



zone soft®

**INSTALAÇÃO
MULTIPOSTO
PORTAS DE COMUNICAÇÃO**



ÍNDICE

ÍNDICE DE IMAGENS.	2
1 – Implementar porta de comunicação MS SQL Server.	3
1.1 – Configurar porta em Microsoft SQL Server.	4
2 – Firewall do Windows.	8
2.1 – Configurar regra na Firewall do Windows.	8
2.1.1 – Tipo de regra em firewall	10
2.1.2 – Tipo de protocolo a utilizado na porta.	11
2.1.3 – Ação da Firewall perante a regra.	12
2.1.4 – Perfil da comunicação na porta 1433.	13
2.1.5 – Atribuir nome identificativo à regra.	14
3 – CONFIGURAÇÃO DOS POSTOS DE TRABALHO.	15
4 – CONFIGURAÇÃO DO Z MONITOR.	18

ÍNDICE DE IMAGENS.

Figura 1 – Aceder Microsoft SQL server manager.	4
Figura 2 – Aceder aos protocolos de TCP/IP	5
Figura 3 – Ativação de protocolo de TCP	5
Figura 4 – Configuração das portas TCP.....	6
Figura 5 – Reiniciar o serviço da instância SQL Zonesoft	7
Figura 6 – Selecionar a Firewall do Windows.....	8
Figura 7 – Selecionar a função Nova Regra.	9
Figura 8 – Aceder às definições avançadas da Firewall	9
Figura 9 – Selecionar a função Porta.....	10
Figura 10 – Atribuição de exceção a porta específica.	11
Figura 11 – Ação e permissão a atribuir á ligação.....	12
Figura 12 – Identificar os perfis a aplicar à regra.....	13
Figura 13 – Atribuir nome à regra.	14
Figura 14 – Inserir dados para acesso ao servidor de dados.....	15
Figura 15 – aceder á função de data link.	16
Figura 16 – Verificação dos dados de ligação.	16
Figura 17 – Teste de ligação á base de dados.....	17
Figura 18 – Aceder às definições do ZS Monitor.....	18
Figura 19 – Menu de configuração ao Servidor de SQL.....	19

1 – Implementar porta de comunicação com MS SQL Server.

Quando da instalação das aplicações ocais da Zone Soft, ZS REST ou ZS POS, é também instalado um conjunto de ferramentas gratuitas do Microsoft SQL Server 2014¹, que utilizam portas dinâmicas, para interligação da aplicação de forma bidirecional com os dados e informações guardados na Base de Dados local.

Para que todos os equipamentos ligados numa rede de comunicações, possam aceder ao PC/Servidor onde está instalada a base de dados, deve o utilizador implementar e configurar um conjunto de permissões e portas de comunicação.

As portas de comunicações associadas ao serviço ZONESOFTSQL e que tem como função principal a ligação dos equipamentos à Base de Dados no envio e recolha de informação.

A necessidade de criar regras na firewall do Microsoft Windows de forma a permitir que as comunicações se possam estabelecer na porta de ligação.

¹ Caso o cliente utilize uma versão diferente de Microsoft SQL Server, é da inteira responsabilidade do cliente a sua utilização, licenciamento e pagamento das referidas taxas de utilização.

1.1 – Configurar porta em Microsoft SQL Server.

Na implementação de portas de comunicações com a base de dados SQL, deve o utilizador selecionar o botão de Início do Windows e no menu dos programas selecionar a pasta de Microsoft SQL Server² 2014, e acionar o botão de função **SQL Server 2014 Configuration Manager**.

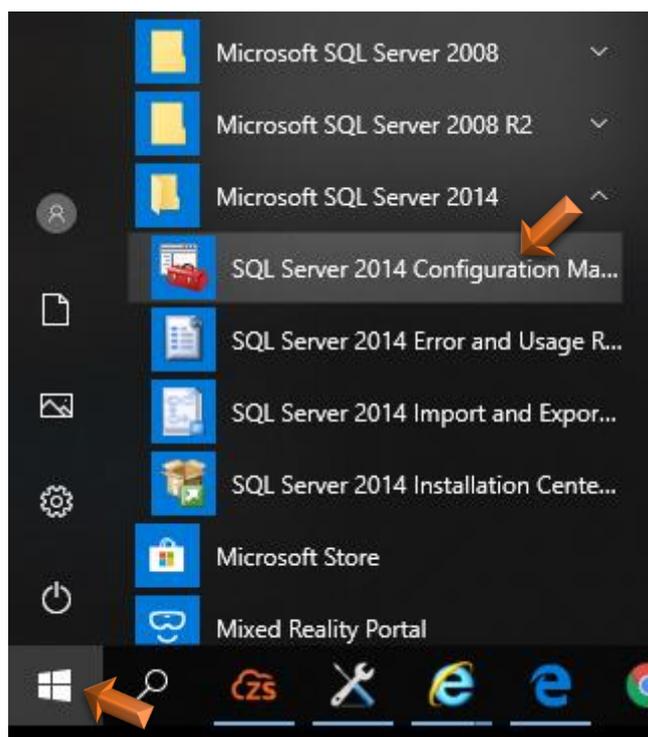


Figura 1 – Aceder Microsoft SQL server manager.

Notas:

- 1.^a – Toda a demonstração está a ser executada sobre a plataforma do sistema operativo Microsoft Windows versão 10, “Funções compatíveis com o MS Windows 7 e 8”.
- 2.^a – A localização das pastas e aplicações anteriormente descritas, poderão ser apresentadas noutra localização, dependendo da versão do Sistema Operativo.

² Designação proprietária da Microsoft Inc.

Na janela de SQL Server Configuration Manager, vamos inserir os protocolos de comunicações TCP/IP.

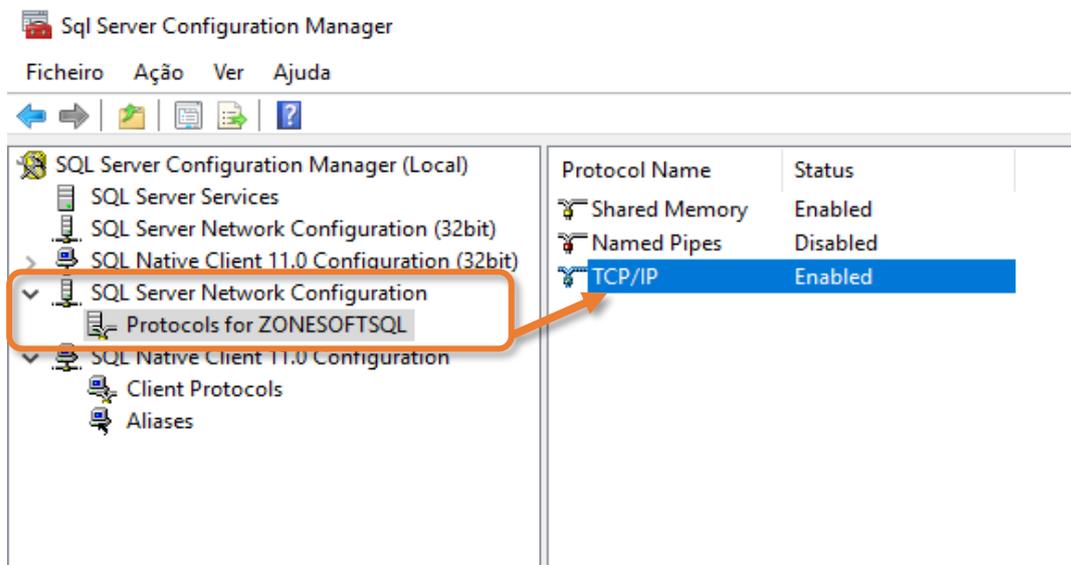


Figura 2 – Aceder aos protocolos de TCP/IP

No quadro de management (esquerdo), deve o utilizador selecionar a função de SQL Server Network Configuration apresentando todos os protocolos de comunicações presentes, acionar a função de protocolo da ZONESOFTSQL. No quadro dos protocolos deve o utilizador acionar o de TCP/IP.

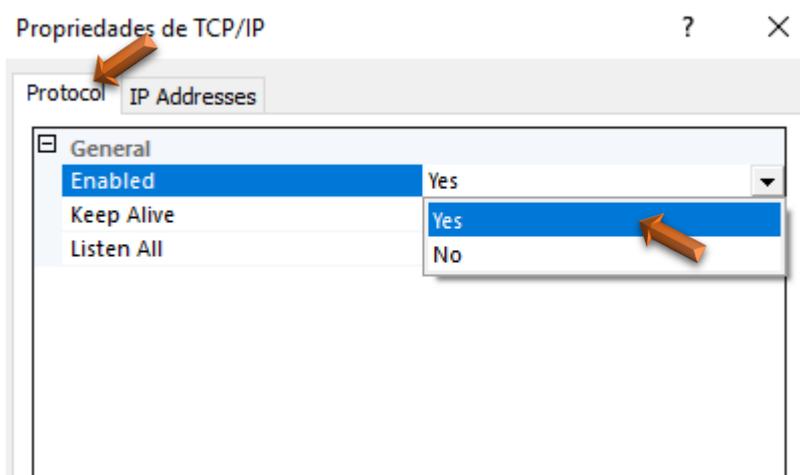


Figura 3 – Ativação de protocolo de TCP

Na janela das propriedades do protocolo de TCP/IP, deve o utilizador no separador de **Protocol** selecionar a função Enabled e selecionar a opção Yes (Sim).

Ainda nas propriedades de TCP/IP, deve o utilizador seleccionar separador IP Addresses. Deve o utilizador efetuar um Scroll Down até quadro IPALL.

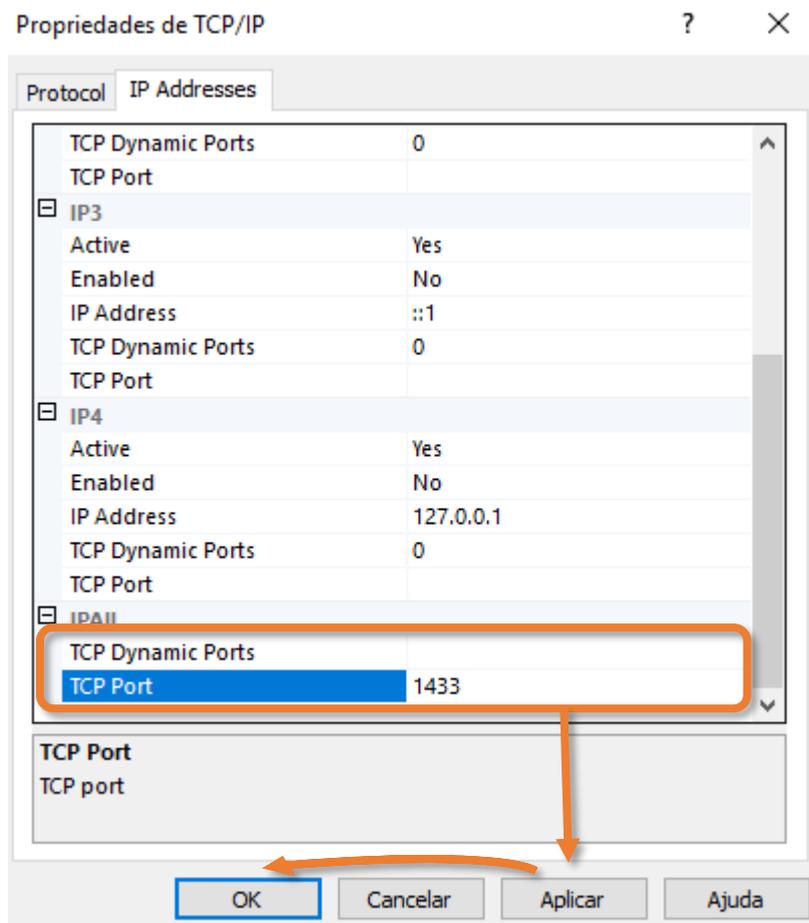


Figura 4 – Configuração das portas TCP

Neste quadro de **IPALL** deve o utilizador seleccionar o campo **TCP Port** para que seja possível adicionar uma porta de comunicações estática, para interligação da base de dados com os equipamentos ligados na rede de comunicações interna.

TCP Dynamic Ports – Deverá por defeito estar com o campo em vazio sem informação.

TCP Port – Deve o utilizador inserir neste campo a porta 1433. Nota: Poderá o utilizador usar outra porta, mas, dentro da range definida pelo sistema.

Depois de definida a porta deve o utilizador acionar o botão **APLICAR** e **OK** para que as alterações sejam salvaguardadas no sistema.

Nota: Sempre que forem efetuadas alterações a serviços ou instâncias do Microsoft SQL Server, estes **devem sempre ser reiniciados**, para que a alteração seja implementada.

Na janela principal do SQL Server Configuration Manager, pode o utilizador efetuar o restart dos serviços.

1º. - Selecionar no quadro esquerdo a função SQL Server Services; vai aparecer o quadro com o Nome dos serviços, deve o utilizador selecionar a instância SQL Server (ZONESOFTSQL).

2º. - Na barra de menus clicar no botão de Restart, vai aparecer uma nova janela com a informação de que o serviço está a efetuar Stopping e de seguida Starting.

Notas: O utilizador não deve fechar a janela durante o processo de restarting.

Verificar se na coluna State o serviço está em Running.

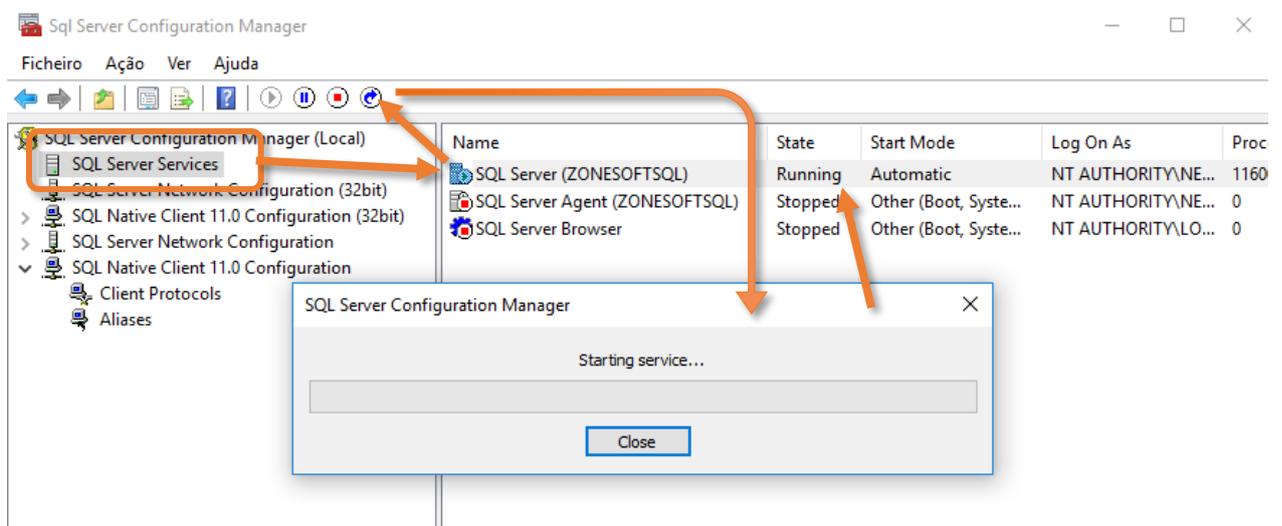


Figura 5 – Reiniciar o serviço da instância SQL Zonesoft.

2 – Firewall do Windows.

Sendo a Firewall um sistema de segurança, devemos criar regras bem definidas, para a porta de comunicação TCT/IP criada nos pontos anteriores.

2.1 – Configurar regra na Firewall do Windows.

No sistema operativo do MS Windows 10, deve o utilizador no campo de procura digitar Firewall do Windows, vai aparecer um conjunto de opções, deve o utilizador seleccionar o botão de Firewall do Windows Defender.

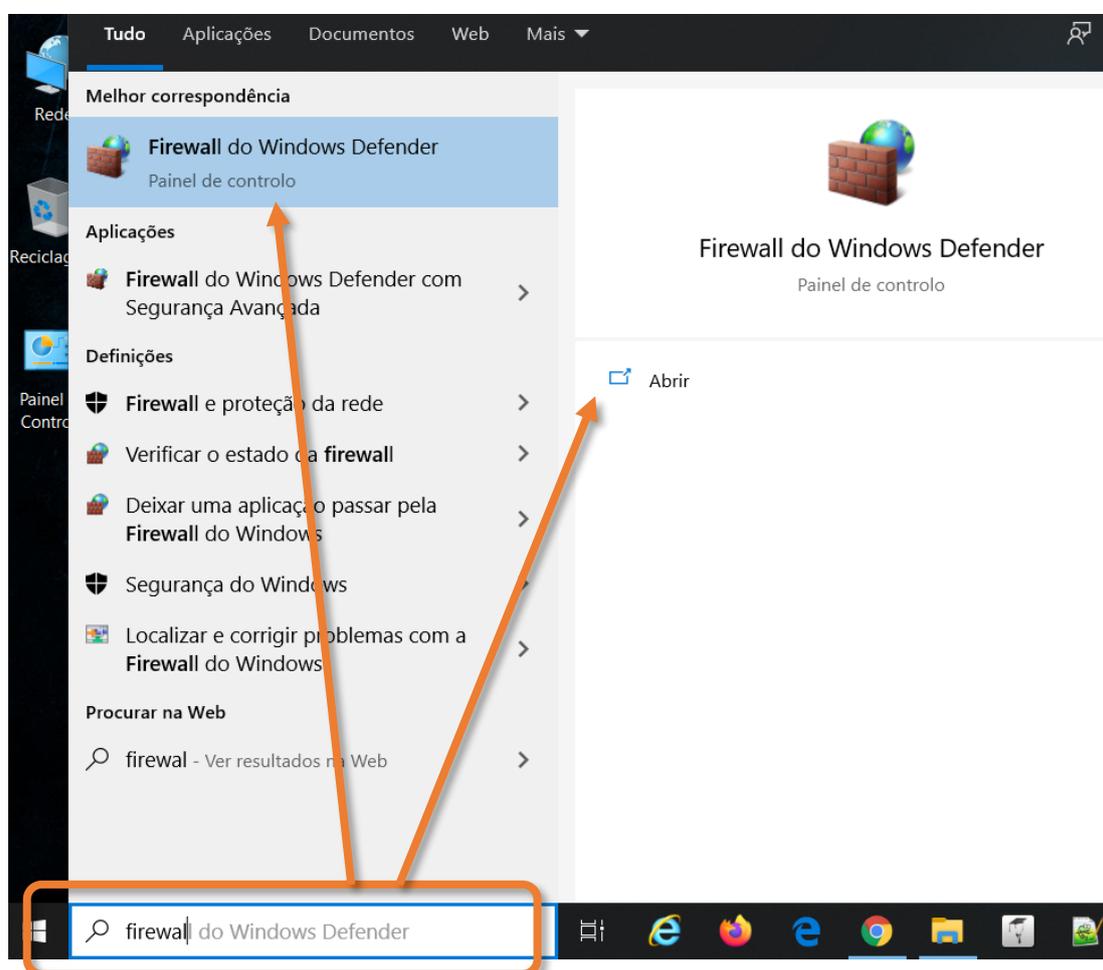


Figura 6 – Selecionar a Firewall do Windows

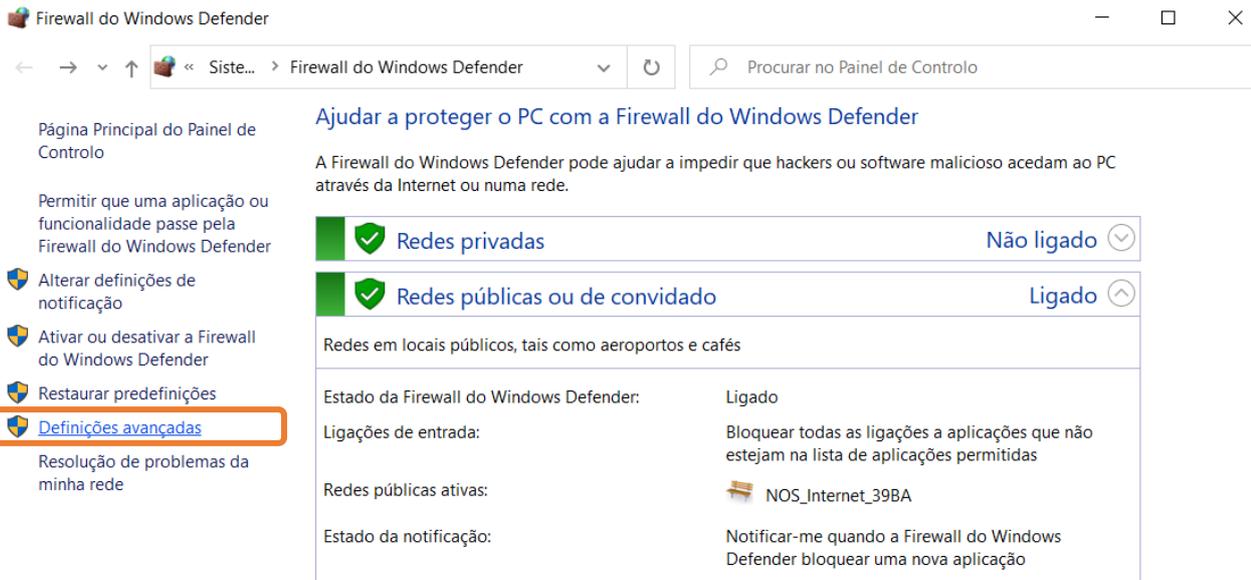


Figura 8 – Aceder às definições avançadas da Firewall

Deve o utilizador seleccionar as definições avançadas para aceder às regras de acesso ao sistema. Na janela do Firewall do Windows, seleccionar o botão de função Nova Regra.

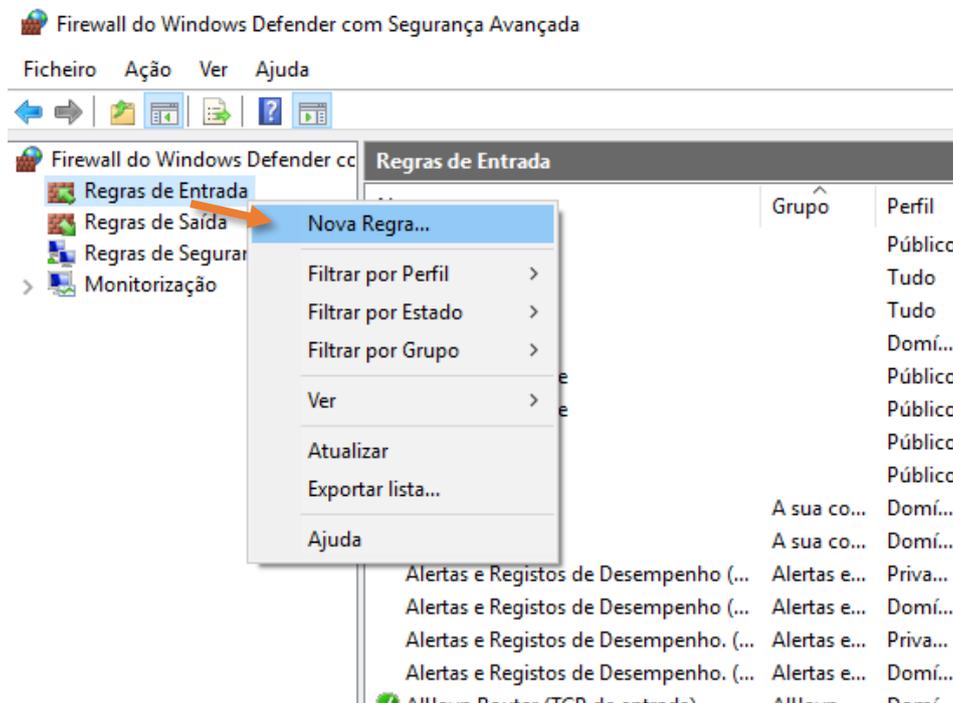


Figura 7 – Seleccionar a função Nova Regra.

Posicionar o ponteiro do rato sobre o botão Regras de entrada e clicar com o botão direito, inicia um quadro de selecção, deve o utilizador acionar o botão de “Nova Regra”.

2.1.1 – Tipo de regra em firewall

Após ter selecionado a função de nova regra, inicia a janela que apresenta um conjunto de passos necessários à implementação de uma regra de exceção.

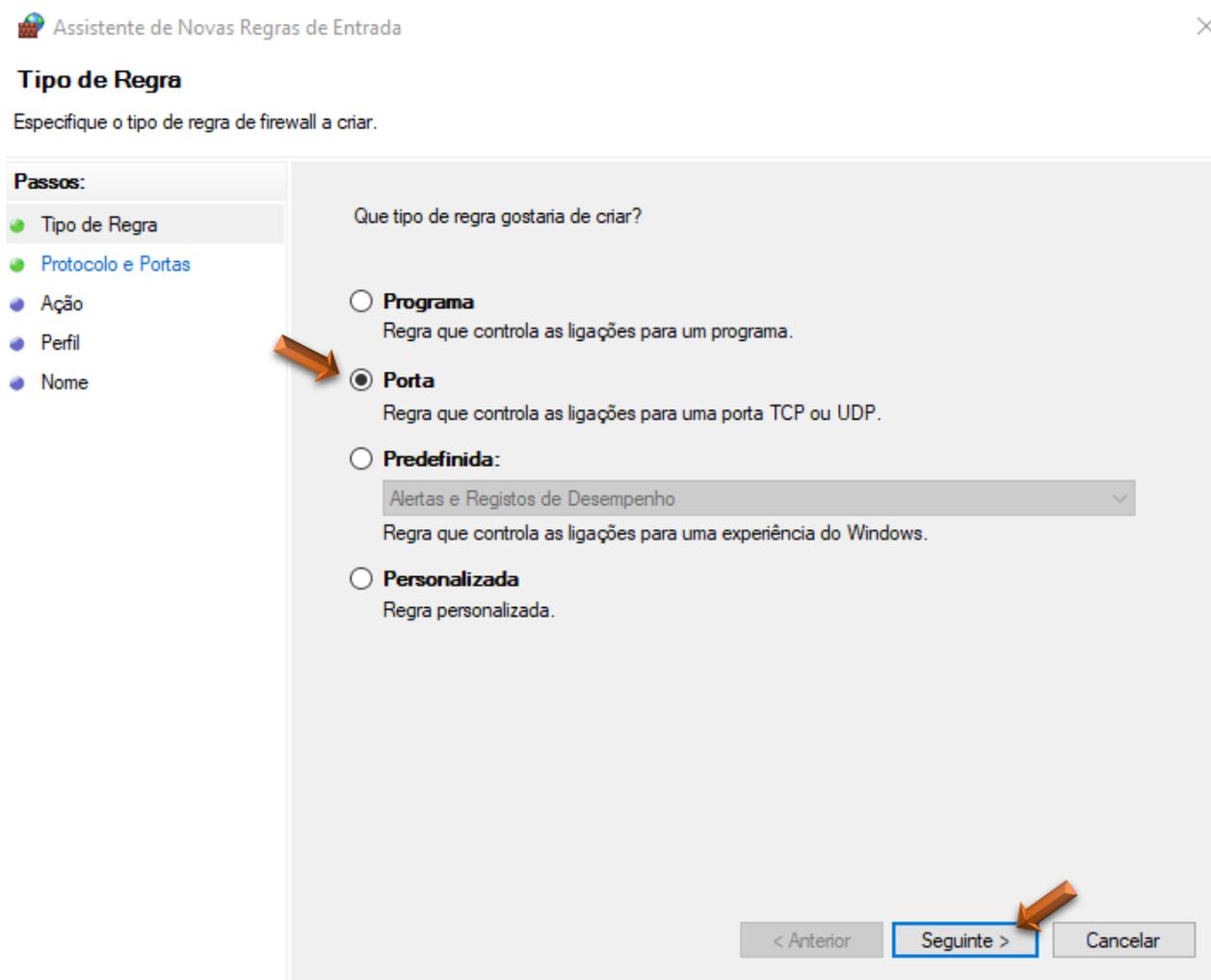


Figura 9 – Selecionar a função Porta.

A primeira regra a definir, é **qual o tipo de regra**.

Vamos ter que efetuar uma permissão para a porta 1433, então devemos selecionar a regra Porta e selecionar o botão seguinte.

2.1.2 – Tipo de protocolo a utilizado na porta.

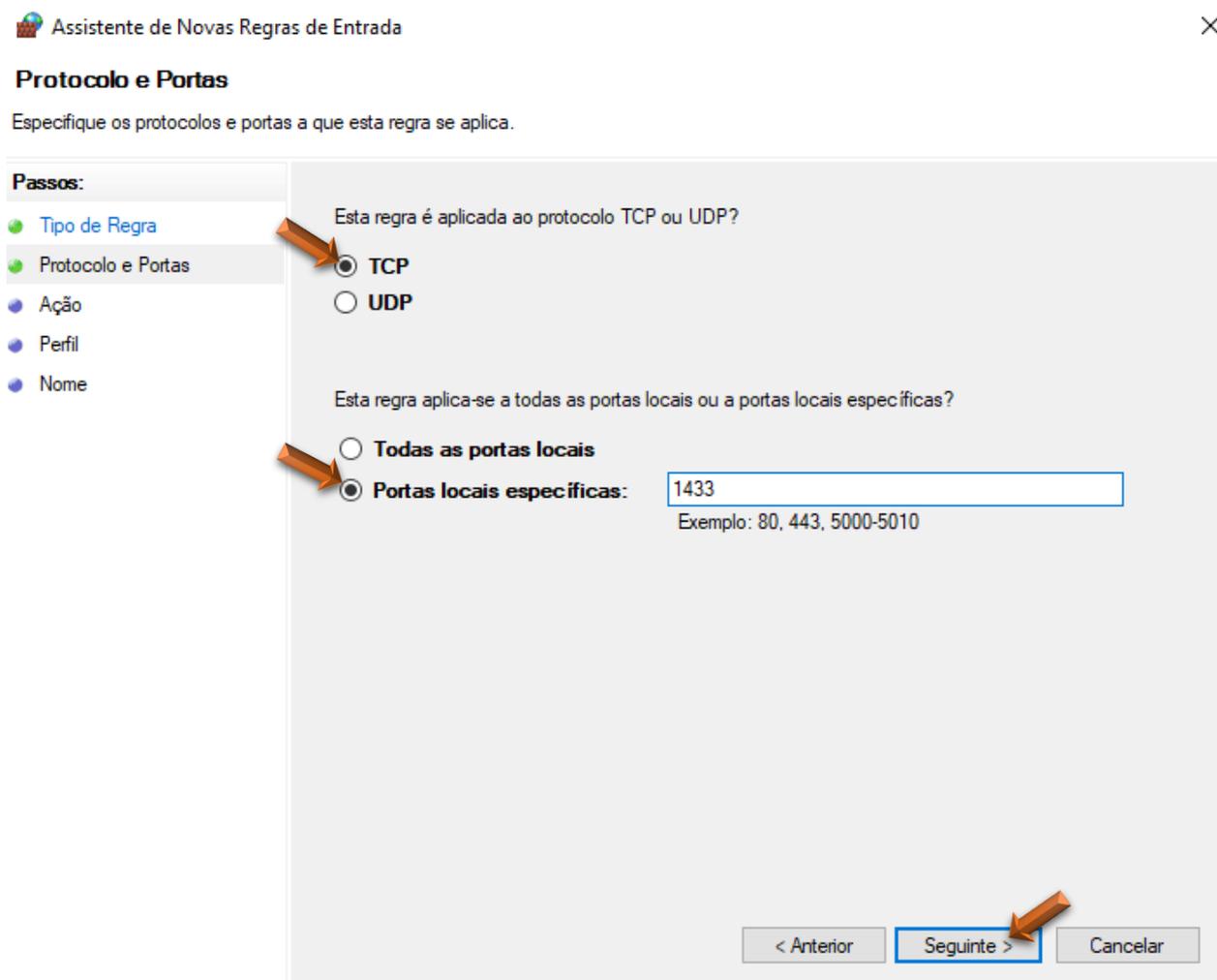


Figura 10 – Atribuição de exceção a porta específica.

Na página de Protocolos e Portas, o utilizador vai seleccionar:

1º - No quadro de Esta regra é aplicada ao protocolo TCP ou UDP? Deve o utilizador seleccionar a opção de **TCP**.

2º - No quadro de Esta regra aplica-se a todas as portas ou a portas locais específicas? Deve o utilizador seleccionar a opção de **Portas locais específicas** e digitar o número da porta anteriormente definida em SQL Server, **1433**

Seleccionar o botão de função Seguinte.

2.1.3 – Ação da Firewall perante a regra.

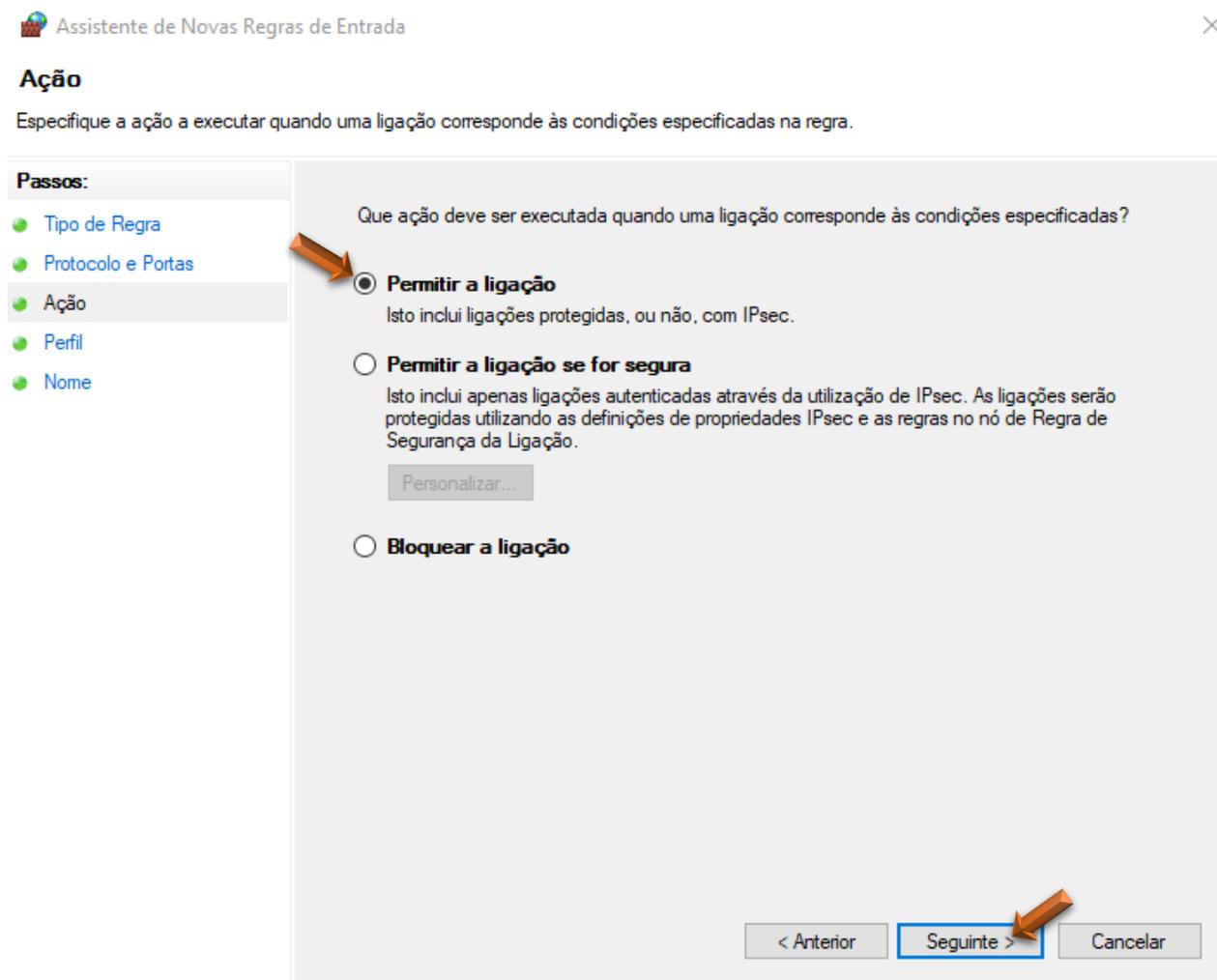


Figura 11 – Ação e permissão a atribuir á ligação.

Na página de Ação, o utilizador vai seleccionar qual é o tipo de permissões a atribuir à ligação da porta anteriormente configurada, no caso vamos seleccionar **Permitir a Ligação**.

Nota: Esta ação vai permitir que todos os equipamentos e periféricos, configurados com a porta 1433, têm permissão para se ligarem á base de dados independentemente do seu IP “*porque a maioria das redes estão configuradas com protocolos dinâmicos DHCP*”.

Selecionar o botão de função Seguinte.

2.1.4 – Perfil da comunicação na porta 1433.

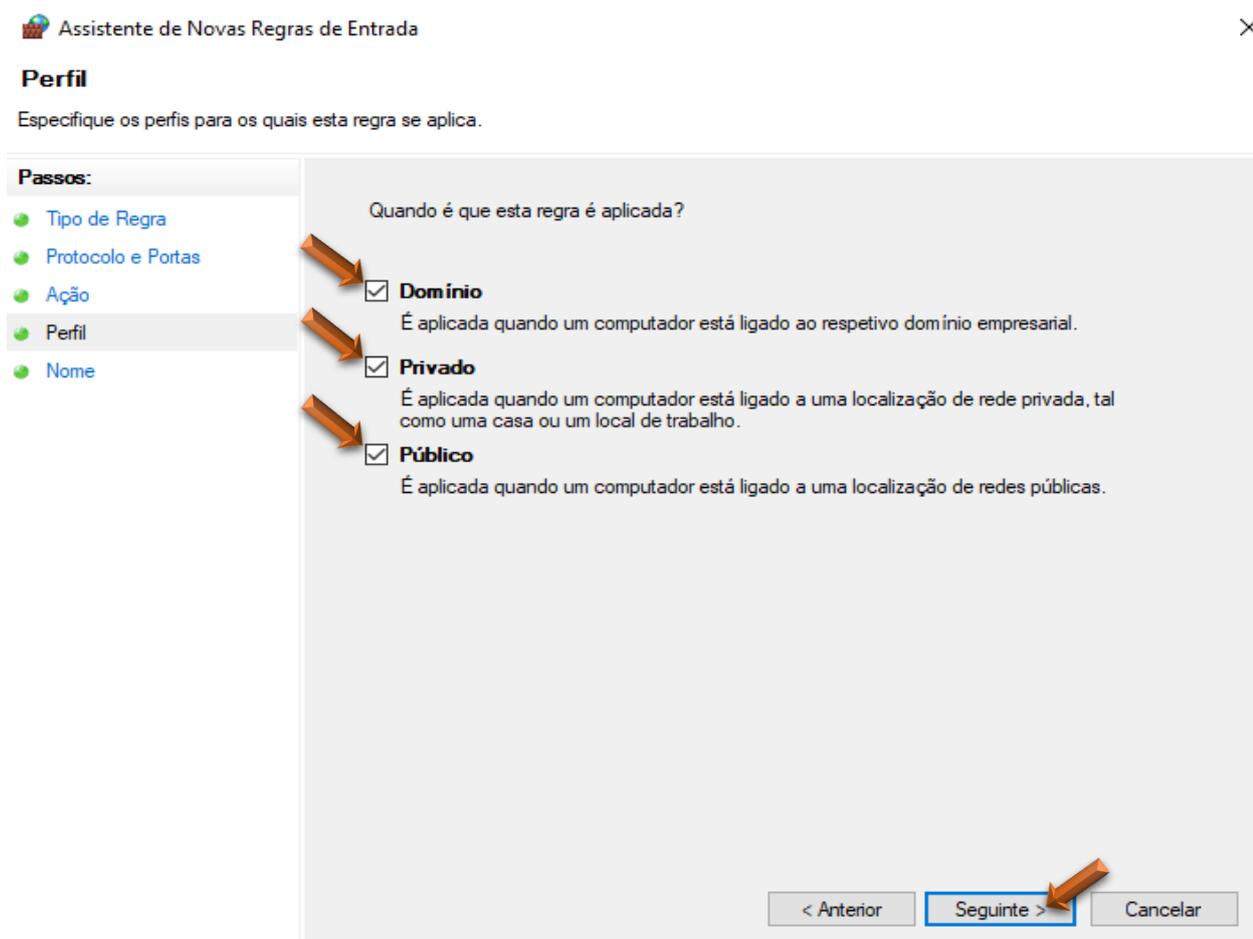


Figura 12 – Identificar os perfis a aplicar à regra.

Nesta página, deve o utilizador selecionar o tipo de domínio para estabelecer ligação da porta 1433. Por norma o utilizador deve selecionar todos os perfis:

Domínio³ – Quando todos os equipamentos têm o domínio da rede definidos.

Privado – Quando os equipamentos estão ligados a uma rede muito específica e com constrangimentos na ligação a outra redes.

Público – Quando o acesso à rede só pode ser efetuado mediante a validação do utilizador no sistema.

Selecionar o botão de função **Seguinte**.

³ Grupo de computadores, programas e dispositivos de rede que são administrados como uma unidade, com normas e procedimentos comuns para uso por um grupo específico de utilizadores.

2.1.5 – Atribuir nome identificativo à regra.

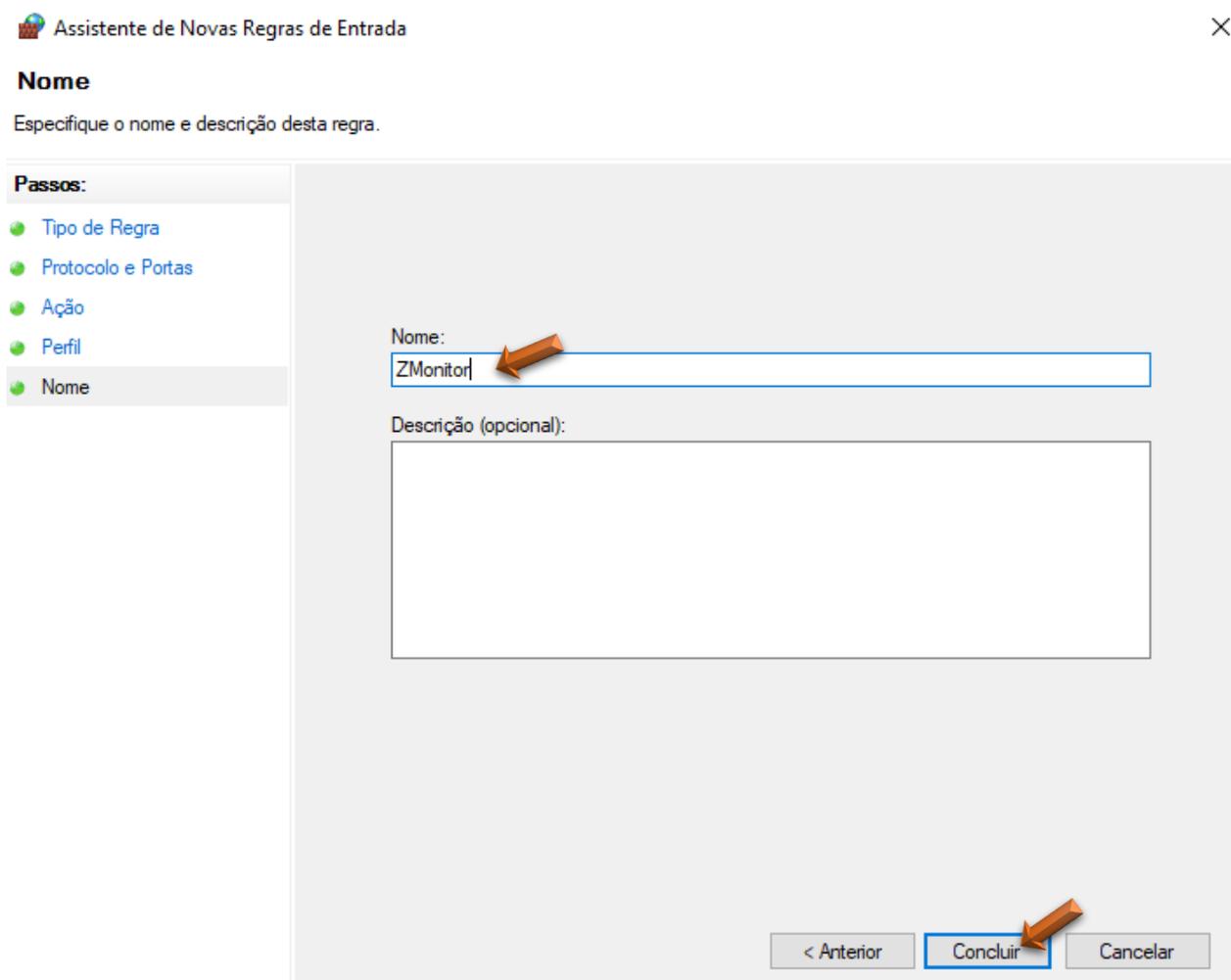


Figura 13 – Atribuir nome à regra.

Nesta janela deve o utilizador introduzir um nome que identifique a regra de exceção a ser utilizada na Firewall e de fácil identificação, para o caso de necessidade de alteração.

Selecionar o botão de função **Concluir** para criar a regra.

3 – CONFIGURAÇÃO DOS POSTOS DE TRABALHO.

Nos pontos de venda deve o utilizador instalar a aplicação do ZS Rest ou ZS POS, mas, para Posto (*Versão disponível no ftp dos parceiros*).

Na instalação da aplicação é pedido os elementos para que seja efetuada a ligação ao PC/Servidor onde está alojada a base de dados:

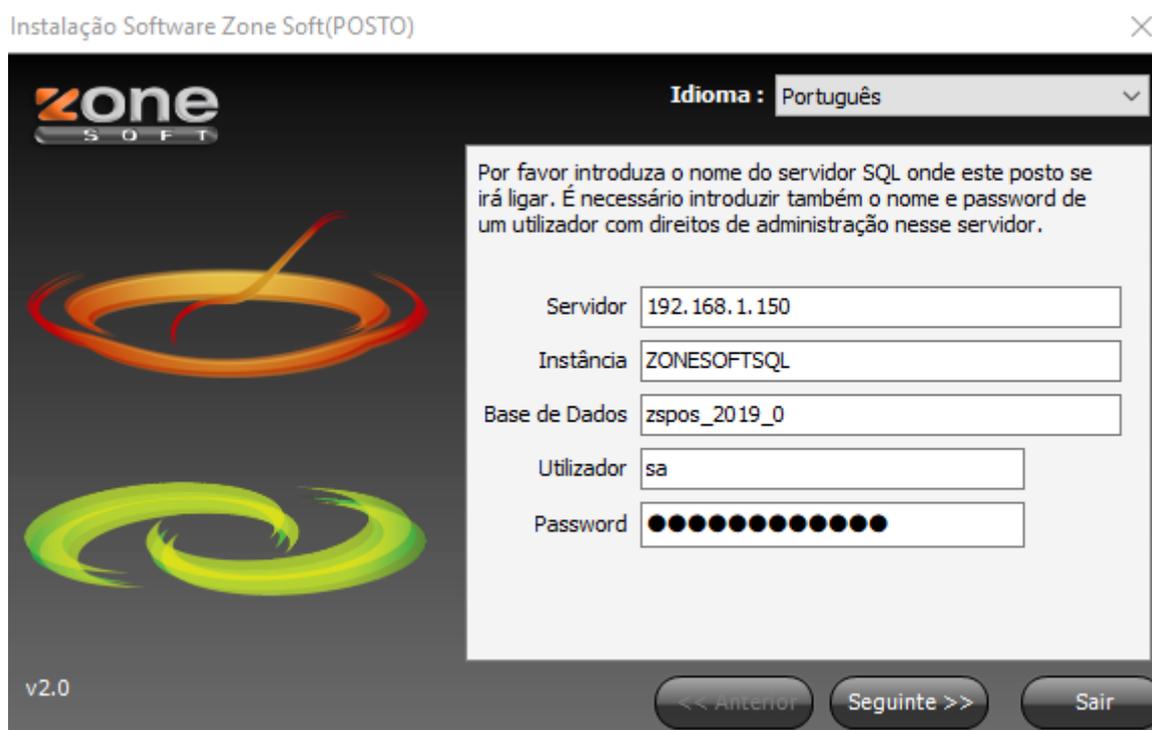


Figura 14 – Inserir dados para acesso ao servidor de dados.

Servidor – Inserir os octetos do IP do servidor

Instância – Inserir o nome da Instância de SQL atribuída quando da instalação do SQL, neste exemplo é a Instância instalada por defeito *ZONESOFTSQL* “*as instâncias são sentive key*”.

Base de Dados – Inserir o nome exato da Base de Dados que pretende recolher e enviar informação.

Utilizador – Inserir o utilizador definido para aceder à Base de Dados.

Password – A Palavra Passe a colocar tem de ser exatamente igual á da Base de Dados para aceder aos dados.

Clicar em **Seguinte** e finalizar o processo de instalação.

Deve o utilizador confirmar que os postos de venda estão a comunicar corretamente. Aceder à pasta onde foi instalada a aplicação ZS REST, ou ZS POS, deve o utilizador fazer duplo click no ficheiro com a designação – **ZSRest.XDL⁴**, ou **ZSPos.XDL**.

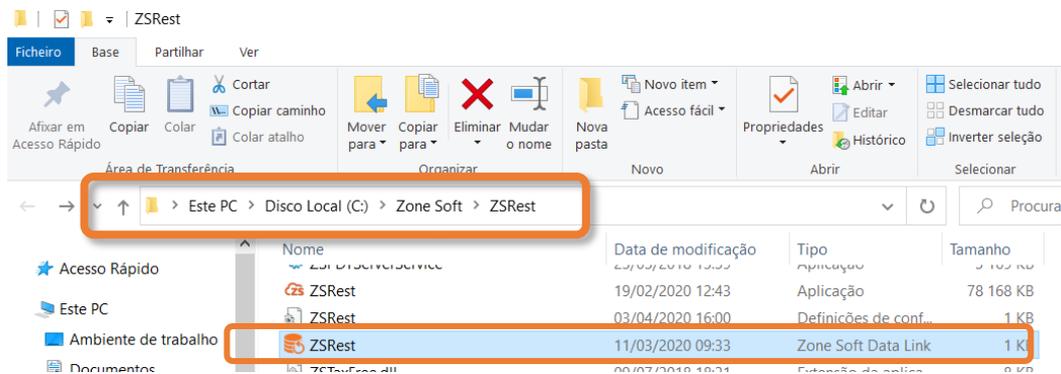


Figura 15 – aceder à função de data link.

O utilizador deve no separador da Ligação apresentado na pagina Propriedades de ligação de dados, ter o cuidado com a informação apresentada nos campos.

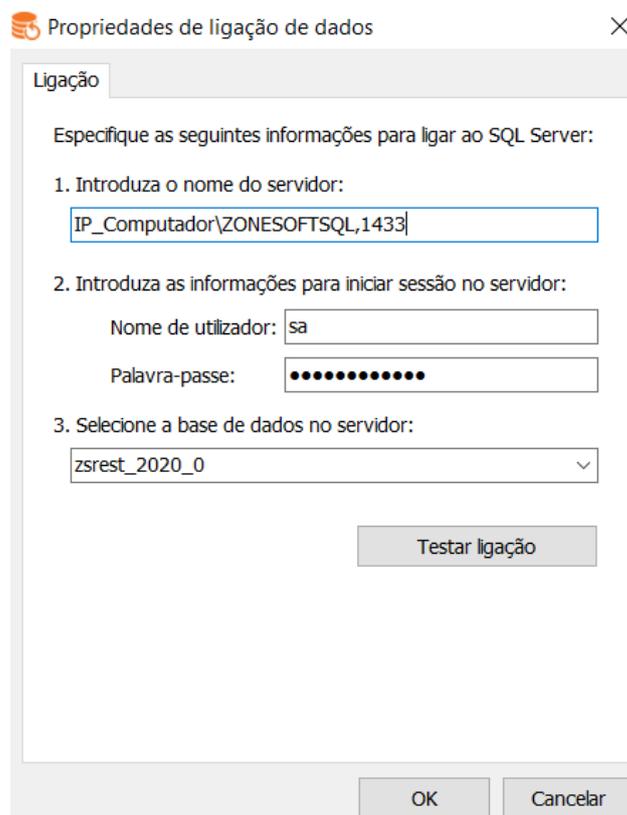


Figura 16 – Verificação dos dados de ligação.

⁴ xdl = Zone Soft Data Link

1 – Selecione ou introduza um nome de servidor:

Neste campo deve o utilizador verificar se está descrito o nome do servidor/PC onde a base de dados está instalada, seguida da instância SQL da Zone Soft e se está identificada a porta de comunicação:

EX: IP_Computador\ZONESOFTSQL,1433

2 – Introduza as informações para iniciar a sessão no servidor:

Deve o utilizador seleccionar a 2ª opção; Utilizar um nome de utilizador e palavra passe específico; inserir os dados de acesso á base de dados quando da sua implementação, se estes dados estiverem incorretos nunca é efetuada a ligação com a base de dados.

3 – Selecione a base de dados no servidor:

Deve o utilizador seleccionar a base de dados ao qual os equipamentos se vão ligar para guardar e importar informação.

Clicar no botão **Testar ligação**, deverá retornar a informação de que o teste da ligação foi efetuado com sucesso, em caso de falha, verificar as configurações.

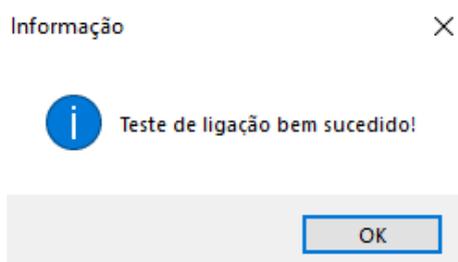


Figura 17 – Teste de ligação á base de dados

4 – CONFIGURAÇÃO DO Z MONITOR.

Após a instalação da aplicação do Z Monitor, disponibilizada na Play Store do Google Play, e ao iniciá-la pela primeira, deve o utilizador seleccionar o botão de **definições**.

Vai iniciar uma janela a pedir acesso, como é a primeira vez que acede às definições, basta o utilizador seleccionar o botão **Entrar**.

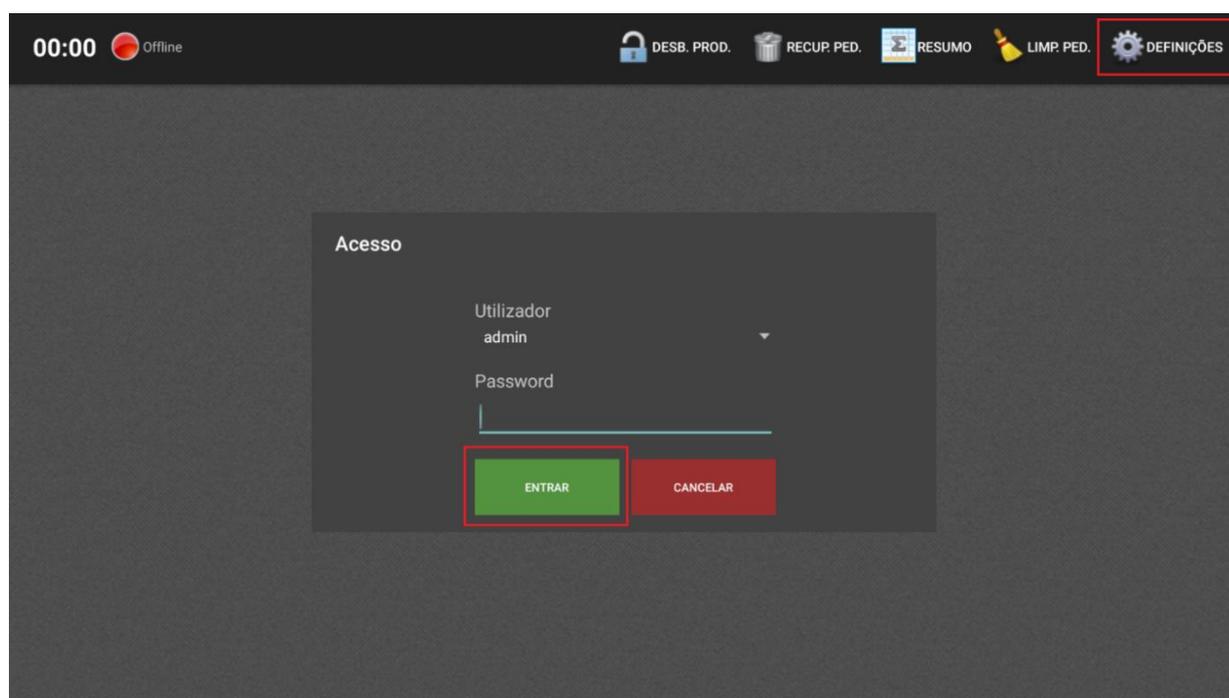


Figura 18 – Aceder às definições do ZS Monitor.

Após seleccionar Entrar, vai iniciar uma nova janela, onde o utilizador deve seleccionar a opção **Ligação ao servidor SQL**.

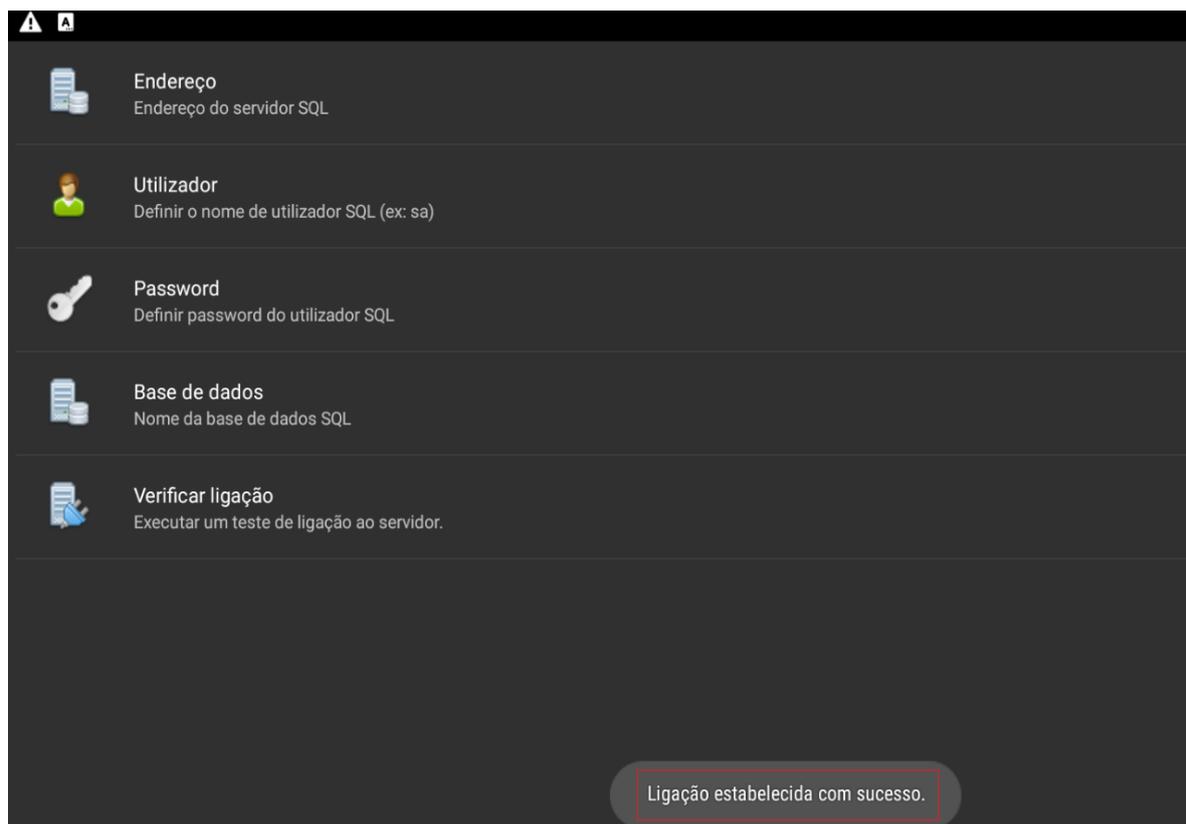


Figura 19 – Menu de configuração ao Servidor de SQL.

Nesta janela, deve o utilizador efetuar as configurações das ligações a estabelecer com o servidor, que deverá estar na mesma rede de IP's:

No campo **Endereço**, o utilizador deve introduzir o endereço IP do Servidor de SQL juntamente com os dois pontos sobrepostos “ : “ e a porta TCP 1433.

Exemplo: **192.168.1.150:1433** endereço IP do servidor : porta de TCP

No campo do **Utilizador**, deve-se colocar a identificação do utilizador da base de dados, exatamente igual, á que está definida na mesma.

No campo da **Password**, deve o utilizador colocar a palavra passe referente ao utilizador e terá que ser exatamente igual, á que está definida na base de dados.

No campo da **Base de dados**, deve-se inserir o nome da base de dados associada aos dois campos anteriores.

Deve o utilizador selecionar o campo de **Verificar ligação**, para se certificar que as configurações anteriores estão corretas e a estabelecer comunicação com a base de dados.

Parceiros ZONE SOFT

Para maiores esclarecimentos, por favor submeta a sua questão através do sistema de tickets do portal My Zone ou consulte a documentação adicional disponível na mesma plataforma

Clientes ZONE SOFT

Por favor, queira contactar o seu parceiro



zone soft®

Contactos:

Estrada Nacional 3, Zona Industrial Lote I-21 2330-210 Entroncamento

www.zonesoft.pt