

2008



ServiceDesk



Tiago Rodrigues

Universidade Lusófona

21-09-2008

Índice

Índice	2
Glossário.....	4
1. Objectivo / Âmbito	5
2. Procedimentos de Configuração de novos Equipamentos.....	6
2.1. Enquadramento e processo de selecção da imagem por parte do Utilizador	6
2.2. Processo de entrega das imagens ao Fornecedor e respectiva actualização.....	8
3. Instalação e Actualização do PT.....	9
3.1. Instalação do PT.....	9
3.2. Adicionar PT ao domínio	9
3.3. Reorganização de Objectos perdidos.....	13
3.4. Actualização do PT	14
3.5. Registo do PT	14
4. Regras de uso da ferramenta de acesso remoto aos Equipamentos desktop e laptop	15
4.1. FAQ – Acesso Remoto	15
5. Configurações	17
5.1. Rede – Estação Padrão	17
5.2. Internet Explorer – Estação Padrão	18
6. Ligação de Equipamentos externos à rede	20
6.1. Pré Requisitos.....	20
6.2. Como Efectuar o pedido	20
6.3. Verificação dos equipamentos	21
6.3.1 Verificação dos equipamentos.....	21
6.4. Decisão para ligação dos equipamentos.....	21
6.5. Configuração do PC.....	21
6.6. Criação de utilizador Helpdesk com permissões de administrador local.....	22
6.7. Compromisso de actualização	22
7. Equipamentos Spare	23
8. Análise da Qualidade de Serviço – Outbound Survey	24
8.1. Survey Global	24
8.2. Outbound Survey	24
9. Staging.....	26
9.1. Espaço.....	26
9.2. Equipamentos	26
10. Impressoras	27
10.1. Pedido de Criação de Impressoras na Rede.....	27
11. Grupo Utilizadores.....	29
12. Password de Rede	30
12.1. Reset Password.....	30
13. Boas Práticas	33
13.1. Computadores	33
13.1.1 Passwords	33
13.1.2 Bloquear o Computador.....	34
13.1.3 Desligar o Computador.....	34
13.1.4 Instalação de software.....	34
13.1.5 Download de Software.....	35
13.1.6 Actualização Automática do Software Base.....	35
13.1.7 Armazenamento de Informação.....	35
13.2. Email.....	35
13.2.1 Divulgação de Informação	35

13.2.2	Divulgação dos endereços de Email	35
13.2.3	Armazenamento de Informação	36
13.2.4	Senders de Mensagens Desconhecidas	36
13.2.5	Regras de utilização do Email	36
13.3.	Shares, Ficheiros e Informação	37
13.3.1	Armazenamento dos Documentos Pessoais	37
13.3.2	Armazenamento dos Documentos da empresa	37
13.3.3	Documentos Finais	37
13.3.4	Informação Sensível e/ou de Negócios	37
13.4.	Impressão	38
13.4.1	Impressão de Informação não necessária	38
13.4.2	Documentos nas Impressoras	38
13.4.3	Destruição de Documentos	38
13.5.	Internet	38
13.5.1	Informação Confidencial	38
13.5.2	Endereço de Email Corporativo	38
13.5.3	Utilização de ActiveX	38
13.5.4	Utilização de Cookies	39
13.5.5	Sites Desconhecidos	39
13.5.6	Utilização de Auto Complete	39
14.	Conclusão	40

Glossário

BD

Base de Dados; Repositório de informação organizada de forma otimizada.

GSM

Global System Mobile; Sistema standard de telecomunicações definido e adoptado a nível mundial.

HLR

Home Location Register; Base de dados de cartões de clientes; contém apenas informação técnica sobre cartões e serviços, não tendo qualquer informação sobre os seus titulares.

NAU

Núcleo de Apoio ao Utilizador;

NC

Não conformidade; Situação de incoerência de dados entre diversos sistemas de informação.

PPP

Plano Personalizado de Preços; Denominação dada aos cartões de assinatura mensal.

PPS

Pré Paid System, Denominação dada aos cartões de carregamento, conceptualizada e desenvolvida originalmente por parte da TMN.

VAX

Virtual Address eXtension; Nomenclatura dada à máquina de suporte dos sistemas de VoiceMail, devido à sua grande capacidade de lidar com um grande quantidade de dados, como é o caso das mensagens de voz.

VDU

Virtual Display Unit; Nome original da equipa.

CS

Centro de Supervisão.

OC

Ordem de Compra.

PT

Posto(s) de Trabalho.

PST

Personal Storage File; Ficheiro de armazenamento de email.

SMS

System Management Service - disponibilização remota de software.

AD

Active Directory.

1 - Objectivo / Âmbito

Este documento tem como objectivo disciplinar a introdução de novos equipamentos na *Active Directory* (AD) pois, cada vez mais, nota-se a importância de obter uma Organização coerente de controlo de um parque informático, que torne eficientes os recursos disponibilizados.

Uma organização coerente é essencial para assegurar ferramentas de gestão de bens que se pretendem vir a adquirir no futuro. Todo o trabalho que está a ser feito para levar a cabo uma AD organizada e coerente, terá invariavelmente de ser efectuado no futuro aquando da aquisição das ferramentas mencionadas. Assim este documento pretende enquadrar os seus destinatários na situação actual, mas também para o futuro.

Este documento foi criado para as equipas de ServiceDesk poderem operar nas melhores condições possíveis, em termos procedimentais. Como tal é da responsabilidade individual de cada membro dessas equipas detectar e informar de incorrecções no documento, ou alterações (pela via prática) aos procedimentos. Enquanto tal não sucede este documento está em conformidade com o exigido para a execução de todos os pontos nele enumerados.

2 - Procedimentos de Configuração de novos Equipamentos

2.1 - Enquadramento e processo de selecção da imagem por parte do utilizador

Tendo por base o Objectivo de reduzir o tempo de disponibilização aos utilizadores final, de novos equipamentos, foi estabelecido um acordo entre a TMN e o fornecedor, que resultou nos processos de instalação da imagem da Estação Padrão definida pela TMN.

Este acordo assenta nos seguintes pressupostos:

O utilizador TMN, sempre que solicite a aquisição de um novo equipamento, deverá incluir na Ordem de compra a Imagem que melhor se adapte ao seu perfil.



Estação Padrão (EP)
Suporte. Estação Padrão

Versão 2.0	Imagem A (V1.0.0)	Imagem B (V1.0.0)	Imagem C (V1.0.0)
	Imagem Padrão (Edifícios)	Imagem NEPAL (Loja)	Imagem NEPAL (Atendimento)
Software Complementar	Quota Server (OCX) Microsoft Office Visio Viewer 2003 Wallpaper ScreenSaver Macromedia Shockwave Player 10.0 Macromedia Flash Player 8.0	Quota Server (OCX) Wallpaper ScreenSaver Macromedia Shockwave Player 10.0 Macromedia Flash Player 8.0 Dr. Sim 2.6 Ms Wait 2.11 Gestão Ms Wait 2.11 Mesa	Quota Server (OCX) Wallpaper ScreenSaver Macromedia Shockwave Player 10.0 Macromedia Flash Player 8.0 FileNet Panagon IDM Desktop 3.3 Gesfax Filenet 3.07 Informix 4 GL (Cardinfo) KeaVT V5.1 (Kea - Mobilix / Mimo / Credimix) FileNet Administrator USupervisor EasyPhone 6.2 Lucent 9.0 (Avaya Center Viewer)
Software Base	Windows XP Professional + Service Pack 2 Microsoft Office Professional 2003 + Service Pack 2 Microsoft Office Proofing Tools 2003 + Service Pack 2 Microsoft Internet Explorer 6.0 + Service Pack 1 Windows Media Player 10 Oracle Client V9.i (Ora2000) Oracle Developer 6.i (OraFrms) SAP / SAPIX / Pro UNO 6.40 FileNet Panagon (Filenet Viewer) 3.3 McAfee VirusScan Enterprise V.8.0.0 Adobe Acrobat Reader V7.0.0 Power Archive V6.1 Java 1.4.2.09 Siebel (KB896156) + (Siebel Option Pack)		

Consoante o perfil de utilização deverá ser seleccionada a Imagem pretendida.
Sempre que na OC for omissa esta informação, por defeito, será instalada a imagem A.

2.2 - Processo de entrega das imagens ao Fornecedor e respectiva actualização

Para que este processo funcione eficazmente exige-se que sejam cumpridos um conjunto de pressupostos por parte dos seus intervenientes, ou seja, a TMN, e o Fornecedor. Como ponto-chave identifica-se o estabelecimento de um canal único de comunicação entre as partes envolvidas.

Sempre que exista uma actualização de software da Estação Padrão, a TMN, compromete-se a elaborar essa mesma imagem actualizada, comunicando esse facto para que de imediato seja entregue ao Fornecedor.

A TMN fará um registo de todas as imagens entregues, bem com a data e respectiva versão (que deverá ser comunicado juntamente com o suporte magnético que transportará a imagem).

Por outro lado é necessário o comprometimento do Fornecedor, para os seguintes pontos:

- Todos os equipamentos deverão ser instalados com os dados da última imagem distribuída;
- Para uma maior facilidade de identificação do lote, na identificação do Hostname de cada equipamento, deverá vir indicada a versão da imagem instalada e o tipo da mesma;
- Sempre que a respectiva imagem for alterada terá de se registar as respectivas alterações;
- Sempre que for iniciada a comercialização de novos modelos de equipamentos, previamente deverá ser entregue um exemplar na TMN, para que possa proceder a testes e elaboração de nova imagem com base no novo tipo de Hardware;
- Deverá sempre ser instalada a imagem solicitada no pedido de aquisição. Caso essa informação esteja omissa, dever-se-á optar pela instalação da imagem A;
- Em situações excepcionais, poderá ser considerada a hipótese de instalação de uma imagem específica para um lote de equipamentos claramente identificados, por exemplo para Projectos que exijam software específico.

3 - Instalação e Actualização do PT

3.1 - Instalação do PT

Os novos PT somente devem ser adicionados ao domínio no seu local de instalação, junto do utilizador final.

Caso haja problemas na instalação do novo PT, a situação deverá ser comunicada. Se o problema não impedir a instalação do PT, esta deverá prosseguir na medida do possível e o destinatário do PT informado de que a instalação ficou incompleta e terá de ser concluída posteriormente (até 24h).

3.2 - Adicionar PT ao domínio

Para se poder adicionar um posto à rede, este tem estar devidamente patrimoniado.

- Para os Desktops

O nome do equipamento deverá conter sempre o prefixo “TMNP” e de seguida o respectivo nº de património.

Exemplo:

Etiqueta colocada no equipamento.	
Nome do equipamento no domínio TMN	TMNP01171426

- Para os Laptops

O nome do equipamento deverá conter sempre o prefixo “TMNL”, seguido do respectivo nº de património.

Os PT devem ser adicionados ao domínio TMN e inseridos na respectiva AD da Direcção/Departamento/Área a que pertencem.

Recordar: Todos os equipamentos devem conter a respectiva etiqueta identificativa do seu nº de património. Esta situação deverá ser verificada **antes** de o equipamento ser entregue ao utilizador final.

O número de Património será utilizado na constituição do Hostname do equipamento que se vai adicionar à AD. A nomenclatura será a seguinte:

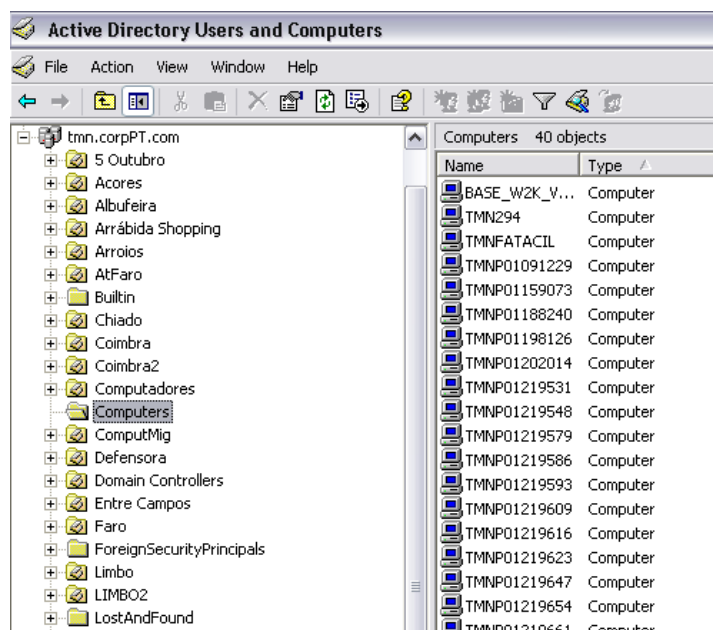
TMNP01157246;
TMNL01157246.

TMN – nome da empresa;
L/P – Colocar de acordo. L – Laptop / P – Desktop;
XXXXXXX – nº de património.

1º Passo – Adicionar o PT ao domínio:

Com esta informação é adicionado ao domínio **tmn.corppt.com**. No momento em que o equipamento é adicionado ao domínio, é obrigatório o envio de um email para o endereço do *ServiceDesk* com a seguinte informação: Nome do colaborador (empresa, caso seja externo) – Direcção/Departamento/Área. Esta informação será crucial para a posterior arrumação do Objecto no contentor correcto.

Quando o Equipamento é adicionado ao domínio, por defeito, vai para a “**Computers**”:



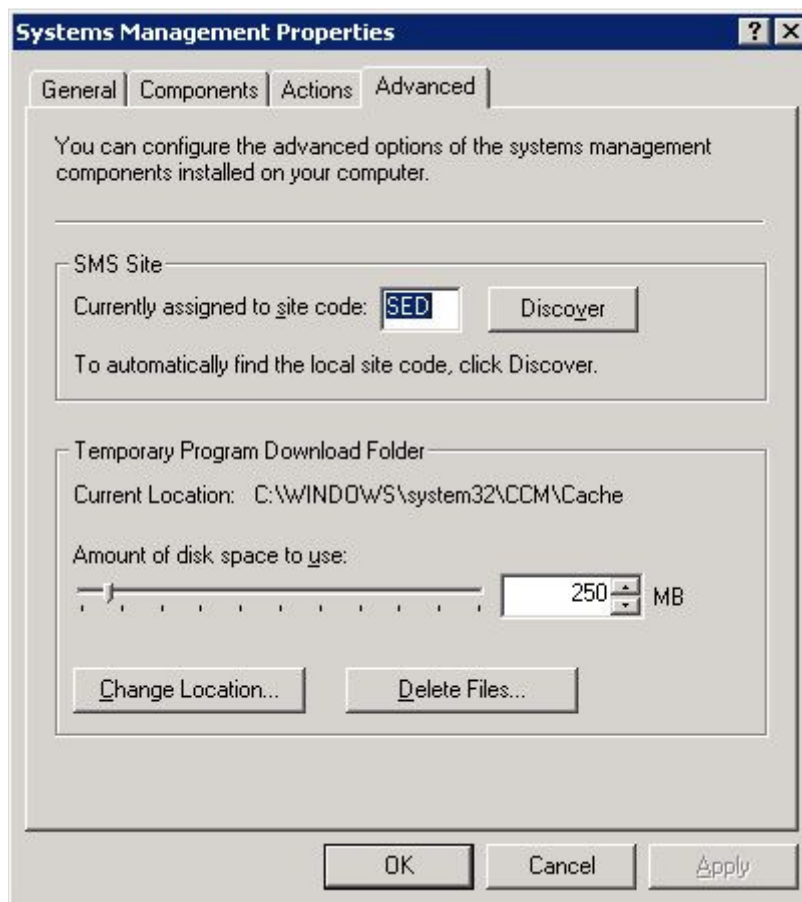
2ª Passo – Descoberta do PC no respectivo site:

A instalação de uma nova máquina (ou nova imagem) na rede, geralmente acarreta algumas acções prévias antes do seu uso final. Estas acções habitualmente incluem a ligação do PC à rede, o registo do DNS, a configuração da impressora, a página inicial inserida no Internet Explorer, etc. Pretende-se assim acrescentar mais um procedimento que é o de forçar a detecção do *site*, no qual a estação de trabalho está atribuída. Este procedimento advém da instalação prévia do agente SMS englobado na imagem padrão.

Procedimento a efectuar para atribuir o agente (cliente SMS) ao *site code* após o pc encontrar-se no local destino:

- Abrir o *Control Panel*;
- Escolher o ícone *Systems Management*;
- Escolher o item *Advanced*;
- Premir o botão *Discover*.

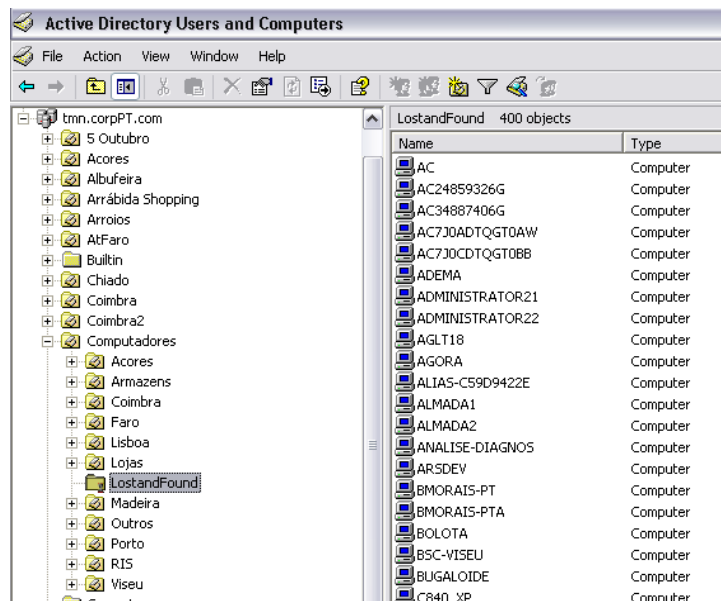
Deverá aparecer um dos possíveis *site codes*: SED; PRT; FAR; SMG; FNC.



Concluir: OK.

3º Passo - Colocação do Equipamento na OU Computadores:

Gestão de Contas move os postos existentes na “**OU Computers**”, de onde só ela tem acesso, para a “**OU Computadores\LostandFound**” (**Processo automático que corre diariamente**):



4º Passo:

Colocação do Equipamento na OU correcta

No dia D+1, a equipa **ServiceDesk 3ª linha** fica responsável por mover os postos para as OU correctas segundo a Direcção, Departamento e Área de quem está atribuído o Equipamento (para esta acção dever-se-á utilizar a informação constante no email).

A nomenclatura deve obedecer a um conjunto de pressupostos, conforme a seguinte tabela:

	Operadores	Responsáveis e colaboradores TMN	Colaboradores Outsourcing	BackOffice
Lojas	Loja X Balcão Y	Nome Utilizador	Nome utilizador (nome Empresa)	Loja X Backofficeyy (Nome do Operador se o posto estiver atribuído univocamente)
Atendimento	Função Local – Extensão telefónica			
Edifícios centrais		Nome Utilizador	Nome utilizador (nome Empresa)	
Armazéns	Armazem X	Nome Utilizador	Nome utilizador (nome	

			Empresa)	
--	--	--	----------	--

3.3 - Reorganização de Objectos perdidos

1 → Exporta-se o nome dos postos existentes na “**OU Lost And Found**” para um ficheiro TXT.

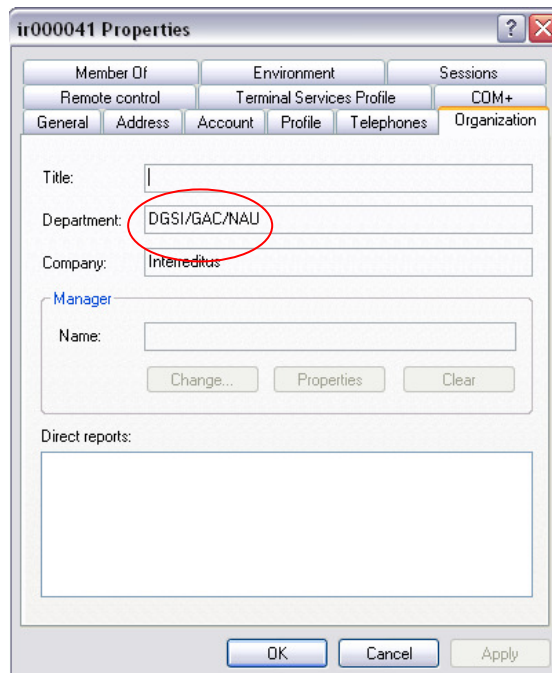
2 → Depois lança-se um “script” para verificar qual o utilizador que está a usar o posto:

O “output” é o seguinte:

NetBIOS Remote Machine Name Table

Name	Type	Status
TMN01183634	<00> UNIQUE	Registered
TMN	<00> GROUP	Registered
TMN01183634	<20> UNIQUE	Registered
TMN01183634	<03> UNIQUE	Registered
TMN01183634\$	<03> UNIQUE	Registered
TMN	<1E> GROUP	Registered
PS017271	<03> UNIQUE	Registered

3 → Em seguida identifica-se o utilizador que está “logado”, e verifica-se na **AD** a que área pertence, de acordo com a informação do campo Department - Direcção/Área/Departamento do utilizador:



The screenshot shows a Windows-style dialog box titled "ir000041 Properties". It has several tabs: "Member Of", "Environment", "Sessions", "Remote control", "Terminal Services Profile", "COM+", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "Organization" tab is currently selected. Inside this tab, there are several text input fields: "Title:", "Department:", "Company:", "Manager" (with a sub-label "Name:"), and "Direct reports:". The "Department:" field contains the text "DGSJ/GAC/NAU" and is circled in red. The "Company:" field contains the text "Intermedius". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

Neste exemplo a máquina é movida para a “OU Computadores / Lisboa”.

3.4 - Actualização do PT

De forma a assegurar o correcto funcionamento do PT, bem como na rede onde se encontra inserido, é necessário efectuar as actualizações que se encontram disponíveis no site da Microsoft.

Para actualizações Windows, utilizar o site: <http://v5.windowsupdate.microsoft.com>. As actualizações a serem efectuadas serão somente as actualizações críticas que se encontram disponíveis no site. As restantes actualizações serão distribuídas gradualmente pelo sistema SMS da TMN.

3.5 - Registo do PT

O registo da actividade e movimentação dos PT tem de ser assegurado de forma a dispormos de um “mapa” dos PT TMN. Esse registo deve ser feito sempre que um novo PT for instalado/movimentado.

4.1 - Regras de uso da ferramenta de acesso remoto aos Equipamentos desktop e laptop da TMN

A intervenção remota deverá ser sempre precedida de uma comunicação verbal da acção que irá acontecer (Ex. "Pretendemos intervir remotamente no seu PC para resolver o problema do Outlook");

Deverá ser dado a conhecer ao utilizador o URL na Intranet, onde poderá consultar as regras de uso da ferramenta, e caso o utilizador não concorde, não deverá acontecer a intervenção remota;

A aplicação deverá ser sempre instalada, com base na mesma versão e nas definições de um ficheiro INI comum, que possua as seguintes características:

- Envio de email para endereço a designar pelo cliente TMN, com indicação do endereço da máquina de onde foi estabelecida a ligação, que user de NT a estabeleceu, e qual a máquina onde foi feito o acesso remoto;
- Apresentação inicial de caixa de diálogo na máquina remota com pedido de permissão de acesso;
- O utilizador final terá a possibilidade de terminar a conexão sempre que o pretenda fazer;
- O utilizador final, tem sempre disponível os periféricos de Input e Output do seu equipamento informático (i.e.: acesso ao rato e ao teclado, visualização do que se está a passar no monitor
- O técnico assume sempre um compromisso de confidencialidade sobre toda e qualquer informação que leia no PC do utilizador final;

O ficheiro INI, em anexo deverá ser copiado para C:\Program Files\DameWare Development\DameWare NT Utilities, substituindo o ficheiro existente neste directório, este ficheiro INI já possui todas as parametrizações acima mencionadas.

4.2 - FAQ – Acesso Remoto

Que tipo de intervenção é realizada através do acesso remoto? Todas as intervenções que sejam do âmbito da actividade do helpdesk, nomeadamente, resolução de problemas aplicativos, sistema operativo, ferramentas Microsoft, instalações, e configurações.

O acesso remoto ao meu PC irá pôr em causa a estabilidade do meu PC? A estabilidade do PC está assegurada visto não ser instalada qualquer aplicação. Trata-se apenas da activação temporária de um serviço.

Após a 1ª vez que acederem à minha máquina, poderão voltar a fazê-lo sem a minha autorização? Não. O acesso apenas acontece mediante a aceitação da instalação do serviço no PC.

Posso introduzir inputs no meu PC durante a intervenção? Sim. Inclusive em alguns casos é fundamental a participação do utilizador final.

Quando introduzo passwords, o técnico consegue ver o que estou a escrever? Não. O técnico vê apenas aquilo que o utilizador também vê. Como já se deve ter apercebido, as passwords são sempre omitidas durante a sua inserção por asteriscos. O técnico vê apenas os asteriscos.

Qual o significado da janela de notificação que surge no meu canto inferior direito? Significa que a ligação ao seu PC, foi estabelecida com sucesso e que os técnicos do serviço de suporte já estão a intervir directamente no seu PC.

Como sei que a conexão terminou? O ícone do serviço de Dameware irá desaparecer.

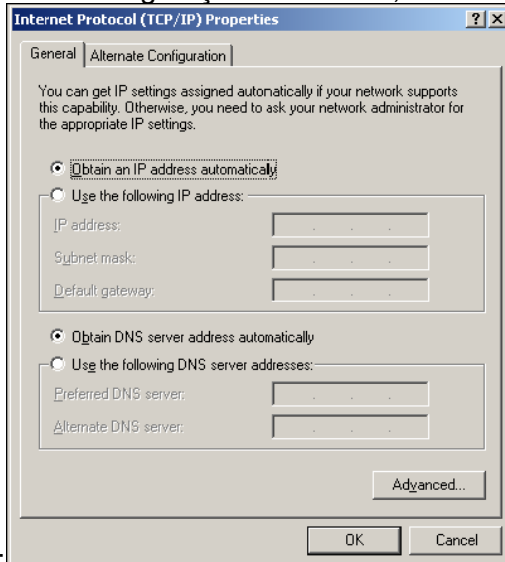
Como posso aceitar/rejeitar a ligação? Após o técnico informar da acção e caso consiga comunicação com o seu PC, irá surgir-lhe uma caixa de diálogo em que pode aceitar a ligação ou rejeitá-la.

Porque razão não consegue aceder remotamente ao meu PC? Geralmente trata-se de casos de anomalias na comunicação entre a LAN/WAN.

5 - Configurações

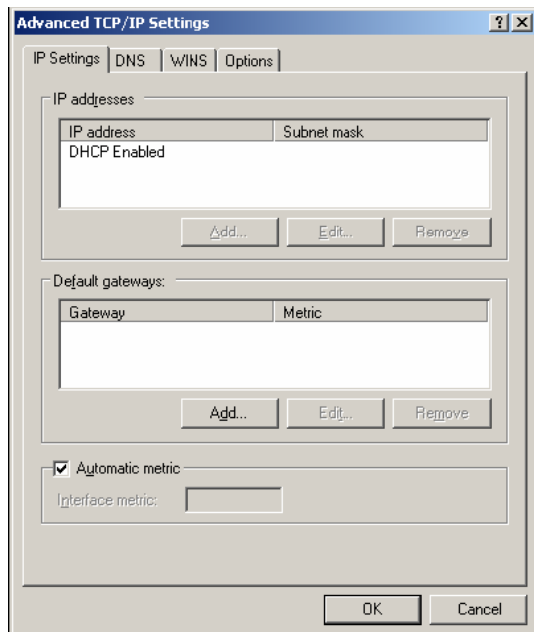
5.1 - Rede – Estação Padrão

Relativamente às configurações de rede, iremos ilustrar de seguida a correcta

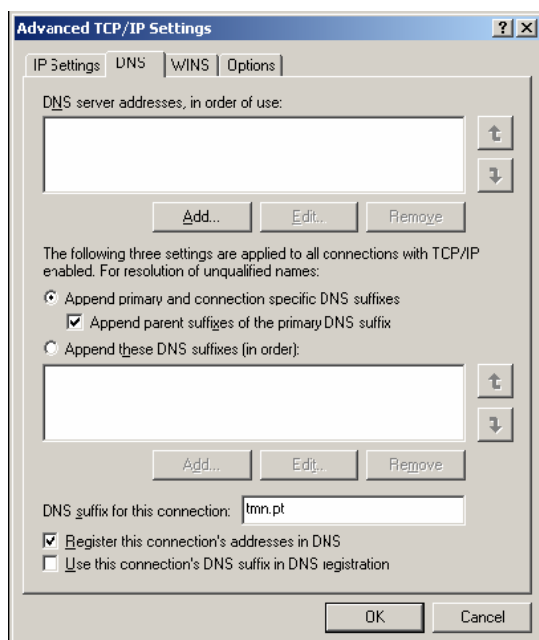


configuração:

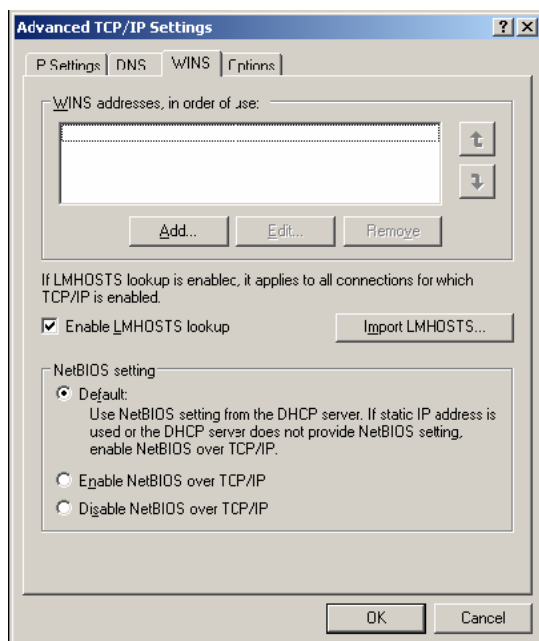
Obtain an IP address automatically, Obtain DNS server address automatically - estes dados são atribuídos pelo DHCP.



Default gateway, é atribuído por DHCP



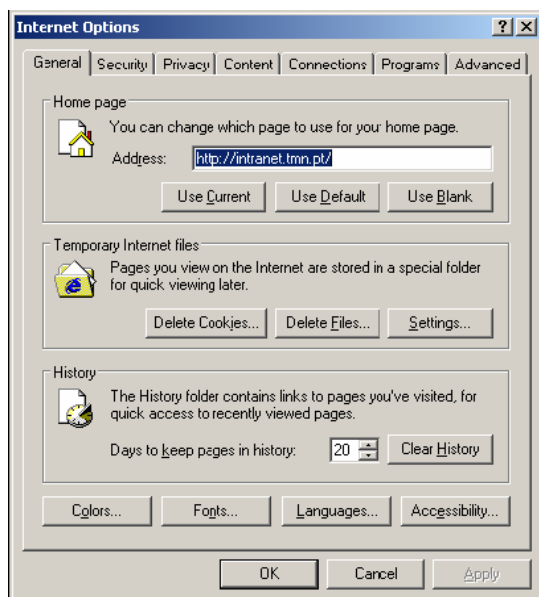
DNS Suffix for this connection, terá de conter tmn.pt



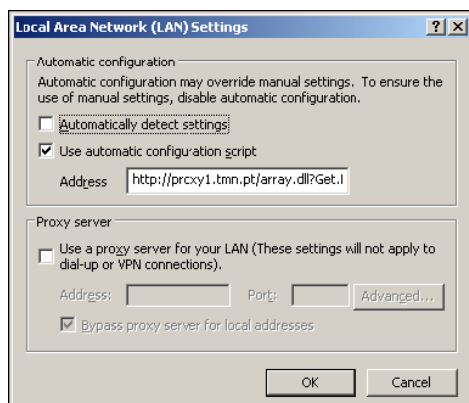
No que diz respeito ao *WINS*, será também atribuído pelo DHCP, é utilizada a opção *Enable LMHOSTS lookup*; *NetBIOS setting* será usado o *Default*.

5.2 - Internet Explorer – Estação Padrão

A TMN dispões de inúmeras aplicações baseadas em WEB, como tal é exigida a correctaparametrização do Internet Explorer. Relativamente às configurações do Internet Explorer, iremos ilustrar de seguida a respectiva configuração:



Address, este endereço é parametrizado automaticamente através de uma política de domínio.



Na tabulação *Connection – Lan Settings* temos esta configuração que também parametrizada automaticamente através de uma política de domínio

6 - Ligação de Equipamentos externos à rede da TMN

A Ligação de equipamentos à rede da TMN constitui, ou poderá constituir, uma ameaça em termos de segurança para o funcionamento da referida rede, podendo originar problemas locais ou globais ao funcionamento de toda a empresa. A origem destes problemas está relacionada com o nível de actualização do Sistema Operativo do equipamento e a inexistência ou deficiente actualização do sistema de antivírus bem como a inexistência de informação sobre o equipamento em si

6.1 - Pré-Requisitos

UPDATES CRITICOS SISTEMA OPERATIVO

Qualquer actualização que seja fundamental ao funcionamento do computador é considerada uma "Actualização crítica". Estas actualizações são fornecidas para ajudar a resolver problemas conhecidos e a proteger o computador de vulnerabilidades de segurança conhecidas como tal deverão estar todas instaladas no respectivo equipamento. Os Updates críticos do sistema Operativo terão que estar actualizados à data do pedido da ligação do equipamento. Sendo no prioritário a actualização de service packs. Esta actualização poderá ser efectuada em <http://windowsupdate.microsoft.com>.

INSTALAÇÃO DE ANTIVÍRUS

Os equipamentos deverão ter um sistema de antivírus instalado e actualizado à data do pedido de ligação do equipamento devidamente configurado. ATMN recomenda a utilização do VirusScan da McAfee/NAI.

6.2 - Como Efectuar o pedido

O pedido de ligação terá que ser efectuado por elemento da TMN que ficará responsável pelos colaboradores externos. Esse pedido deverá ser efectuado via eHelpdesk pelo referido responsável, com informação do nome e local de trabalho do(s) colaborador(es) a fim de ser combinada a verificação do equipamento nas instalações do Helpdesk.

Está disponível um formulário que deve ser enviado, será registada a seguinte informação acerca do pedido:

- Nome do responsável TMN
- Nome do colaborador externo
- Local de trabalho
- Contacto
- Informação relevante que caracterize o equipamento

- “hostname” do equipamento

6.3 - Verificação dos equipamentos

A verificação dos equipamentos pelo Helpdesk é constituída pelas seguintes acções:

- Verificação das actualizações do sistema Operativo Base
Será verificado se as actualizações do Sistema Operativo estão efectuadas até a data do pedido.
- Verificação da existência de antivírus e da respectiva actualização
Será verificado a existência de sistema de antivírus e se a actualização desse sistema está efectuada à data do pedido ou outra que seja julgada conveniente.
- Verificação do Software existente no Equipamento
Será efectuada verificação sumária ao Software existente no equipamento.
(Será que não era possível arranjar um utilitário que retirasse alguma informação, por exemplo do software instalado, de forma a tornar mais rápida esta validação?)

Verificação dos equipamentos

O âmbito de actuação do Helpdesk restringe-se às verificações dos equipamentos acima referido, sendo que todas as acções correctivas identificadas serão efectuadas pelos colaboradores externos. No caso de o equipamento não corresponder às premissas anteriormente indicadas será informado de que não deve ser ligado à rede da TMN directamente e reforçado com email para o responsável pelo pedido.

6.4 - Decisão para ligação dos equipamentos

A decisão de ligação do equipamento será tomada imediatamente após a verificação, e será concretizada em formulário a enviar ao elemento da TMN responsável pelos colaboradores externos. Caso alguma das verificações não correspondam aos requisitos indicados não será permitida a ligação dos equipamentos.

Caso os equipamentos cumpram os requisitos indicados, serão efectuadas pelo Helpdesk as seguintes acções adicionais.

6.5 - Configuração do PC

A configuração de rede do Pc será configurada segundo a norma da TMN, referida no ponto [5](#).

6.6 - Criação de utilizador Helpdesk com permissões de administrador local

Será criada uma conta local ao equipamento que permitirá, em condições idênticas aos restantes utilizadores na TMN. Esta conta não poderá ser alterada enquanto esse equipamento se encontrar ligado à rede da TMN.

6.7- Compromisso de actualização

O Colaborador externo e o seu responsável na TMN comprometem-se a manter o nível de actualizações do Sistema Operativo e do Antivírus actualizada com carácter diário.

7 - Equipamentos Spare

A saída de equipamentos requer a aprovação do responsável por alguém delegado para o efeito. Em caso algum, estes equipamentos deverão ser utilizados como Spares, a menos que haja indicação clara fornecida pelo mesmo responsável de área, para esse efeito.

8 - Análise da Qualidade de Serviço – Outbound Survey

Em virtude de ser necessário medir os níveis de Qualidade do serviço HelpDesk, são disponibilizados dois tipos de Survey que poderão ser efectuados:

- Survey global a todos os utilizadores TMN
- Outbound Survey

8.1 - Survey Global

Este Survey será enviado a todos os utilizadores TMN, e tem como objectivo avaliar a qualidade global do serviço de HelpDesk. Este Survey terá uma data de início e de fim e será efectuado através de uma página Web, desenvolvida com a garantia que cada utilizador só responderá ao Survey uma única vez. A elaboração do Survey é efectuada por uma equipa mista TMN/Helpdesk, bem como a avaliação dos resultados.

8.2 - Outbound Survey

Este tipo de Survey é efectuado diariamente, a 20% dos pedidos abertos. Neste caso a análise de qualidade é efectuada por pedido e será efectuada poucas horas após da sua resolução, para que o utilizador tenha ainda presente o que se passou na resolução do incidente reportado. Nesta situação, o ServiceDesk compromete-se a enviar relatórios periódicos (a definir) com os resultados do Survey. Será composto por quatro questões:

- 1) Quando ligou para o Helpdesk, acha que foi atendido (a) de uma forma correcta? (S/N)
- 2) Qual o motivo de satisfação/insatisfação?
- 3) Na sua opinião a resolução do problema foi eficaz? (S/N)
- 4) Qual o motivo de satisfação/insatisfação?

No caso de o incidente ter sido resolvido, então o pedido deverá passar ao estado fechado.

Assim, com base nas observações e expectativas acerca do tema, será feito o seguinte:

- Diariamente um agente do Servicedesk irá ligar para os utilizadores que solicitaram serviços ao Servicedesk, numa proporção de 25% correspondentes a 25% dos pedidos fechados no dia útil anterior; O agente não se identificará como sendo do Helpdesk;

- Serão realizadas as 4 questões referidas para aferir da qualidade do serviço prestado; Qualquer pedido será alvo de análise à excepção dos que tiverem sido realizados pelo operador que está a realizar o "Outbound Survey";
- Os resultados serão enviados semanalmente através do relatório semanal, e de um report mensal;

9 - Staging

É da inteira responsabilidade do serviceDesk, manter este espaço em perfeitas condições de trabalho e segurança.

9.1 - Espaço

Para um bom ambiente de trabalho, devem ser reunidas algumas condições:

- A bancada técnica deve ser mantida arrumada.
- Spares, cabos e restante material informático devem estar correctamente acondicionados nos respectivos armários
- Devem ser mantidos todos os registos actualizados para os activos informáticos utilizados
- Material logístico, carrinhos de transporte, devem também ser acondicionados de forma a não perturbar o bom funcionamento desta área

9.2 - Equipamentos

Todos os equipamentos existentes na área de staging, devem estar correctamente identificados. Os pc's que se encontram em bancada técnica para intervenção, devem estar identificados com o respectivo pedido que lhe está atribuído.

10 - Impressoras

10.1 - Pedido de Criação de Impressoras na Rede

O procedimento para criação/instalação de impressoras será efectuado da seguinte forma: O Utilizador abre um pedido para o Helpdesk com a seguinte Tipificação:

Tipo 1: Posto de Trabalho (PC's)
Tipo 2: Instalação
Tipo 3: Impressora de rede
Titulo: instalação nova impressora

Indicando, o modelo, nº de série, MacAddress (HW Address), localização Piso/Ala/Loja/Armazém da impressora. Com esta informação, o Helpdesk atribui um IP, nome da impressora e respectivo “queue” de impressão.

Tipo 1: Posto de Trabalho (PC's)
Tipo 2: Impressão
Tipo 3: Criação Spooler
Titulo: criação de “queue” de impressão

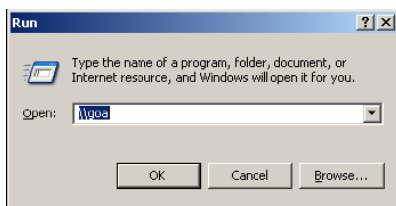
O Helpdesk imprime uma etiqueta de identificação da impressora e envia um técnico para a configuração da impressora no local.

As impressoras devem ser sempre parametrizadas/instaladas pela respectiva queue de impressão, não se deverão ser instaladas impressoras através do IP. O Servicedesk, depois de efectuar a configuração de uma impressora, disponibiliza no local cópias do documento de configuração da impressora no posto de trabalho do utilizador.

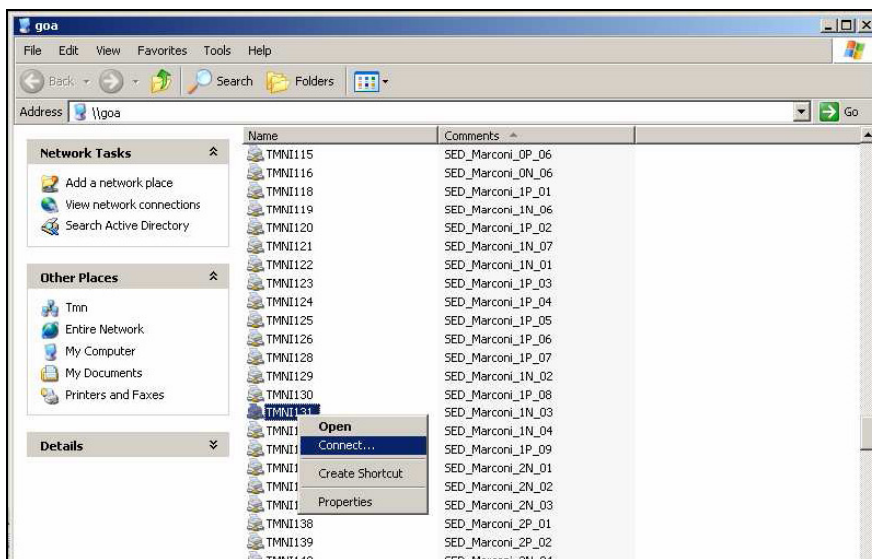
Toda a informação necessária ao utilizador é fornecida nas instruções que são distribuídas, bem como na etiqueta que é colocada na impressora.

Uma forma simples e eficaz de se efectuar a instalação da impressora são:

Aceder ao *Print Server* (indicado na etiqueta)



Identificar a queue de impressão criada (nome do tipo TMNXXX, também na etiqueta), e seleccionar *Connect*.



Caso o PC não disponha dos drivers, ou seja, não tenha os drivers instalados para o respectivo modelo, o técnico terá que os instalar.

11 - Grupo Utilizadores

Existe um grupo de utilizadores designado de ServiceDesk, no qual os elementos previamente identificados pelo responsável do serviço, farão parte.

Este grupo de utilizadores, é um grupo de domínio, e está como administrador local de todos os novos equipamentos; tem algumas permissões, nomeadamente:

- Add To Domain
- Reset Password
- Local Computer Administrator
- Domain User

Este grupo designa-se de ServiceDesk.

12 - Password de Rede

12.1 - Reset Password

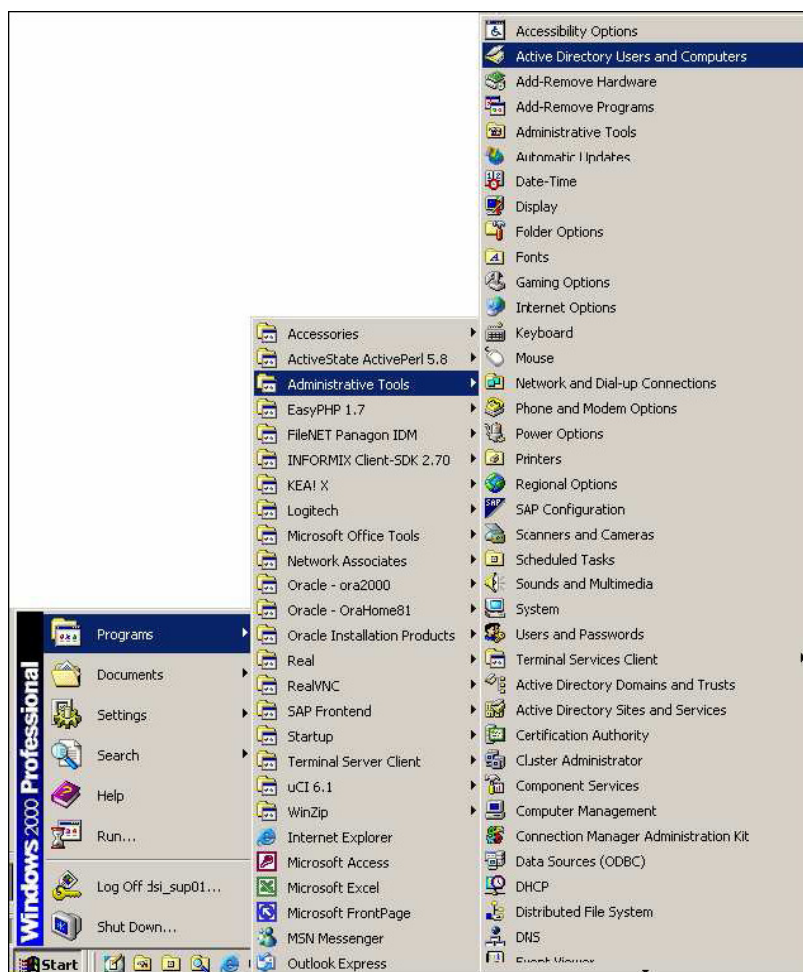
Este tipo de operação acarreta algumas responsabilidades, como tal é necessário um mecanismo de controlo, para efectuar um *reset* a password.

De forma a certificarmo-nos que é o respectivo utilizador que solicitou o reset, é necessário efectuar uma chamada de Outbound a confirmar a solicitação de *reset* à password

Para reinicializar a password de rede associado ao login de rede, os seguintes passos deverão ser efectuados:

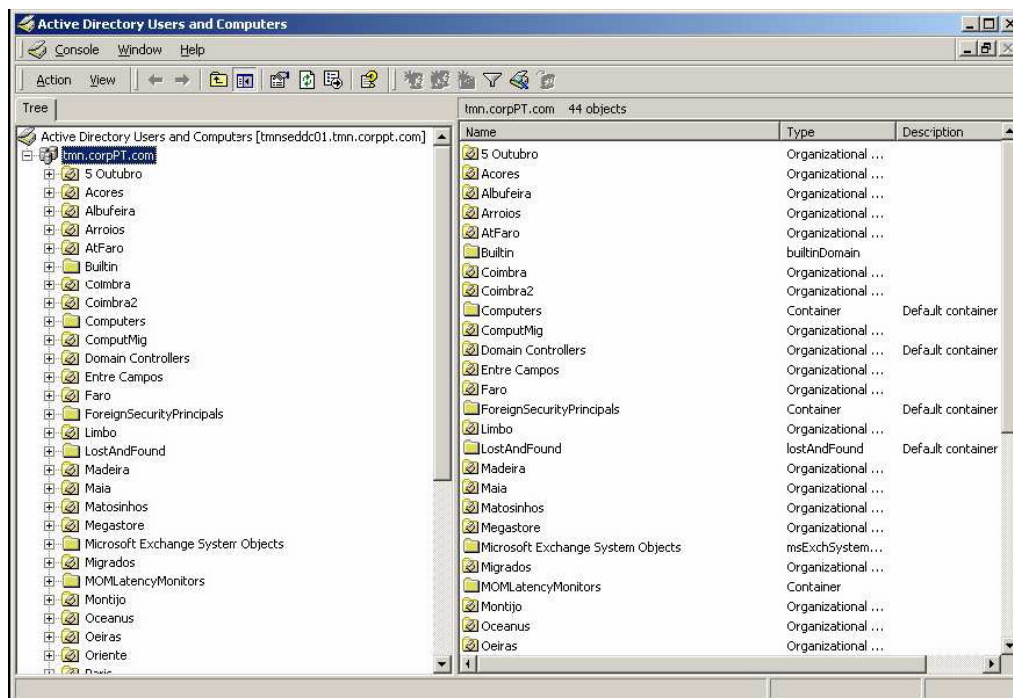
1º Passo

Através do *Start*, seleccionar *Programas*, *Administrative Tools*, *Active Directory Users and Computers*.



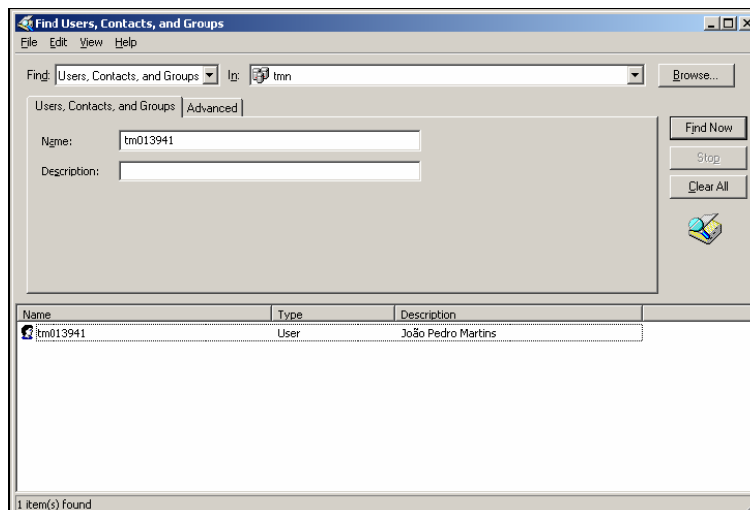
2º Passo

Depois de seleccionar o *icon* indicado, aparece a ferramenta em questão.



Com a estrutura apresentada, seleccionar com a tecla direita do rato por cima do objecto *tmn.corpPT.com*, a opção *Find*.

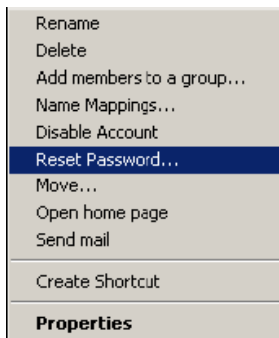
De seguida aparece a janela indicada.



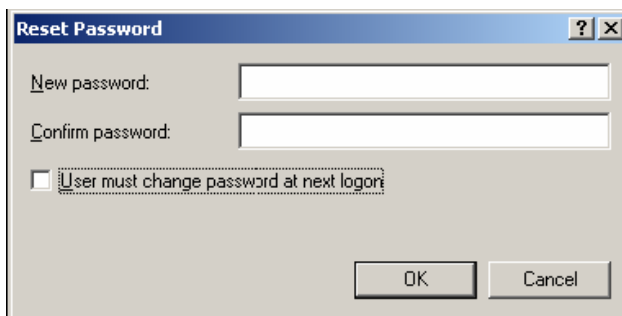
No campo *Name* introduz-se o *login* em causa e prime-se o botão *Find Now*.

3º Passo

Sob o item encontrado (apenas deverá aparecer um), seleccionar com a tecla direita do rato a opção
Reset Password...



Por último, introduz-se a *password* duas vezes e carrega-se no botão *OK*.



13 - Boas Práticas

A TMN é uma organização com milhares de utilizadores de sistemas colaborativos.

Se não existirem determinados cuidados por parte de todos os utilizadores podemos incorrer em falhas de segurança (e.g. incorrecta utilização da Internet, email).

Por outro lado podem também estar a ser dispendidos recursos de forma indevida ou incorrecta, causando indisponibilidade nos sistemas e muitas vezes diminuição abrupta da largura de banda (isto, entre outras situações).

A produção deste documento tem o propósito de ilustrar a boa utilização desses sistemas.

As *boas práticas* apresentadas neste documento têm somente esse objectivo, não obrigando de forma vinculativa a sua execução.

É aconselhada a leitura deste documento a todos os colaboradores TMN, independentemente da Direcção a que reportam.

Computadores

13.1 - Passwords

Sendo a *password* o comprovativo, aos olhos do sistema, de que se é quem se diz ser, torna-se importante evitar que terceiros se apoderem dela, o que lhes concederia acesso aos dados do utilizador e por conseguinte, uma porta de acesso à concretização de acções mais gravosas contra os sistemas. A escolha da *password* deve por isso ser cuidada, respeitando as seguintes regras:

- Conter pelo menos 6 caracteres;
- Não formar uma palavra ou referência facilmente associável ao utilizador (por exemplo, nome próprio ou *login*);
- Conter uma mistura de letras (preferencialmente maiúsculas e minúsculas), algarismos e caracteres especiais (e.g. "%"; "#"; "\$");
- A *password* deve também ser alterada periodicamente e, como já referimos, não ser concedida a um qualquer outro utilizador. Note-se que isto não representa desconfiança para com outra pessoa mas sim o assumir de uma atitude responsável que reflecte a posição a tomar ao longo de toda a vida como profissionais de uma área tão sensível a fugas de informação.
- Pelas mesmas razões, todos os utilizadores deverão assegurar-se que não abandonam as máquinas (por qualquer período de tempo) sem proceder ao fecho do computador. (*Lock Computer*).

- Altere regularmente os códigos pessoais (*passwords*) dos sistemas a que acede.
- Os códigos são pessoais e intransmissíveis, por conseguinte não os deverá dar a conhecer a ninguém.

13.1.2 - Bloquear o Computador

Sempre que o utilizador *owner* do computador, se ausentar do seu local de trabalho, deverá efectuar um *lock computer* (*ctrlaltdel*).

Se não efectuar este procedimento pode alguém entrar nos sistemas e efectuar operações para as quais poderá não ter acesso. Se isso acontecer o que ficará registado nos sistemas que foram acedidos é que o executor de tais operações foi o utilizador (e consequente *login*) do computador em causa.

Para garantir que ninguém acede a sistemas sem a devida autorização e/ou sem a devida credenciação, os utilizadores deverão efectuar o *lock computer*, garantindo desta forma que quem opera nos sistemas é o utilizador do *login* e não um outro utilizador com o *login* do utilizador que não efectuou o *lock computer*.

13.1.3 -Desligar o Computador

De forma a economizar energia e a vida útil dos monitores, no final do expediente os utilizadores dos computadores deverão desligar os monitores e efectuar um *shut down* ao computador.

Aquando da reinicialização dos computadores, correm políticas que fazem *updates* ao software base.

Por vezes esses *updates* necessitam de uma reinicialização ao sistema.

Ao desligar os computadores garantimos que aquando da sua reinicialização esses *updates* ficam operacionais.

13.1.4 - Instalação de software

Não deverá ser instalado software que não seja estritamente necessário ao bom desempenho da função do utilizador.

Nunca instale por sua iniciativa qualquer software cuja licença não tenha sido previamente adquirida pela TMN, devendo sempre contactar o DGSJ/GAC/NAU para solicitar essa instalação.

É fundamental, por questões de segurança, que o software base do seu computador esteja sempre actualizado. Na TMN as actualizações de software são automaticamente efectuadas (diariamente às 13H15m).

Ter atenção à instalação de *software adware*. Existe muito *software*, que apesar de ser *freeware* tem procedimentos que sobrecarregam a rede, como por exemplo, efectuar muitos pedidos de informação ao *proxy*.

Todo o *software* deverá ser instalado no disco C:

13.1.5 - Download de Software

Não deverão ser efectuados *downloads* de *software*, a não ser que seja *software* necessário ao bom desempenho das funções do utilizador do sistema.

Aquando da necessidade de *download* de *software*, esse *download* deverá ser efectuado em horário fora do expediente (e.g. hora de almoço). Garantindo dessa forma que a rede não está a ser sobrecarregada, dificultando a rapidez de execução de tarefas por parte de todos os utilizadores.

13.1.6 - Actualização Automática do Software Base

Na TMN as actualizações de *software* são automaticamente efectuadas (diariamente às 13H15m).

Instale as actualizações de *software*. Existem actualizações de *software* que necessitam de uma reinicialização do computador. Essa reinicialização deverá ser efectuada o mais rápido possível.

13.1.7 - Armazenamento de Informação

O armazenamento de informação deverá ser efectuado no disco D: Pode acontecer que o disco C: tenha que ser formatado, e consequentemente, perdida toda a informação aí contida.

13.2 - Correio electrónico

13.2.1 - Divulgação de Informação

Aquando da necessidade de divulgação de informação para toda a TMN, deverão ser utilizadas as *Public Folders* do servidor de email (*Exchange*).

O envio de emails para toda comunidade TMN, causa elevado tráfego na rede, tornando-a mais lenta.

13.2.2 - Divulgação dos endereços de Correio electrónico

Deve-se ter especial atenção à divulgação do endereço de email. Quando for

necessário indicar o endereço de email em formulários na Internet, deverá ser indicado um endereço de email externo à TMN (e.g. *hotmail*).

Muito do *Spam* é originado devido ao facto da apoderação indevida de endereços de email.

13.2.3 - Armazenamento de Informação

Devemos ser prudentes e não abrir *anexos* em que o *sender (from)* da mensagem nos é desconhecido.

Muitos dos vírus propagam-se dessa forma.

Tornam-se activos no momento de abertura do *anexo*.

13.2.4 - Senders de Mensagens Desconhecidas

Ter especial atenção com às mensagens em que o *sender (from)* é desconhecido, se for esse o caso apague imediatamente o email.

13.2.5 - Regras de utilização do Email

Tamanho das Mensagens

O tamanho das mensagens está limitado a 4096Mb. Todas as mensagens que ultrapassem este limite não serão enviadas nem recebidas, gerando um email com a respectiva informação, de não enviado.

Criação de PST's Locais

Deverão ser criados arquivos de email (*PST*) locais para o armazenamento das mensagens contidas na caixa de correio (*Inbox*). O espaço de armazenamento é limitado a 70Mb.

Se o utilizador pretender ter todos os emails guardados, deverá criar um arquivo de emails (*PST*) local, ou seja, no próprio computador.

Limpeza da Caixa de Correio

Quando se limpar a caixa de correio (*Inbox*), deverão também ser limpas a seguintes directorias:

- Mensagens enviadas (*Sent Items*);
- Mensagens apagadas (*Deleted Items*);
- Mensagens em composição (*Drafts*); Todas estas directorias utilizam espaço de armazenamento no servidor de email (*Exchange*) O volume total do espaço ocupado, é um composto do somatório do espaço utilizado pelas directorias supracitadas.

Envio de mensagens com informação Sensível

Devemos ter especial atenção ao envio de mensagens de email que contenham informação de negócio.

Este tipo de mensagens deve circular de forma encriptada (e.g. formato *zipfile*).

Utilização dos Endereços de Email com Propósitos de Caridade

As mensagens que apelem à caridade devem ser tratadas como *Spam*. Se as mensagens apelarem a donativos, o recipiente da mensagem deve reportar o mesmo a quem de direito dentro da organização. Nenhuma informação deverá ser enviada via email.

13.3 - Shares, Ficheiros e Informação

13.3.1 - Armazenamento dos Documentos Pessoais

Os documentos pessoais devem ser armazenados no disco *D:* do computador.

O disco *C:* pode ser formatado, e para não serem perdidos os documentos pessoais e alguns empresariais¹, os mesmos deverão ser guardados numa partição diferente da que contém software. Deverá portanto ser utilizada a partição *D:*

13.3.2 - Armazenamento dos Documentos da empresa

Os documentos da empresa deverão ser guardados na área de rede respectiva. Essas áreas são alvo de cópias de segurança (*backups*) garantindo assim que a informação não se perde.

13.3.3 - Documentos Finais

Os documentos na versão final produzidos para a TMN deverão ser catalogados e inseridos na Gestão Documental (*File Net*).

13.3.4 - Informação Sensível e/ou de Negócios

Informação sensível e ou de negócio não devem figurar em áreas públicas. Deverá ser guardada na respectiva área, garantindo que essa informação seja visualizada somente por quem de direito.

Dessa forma é garantido que só consulta essa informação quem tiver as permissões necessárias para aceder às respectivas áreas de rede.

13.4 - Impressão

13.4.1 - Impressão de Informação não necessária

Evitar a impressão de documentos não necessários. Desta forma conseguimos otimizar a utilização dos recursos disponíveis.

13.4.2 - Documentos nas Impressoras

Evitar esquecer documentos impressos nas impressoras. Esses documentos podem conter informação sensível que pode ser tornada pública e/ou visualizada por pessoas que não tenham os privilégios necessário e/ou devidos.

Evitando o esquecimento de documentos nas impressoras garantimos que a fuga de informação é muito menor.

13.4.3 - Destruição de Documentos

Sempre que um documento impresso deixar de ter utilidade deve ser destruído.

13.5 - Internet

13.5.1 - Informação Confidencial

Não se deve divulgar informação considerada confidencial ou sensível ao negócio via Internet.

13.5.2 - Endereço de Email Corporativo

Não deve ser divulgado o endereço de email corporativo, em formulários existentes na Internet.

O endereço de email corporativo deverá somente ser revelado em caso de necessidade de negócio ou para o bom desempenho das funções dos utilizadores. Em todos os outros casos deverá ser indicado um endereço de email externo previamente criado (e.g. *hotmail*).

13.5.3 - Utilização de ActiveX

Não devem ser utilizados *ActiveX*. Aquando da necessidade de utilização devemos cuidado com a sua utilização.

Os *ActiveX* podem conter vírus ou então activar vírus previamente “plantados” nos computadores.

Devemos garantir que quando utilizamos *ActiveX* na Internet, esses *ActiveX* são de *sites* seguros, credíveis e conhecidos.

13.5.4 - Utilização de Cookies

Não devem ser utilizados *cookies*.

Os *cookies* normalmente são utilizados para guardar informações da navegação efectuada pelos utilizadores.

Podem também guardar *passwords*. Assim sendo, quem aceder aos *cookies* pode ficar a conhecê-las.

13.5.5 - Sites Desconhecidos

Devemos ter atenção quando visitamos *sites* desconhecidos.

É necessária também atenção às mensagens que por vezes esses *sites* nos enviam. Ao aceitar “propostas” feitas por essas mensagens podemos estar a dar autorização à execução de processos maliciosos para o nosso computador e consequentemente para toda a comunidade de sistemas colaborativos TMN.

Devemos ler com atenção as mensagens e não “aceitar” tudo.

13.5.6 - Utilização de Auto Complete

O *Auto Complete* deve estar desactivo. Através do *Auto complete* pode alguém entrar no computador de um outro utilizador e aceder a sistemas que não tenha acesso.

14. Conclusão

O objectivo deste projecto era implementar um manual para facilitar a introdução de novos equipamentos na Base de dados de uma empresa, para demonstrar como se pode criar e desenvolver uma imagem para um posto de trabalho de forma simples, de gerir utilizadores e manter em bom funcionamento o parque informático.

Chegamos á conclusão que é necessário:

- Supervisionar, orientar e promover todas as necessidades das tecnologias de informação, dentro dos padrões adequados de qualidade, eficiência e segurança;
- Coordenar a manutenção de equipamentos de informática e de serviços em rede;
- Manter mecanismos de tratamento da informação em diferentes meios, para se assegurar a sua utilização;
- Coordenar as actividades relacionadas à administração física e lógica da rede de computadores garantindo a integridade e segurança dos dados e informações;
- Desenvolver, coordenar e aperfeiçoar sistemas inerentes aos programas e acções desenvolvidas pela empresa;

Um aspecto importante que ficou aqui relatado é o cuidado para uma ajuda constante entre o cliente e o helpdesk, com manuais do utilizador e ajudas informativas.

Neste projecto são dadas a conhecer algumas medidas de prevenção e organização ao nível do ServiceDesk e fica demonstrado o que eu pretendo, quero mostrar que se pode gerir um parque informático de uma forma simples, sem a desorganização que eu já assisti em algumas empresas em que trabalhei onde não existe normas e tudo é feito de uma forma leviana, sem uma preocupação com o futuro.

Neste projecto foi utilizado a empresa TMN como poderia ter sido outra, visto eu já lá ter trabalhado e esse facto ajudou me muito, por ser uma empresa que faz esforços para ser sempre a melhor.

Eu como helpdesk de 3º linha consegui aprofundar mais esta temática e ao mesmo tempo desenvolvi algumas medidas que foram apenas desenvolvidas para o trabalho final de curso e que podem ser usadas no mundo empresarial.

Na empresa onde trabalho actualmente INFORESTILO, que é uma empresa que gere parques informáticos de PME's, a pedido deles desenvolvi 90 % das medidas referidas neste projecto, com o devido enquadramento tanto na dimensão como na área de negócio.