim como devem melhorar as documentações e procedimentos para deixarem mais claros e objetivos, dada a dificuldade em realizar alguns procedimentos e até a solução de problemas enfrentados.

O processo definido para escolher uma solução dentre várias soluções para o gerenciamento de dispositivos moveis se mostrou eficaz, e apoiado com as normas ISO/IEC 25010 e ISO/IEC 25040 passam maior confiabilidade no resultado. Porém, vale ressaltar que as características e subcaracterísticas de qualidade selecionadas para validação podem mudar de acordo com a necessidade do adquirente.

A fim de aprimorar o processo avaliativo para escolha de soluções de gerenciamento de dispositivos moveis, deve-se considerar alguns fatores para realizar uma avaliação mais assertiva de acordo com o proposito estabelecido. O primeiro fator a ser considerado é definir o tamanho da organização corporativa, seguido da informação se serão utilizados apenas dispositivos fornecidos pela empresa ou se

também serão utilizados dispositivos de propriedade do funcionário para tarefas da empresa.

Outro ponto sensível é referente sobre as escolhas das características e subcaracterísticas de qualidade presentes na ISO/IEC 25010. Devido a serem 8 características de qualidade e 38 subcaracterísticas, para este trabalho foram selecionadas apenas algumas. O escopo pode ficar grande e demandaria muito tempo para validação, entretanto quanto mais abrangente e padronizado melhor.

Destaca-se também que o processo comparativo foi aplicado sobre uma pré-seleção com base em uma lista tida como atual e mais fundamentada que as demais encontradas e outra solução bem colocada neste nicho na américa latina. Mas a metodologia e os critérios definidos podem ser aplicados sobre outras ferramentas além daquelas pré-selecionadas.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 14598-1:2001: Tecnologia de Informacao: Avaliacao de Produto de Software**. [S.l.: s.n.], 2001.

ABNT. **NBR ISO/IEC 9126-1:2003: Engenharia de Software - Qualidade de Produto**. [S.l.: s.n.], 2003.

CARLOS, Dener. **O que é consumerização?** Linkedin. 2020. Disponível em: https://pt.linkedin.com/pulse/o-que-%C3%A9-consumeriza%C3%A7%C3%A3o-dener-carlos. Acesso em: 5 mar. 2022.

CASAS BAHIA. **Smartphone Samsung Galaxy A03 Core Preto 32GB, 2GB RAM, Câmera Traseira de 8MP, Selfie de 5MP, Tela Infinita de 6.5" e Processador Octa Core**. 2022. Disponível em: https://www.casasbahia.com.br/. Acesso em: 17 nov. 2022.

CHECKPOINT. **MOBILE SECURITY REPORT 2021.** 2022. Disponível em: https://www.checkpoint.com/downloads/resources/mobile-security-report-2021.pdf?mkt_tok=NzUwLURRSC01MjgAAAGDTRT7EHabRrvEmGMCYW6QkEJJs6Ee-IKX5J5foJLZOv_ClrvQLbECOR4ozTde4WFvkaBhCIk0BsOXzJ1R-WNu65vf9ZrWqwHBKo-ztzcuucNL0YBB. Acesso em: 7 mar. 2022.

COOPER, Stephen. **11 Best Mobile Device Management (MDM) Solutions for 2022**. Comparitech. 2022. Disponível em: https://www.comparitech.com/net-admin/mobile-device-management-software/. Acesso em: 10 mai. 2022.

IBM. **Soluções de gerenciamento de dispositivos móveis.** 2022. Disponível em: https://www.ibm.com/br-pt/security/mobile-device-management. Acesso em: 18 mai. 2022.

ISO/IEC.; **COMMISSION the I. E. ISO/IEC 25010-1:2011: Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models.** [S.l.: s.n.], 2011.

ISO/IEC. **COMMISSION the I. E. ISO/IEC 25040-1:2011:Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - Evaluation Process.** [S.l.: s.n.], 2011.

LAM, Lauro. **Startup brasileira marca presença no maior evento de tecnologia mobile do mundo**. Olhar Digital. 2022. Disponível em: https://olhardigital.com.br/2022/02/25/pro/pulsus-marca-presenca-no-maior-evento-de-tecnologia-mobile-do-mundo/. Acesso em: 12 ago. 2022.

MANAGEENGINE. **Mobile Device Management (MDM) software.** 2022. Disponível em: https://www.manageengine.com/mobile-device-management/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=MDM-MDMgmt. Acesso em: 17 mai. 2022.

MELO, Vinicius. **Consumerização: a utilização dos dispositivos móveis dentro das empresas.** Izap. 2020. Disponível em: https://izap.com.br/blog/consumerizacao-a-utilizacao-dos-dispositivos-moveis-dentro-das-empresas/. Acesso em: 05 mar. 2022.

MIRADORE. **Mobile Device Management (MDM).** 2022. Disponível em: https://www.miradore.com/device-management/mobile-device-management-mdm/. Acesso em: 16 mai. 2022.

MWC BARCELONA. **360 Pulsus**. 2022. Disponível em: https://www.mwcbarcelona.com/exhibitors/360-pulsus. Acesso em: 12 ago. 2022.

NIEHAVES, Bjorn; KOFFER, Sebastian; ORTBACH, Kevin. **It consumerization:** A theory and practice review. Association for Information Systems. Alemanha: Muenster, 2012. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1467&context=amcis2012. Acesso em 7 mar. 2022.

PHIFER, Lisa. **Mobile device management checklist.** TechTarget. 2013. Disponível em: https://docplayer.net/11438849-E-guide-mobile-device-management-checklist.html. Acesso em: 21 mar. 2022.

PULSUS. **Impulsionando o que faz a diferença.** 2022. Disponível em: https://pulsus.mobi/sobre/. Acesso em: 13 mai. 2022.

SILVESTRIN, Paulo Vitor. **Sistema para gerenciamento de dispositivos móveis baseado em Android**. Porto Alegre. 2013. Disponível em: < https://www.lume.ufrgs.br/bitstream/handle/10183/86437/000910067.pdf;seque>. Acesso em: 5 abr. 2022.

SHISHKOVA, Tatyana; KIVVA, Anton. **Mobile malware evolution 2021**. Kaspersky. 2022. Disponível em: https://securelist.com/mobile-malware-evolution-2021/105876/. Acesso em: 9 mar. 2022.

SOFTEX. **MPS.BR Melhoria de Processo de Software Brasileiro: Guia de Aquisicao**. [S.l.:s.n.], 2013.

SOTI MobiControl. **Manage Your Devices Securely with SOTI MobiControl**. 2022. Disponível em: https://soti.net/products/soti-mobicontrol?utm_source=Internal&utm_medium=organic&utm_campaign=mobicontrol_vanity. Acesso em: 10 ago. 2022.

WAZLAWICK, R.S. **Metodologia de Pesquisa para Ciência da Computação**. 3.ed. Rio de Janeiro: LTC, 2021.