Miguel Alexandre Santos
Gomes da Conceição

ADMINISTRAÇÃO DE UMA INFRAESTRUTURA
INFORMÁTICA AO NÍVEL DE SEGURANÇA E REDE

1 2 9 0 UNIVERSIDADE D COIMBRA

1 2 9 0

UNIVERSIDADE D
COIMBRA

Miguel Alexandre Santos Gomes da Conceição

ADMINISTRAÇÃO DE UMA INFRAESTRUTURA INFORMÁTICA AO NÍVEL DE SEGURANÇA E REDE

Relatório da disciplina de Estágio/Dissertação, no âmbito do Mestrado em Segurança Informática, sob orientação do Eng. Paulo Pais e do Doutor Paulo Simões
Departamento de Engenharia Informática da
Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2020

This page is intentionally left blank.

Abstract

This report describes the activities developed in the Curricular Internship, integrated in the Master in Computer Security, in the Moviflor group, based in Oiã. The Moviflor group is a group that constitutes some stores and logistics centers, having an IT infrastructure that has been evolved over its growth. The internship lasted one year and aimed to contribute to the implementation and development of the same infrastructure. From conducting an analysis of the entire existing computer system and making corrections to certain flaws, to creating a proprietary application that would be used for the group's computer department, this stage contributes to the development of organizational, social and organizational procedures. existing in the group, which improves the performance level of all its constituents. This experience was, therefore, beneficial for the author, in that it allowed him to have direct contact with the reality and the context of an operational computer system and all the risks associated with it. In this context, it was possible to verify the importance of a good organization and planning in the scope of a computer implementation regarding its future operation.

Keywords

Appliance, Management, Infrastructure, Security, Control

This page is intentionally left blank.

Resumo

O presente relatório descreve as actividades desenvolvida no Estágio Curricular, integrado no Mestrado em Segurança informática, no grupo Moviflor, sedeada em Oiã. O grupo Moviflor é um grupo que constitui algumas lojas e centros logísticos, possuindo uma infraestrutura informática que tem sido evoluída ao longo do seu crescimento. O estágio teve a duração de um ano e visava contribuir para a implementação e desenvolvimento da mesma infraestrutura. Desde a realização de uma análise a todo o sistema informático existente e realização de correções a certas falhas, até à criação de uma aplicação proprietária que seria usada para o Departamento informático do grupo, este estágio contribui para o desenvolvimento dos procedimentos organizacionais, sociais e de segurança existentes no grupo, o que melhora o nível de desempenho de todos os seus constituintes. Ainda neste tópico, foi melhorado o sistema de suporte do grupo e a forma como a informação pode e deve circular, com a criação de um Portal Interno onde todos os Colaboradores deverão se dirigir para quando possuem problemas relacionados com o Departamento de Informática, para visualizar as ultimas noticias do grupo ou até para tirar duvidas dos procedimentos necessários para uma das suas tarefas. Esta experiência foi, assim, benéfica para o autor, na medida em que lhe permitiu o contacto direto com a realidade e o contexto de um sistema informático operacional e de todos os riscos associados a este. Neste contexto, foi possível verificar a importância de uma boa organização e planeamento no âmbito de uma implementação informática quanto ao seu funcionamento futuro.

Palavras-Chave

Appliance, Gestão, Infraestrutura, Segurança, Controlo

This page is intentionally left blank.

Contents

This page is intentionally left blank.

Acronyms

DSI Departamento de Sistemas Informáticos. 6, 17, 18, 27–29, 33, 36, 37

ERP Enterprise resource planning. 18

LAN Rede de área local. 13

MSP Managed Service Provider. 19–21

PSA Professional Service Provider. 20

PT Portugal Telecom. 13

RMM Remote Monitoring and Managment. 6, 19, 21

SAAS Software as a Service. 20

VLAN Virtual LAN. 9, 10

VNC Virtual Network Computing. 25

This page is intentionally left blank.

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1

Introdução

1.1 Âmbito e Enquadramento

O presente relatório de estágio é elaborado no âmbito da disciplina de Dissertação/Estágio do Mestrado em Segurança Informática do Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra. O estágio foi desenvolvido no grupo Moviflor, que inclui diversas empresas, tais como a própria Moviflor, os Armazéns Reis, a Streightex, a Barreta Azul e os respetivos Centros Logísticos 1 e 2. Este estágio permitiu aprofundar os conhecimentos na área de administração de redes e infraestruturas informáticas, tendo como principal foco a vertente de segurança – além de aperfeiçoar competências em diversas áreas, sejam estas sociais, profissionais ou organizacionais. O objetivo inicial deste estágio é a melhoria da infraestrutura informática da empresa ao nível da segurança e da interligação de todos os seus constituintes. Em termos de condições de acolhimento, supervisão e enquadramento, são de referir as seguintes circunstâncias:

- O estágio foi orientado pelo Eng. Paulo Pais, responsável pelo Departamento de Informática da Moviflor, e orientado pelo Prof. Paulo Simões, por parte da Universidade de Coimbra;
- O acompanhamento técnico regular do estágio, pelo lado da empresa acolhedora, foi realizado diariamente por diversos meios tais como, reuniões, formações, realização de chamadas, entre outros. Este acompanhamento mais regular foi complementado com reuniões de acompanhamento com os dois orientadores, para planeamento e preparação do relatório de estágio e planeamento das atividades do estágio.
- O trabalho técnico foi conduzido nas instalações do Grupo Moviflor, com base nas instalações de Oiã e com diversas intervenções de campo nas instalações da empresa em outros locais.

1.2 Organização do Documento

A Figura 1.1 ilustra a forma como se encontra organizado este relatório de estágio.

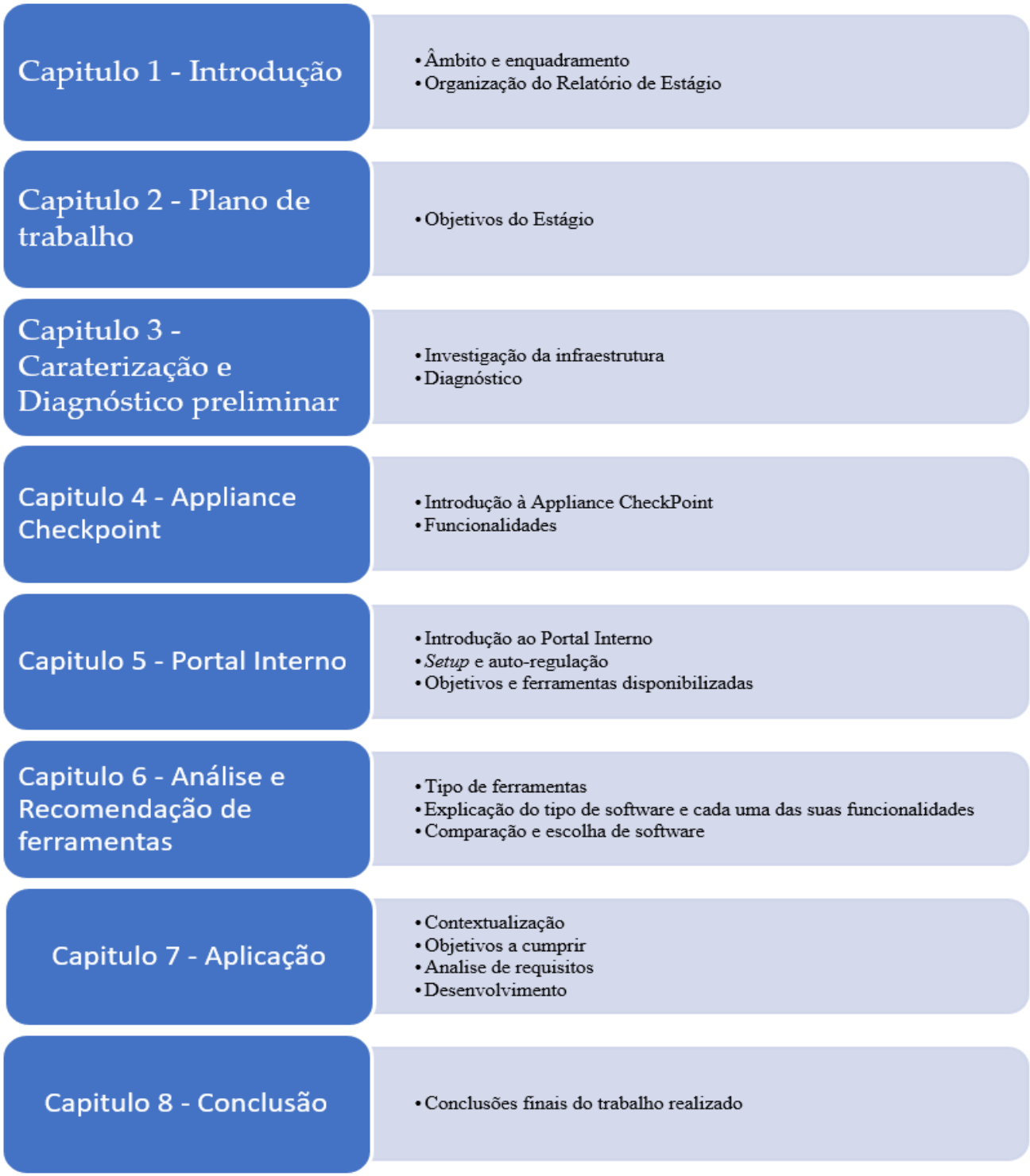


Figure 1.1: Organização do Relatório de Estágio

O capítulo 1 apresenta o estágio e a entidade acolhedora, e tem como propósito explicar de que forma está, a organização idealizada para este relatório de estágio.

No capítulo 2 é explicado o plano de trabalho associado a este estágio, identificados os objetivos iniciais, definidos pela entidade acolhedora, e também discutida a forma como esses objetivos evoluíram ao longo da realização do estágio.

O capítulo 3 mostra o diagnóstico resultante da investigação e recolha de dados realizada na infraestrutura do grupo Moviflor, com uma descrição da estrutura informática já implementada. Com base nas informações obtidas, serão apresentados os problemas existentes, assim como soluções que permitam não só corrigir estes problemas, como também prevenir/identificar outras possíveis falhas no sistema.

O capítulo 4 descreve a *appliance Checkpoint*, o mecanismo que assegura a defesa virtual interna e externa do grupo. Será realizada uma descrição da *appliance* e vão ser mencionadas diversas ferramentas que fazem parte do seu sistema.

No capítulo 5 será apresentado o Portal Interno criado para o grupo Moviflor, onde estão presentes diversas ferramentas e mecanismos implementados para melhorar o funcionamento da empresa.

O capítulo 6 enuncia a investigação realizada, a pedido da entidade acolhedora, sobre algumas ferramentas RMM (Remote Monitoring and Managment), a ferramenta escolhida, os problemas encontrados e a solução final que foi encontrada para este problema.

O capítulo 7 manifesta a criação de uma aplicação que nasce do *setup* criado pelos outros capítulos. Ou seja, este capitulo é o aglomerado de todo o trabalho realizado ao longo do estágio, envolvendo diversos pontos já mencionados ao longo dos capítulos anteriores, e que permitem que esta aplicação possua as funcionalidades que contém. A aplicação é o foco central deste estágio sendo algo necessário e requisitado pela Entidade acolhedora.

Por fim, no capítulo 8 será realizada a conclusão deste relatório de estágio e serão feitas algumas ponderações sobre todo o processo de trabalho do estágio e todos os resultados obtidos.

This page is intentionally left blank.

Chapter 2

Plano de Trabalhos

O objetivo deste estágio consiste na melhoria da infraestrutura informática do grupo Moviflor, ao nível da segurança e da interligação de todos os seus constituintes. Embora que, no plano de trabalhos inicial existam alguns ponteiros concretos para o trabalho a desenvolver (e.g. explorar os serviços da Appliance Check Point e testes aos websites institucionais da Moviflor, no primeiro semestre), considerou-se necessário efetuar primeiro um levantamento da infraestrutura informática da empresa, a fim de documentar essa implantação e identificar áreas-alvo para posterior intervenção. Adicionalmente, logo na fase inicial do estágio, foram identificados alguns problemas sérios com a infraestrutura informática da empresa, o que levou à necessidade de tomar algumas medidas de modo a corrigir estas vulnerabilidades nela presentes. Alguns destes problemas já haveriam sido identificados pelo informático do grupo, mas como a infraestrutura tem vindo a ser alterada desde a sua entrada para o grupo, existiam ainda pormenores que apresentavam falhas de segurança. Por este motivo, foram adicionados alguns objetivos extra aos que já estavam pretendidos para este estágio. Deste modo, os objetivos para este estágio são os seguintes:

- Exploração da Appliance CheckPoint;
- Melhoria e gestão de redes via VmWare;
- Aprender a administrar uma infraestrutura informática;
- Gestão da appliance de segurança Panda Adaptive Defense;
- Estudo de uma ferramenta para a gestão e controlo de dispositivos;
- Caraterização e diagnóstico da infraestrutura do grupo Moviflor;
- Criação de um Portal Interno para o grupo Moviflor;
- Criação de uma aplicação de gestão de dispositivos, computadores, acesso remoto, etc.

A exploração da *appliance* Checkpoint será realizada em diversas etapas, de acordo com a necessidade e aplicabilidade de regras. Como as regras base que permitem que a empresa funcione já foram aplicadas, o trabalho a ser realizado será no âmbito de aprender o que a CheckPoint é e tem para oferecer, no contexto de segurança e gestão, e aplicar regras quando estas forem necessárias para o grupo.

Ao nível do VMWare, será possível usar a virtualização para poupar certos recursos ao grupo, permitindo que diversas máquinas sejam alocadas a outros sistemas mais críticos do grupo.

Como medida de segurança usada pelo grupo, o Panda Adaptive Defense é um antivírus com endpoint escolhido para proteger os dispositivos. Esta ferramenta será usada para melhorar os parâmetros de segurança já existentes, e gerir os seus dispositivos, mantendo assim a integridade da rede interna e cada dispositivo usado no grupo.

Para uma melhor compreensão dos problemas e dificuldades existentes na infraestrutura do grupo Moviflor, a caraterização e diagnóstico é um dos objetivos estabelecidos para que seja possível obter uma visão geral de todo o grupo. Este é um objetivo essencial deste estágio, criando assim o alicerce que permitirá que todos os outros objetivos se concretizem.

Será realizado um estudo sobre diversos software de gestão e controlo de dispositivos a serem usados pelo informático do grupo. Este tipo de software permite que seja possível manter um controlo mais rigoroso sobre os funcionários do grupo, e permite também que qualquer auxílio necessário possa ser cumprido de forma rápida e eficaz. Deste modo, serão escolhidos e explicados diversos tipos de software alternativos, e depois será escolhida uma ferramenta em concreto para ser implementada.

Será realizada alguma administração da rede do grupo que permitirá obter competências a nível social e profissional, como também permitirá o contacto com toda a infraestrutura implementada. Este ponto permite desenvolver capacidades que com o trabalho escolar não se conseguiria obter, permitindo que experiências sejam criadas ao longo de todo o estágio.

Como forma de melhorar a circulação de informação pelo grupo, como também criar um local onde todos os colaboradores se possam "deslocar" para comunicar problemas técnicos, foi criado um portal interno para o grupo Moviflor. Este portal vem melhorar a circulação de informações como também a eficácia do suporte prestado pelo Departamento de Sistemas Informáticos (DSI).

Por último, a criação de uma aplicação que facilitará o dia-a-dia deste Departamento de Informática. Esta aplicação vai permitir o controlo de dispositivos e outros dados importantes, facilitando o manuseamento de todos os dados voláteis que se encontravam espalhados por diversos ficheiros, num único lugar.

Com base nestes objetivos, o trabalho a ser realizado na Entidade acolhedora será feito por etapas, consoante a necessidade e importância do mesmo. No entanto, não tentando levar a um pensamento de falta de estrutura de trabalho, todo o trabalho realizado será com um objetivo final, a aplicação criada para o grupo.

É importante mencionar que estes objetivos foram agilizados devido à pandemia que afetou todo o país, incluindo o grupo onde o estágio decorreu, tendo sido este obrigado a fechar portas durante um período prolongado, levando a adiar o estágio em curso e todos objetivos planeados, como era o caso da auditoria. No entanto, uma vez que havia necessidade de criar uma aplicação de controlo do tipo Remote Monitoring and Managment (RMM), e de forma a conseguir prosseguir com o normal funcionamento do estágio, optou-se por realizar este objetivo e descartar a auditoria pretendida inicialmente.

Chapter 3

Caracterização e diagnóstico da Infraestrutura

3.1 Caracterização da Infraestrutura

O grupo Moviflor corresponde a um conjunto de empresas como a própria Moviflor, os Armazéns Reis, a Streightex, a Barreta Azul e 2 Centros Logísticos (Centro Logístico 1 e 2) , como mencionado anteriormente. Este grupo possui, portanto, diversas estruturas que necessitavam de se interligar para que fosse possível aceder remotamente aos diversos serviços presentes nas instalações principais. Por este motivo, a rede encontra-se estruturada da seguinte forma:

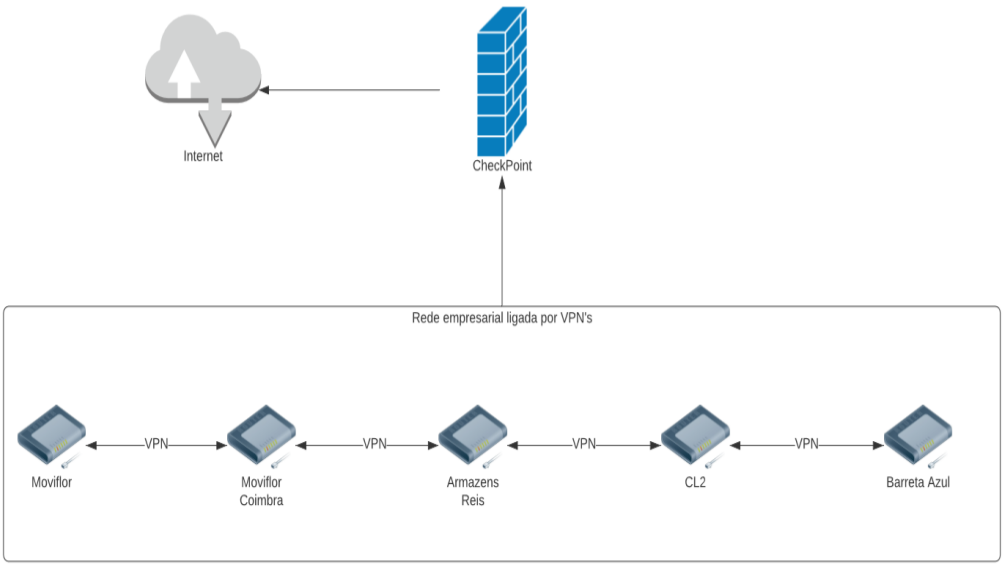


Figure 3.1: Rede do grupo Moviflor

A Figura 3.1 permite visualizar a existência de uma variedade de VPN's que interligam

site a site, sendo depois todo o tráfego direcionado para a CheckPoint, e posteriormente à Internet. Estas diversas interligações entre cada empresa, através de 's, permite a segurança das comunicações uma vez que o canal por onde segue toda a informação fica assegurado. Também é possível visualizar a CheckPoint e de que forma esta protege toda a estrutura presente. Na Figura, a CheckPoint está simbolizada pela Firewall, sendo que não se trata de uma firewall centralizada, mas sim um serviço de CheckPoint com diversos outros serviços associados. A CheckPoint é o ponto de segurança onde todo o tráfego é analisado e aprovado, sendo depois rececionado ou enviado, conforme a política estabelecida. Através desta estrutura é assegurado que todas as empresas estão interligadas, protegendo todas as suas comunicações, os serviços presentes em cada uma das empresas, e todo o tráfego de dentro para fora da rede interna. É relevante mencionar que cada rede possui uma linha de backup 4G que entra em vigor caso a ligação Fibra, por qualquer motivo fique em baixo, permitindo assim a continuação do normal funcionamento do grupo.

Ficheiro Externo com informações privadas

Foram identificados outros constituintes presentes na estrutura do grupo. Estes constituintes são os bastidores presentes em todas as empresas que permitem a interligação e o fornecimento de serviços das mesmas. A representação destes estão presentes no Apêndice A. Estão presentes ao longo de todos os bastidores os seguintes componentes:

- Painéis de ligação RJ 45;
- Escovas de passagem de cabos;
- Fonte de alimentação;
- Switch;
- UPS;
- Tomadas de alimentação.

Por outro lado, estes são os componentes que variam consoante o bastidor em questão e a sua importância dentro da empresa:

- Gravador para videovigilância,
- Servidores;
- Storage;
- Painéis de Fibra;
- Router;
- Central de telefones.

3.2 Diagnóstico

Ao longo deste estágio, foi possível trabalhar e explorar diversas configurações relativas aos bastidores presentes em cada empresa, como também a todos os serviços presentes. Por este motivo, e por ser um dos objetivos deste estágio, para além da caraterização da

infraestrutura, é preciso evidenciar um pouco do diagnóstico realizado quanto à segurança relativa à rede interna.

A rede interna mantém-se segura contra ataques externos devido à estrutura idealizada para toda a rede. Todo o tráfego é conduzido e verificado através da CheckPoint para o exterior e vice-versa, permitindo assim que a gestão e controlo sejam assegurados. Uma vez que a mudança da infraestrutura do grupo é recente, alguns pormenores "menos importantes" foram deixados para último lugar. Esses problemas foram:

- Falta de configuração e atribuição de VLAN's;
- A rede wifi permitia acesso à rede interna;

3.2.1 VLAN's

Em relação às VLAN's, muitos dos dispositivos que deveriam ser assegurados e separados da Virtual LAN (VLAN) principal estavam ainda por configurar, como era o caso de diversas câmaras de vigilância, servidores e ap's. Neste assunto, a solução baseou-se numa verificação generalizada dos dispositivos que importava assegurar, e depois, passo-a-passo, a devida configuração foi realizada colocando-se cada um dos dispositivos na VLAN correta. Neste âmbito, foram definidas algumas VLAN's específicas, sendo estas usadas em dispositivos próprios para assegurar que estes se mantêm excluídos da rede principal e apenas são acedidos por vias permitidas.

3.2.2 Rede e portal *guest*

Uma rede *guest* ou portal *guest*, é uma rede wifi para clientes. Ou seja, é uma rede que as empresas/organizações criam para que os seus clientes possam aceder à Internet. Este tipo de redes permitem que qualquer utilizador que esteja ligado a esta rede não comunique com a rede interna da empresa/organização, impedindo assim que utilizadores desconhecidos ao serviço acedam a serviços e a sistemas internos. Neste âmbito, foram criados 2 portais *guest* uma vez que não existia apenas um tipo de em todo o grupo. Como era pretendido que os clientes utilizassem um e-mail para poderem aceder à rede wifi e consequentemente guardar esse e-mail, foi necessário a criação destes portais.

Cada controlador de apenas apresentava soluções típicas de acesso a um portal *guest* como: password mensal, utilizador e password, redes sociais e portal externo. Uma vez que era necessário alguma personalização para a recolha de dados, a solução escolhida foi o portal externo.

No desenvolvimento dos portais *guest*, foram usadas algumas informações provenientes do website da Ubiquiti[16], da TP-Link[12] e do CodexWorld[17], como também alguns recursos presentes no GitHub[24]. Cada portal possui uma verificação do texto introduzido, sendo depois verificado se o e-mail existe. Este método é baseado no script presente no website da CodexWorld [17], e permite realizar uma verificação de um e-mail introduzido em fatores como domínio, resposta a um "Helo" e verificação de *syntax*. Como não existe uma grande necessidade de manter a integridade dos dados guardados, não foi criada uma base de dados especifica para os e-mails, sendo desta forma, excluídos alguns métodos de proteção contra possíveis acessos não autorizados.

A criação dos portais gera a necessidade de formar um servidor para se alojar todo o serviço por detrás de cada portal. Por este motivo, foi criado um servidor virtual Ubuntu

que permitisse o alojamento dos portais criados e de futuros portais que a empresa fosse precisar. Este servidor foi gerado e configurado com base num tutorial de configuração de um servidor Ubuntu [23]. Juntamente deste servidor, foram criadas as respetivas redes *guests* para cada Loja, associadas a uma VLAN própria para *guests* e outras configurações como tráfego limitado, bloqueio de websites, etc.

Antes de qualquer implementação dos portais, foi montado um *setup* de teste utilizando um dos *ap's* como transmissor de rede e um computador como controlador. Deste modo, seria possível, através de um sistema mais simples e semelhante ao que seria implementado na empresa, testar os portais antes de qualquer implementação final. O objetivo deste *setup* era permitir testar diversas configurações até ficar definido o que acabaria por permanecer em cada uma das lojas do grupo. Deste modo, todo o trabalho e testes seriam realizados antes, e consequentemente, a implementação final seria mais simples.

No momento da implementação final, foram implementados dois portais (Armazéns Reis e Moviflor), sendo que está a ser criado mais um para a nova loja que será aberta em Viseu, que consistirá numa junção das duas. O resultado final dos portais é o seguinte:

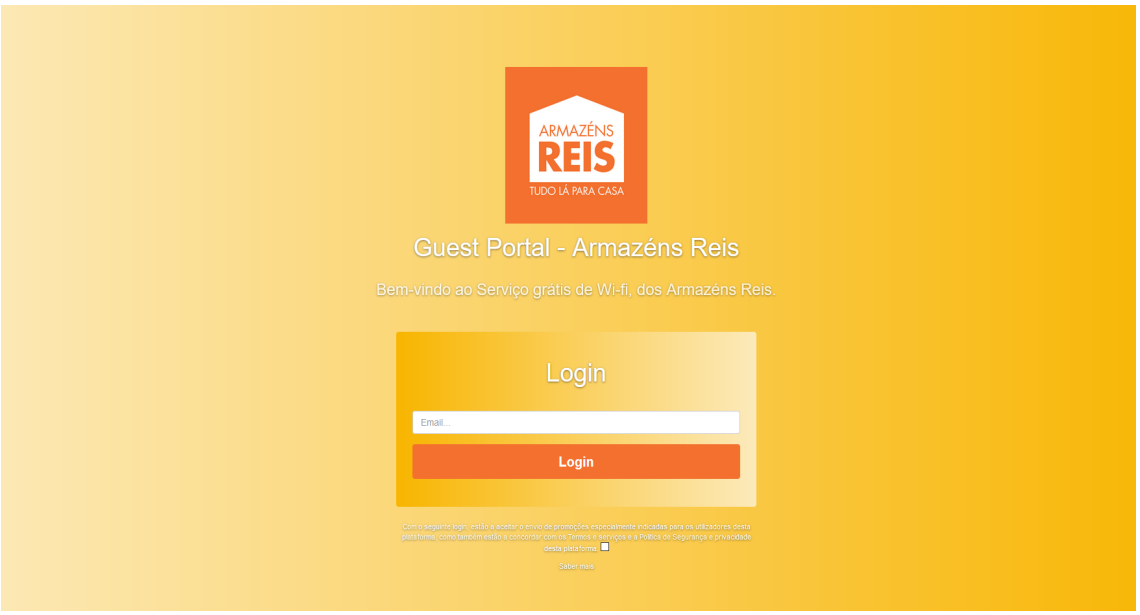


Figure 3.2: Portal Armazéns Reis

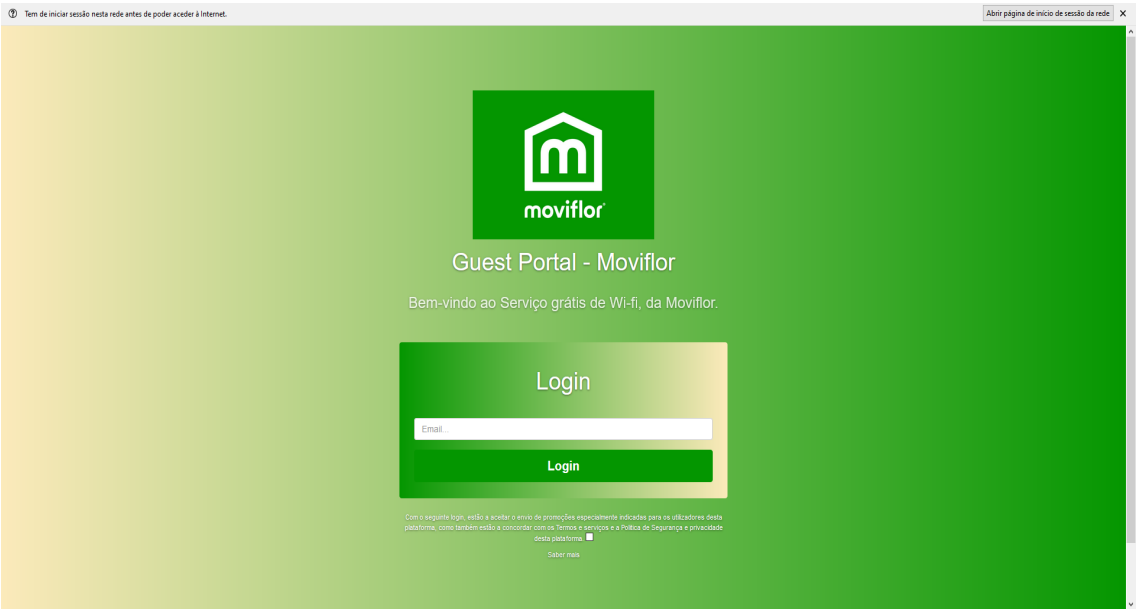


Figure 3.3: Portal Moviflor

Chapter 4

Appliance CheckPoint

4.1 Introdução à *Appliance CheckPoint*

Uma appliance CheckPoint é um sistema que permite o controlo de tráfego entre a rede interna e externa e apresenta-se como o core de uma política de segurança de rede. [1] CheckPoint Software Blades é um conjunto de funcionalidades de segurança que permitem que uma gateway de segurança ou um servidor de gestão de segurança, forneça o desempenho correto e as devidas funcionalidades. [1] A CheckPoint Firewall faz parte da arquitetura do software Blades que fornece funcionalidades de firewall da nova geração, incluindo:

- Capacidades de VPN e conectividade com dispositivos moveis;
- Identificação e conhecimento de dispositivos;
- Acesso e filtro de internet;
- Controlo de aplicações;
- Prevenção de intrusões e ameaças;
- Prevenção de perda de informação.

A Figura 4.1 pretende mostrar uma típica solução CheckPoint, onde estão presentes os componentes que a constituem e que permitem que a solução seja fiável e segura, atribuindo-lhe todas as funcionalidades necessárias de segurança. De um modo simples, cada número corresponde a:

1. Redes externas e Internet
2. Gateway de Segurança
3. SmartDashboard
4. ervidor de gestão de segurança
5. Rede Interna

Os componentes primários de uma solução CheckPoint são:

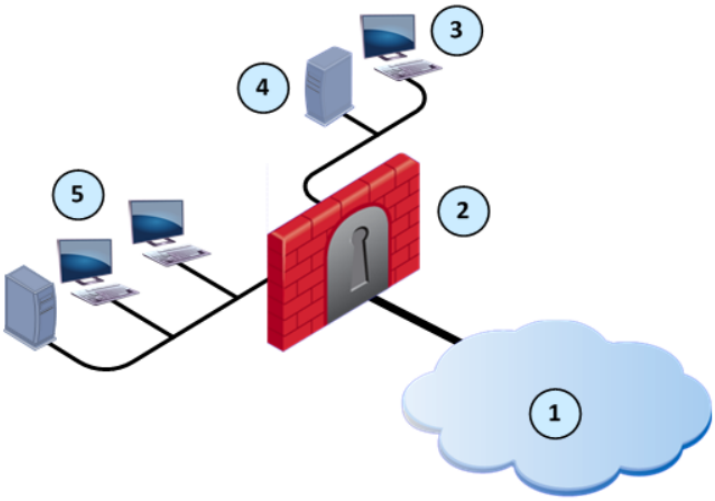


Figure 4.1: Componentes da Solução CheckPoint

- Gateway de Segurança – É o motor que implementa a política de segurança da organização, sendo este o ponto de entrada para a Rede de área local (LAN), e é gerido pelo servidor de gestão de segurança;

- Servidor de Gestão de Segurança – A aplicação que gere, armazena e distribui as políticas de segurança para as gateways de segurança;

- SmartDashboard – Um cliente CheckPoint usado e criado para gerir as políticas de segurança.

Todos estes componentes estão presentes na solução aplicada no grupo Moviflor sendo que os constituintes da CheckPoint se localizam na rede da Portugal Telecom (PT). Este serviço prestado apresenta diversas funcionalidades como:

- Firewall – Controlar o tráfego na periferia da rede corporativa, no acesso à Internet;

- IDS/IPS – Permite a prevenção de intrusão de ataques com base em padrões tipificados e conhecidos;

- URL Filtering - Permite o acesso a determinados sites web, com base numa classificação por categoria, aplicado a utilizadores ou grupo de utilizadores com definição de faixas horárias;

- Application Control - Identificar, bloquear ou limitar o uso de aplicações web;

- Anti-Bot - Detetar máquinas infetadas com software malicioso, e dar informação que possibilita o isolamento do dispositivo em questão;

- Antivírus - Bloquear a entrada dentro do perímetro corporativo de ficheiros infetados com vírus;

- IPSec VPN - Configuração de túneis site-to-site;

4.2 Funcionalidades

Como a CheckPoint possui diversas funcionalidades e ainda não houve necessidade de as explorar, as regras de firewall e URL Filterting foram as únicas possíveis de experienciar. A Figura seguinte permite visualizar algumas destas regras mencionadas:

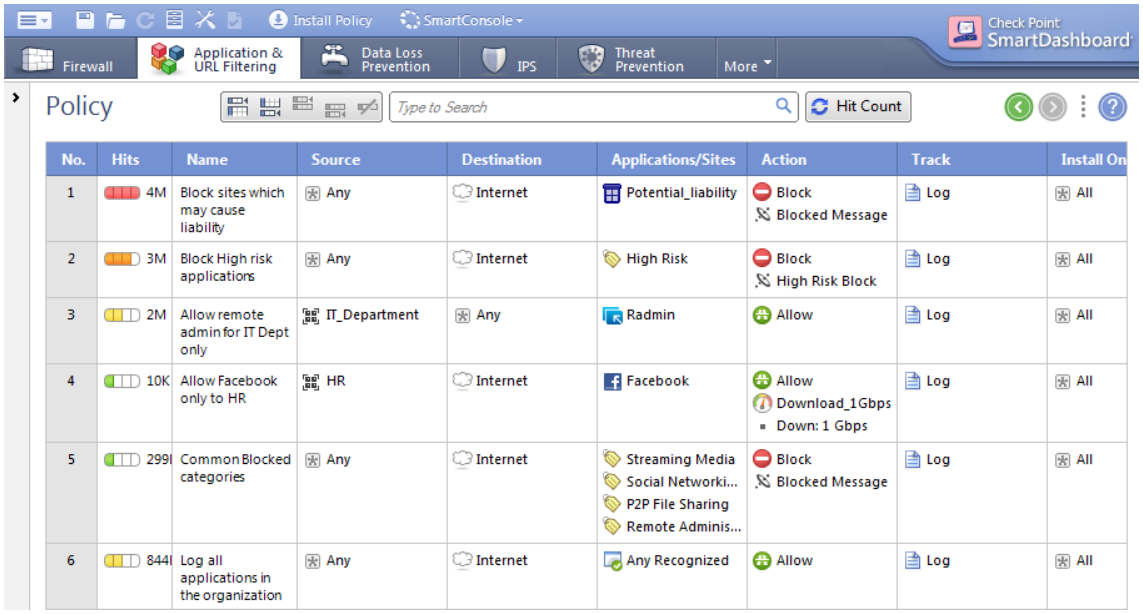


Figure 4.2: Regra de URL Filtering - SmartDashboard

A Figura 4.2 foi retirada de [1], com o intuito de mostrar de que forma são apresentadas as regras que estão empregues nas aplicações e ao filtro de URL, dentro do SmartDashboard. Ao aceder ao menu da política de filtragem de URL e aplicações, dentro do SmartDashboard, para introduzirmos uma regra nova apenas é necessário adicionar uma nova linha nas regras e depois preencher campo a campo com os dados pretendidos. Estas regras presentes na Figura 4.2 são templates que são providenciadas na versão Demo do SmartDashboard, mas muitas delas estão presentes no serviço implementado no grupo. Neste caso, podemos visualizar que já houve um número elevado de ligações que combinam com as regras apresentadas, tendo sido bloqueadas ou permitidas conforme a regra que corresponderam.

Por outro lado, também podemos aplicar regras à Firewall, como mostra a Figura seguinte:

A Figura 4.3 foi retirada do mesmo documento que a Figura 4.2, podendo representar uma tabela típica de regras de Firewall aplicadas no SmartDashboard. Estas regras são divididas em regras explícitas e implícitas. Regras explícitas são regras criadas pelo administrador tendo como objetivo configurar quais as ligações permitidas pela Firewall, enquanto que as regras implícitas são as que se baseiam nas definições presentes no menu de propriedades globais. Este último tipo de regra permite ligações para diversos serviços que a gateway de segurança utiliza. Um exemplo é a opção de "Accept Control Connections" que permite pacotes que controlam os seguintes serviços:

- Instalar a política de segurança nos gateways de segurança;
- Envio de ficheiros Log do gateway de segurança para o servidor de gestão de segurança;

- Ligação com aplicações third party, como os servidores de autenticação RADIUS e TACACS.

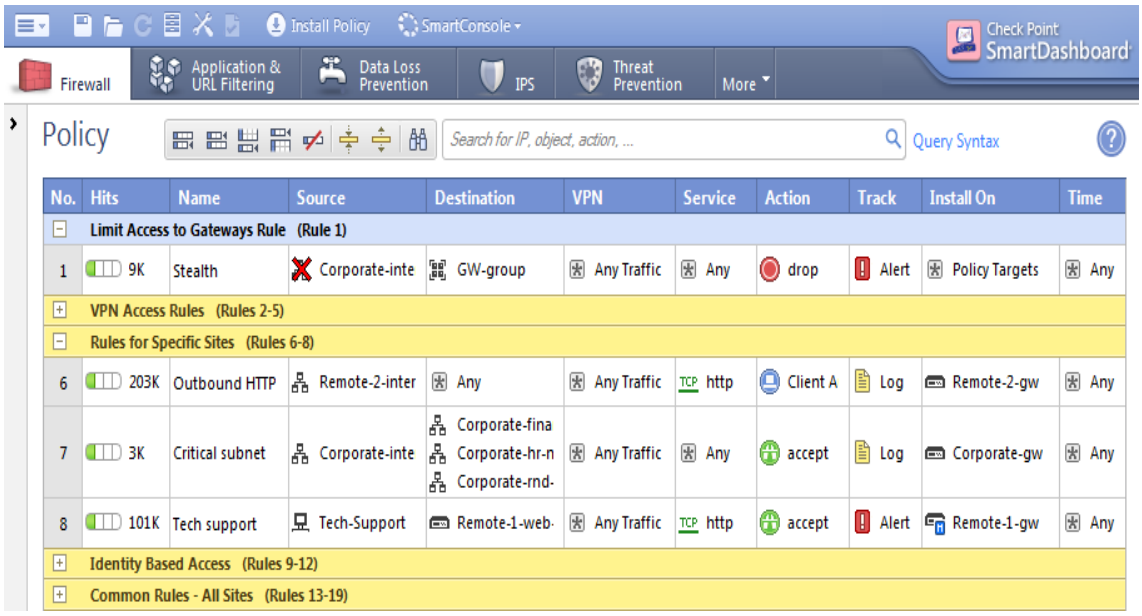


Figure 4.3: Regra de Firewall - SmartDashboard

Todo este processo de criação de regras serve para se ter uma base de como serve o sistema de criação e desempenho da Checkpoint. O objetivo final é reduzir o conteúdo disponível para todos os colaboradores. Não o conteúdo didáctico mas sim o conteúdo não apropriado para se visualizar e aceder no local de trabalho. Deste modo, foi necessário criar diversas regras de URL filtering para que diversos conteúdos específicos, que as bases de dados já implementadas na Checkpoint não detetavam, pudessem bloquear. Desta forma, ao ser bloqueado este tipo de conteúdo, a rede fica menos obstruída por tráfego desnecessário, melhorando a performance de todo o grupo para o conteúdo realmente importante.

Chapter 5

Portal Interno

5.1 Introdução ao Portal Interno

Como grandes empresas (exemplo: Millennium BCP), e em conversa com o Eng. Paulo Pais, foi proposto a criação de um portal Interno para o grupo Moviflor. Este portal Interno consiste numa página web onde todos os funcionários se irão dirigir para consultar todas as notícias mais relevantes sobre o grupo, aceder a tutoriais sobre certas tecnologias usadas no grupo e abrir tickets para o departamento de Informática.

Este portal foi alojado no servidor Ubunto já mencionado em cima, onde os portais *guest* estão alojados, sendo que o portal será criado em Wordpress. O Wordpress é um software *open-source* que permite criar um website, aplicação ou blog de uma forma simples. [5] Foi escolhido fazer o portal em Wordpress pela sua facilidade de utilização, manutenção e desenvolvimento.

De forma a cumprir com um dos objetivos deste portal, foi instalado o *plugin* gratuito de tickets da "Awesome Support". Esta escolha não foi documentada, mas quanto ao método de seleção do *plugin*, este deveu-se às inúmeras instalações e testes realizados aos *plugins* que cumpriam com os seguintes requisitos:

- Funcionalidades disponibilizadas;
- *User-Friendly*;
- Personalização;
- Opções administrativas.

De todos os *plugins* testados, o "Awesome Support" foi o que mais se revelou promissor, cumprindo inteiramente com todos os requisitos ou parcialmente. Neste âmbito, alguns pontos como a personalização de campos a preencher no aspeto da abertura de tickets por parte dos Colaboradores, foi um dos pontos onde este *plugin*, e tantos outros, não conseguiram cumprir por inteiro, com o requisito proposto. É importante mencionar que, todos os testes foram efetuados de forma a encontrar um *plugin* grátis que possuísse todo o conteúdo pretendido para o grupo. Todos os *plugins* acabavam por conter potenciais *add-ons* onde são adicionadas novas funcionalidades permitindo melhorar a experiência do utilizador, e por esta razão existe a necessidade de mencionar que todo o processo de seleção foi à volta de um *plugin* grátis.

Figure 5.1: Página inicial do Portal Interno

5.2 *Setup* e auto-regulação

Para que o portal não precisa-se de muita manutenção e atenção, e de forma a se poder configurar pontos necessários de acesso a certos colaboradores, foi essencial instalar alguns *plugins* para que fosse possível que algumas funcionalidades existissem. Desta forma, os seguintes *plugins* servem para o seguinte:

- UpdraftPlus - Backup/Restore - Como o próprio nome indica, este *plugin* permite que sejam agendados backup's do portal, assegurando a sua estrutura e a segurança dos dados no caso de uma falha de updates, erros ou outro problema que surja e cause danos ao sistema implementado. Neste caso, os backups foram configurados para serem diários.
- User Role Editor - Uma vez que, pessoalmente, o wordpress não é tão *straightforward* no âmbito das permissões por utilizador, foi implementado um *plugin* que permite gerir as permissões de todos os utilizador e até criar perfis consoante a necessidade e o gosto do administrador. Este aspecto é importante uma vez que era necessário separar as permissões dos utilizadores regulares, dos gerentes, dos responsáveis pelas notícias e do DSI.
- Outros - Este campo é dedicado a *plugins* para modificação de publicações. Visto que são diversos e não constituem uma grande importância na regulação do portal, mas sim na modificação e capacidades de publicar algo, estão presentes como forma de apresentação. Alguns exemplos de *plugins* são: Elementor, Ninja Forms, Sticky side buttons, WeDocks.

5.3 Objetivos e ferramentas disponibilizadas

Este Portal interno tem como objetivo principal servir de plataforma de *tickets* para que os Colaboradores possam, de uma forma simples, pedir auxílio ao DSI. Este mecanismo de

tickets baseia-se no esquema seguinte:

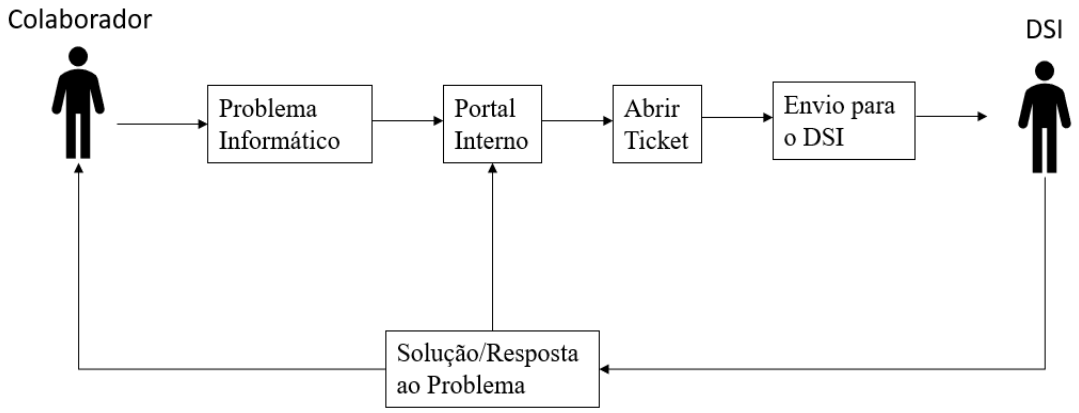


Figure 5.2: Esquema da abertura de tickets

Com base na Figura acima, a ideia transmitida é de quando um Colaborador se depara com alguma dificuldade/problema no âmbito da informática, dirige-se ao Portal Interno e abre um ticket com esse mesmo problema. Depois de preenchidos os campos da solicitação de suporte, o DSI recebe uma notificação do ticket e toma as devidas providências para o resolver, com a maior brevidade.

Este mecanismo foi necessário devido ao excesso de chamadas de suporte que o Eng. Paulo Pais recebia ao longo do seu dia de trabalho, o que dificultava que este se focasse noutras vertentes mais importantes do grupo e ao mesmo tempo não conseguisse gerir tantos pedidos, sendo que depois muitos acabavam por ser esquecidos por falta de registo.

No entanto, também proporciona outras funcionalidades tais como centro de notícias e alertas, centro de tutoriais para o Enterprise resource planning (ERP), centro de contactos atualizado onde constam todos os contactos da empresa e por último, um link direto para o seu email através do portal. Incluindo todos estes recursos numa única plataforma permite que os colaboradores percam menos tempo no menos importante e mais tempo no que realmente interessa, aumentando a sua produtividade. É importante mencionar que se se criar um local onde é possível juntar todas as informações relativas a tutoriais que dizem respeito ao ERP usado no grupo, permite-se que qualquer colaborador com dificuldades/dúvidas possa seguir e aprender com os guias introduzidos no portal, aumentando o seu conhecimento e também, ao longo do tempo, a sua importância na empresa. Todos os guias e tutoriais provêm do responsável da empresa que dá formações sobre o ERP, e da própria empresa que desenvolveu o ERP. Outros documentos presentes como procedimentos foram criados por chefes de departamento para que os colaboradores executem quando, por exemplo, um novo colaborador entra para a empresa sendo o seu cargo na loja da Moviflor, através deste procedimento, o colaborador sabe o que terá que enviar ao DSI para se poder criar todos os acessos do novo colaborador.

Este portal foi um dos pontos que contribui para a criação da aplicação mais a frente neste relatório. Estão disponíveis *prints* de vários outros menus disponibilizados no portal, sendo que não foram colocados neste capítulo visto que seriam informações auxiliares ao contexto do mesmo, e por este motivo todos estes *prints* estão disponíveis no apêndice.

Chapter 6

Análise e recomendação de ferramentas

6.1 Análise

Foi proposto que fosse realizada uma investigação sobre alguns software, de forma a que este fosse implementado na empresa. Este software permitiria ao departamento de informática, realizar um maior controlo sobre os endpoints existentes em todo o grupo Moviflor, prevenindo possíveis problemas ou até intrusões no sistema interno do grupo.

Com o crescimento deste grupo, surgiu a necessidade de haver um mecanismo de controlo e respetivo acesso a grande parte dos constituintes informáticos espalhados por todas as suas empresas. Para este fim, foi necessário escolher uma ferramenta que monitorize os dispositivos pertencentes ao grupo, como também concedesse acesso remoto aos responsáveis de informática. Aqui surgem as ferramentas de Remote Monitoring and Managment (RMM).

Segundo a [8], RMM ou software de gestão de rede, é um tipo de software de gestão remota usado por Managed Service Provider (MSP) para poderem gerir remotamente endpoints, redes e computadores. Através desta tecnologia, MSPs podem, remotamente, enviar correções e atualizações, instalar e configurar software, corrigir problemas, entre outras funcionalidades.

Estas ferramentas são implementadas através de um *agent*(small software footprint), aos quais são instalados nos sistemas dos trabalhadores: computadores, servidores, dispositivos móveis, etc. [8] São estes *agents* que permitem aos MSPs obter o controlo remoto dos dispositivos, sendo através destes que são enviados os dados entre os MSPs e o dispositivo em questão. [8] Não só é possível prevenir possíveis intrusões através do uso destas ferramentas como também é possível prevenir uso de software não autorizado pela empresa em questão, restringindo alguns dos problemas de segurança [22] mais usuais.

É possível a configuração deste tipo de software para que envie alertas para os responsáveis de informática, caso existam problemas associados a um dispositivo, problemas de intrusão, entre outros, permitindo aos responsáveis tomar as medidas necessárias para resolver os problemas em questão. Uma vez que o grupo está em constante evolução, a ferramenta a ser escolhida deverá cumprir com alguns requisitos:

- Compatibilidade com sistemas operativos como: Windows, Android;

- Capacidade para um grande número de dispositivos;
- Acessibilidade de preço;
- Facilidade de instalação e configuração.

Estes requisitos serão usados como forma de distinção e avaliação, quando for realizada a comparação dos diversos software, sendo a compatibilidade de software e o preço, os fatores com maior ponderação, uma vez que o sistema operativo predominante no grupo é o Windows e dispositivos móveis que possuem Android.

Entre todas as ferramentas existentes no mercado, foram escolhidas algumas para apresentar e realizar a devida comparação ao responsável da informática da empresa. Os software foram selecionados com base em algumas sugestões do responsável e com base na informação apresentada em [2]. Deste modo, as seguintes ferramentas foram escolhidas como potenciais soluções: Atera, Comodo One, SolarWinds, Pulseway, ConnectWise Automate e Panda.

6.1.1 Atera

O Atera é um software do tipo MSP que segue um esquema de Software as a Service (SAAS) e possui diversas funcionalidades. Este software, não só possui um sistema de tickets incluído, como também uma estratégia que, segundo o seu website: "... an MSP strategy that actually works." [3][21]. Fazem parte das suas funcionalidades a capacidade de controlo e gestão remota (RMM), Professional Service Provider (PSA), várias integrações com *third party apps* e comparação de métricas entre empresas. [3] Por último, este software possui uma versão de *trial* que permite ao utilizador final testar as diversas funcionalidades presentes no software, de maneira gratuita, durante 30 dias. Os preços para este tipo de software começam a 79 dollars, aumentando para 149 dollars na categoria mais alta. É importante mencionar que estes preços são mensais e não anuais, sendo que cada pacote possui um número de *endpoints* específico. [3]

6.1.2 Comodo One

O Comodo One apresenta a plataforma chamada de "Dragon Platform". Esta plataforma possui muitas das funcionalidades que o Atera oferece. Todas as funcionalidades são providenciadas pelo sistema incorporado da Itarian. Este sistema possui gestão de patches, serviço de controlo e gestão remota (RMM), sistema de tickets Zendesk incorporado, compatibilidade com vários sistemas operativos e controlo e acesso remoto a dispositivos [4] Esta plataforma foi criada e introduzida na indústria dos MSPs de forma gratuita, disponibilizando as suas funcionalidades mais básicas, sendo que outras como antivírus, centro de quarentena de software, monitorização em tempo real, seriam cobradas conforme o número de *endpoinsts* usados. [4] A partir de 2020, esta plataforma restringe as funcionalidades gratuitas para todos os utilizadores que apenas usem até 50 *endpoints*, sendo que quando este número é superado, é cobrado um valor por cada *endpoint*. O valor cobrado corresponde consoante quantos *endpoints* estarão a ser usados pela organização, por exemplo: de 51 – 99 são cobrados 1.25 dollars por cada *endpoint* , ou para mais de 10 mil endpoints é cobrado 0.80 dollars. [4]

6.1.3 SolarWinds

O SolarWinds permite que o "operador" possa visualizar o endereço de rede de cada dispositivos adicionado à plataforma como também o acesso remoto, a monitorização e manutenção automatizadas, o gerenciamento de *patches*, a análise de dados, o backup e recuperação de dados, a proteção web e antivírus. [11] Estes serviços sao disponibilizados pelo SolarWinds como tambem é possivel personalizar o pacote de serviços. Ou seja, é atribuida a possibilidade de escolher quais serviços é que uma organização pretende usar e remover todos os outros, permitindo assim uma redução do preço final deste produto. [11] Por último, apenas é possível obter valores contactando o serviço disponível, sendo que este será contabilizado consoante os diversos serviços que uma empresa deseje usar. [11]

6.1.4 Pulseway

O Pulseway foi desenhado para pequenas empresas, de modo a fornecer as funcionalidades mais significantes, presentes nos software mais *High-End*. O seu objetivo é apresentar uma plataforma onde seja possível visualizar o *health status* de cada um dos seus dispositivos, possuindo estes, sistemas operativos como Mac OS, Android, Linux ou Windows. Permite a automação e implementação de scripts nos dispositivos existentes, como também o agendamento de patches de software. É possível aceder aos dispositivos adicionados de uma maneira rápida, através da plataforma, e ao mesmo tempo criar relatórios personalizados sobre detalhes dos dispositivos e outros detalhes que interessem ao utilizador. [14] Este software apresenta uma versão de *trial* que abrange até 2 dispositivos, possuindo total controlo sobre todas as funcionalidades existentes. A adição de *add-ons* ao pacote escolhido, irá variar o preço final, sendo este aumento relativo às funcionalidades escolhidas. [14]

6.1.5 ConnectWise Automate

Como os software já mencionados, o ConnectWise Automate possui automação, descoberta da rede, gestão, monitorização e *patching*. Estas funcionalidades são uma repetição constante presente em todos os software já mencionados, sendo a forma como cada um explora e oferece cada serviço, o fator que os diferencia. Por esta razão, este software em questão, foca-se na automação dos serviços e tarefas necessárias ao *daily-basis* da empresa, permitindo automatizar e até disponibilizar uma experiência *self-service* ao utilizador final. [9] Os dispositivos podem ser adicionados atravês de uma funcionalidade existente no software, capaz de procurar/detetar dispositivos existentes numa rede, de uma maneira simples e que permite ao gestor apenas se focar na automação dos serviços e funcionalidades. [9] Está presente uma versão de *trial* uma vez realizado o pedido, sendo que não existe informação do preço exigido pelo software. Segundo o seu website, “We’ve Designed ConnectWise Automate to Meet Your Unique Business Needs”, o que permite concluir que apenas serão cobradas as funcionalidades que são requisitadas pelo utilizador. [9]

6.1.6 Panda System Managment

O Panda é primariamente uma ferramenta de antivírus que permite proteger um dispositivo contra aplicações e software não desejáveis. Uma vez que este software será tratado com mais detalhe, apenas será explicado brevemente, quais as funcionalidades do modulo de gestão e monitorização.[10] Uma vez que o foco desta plataforma não é o de um MSP ou RMM, as funcionalidades são mais reduzidas. No entanto, estão presentes as

funcionalidades mais básicas e que permitem ao utilizador gerir os seus dispositivos. As funcionalidades resumem-se em acesso remoto aos dispositivos, controlo de estados através da sua plataforma, *patching* e alertas. [10] Este software foi mencionado, uma vez que já tinha sido testado e utilizado por parte da empresa, juntamente do atual antivírus.

6.1.7 NinjaRMM

Segundo o seu website, esta plataforma apresenta-se como a mais fácil de se usar, de todo o mercado.[6] O NinjaRMM é uma plataforma de monitorização e gestão remota que fornece uma visão única sobre todos os seus endpoints e as ferramentas que são necessárias para melhorar o seu sistema. A plataforma simplifica e automatiza o trabalho diário dos fornecedores de serviços IT, de forma a ser possıvel que estes se possam focar em serviços complexos, relacionados com os utilizadores finais e o crescimento da organização.[6] Como funcionalidades principais, o NinjaRMM possui algumas já mencionadas como, monitorização e alertas, gestão de endpoints e da rede, gestão de maquinas virtuais, automação e *scripts*, gestão de *patches*, antivırus, acesso remoto, gestão de acessos, relatórios e administração de utilizadores. Todas estas funcionalidades são comuns em grande parte das plataformas/ferramentas já mencionadas. O NinjaRMM tenta-se destacar através da sua usabilidade, permitindo que cada utilizador que o use seja capaz de realizar qualquer ação de uma forma rápida e fácil. Por ultimo, este software possui uma versão de trial, permitindo assim que cada utilizador possa testar as suas funcionalidades e assim retirar as suas próprias conclusões.

Software		G2CROWD				
		Overall	MEETS REQUIREMENTS	EASE OF SETUP	EASE OF ADMIN	QUALITY OF SUPPORT
Atera		4.6 ★★★★½	4,4	4,7	4,5	4,6
Comodo One		4 ★★★★☆	N/A	4,4	4,4	3,7
SolarWinds		4.1 ★★★★☆	4,3	4,3	4,3	3,9
Pulseway		4.4 ★★★★☆	4,3	4,4	4,4	4,3
ConnectWise		4.1 ★★★★☆	4,2	3	3,5	3,7
Panda		4.3 ★★★★☆	4,7	4,3	4,1	4,2
NinjaRMM		5 ★★★★★	4,6	4,7	4,7	4,8

Figure 6.1: Tabela 1 de comparação dos software escolhidos - G2Crowd

As Figuras 6.1 e 6.2 consistem numa recriação de uma tabela já existente em [2], mas possui os software já mencionados em cima com dados devidamente atualizados. É importante mencionar algumas notas:

- Os valores presentes nas Figuras 6.1 e 6.2 foram retirados das páginas web, de reviews de software, G2Crowd e Capterra;
- Todos os valores presentes remetem para reviews de 10 ou mais pessoas;
- Estes dados de reviews servem de auxílio e serão usados para a ponderação final da ferramenta e devida escolha.

Software		CAPTERRA				
		OVERALL	EASE OF USE	CUSTOMER SERVICE	FEATURES	VALUE FOR MONEY
Atera		4.5 ★★★★½	4,6	4,5	4	4,7
Comodo One		5 ★★★★★	4,5	5	4,5	5
SolarWinds		4.4 ★★★★☆	4,3	4,2	4,4	4,3
Pulseway		4.7 ★★★★½	4,7	4,8	4,5	4,8
ConnectWise		4 ★★★★☆	3,5	4	4,4	3,9
Panda		4.1 ★★★★☆	4,1	3,9	4	3,7
NinjaRMM		5 ★★★★★	4,9	4,7	4,6	4,8

Figure 6.2: Tabela 2 de comparação dos software escolhidos - Capterra

Esta Figura serve para que seja possível ter *feedback* de outros utilizadores de cada um dos softwares, contribuindo assim para a decisão final sobre o software a ser usado pela empresa.

Com base na informação das figuras, o NinjaRMM é o software com maior índice de aprovação e um dos candidatos mais fortes, pois apresenta uma grande variedade de funcionalidades, tanto a nível do administrador como a nível do utilizador final.

Por fim, juntando toda a informação relativa a cada ferramenta, e as informações provenientes das Figuras 6.1 e 6.2, a ferramenta escolhida foi o Comodo One. Chegou-se a esta decisão com base no fator preço/compatibilidade. Não foi possível apresentar os preços individuais de cada ferramenta, mas com base na informação que foi encontrada, a decisão tomada pelo grupo foi de se usar este software.

6.2 Aplicação e testes

Uma vez escolhida a ferramenta, esta foi implementada no Centro Logístico 1, um dos locais de armazenamento de produtos e realização de parte da Logística presente no grupo. Este local foi escolhido pois apresenta um número de dispositivos relevante para a realização de testes, como também a variedade necessária de dispositivos para que fossem testadas as funcionalidade do software. A instalação do *endpoint* foi efetuada de 2 formas:

- Através do *download* do aplicativo gerado na plataforma do Comodo One quando é efetuada uma nova adição de um dispositivo. Ao realizarmos esta adição é pedido o tipo de sistema operativo e depois gerado o aplicativo que deverá ser instalado manualmente nos dispositivos, ficando imediatamente disponível na plataforma. No Apêndice A é possível visualizar o ultimo passo para a criação do *installer* que será usado para instalar e consequentemente adicionar um dispositivo na plataforma.
- Através do software de *Auto Discovery and deployment*. Esta *tool* consta nas ferramentas associadas ao Comodo One e permite que sejam detetados dispositivos numa

certa gama de ip's, e realizada a instalação do *endpoint* em cada um dos dispositivos.

Uma vez instalados nos dispositivos do Centro Logístico 1, foram realizados alguns testes. Estes consistiram, nomeadamente, nas funcionalidades de controlo remoto, obtenção de informação, controlo do uso de aplicações e alertas.

- Controlo remoto: Testado o impacto e o processamento existente quando existe um acesso via remoto ao dispositivo em questão, e quando não existe qualquer interação com o mesmo (standby).
- Obtenção de dados: Confirmação se os dados que são retirados através do *endpoint* coincidem com os dados reais. Visualizar no Apêndice A , Figura que possui informações relativas a um PDA.
- Controlo de aplicações: Este teste foi realizado, nomeadamente em PDA's (dispositivos para realização de inventário e picagem de material). Através da plataforma, foi criado um perfil que contem as aplicações permitidas pela empresa, sendo depois este perfil atribuído ao grupo de dispositivos Android. Assim, foi possível testar que nenhum trabalhador poderia aceder a aplicações que não constam na lista de aplicações permitidas. Este perfil também permite que sejam adicionadas redes Wifi, sendo depois adicionadas automaticamente a todos os dispositivos do grupo atribuindo, reduzindo o tempo usado para a configuração de todos os PDA's. É possível visualizar parte destes dados no Apêndice A, onde estão apresentadas algumas aplicações permitidas e redes wifi associadas ao perfil dos PDA's.

Depois de realizados estes testes, foi efetuado o *deployment* do *endpoint* nas outras instalações do grupo. A ferramenta mencionada para a realização do *deployment* não funcionava a 100%, tendo sido necessário instalar o *endpoint* individualmente em muitos dos dispositivos.

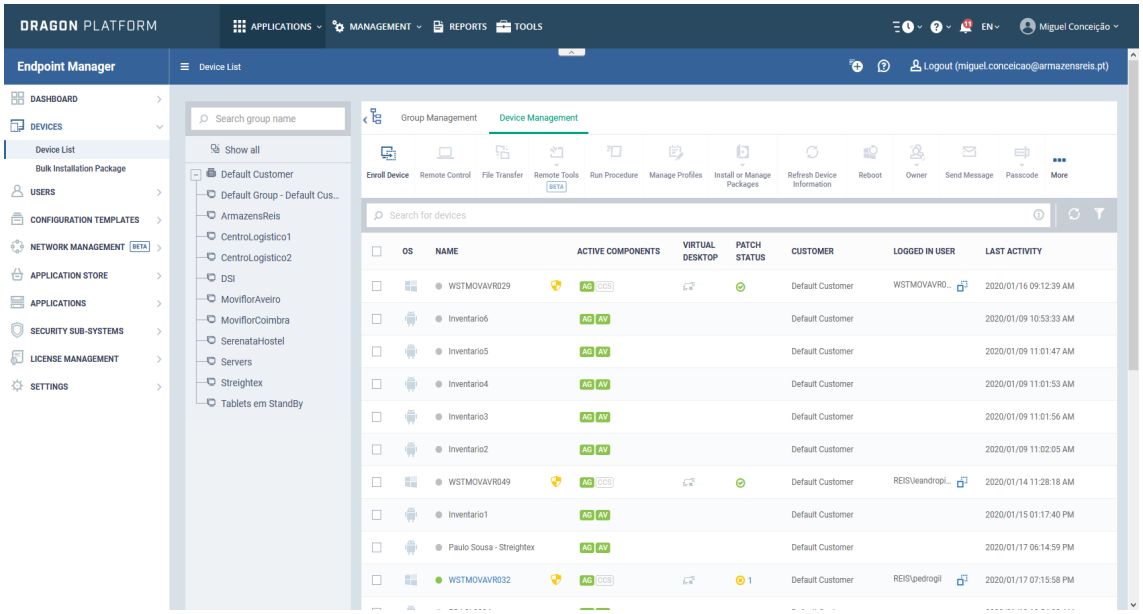


Figure 6.3: Dashboard do Comodo One possuindo diversos dispositivos já adicionados

A Figura 6.3 pretende mostrar o *dashboard* do Comodo One, como também mostrar alguns dos dispositivos já introduzidos na plataforma. É importante mencionar que cerca de 85%

dos dispositivos do grupo já possuem o *endpoint* instalado e estão a ser geridos através da plataforma.

No entanto, uma vez que esta escolha foi realizada em finais de Novembro e inícios de Dezembro, o Comodo One manteve-se totalmente grátis, sendo que nas ultimas semanas do ano foi anunciado que este passaria a cobrar por *endpoint* instalado. Esta informação foi anunciada umas semanas depois de termos efetuado a instalação em todo o grupo. Devido a esta mudança de politica por parte da plataforma, foi decidido que esta apenas seria usada para método de controlo e segurança nos pockets.

Uma vez que este método não funcionou, foi implementada uma alternativa. Esta alternativa é o Virtual Network Computing (VNC), e veio complementar a solução final, concretizada no grupo para a gestão e monitorização de dispositivos.

6.3 VNC

O VNC ou *Virtual Network Computing* é um software *open-source* que permite a partilha de ecrãs entre dois dispositivos, disponível para diversos sistemas operativos como Linux, Mac OS, Windows, entre outros. [18] Este tipo de serviço não vem substituir por completo todas as funcionalidades que eram pretendidas pelo software anterior, mas ajuda a que o departamento de informática consiga prestar *support*, de uma forma mais eficaz, a todos os trabalhadores do grupo.

Segundo uma análise realizada pelos especialista da kaspersky :"...found 37 vulnerabilities in four VNC implementations." [19], foram encontradas 37 vulnerabilidades em 4 diferentes plataformas de VNC, sendo estas o TightVNC 1.x, LibVNC, UltraVNC e o TurboVNC. Muitas destas vulnerabilidades foram resolvidas, mas é feito o alerta que algumas plataformas deixaram de prestar suporte a uma versão específica do seu software, como é o caso do TightVNC e a versão 1 do seu software.

Visto que o TightVNC se apresenta, neste momento, na versão 2.8.X, e não existem reportadas nenhumas vulnerabilidades conhecidas, optámos por testar esta ferramenta, para além de ser grátis para empresas e dispor de compatibilidade com sistemas Windows e Unix.[15] Auxiliando o TightVNC, teremos o VNC Viewer para poder aceder aos dispositivos. Esta ferramenta é uma ferramenta grátis do RealVNC [7], que apresenta uma interface simples e que permite a organização dos dispositivos por loja/grupo.

6.3.1 Implementação do VNC e teste

Foi efetuada a instalação do tightVNC e do VNC Viewer em dois computadores diferentes, sendo que um servirá de servidor e o outro de cliente. Desta forma poderemos testar se a comunicação entre estes dois dispositivos é estável e alterar as configurações para que seja mantida a segurança. As imagens seguintes ilustram o teste de comunicação entre os dois computadores:

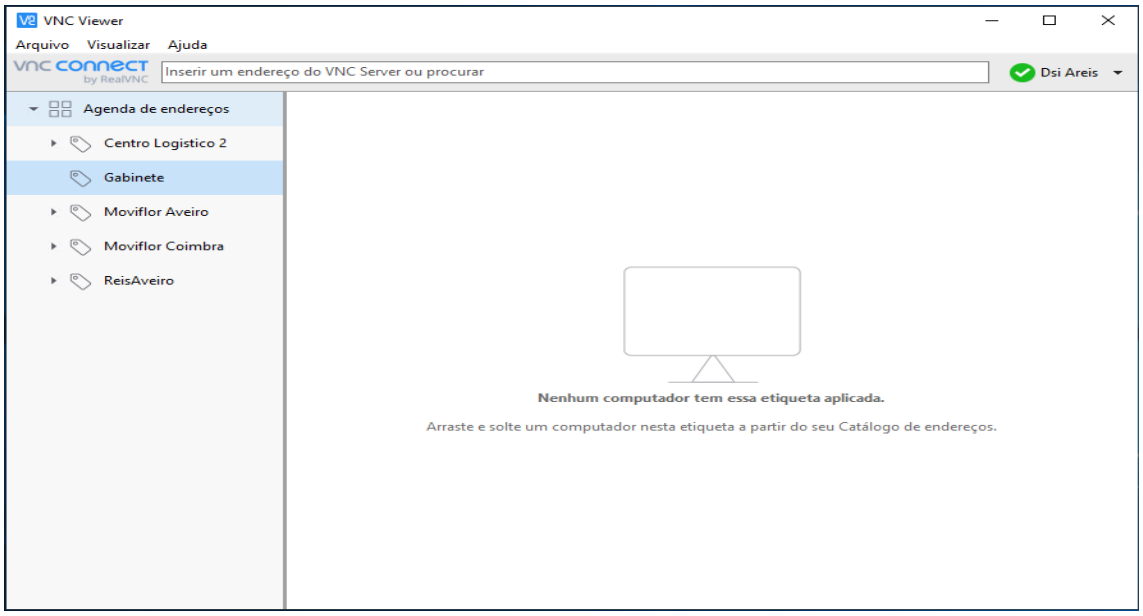


Figure 6.4: VNC - VNC Viewer

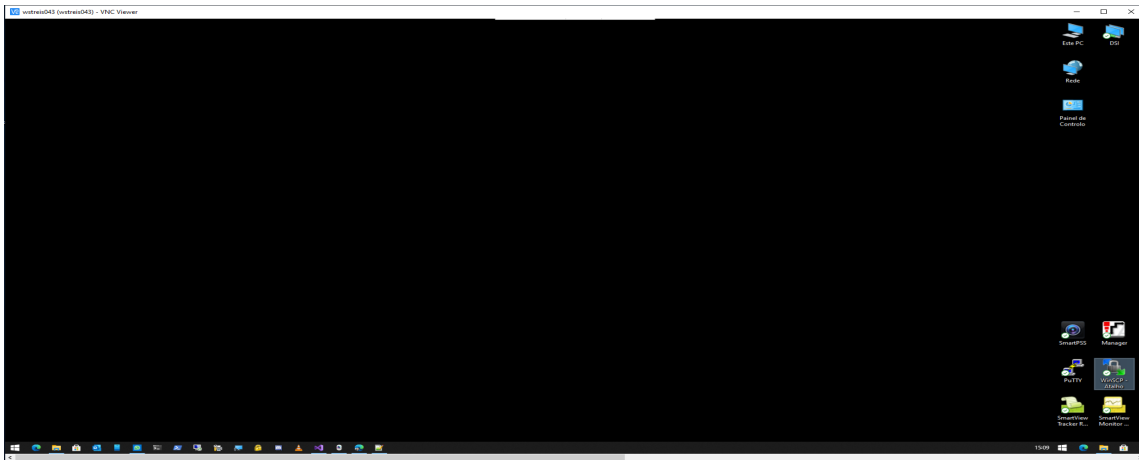


Figure 6.5: VNC - Acesso remoto a um computador

Chapter 7

Aplicação

7.1 Contextualização

Esta aplicação entra neste estágio como o ponto central de grande parte do trabalho realizado até este ponto. Serão interligados diversos pontos criados e implementados no grupo até este momento com a aplicação, o que irá permitir que seja feito uma melhor gestão dos dispositivos e que o administrador tenha em seu poder toda a informação necessária, à distancia de um *click*. Deste modo, alguns dos pontos que estarão interligados entre a aplicação e o trabalho previamente realizado são o Portal Interno (Sistema de tickets), informação relevante do RP, informações sobre dispositivos do grupo, acesso via VNC, .

Para além de se incorporar com a aplicação certas ferramentas que foram ao longo do estágio implementadas no grupo, foram também introduzidas algumas outras funcionalidades para ajudar o administrador do grupo a aumentar o seu controlo sobre todos os dispositivos.

É relevante mencionar que esta aplicação foi desenvolvida em VB.NET, tendo sido criado com base numa interface do tipo Metro, juntamente com diversos outros componentes do SyncFusion [13], complementado com uma base de dados em access para guardar alguns dados, menos importantes, que serão alterados regularmente.

7.2 Objetivos

Com esta aplicação, existem alguns objetivos definidos inicialmente de modo a ser possível afirmar que o trabalho foi realizado com sucesso. Deste modo, os objetivos que se desejam cumprir com esta aplicação são:

- Criação de um "Centro de Controlo" de todos os dados relevantes para o DSI do grupo;
- Criação de um sistema com mecanismos automatizados para alertar quando algum dispositivo relevante se encontra com problemas;
- Criação de um sistema que interligue todas as informações relevantes de um utilizador e os seus "pertences*";
- Criação de um sistema que permita reduzir o total de aplicações externas usadas pelo grupo;

- Criação de um sistema que ajude o DSI do grupo a prestar serviços de apoio mais eficazes e rápidos;
- Criação de uma aplicação que interligue algumas funcionalidades (ex: tickets) já implementadas na empresa, num único ambiente;

  * pertences - Neste contexto, refere-se a qualquer informação ou objeto/dispositivo relativo a um utilizador ou pessoa.

A criação de um Centro de Controlo que possua dados relevantes tem como objetivo criar um ambiente onde estejam presentes todas as informações para que o DSI realize o seu trabalho diário sem precisar procurar por informações, de aplicação em aplicação.

Os mecanismos automatizados de alerta que permitirão que quando algum dispositivo mais relevante, por exemplo um switch ou servidor, se encontre com algum problema seja enviado uma aviso para o DSI e assim, com esta informação, seja possível tomar as medidas necessárias.

A interligação de todas as informações de um utilizador e os seus "pertences" permite que seja feita uma gestão mais regular de todos os utilizadores e todos os seus dispositivos no grupo, como também a criação de um sistema de controlo mais robusto aos dispositivos de cada pessoa/utilizador.

A redução do uso de aplicações externas permite que existam menos pontos de entrada externos ao serviço do grupo. Sendo o grupo, primariamente assegurado pela Checkpoint, quanto menos serviços externos o grupo possuir, menor serão os pontos de entrada existentes.

Com o crescimento do grupo, cada vez mais é necessário um serviço de apoio mais eficaz e rápido, e por isso este objetivo existe no sentido em que a aplicação terá que ser o mais simples possível mas capaz de cumprir com todas as tarefas necessárias que possam surgir no futuro, permitindo que o DSI as possa resolver com a maior brevidade possível.

Por último, a interligação de diversas funcionalidades já implementadas no grupo vai permitir que não seja necessário que o DSI tenha que ter diversas aplicações ou páginas web abertas para cumprir o seu trabalho mas sim apenas uma aplicação, que lhe permitirá fazer todo o trabalho. Este mecanismo permite poupar recursos e ao mesmo tempo centralizar a informação necessária para a realização do trabalho.

Estes são todos os objetivos iniciais para a criação desta aplicação, acordados com o Eng. Paulo Pais. Uma vez que envolve diversas tecnologias e aplicações já desenvolvidas, existe alguma complexidade no modo em como terá de ser criada a aplicação final, mas o resultado possuirá estes objetivos, sendo depois deixado ao critério do engenheiro, qualquer outra adição de novas funcionalidades e outros pormenores. Estes objetivos vão permitir que a análise de requisitos seja mais fluida, uma vez que grande parte dos objetivos são necessários, funcionais ou não-funcionais, podendo vir a ser atribuídos aos requisitos do sistema.

7.3 Análise de requisitos

Segundo o IEEE [25], o que se entende por requisito são três pontos:

- A condição ou capacidade necessária do utilizador resolver um problema ou resolver um objetivo;

- A condição ou capacidade que deve ser cumprida ou possuída por um sistema ou componente de sistema para satisfazer um contracto, um *standard*, uma especificação ou outro documento formalmente imposto;
- Uma representação documentada de uma condição ou capacidade , conforme os pontos (1) e (2).

Por outras palavras, seriam as necessidades de um utilizador ou cliente, as exigências de um negócio e os desejos ou solicitações de uma empresa, realizadas por um sistema ou produto.

7.3.1 Levantamento de Requisitos

Esta aplicação surge para criar um centro de controlo onde é possível conter todas as informações necessárias para o dia-a-dia do DSI. Este centro de controlo tem como meta resolver problemas como a falta de organização de informação, a falta de estrutura e hierarquia presente na empresa e vai permitir melhorar significativamente o serviço de suporte do grupo. Neste âmbito, o único *stakeholder* que vai interessar obter informações para os requisitos do software será o Eng. Paulo Pais, visto ser a única pessoa que fará uso desta aplicação. Este software será exclusivo para o departamento de informática do grupo e por essa razão, este será o único *stakeholder* em causa.

7.3.2 Especificação de Requisitos

A especificação de requisitos vai conter os requisitos funcionais e não-funcionais que o software possuirá, podendo vir a ser exemplificados alguns casos de uso como exemplos, para que a análise fique mais robusta e completa. Desta forma, os requisitos serão divididos em duas Figuras, onde estarão presentes os requisitos funcionais e não-funcionais.

Na figura 7.1 podemos visualizar todos os requisitos funcionais pretendidos para este software. Alguns deles foram baseados nos objetivos idealizados inicialmente, outros foram ideias que ao longo do projeto foram acrescentadas. Estes requisitos vão permitir que a criação das funcionalidades da aplicação seja mais estruturada e simples.

A Figura 7.2 apresenta os requisitos não-funcionais. Estes requisitos foram decididos com foco no utilizador final, o Eng. Paulo Pais. Uma vez que, numa primeira instância, o único utilizador seria o Eng., a preocupação quanto ao funcionamento do software baseou-se no seu desempenho, usabilidade, realização de pedidos e tempos de resposta. Os fatores com maior peso foram a usabilidade e os pedidos realizados, uma vez que o objetivo era ter um software simples mas completo e manter a rede livre de um fluxo enorme de pedidos por causa do software. É importante mencionar que, mesmo que o Eng. fosse o único utilizador alvo, a aplicação foi criada ao seu gosto mas com uma visão de que qualquer utilizador acabaria por facilmente se adaptar ao sistema.

#RF	Nome RF	Descrição do requisito funcional
CU-1	Efetuar Login	Autenticação de Utilizadores, permitindo a realização de operações no software.
CU-2	Visualizar/adicionar/atualizar dispositivos	Capacidade de visualizar, adicionar e atualizar dispositivos do grupo.
CU-3	Receber alertas	Capacidade de receção de alertas sobre problemas ou informações.
CU-4	Aceder remotamente a um computador	Acesso remoto a computadores através do software.
CU-5	Visualizar/adicionar/atualizar utilizadores	Capacidade de visualizar, adicionar e atualizar informaçoes relativas a utilizadores do grupo.
CU-6	Visualizar/adicionar/atualizar informações	Capacidade de visualizar, adicionar e atualizar informações gerais presentes no software.
CU-7	Responder/Visualizar/atualizar tickets	Capacidade de visualizar, responder e atualizar tickets para o DSI.
CU-8	Atualizar BDT	Atualização da base de dados temporaria do software, de forma manual, quando são criados novos utilizadores.
CU-9	Pingar Ip's	Capacidade para pingar IP's através do Software.
CU-10	Enviar mensagens para Utilizadores	Capacidade para o envio direto de mensagens diretas para o computador dos utilizadores.
CU-11	Imprimir informações	Impressão de informações presentes no software, sejam estas de dispositivos, utilizadores ou gerais.

Figure 7.1: Requisitos Funcionais

#RNF	Nome RNF	Descrição do requisito não-funcional
CU-1	User-Friendly	O sistema deverá conter todas as funcionalidades pedidas, apresentando-as de uma forma simples e de facil usabilidade.
CU-2	Sistema responsivo	O sistema deverá-se manter estável e responder sempre de forma adequada aos pedidos realizados.
CU-3	Realização de pedidos	O sistema deverá manter o número de pedidos realizados ao servidor no minimo necessario, de forma a manter a estabilidade da rede interna.

Figure 7.2: Requisitos Não-Funcionais

7.3.3 Prototipagem

Como forma de se poder ter uma exemplificação do resultado final do software pretendido, foram desenvolvidos alguns protótipos de baixo nível. Estes foram os únicos tipos de protótipos desenvolvidos e necessários para o projeto, uma vez que para além de falta de disponibilidade para se poder desenvolver um protótipo com mais alto nível, o resultado do protótipo de baixo nível foi o suficiente para a idealização da estrutura e *layout* do software. As figuras seguintes são todos os protótipos de baixo nível criados:

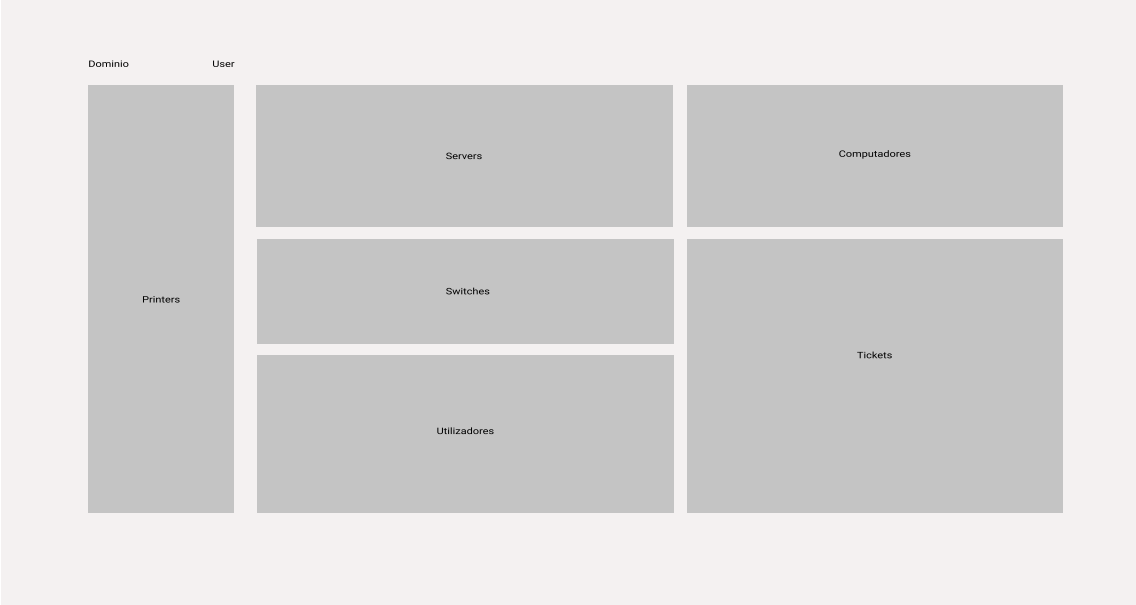


Figure 7.3: Prototipo de baixo nível - teste número 1

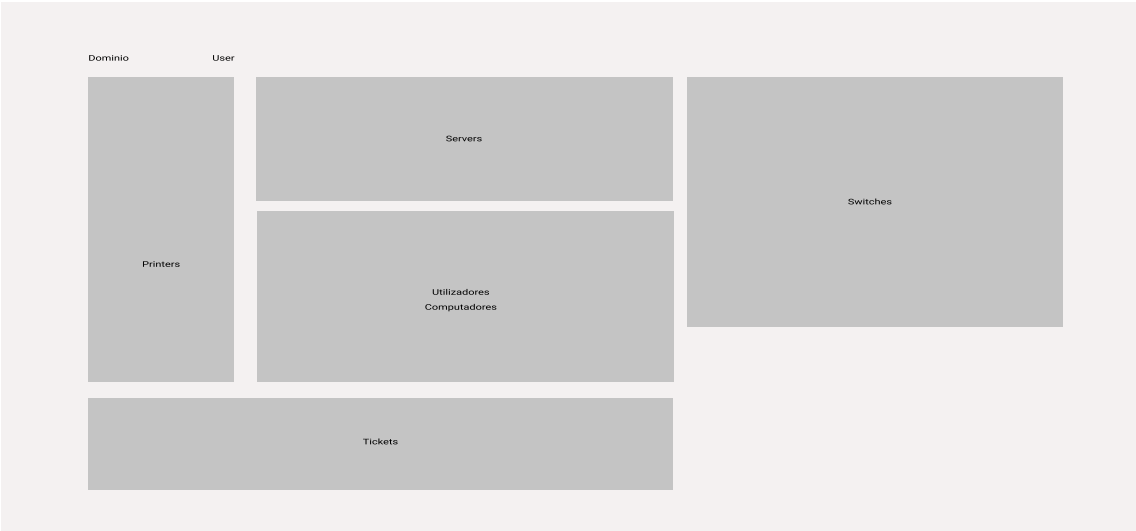


Figure 7.4: Prototipo de baixo nível - teste número 2

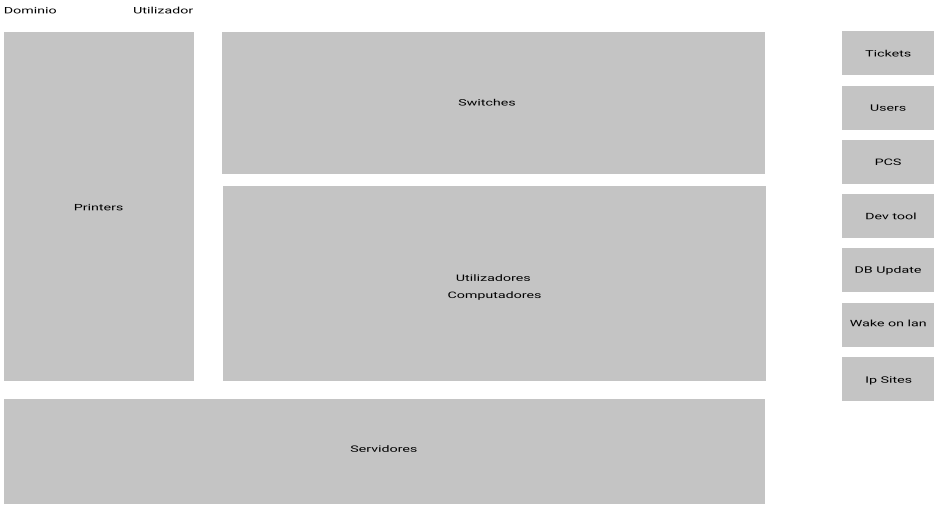


Figure 7.5: Prototipo de baixo nível - teste número 3

7.4 Desenvolvimento

Depois de efetuada a análise de requisitos, foi tempo de começar o desenvolvimento do software. Este decorreu como previsto, tendo sido realizado de uma forma estruturada seguindo o modelo de desenvolvimento mais tradicional (levantamento e análise de requisitos, desenho da arquitetura, implementação, etc). Sendo este modelo mais rígido e formal, tem a desvantagem de não facilitar a chegada do produto ao cliente, ou seja, comparado aos modelos de desenvolvimento mais recentes, este modelo não permite que os "clientes" possam ter o seu software em mãos, o mais rápido possível. Neste caso em específico, esta desvantagem não é muito importante uma vez que a entidade acolhedora que serve como cliente, não tem uma necessidade de rapidez no processo de desenvolvimento do produto e precisa sim que este seja criado o mais completo possível. Deste modo, a figura seguinte permite visualizar o menu de entrada do software:

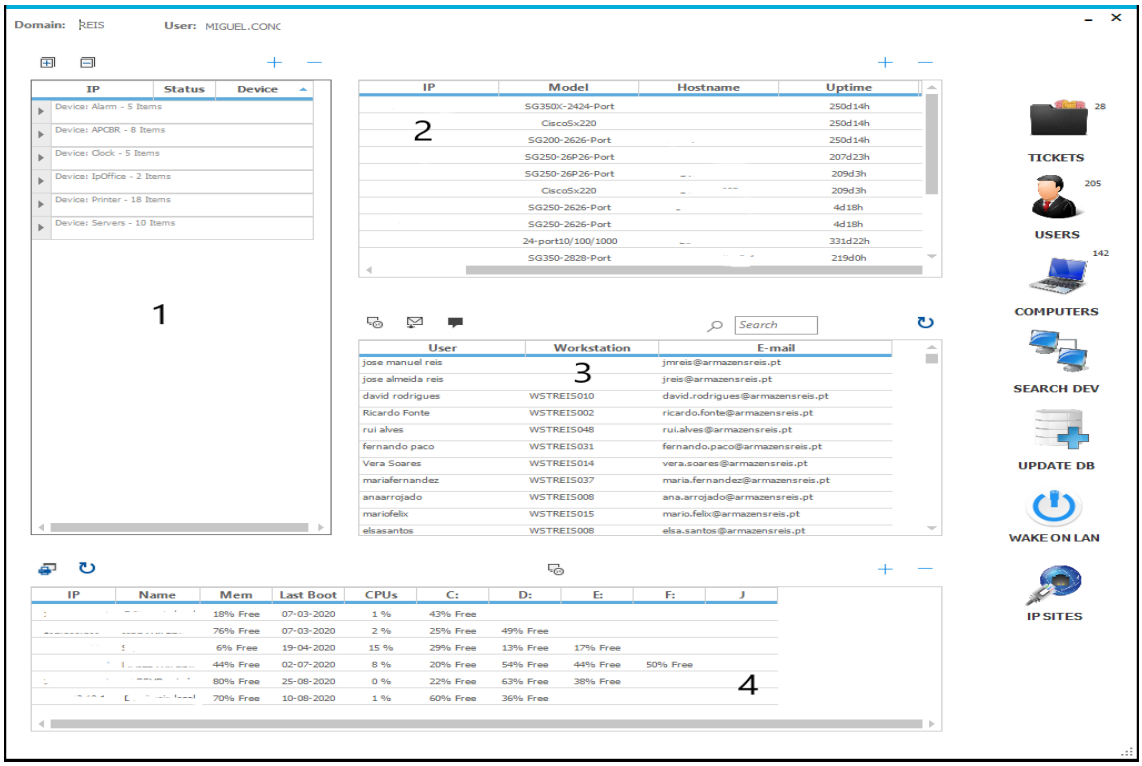


Figure 7.6: Menu principal - Software

Em primeiro lugar, é preciso mencionar que alguns pontos da figura estão rasurados por motivos de segurança. Este menu inicial será o centro de controlo onde o Eng. Paulo Pais poderá aceder a diversas informações relevantes sobre servidores, utilizadores, dispositivos etc. Neste âmbito, ao entrar no software, este deteta automaticamente o domínio e de forma a facilitar o processo de *login* entra conforme os dados do utilizador do computador. Este método foi utilizado durante todo o desenvolvimento e deixado desta forma na versão final, uma vez que nenhum utilizador sem autorização conseguiria correr o software, pois este seria bloqueado pelo antivírus como não reconhecido e autorizado para aquele utilizador específico.

Existem 4 tabelas e 7 botões principais no menu inicial. Estes são os elementos que contêm a informação necessária ao dia-a-dia do DSI, de forma a ser possível visualizar problemas tanto ao nível de dispositivos como computadores, servidores ou *switches*, ou então prestar

auxílio e suporte aos colaboradores do grupo. Desta forma, temos pela seguinte ordem:

- Tabela 1: Tabela de todos os dispositivos que se deseja receber avisos como alarmes, impressoras, ap's, *switches*, servidores, etc. Aqui são adicionados os dispositivos que se deseja receber notificações quando algo vai a baixo, ou seja, se um servidor tiver um problema e se desligar, recebemos um aviso a dizer que o servidor "A" com o ip "xxx.xxx.xxx.xxx", não se encontra disponível. Nesta tabela é possível apenas adicionar ou eliminar dispositivos.

- Tabela 2: Tabela onde são apresentados todos os *switches* com os seus modelos e respetivos *uptimes*. Este tipo de tabela é possível através de comunicações snmp..... Nesta tabela é possível apenas adicionar ou eliminar dispositivos.

- Tabela 3: Tabela dos Utilizadores onde é possível visualizar todos os utilizadores do grupo Moviflor, com o seu respetivo computador e o seu email. É através desta tabela que se consegue aceder aos computadores de cada colaborador, clicando no utilizador que se deseja, e caso este possua um computador, a ligação por VNC será estabelecida. Também existem outras funcionalidades como o envio de mensagens diretas para os computadores de cada um dos utilizadores, de uma forma individual; interligação direta com o outlook quando se deseja enviar um email para um dos utilizadores, assim é aberta uma janela do outlook com o email já preenchido e só é necessário escrever a mensagem e o assunto desejado; e por fim, um mecanismo de pesquisa.

- Tabela 4: Tabela dos servidores onde podemos visualizar informações de *status* dos servidores presentes no grupo como: percentagem de memória restante, percentagem de processamento, espaço dos discos, etc.

Uma vez explicadas as informações das tabelas presentes no menu principal, resta explicar o que cada botão do lado direito permite realizar. Deste modo, e de uma forma descendente, temos os botões de : Tickets, Utilizadores, Computadores, *Search Dev*, *UpdateDB*, "Wake On Lan" e IP sites.

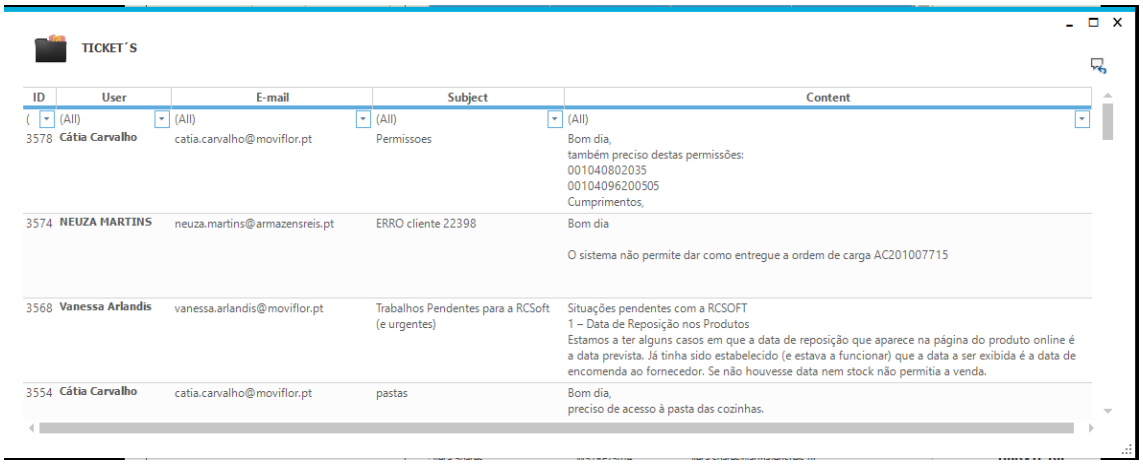


Figure 7.7: Menu secundário - Tickets

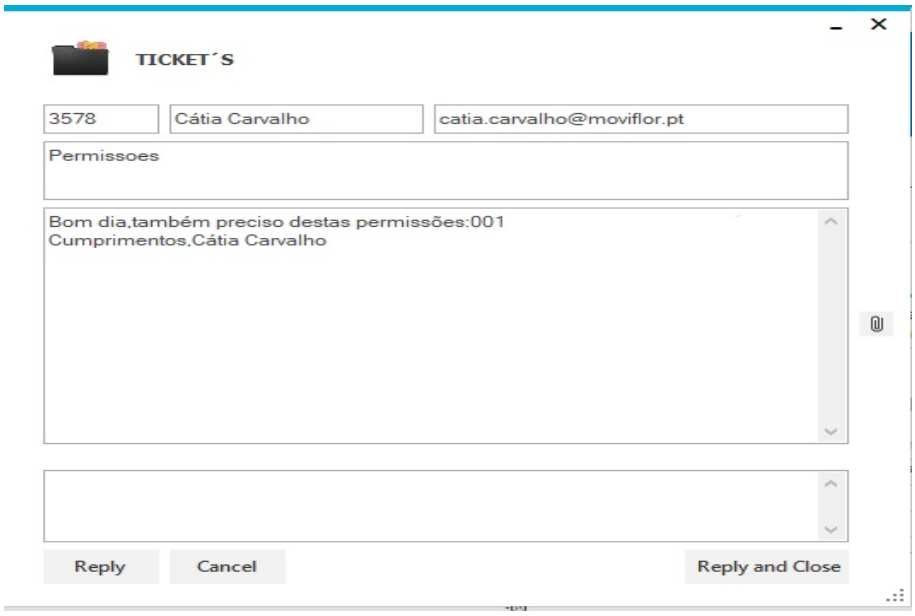
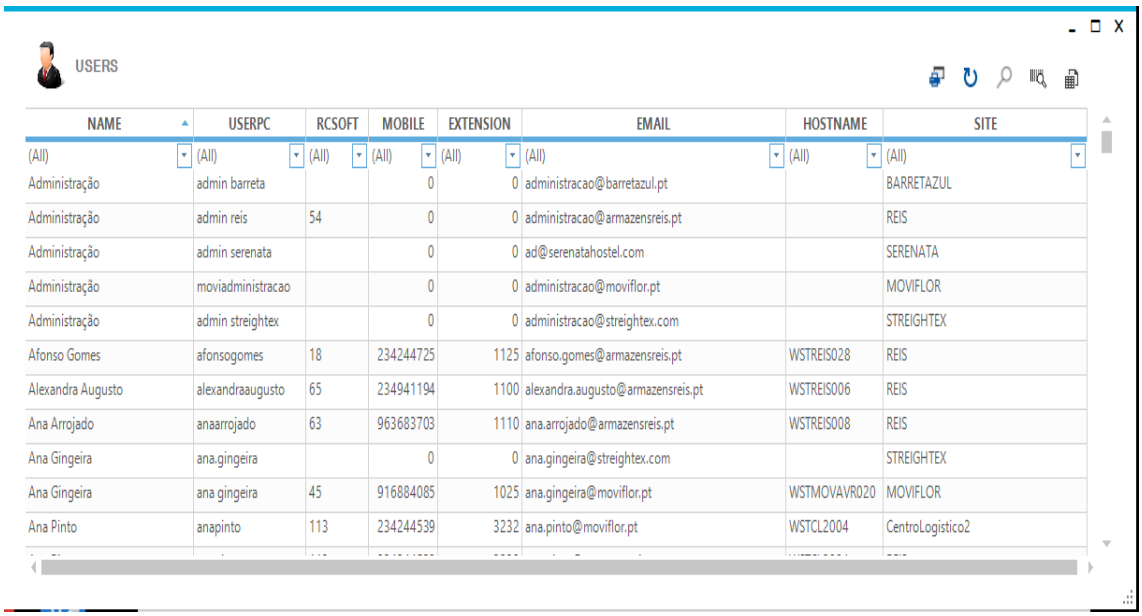


Figure 7.8: Menu secundário - Ticket detalhado

As figuras a cima permitem visualizar os dois sub menus do botão dos tickets. A figura 7.7 refere-se à lista de todos os tickets retirados do portal interno, e a figura 7.8 refere-se a um ticket em detalhe. Através deste último menu (figura 7.8), é possível responder ao ticket ou responder e fechar o mesmo, permitindo que este seja arquivado e o colaborador que o abriu receba uma resposta e o aviso do fecho. Desta forma, é possível manter organizados os tickets que faltam resolver e os que já foram resolvidos.



NAME	USERPC	RCSOFT	MOBILE	EXTENSION	EMAIL	HOSTNAME	SITE
(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)
Administração	admin barreta		0	0	administracao@barretazul.pt		BARRETAZUL
Administração	admin reis	54	0	0	administracao@armazensreis.pt		REIS
Administração	admin serenata		0	0	ad@serenatahostel.com		SERENATA
Administração	moviadministracao		0	0	administracao@moviflor.pt		MOVIFLOR
Administração	admin streightex		0	0	administracao@streightex.com		STREIGHTEX
Afonso Gomes	afonsogomes	18	234244725	1125	afonso.gomes@armazensreis.pt	WSTREIS028	REIS
Alexandra Augusto	alexandraaugusto	65	234941194	1100	alexandra.augusto@armazensreis.pt	WSTREIS006	REIS
Ana Arrojado	anaarrojado	63	963683703	1110	ana.arrojado@armazensreis.pt	WSTREIS008	REIS
Ana Gingeira	ana.gingeira		0	0	ana.gingeira@streightex.com		STREIGHTEX
Ana Gingeira	ana gingeira	45	916884085	1025	ana.gingeira@moviflor.pt	WSTMOVAVR020	MOVIFLOR
Ana Pinto	anapinto	113	234244539	3232	ana.pinto@moviflor.pt	WSTCL2004	CentroLogistico2

Figure 7.9: Menu secundário - Utilizadores

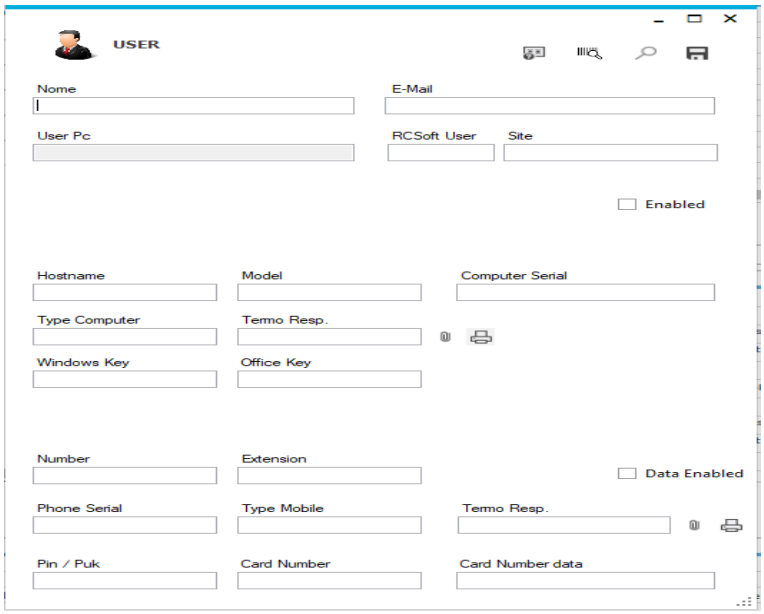


Figure 7.10: Menu secundário - Informações do utilizador

Nesta secção, temos uma lista de todos os utilizadores existentes no grupo, não só estão presentes as suas informações básicas mas também informações relacionadas com o ERP e dispositivos. Neste sub-menu é possível realizar uma pesquisa por utilizador, fazer uma impressão das informações de um utilizador em específico, imprimir um QR code referente a um utilizador e, por fim, exportar toda a lista de utilizadores para uma lista de excel. .

Ao se realizar a pesquisa, ou para se visualizar todas as informações de um determinado utilizador, é necessário clicar na lupa que abrirá o menu da figura 7.10. Neste menu, estão presentes todas as informações do utilizador, os dispositivos relacionados ao mesmo e informações dos dispositivos para que o DSI seja capaz de relacionar os dispositivos aos colaboradores. Através deste menu é possível imprimir o termo de responsabilidade do dispositivo que o colaborador irá receber, seja este um computador ou um telemóvel, imprimir uma etiqueta QR com o distintivo do seu dispositivo, contendo esse código QR o contacto e os dados do colaborador responsável pelo dispositivo. Esta etiqueta é um mecanismo implementado no grupo pelo DSI de forma a identificar cada dispositivo com o seu respetivo *hostname* e outras informações, o que melhora a comunicação entre o colaborador e o agente de suporte e a identificação de problemas nos dispositivos.

A figura 7.11 apresenta uma lista de todos os computadores e os grupos aos quais estão associados. Para além de ser necessário uma localização para se poder arquivar toda a informação relativa aos dispositivos do grupo, nomeadamente os computadores, esta secção permite que sejam apresentados alguns campos, que o Eng. Paulo Pais escolheu, e que sejam úteis ao seu trabalho do dia-a-dia. Estas informações são de caratér temporário uma vez que muitos dos computadores acabam por mudar de proprietário rapidamente, sendo que depois estes dados são atualizados e consequentemente os dados associados ao utilizador também o serão.

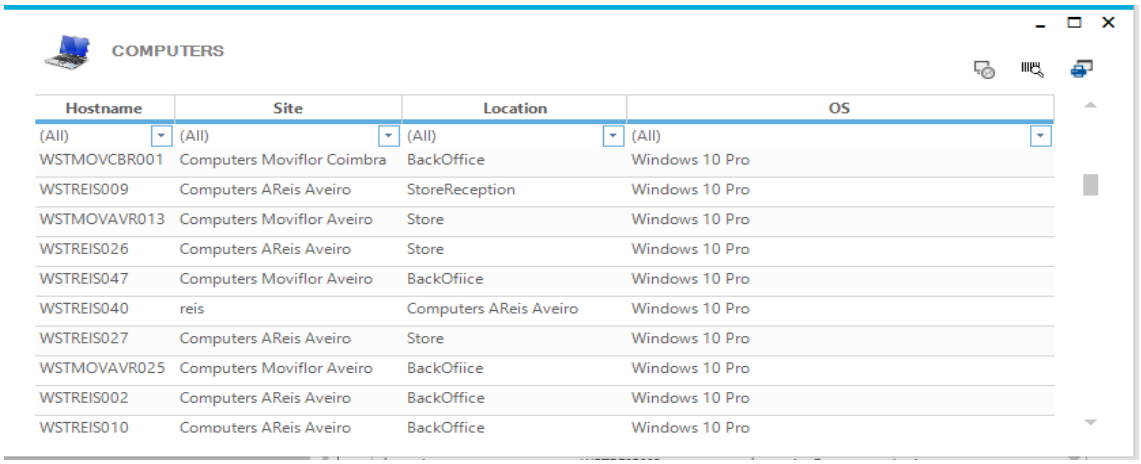


Figure 7.11: Menu secundário - Computadores

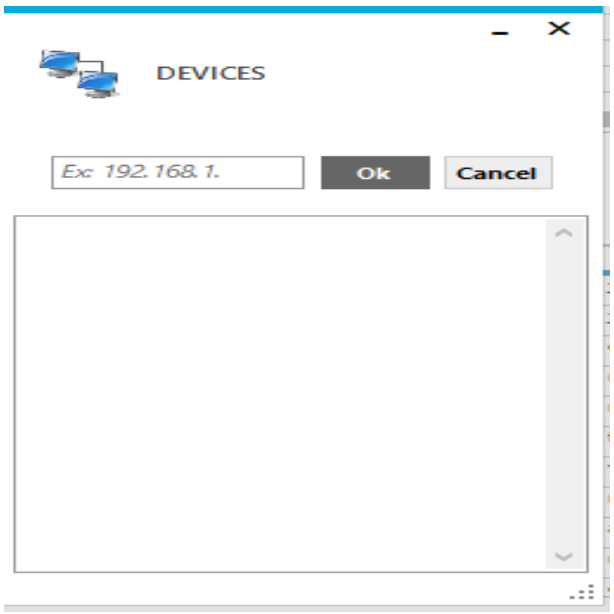


Figure 7.12: Menu secundário - Ferramenta de Ping

A ferramenta presente na figura 7.12 é algo que normalmente é realizado numa janela de "CMD" ou num *third-party software*. Neste caso, a ideia aqui presente é uma implementação de uma ferramenta usada diariamente no trabalho do Eng. mas presente no software. Para além de englobar diversas outras informações e ferramentas, também se engloba uma ferramenta muito usada, o "ping".

O Wake On Lan é um protocolo que permite ligar computadores, de uma forma remota, através de um modo de baixa potência. [20] Com o evoluir da tecnologia, pode-se interpretar que um computador em modo de baixa potência é sempre que este não se encontra ligado mas tem acesso a energia. [20]

Esta ferramenta é um ótimo auxiliar ao VNC quando existe a necessidade de ligar um computador remotamente. Deste modo, através de um pacote "mágico", podemos ligar um determinado computador e realizar as ações necessárias, sem que o DSI tenha que se deslocar ao local do dispositivo.

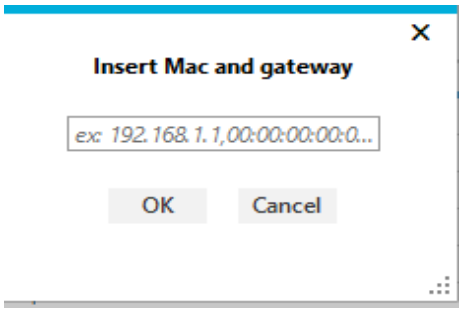


Figure 7.13: Menu secundário - Wake On Lan

Chapter 8

Conclusão

Com este estágio foi possível ganhar muita experiência a nível social, pessoal e profissional. Com uma grande diversidade de dispositivos e tecnologias ao meu dispor, e os diversos desafios com níveis de exigência diferentes, permitiu-me crescer e ganhar experiência fazendo com que este estágio fosse um sucesso.

Ao nível dos objetivos planeados para o estágio, tínhamos inicialmente os seguintes pontos:

- Exploração da Appliance Check Point;
- Melhoria e gestão de redes via VmWare;
- Administração de toda a infraestrutura informática;
- Gestão da appliance de segurança Panda Adaptive Defense;
- Estudo de uma ferramenta para a gestão e controlo de dispositivos;
- Caraterização e diagnóstico da infraestrutura do grupo Moviflor;
- Realização de uma auditoria.

De uma forma geral, todos os pontos foram explorados e concretizados ao longo do estágio, com a excepção de um, a auditoria. Devido à pandemia que infelizmente afetou todo o mundo, provocando inúmeras condições sobre a Entidade acolhedora onde o estágio decorrera, o estágio em si teve que ser posto em pausa, o que provocou uma alteração de planos. Nesta alteração, foram adicionados alguns objetivos ao plano inicial:

- Criação de um Portal Interno para o grupo Moviflor;
- Criação de uma aplicação de gestão de dispositivos, computadores, acesso remoto, etc.

Com estes dois pontos, foi possível criar um portal muito necessário para o grupo onde estão localizadas diversas ferramentas e onde futuramente poderão adicionar ainda mais, melhorando a comunicação e os serviços prestados dentro do grupo conforme o seu crescimento.

Também foi possível criar uma ferramenta para o informático do grupo poder centralizar a informação necessária para o seu trabalho diário e que o vai ajudar a controlar, não só os dispositivos e os utilizadores dentro do grupo, mas também a relação entre eles.

Conforme os objetivos acordados para a aplicação, esta apresenta-se estável e com pedidos moderados aos servidores, tendo sido aprovado o layout e a disposição e a forma de interação e usabilidade do sistema pelo Eng. Paulo Pais. No que toca às funcionalidades, estão todas operacionais.

Por fim, este trabalho foi uma experiência muito enriquecedora tanto a nível pessoal como a nível do grupo. A experiência de estagiar neste grupo fez com que me dessem a oportunidade de ficar a trabalhar durante 6 meses para ajudar com a nova loja que irá abrir em Viseu, e a Entidade acolhedora ganhou diversas melhorias no sistema, aumentando a eficácia de várias metodologias existentes no grupo e vários outros procedimentos que eram realizados de forma desorganizada e muitas vezes sem qualquer controlo nenhum e de maneira insegura.

References

[1] Administration guide. http://dl3.checkpoint.com/paid/79/7916511f80908c3056af526bae304602/CP_R77_Firewall_AdminGuide.pdf?HashKey=1578761522_95b791e9400231e30d6f1b584e8c88ac&xtn=.pdf. (Acedido em 22/11/2019).

[2] Best msp software. https://www.ninjarmm.com/blog/best-msp-software/. (Acedido em 1/11/2019).

[3] Complete rmm software the whole enchilada. https://www.atera.com/. (Acedido em 1/11/2019).

[4] Get the only complete, scalable it management platform. https://one.comodo.com/. (Acedido em 2/11/2019).

[5] Meet wordpress. https://wordpress.org/. (Acedido em 1/11/2019).

[6] ninjarmm. https://www.ninjarmm.com/rmm/. (Acedido em 01/11/2019).

[7] Realvnc. https://www.realvnc.com/en/. (Acedido em 15/01/2020).

[8] Rmm definition. url = https://www.itarian.com/rmm.php?af=7639. (Acedido em 2/11/2019).

[9] The rmm tool that puts automation in your hands. https://www.connectwise.com/software/automate. (Acedido em 4/11/2019).

[10] Security, management and control. https://www.pandasecurity.com/en/business/solutions/. (Acedido em 15/11/2019).

[11] Solarwinds remote monitoring management. https://www.solarwindsmsp.com/products/rmm. (Acedido em 1/11/2019).

[12] Source code template for external web portal (controller 3.1.4 or above). https://www.tp-link.com/us/support/faq/2390/. (Acedido em 18/10/2019).

[13] Syncfusiondocumentation. https://help.syncfusion.com/windowsforms/overview. (Acedido em 02/05/2020).

[14] There's a better way to remotely manage your it. https://www.pulseway.com/. (Acedido em 1/11/2019).

[15] tightvnc. https://www.tightvnc.com/. (Acedido em 15/01/2020).

[16] Unifi - guest network, guest portal, and hotspot system. https://help.ubnt.com/hc/en-us/articles/115000166827-UniFi-Guest-Network-Guest-Portal-and-Hotspot-System. (Acedido em 11/10/2019).

[17] Verify email address check if real exists domain. https://www.codexworld.com/verify-email-address-check-if-real-exists-domain-php/. (Acedido em 10/10/2019).

[18] Virtual network computing. https://www.sciencedirect.com/topics/computer-science/virtual-network-computing. (Acedido em 14/01/2020).

[19] Vnc remote access vulnerabilities. https://www.kaspersky.com/blog/vnc-vulnerabilities/31462/. (Acedido em 15/01/2020).

[20] wakeonlan. https://www.howtogeek.com/70374/how-to-geek-explains-what-is-wake-on-lan-and-ho (Acedido em 15/05/2020).

[21] What is rmm? https://www.atera.com/what-is-rmm/. (Acedido em 1/11/2019).

[22] Eric Dosal. 5-common-network-security-problems-and-solutions. https://www.compuquip.com/blog/5-common-network-security-problems-and-solutions. (Acedido em 10/12/2019).

[23] Kathleen Juell Justin Ellingwood. How-to-install-the-apache-web-server-on-ubuntu-18-04. https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-18-04. (urldate 27/04/2018).

[24] Malle Pietje. Unifi-api-client. https://github.com/Art-of-WiFi/UniFi-API-client. (Acedido em 1/11/2019).

[25] D.T. Ross. Structured analysis for requirements definition. *IEEE Transactions on Software Engineering*, SE-3(1):6 – 15, 1977.

Appendices

This page is intentionally left blank.

Apêndice A

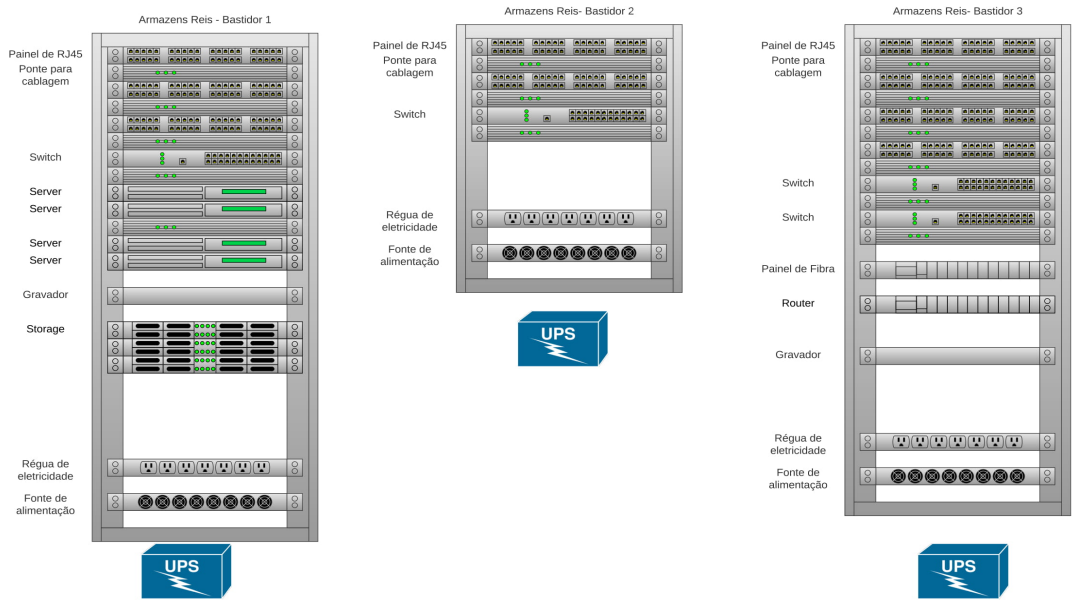


Figure 1: Bastidor dos Armazéns Reis

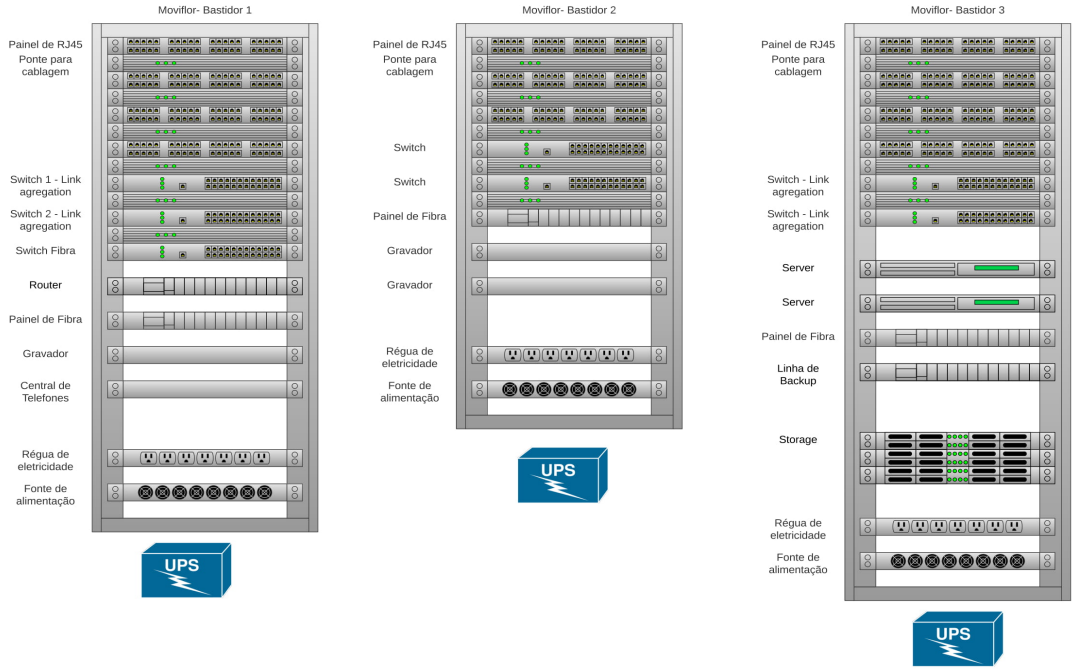


Figure 2: Bastidor da Moviflor Aveiro

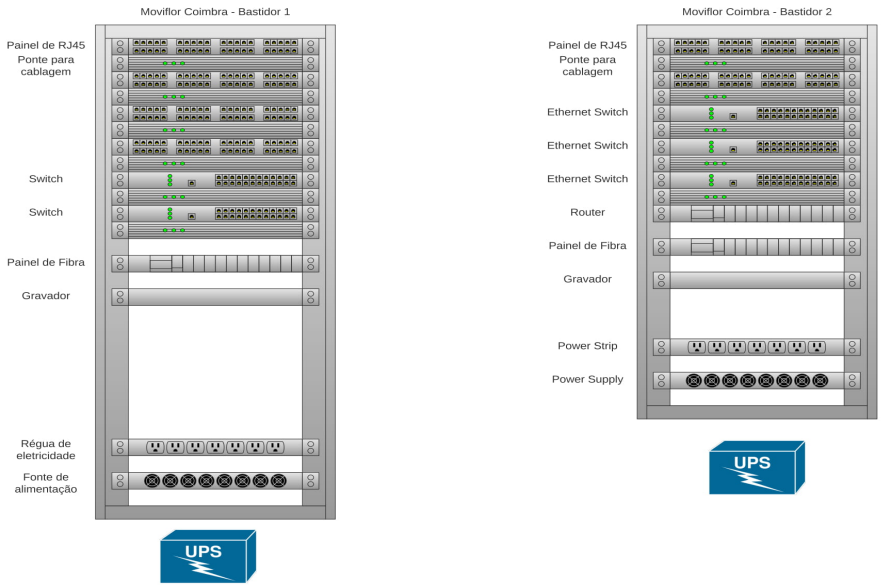


Figure 3: Bastidor da Moviflor Coimbra

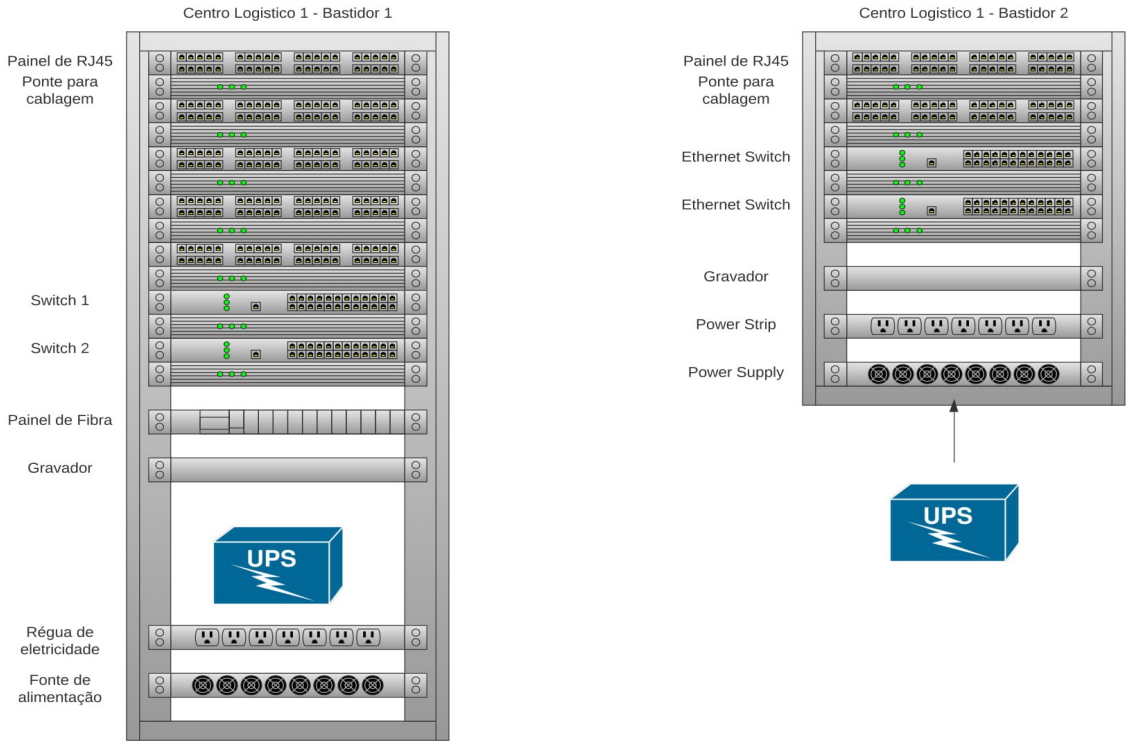


Figure 4: Bastidor do Centro Logístico 1

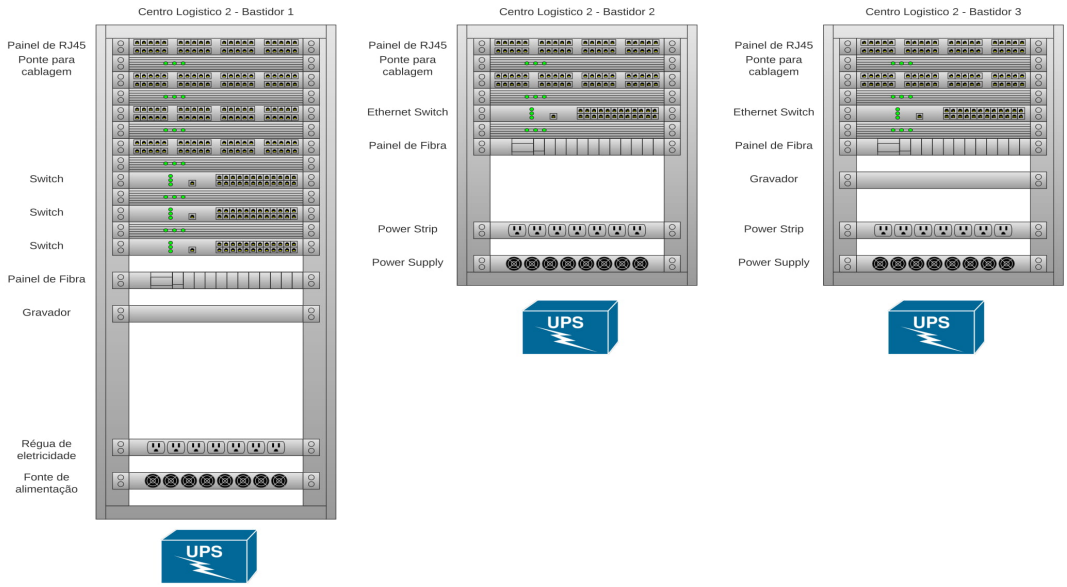


Figure 5: Bastidor Centro Logístico 2

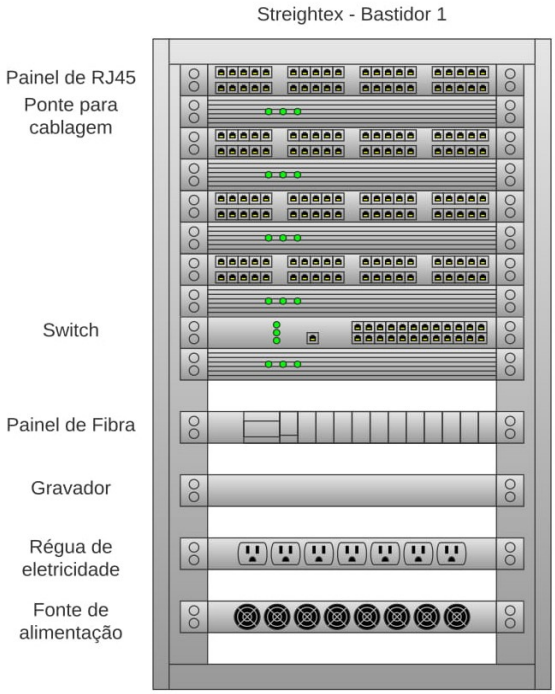


Figure 6: Bastidor da Streightex

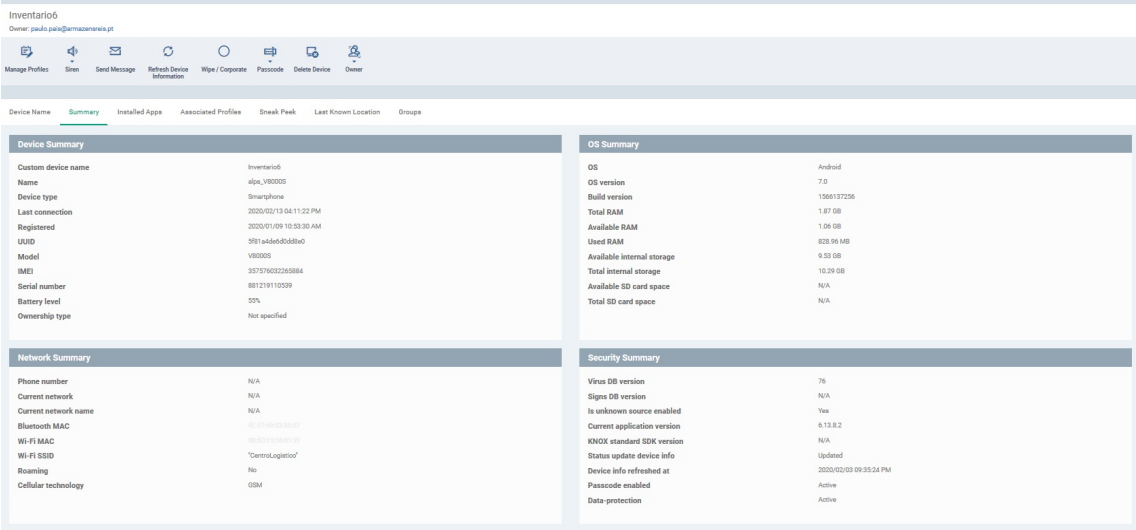


Figure 7: Informações de um PDA apresentadas na plataforma

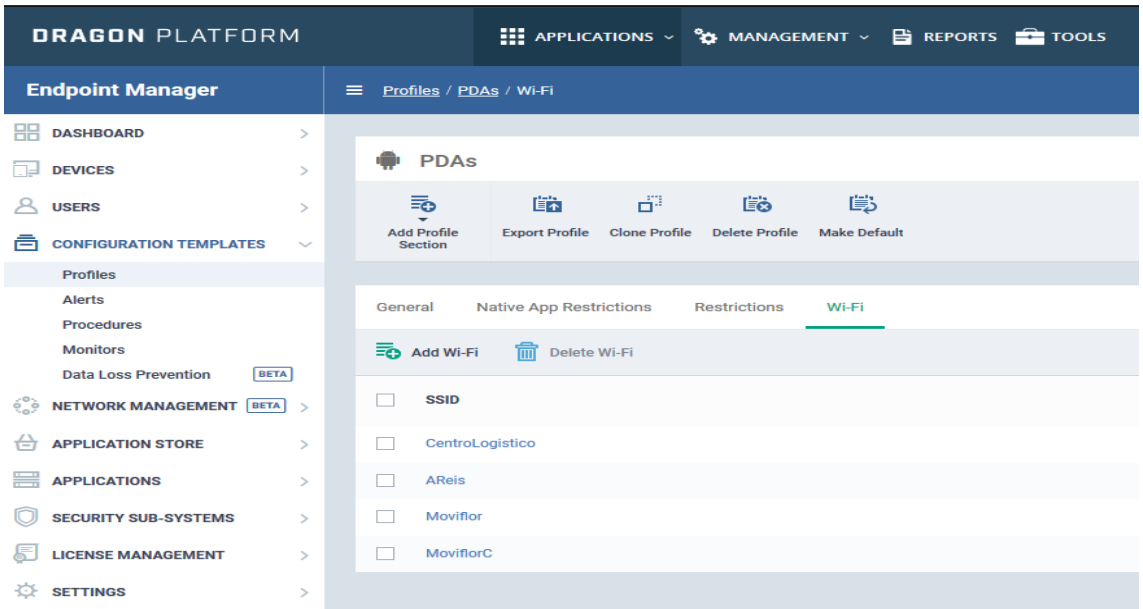


Figure 8: Redes wifi associadas ao perfil dos PDA's - Comodo One

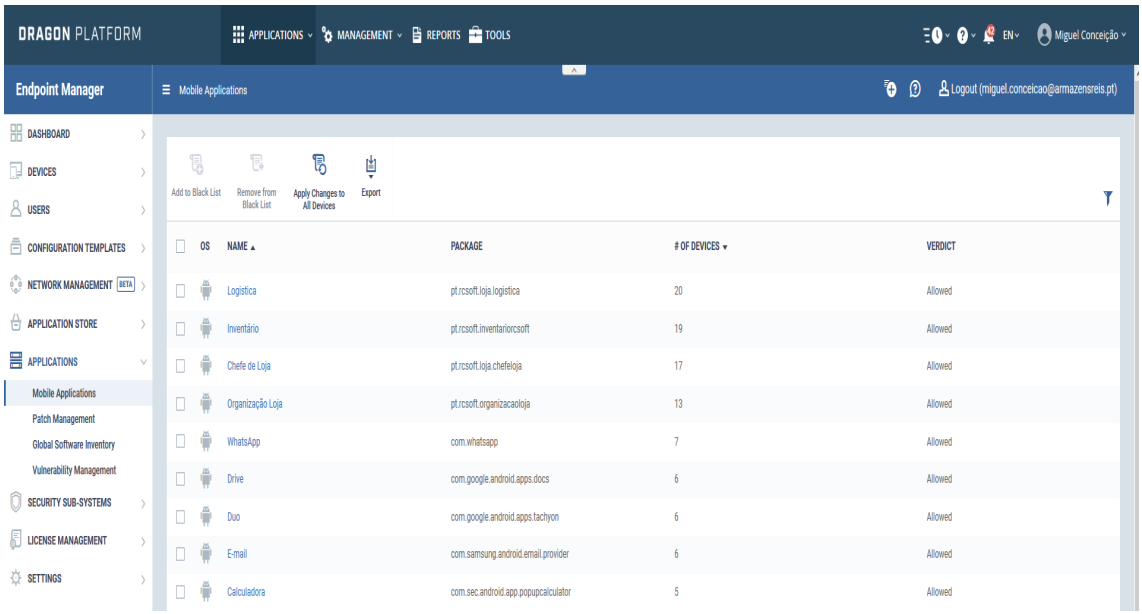


Figure 9: Aplicações permitidas para utilização associadas ao perfil dos PDA's - Comodo One

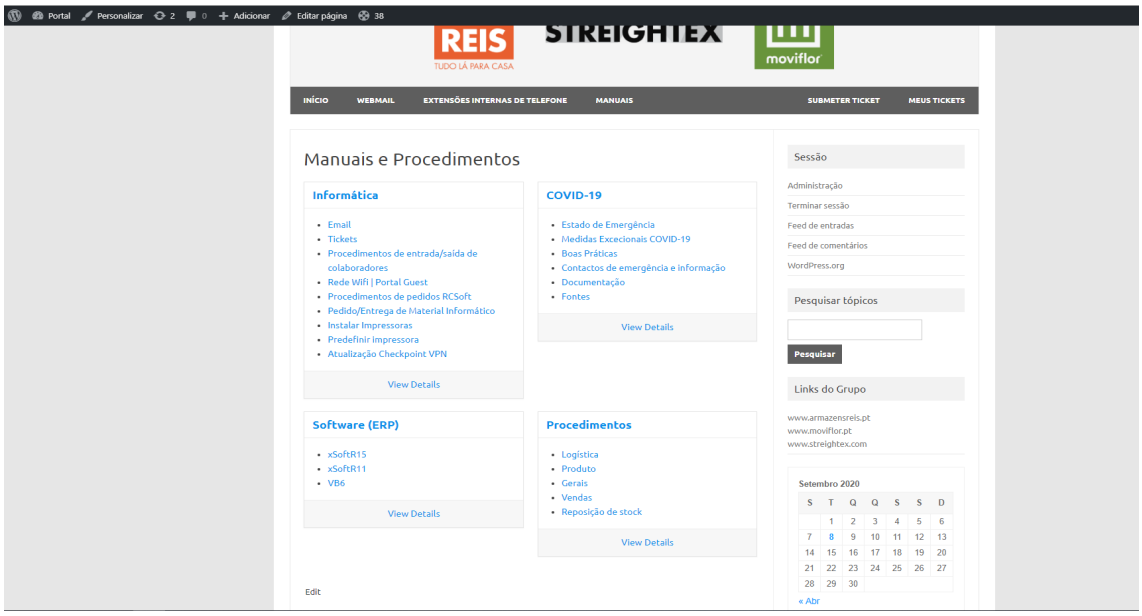


Figure 10: Portal Interno - Manuais e procedimentos para os Colaboradores

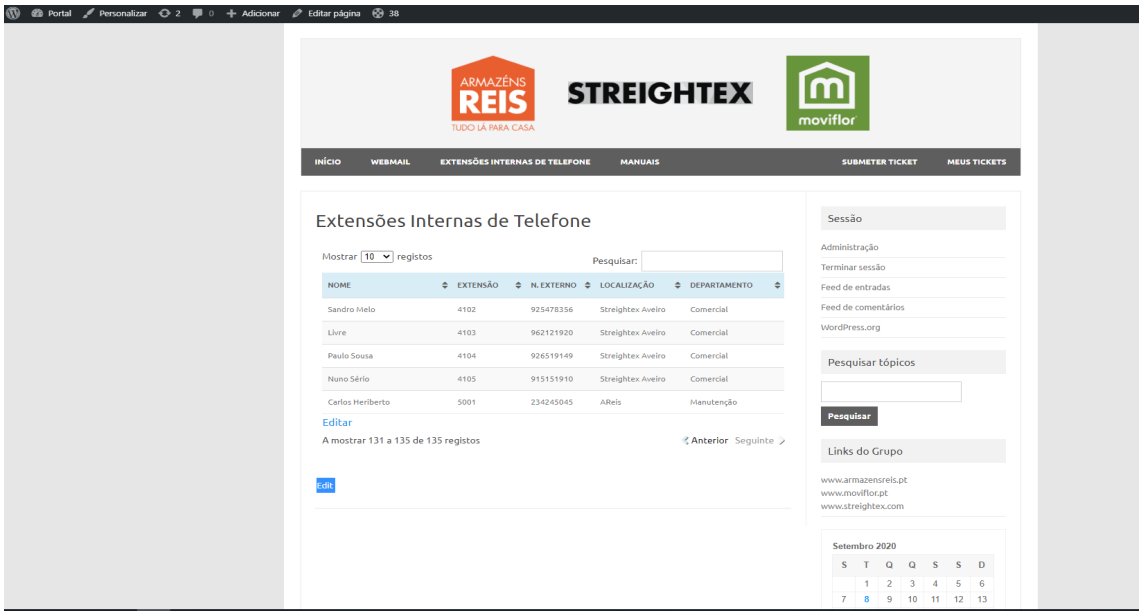


Figure 11: Portal Interno - Lista telefónica de todos os contactos do grupo

This page is intentionally left blank.

Apêndice B

.0.1 Software Painel publicitário

Durante o estágio surgiram alguns problemas com a plataforma e correspondente software dos painéis publicitários presentes no grupos. Para corrigir este problema, e prevenir futuros problemas, foi criada uma aplicação em Android com o auxilio do Android Studio para se poder carregar conteúdo via Diretório e desta forma transmitir a publicidade desejada. Uma vez que este trabalho realizado não alinhava com a estrutura do relatório, foi introduzido no Apêndice para sinalizar a sua realização. De seguida, estão presentes os ecrãs da aplicação criada:

Figure 12: Ecrã inicial da aplicação

A Figura 12 do apêndice B refere-se ao Menu inicial onde estarão a ser transmitidos os conteúdos de publicidades sejam estes imagens ou vídeos, num esquema de carrossel. Enquanto que a Figura 13, permite visualizar o menu onde se pode trocar a loja a que pertence o painel, alterando assim a publicidade que este iria transmitir.

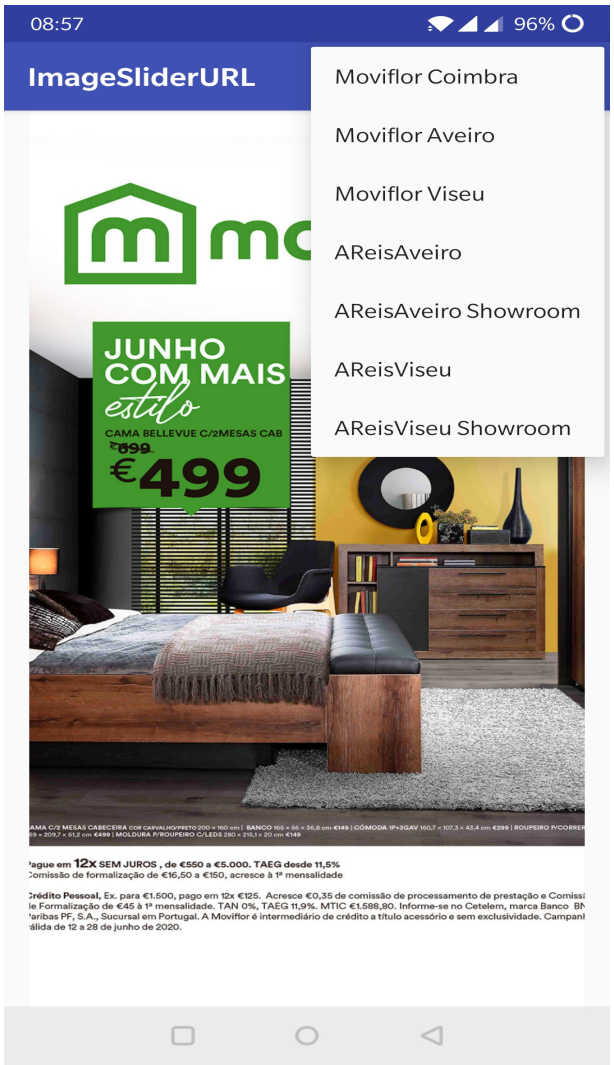


Figure 13: Menu de lojas da aplicação