



---

# **Relatório Final - Supermercado**

---

**RELATÓRIO FINAL**

**UNIVERSIDADE LUSÓFONA – PÓS-GRADUAÇÃO CIBERSEGURANÇA APLICADA**

**SEGURANÇA EM CLOUD**

Daniel Rodrigues | Rafael Azevedo

6 de janeiro de 2026

# Conteúdo

|   |          |
|---|----------|
| <b>Índice de Figuras</b>                                      | <b>1</b> |
| <b>Índice de Tabelas</b>                                      | <b>2</b> |
| <b>1 Introdução</b>   | <b>3</b> |
| <b>2 Cenário Alvo</b>   | <b>4</b> |
| 2.1 Descrição do Cenário e Estrutura Organizacional . . . . . | 4        |
| 2.2 Áreas . . . . .   | 4        |
| 2.2.1 IT . . . . .  | 4        |
| 2.2.2 Administração . . . . .                                 | 4        |
| 2.2.3 Área de Fornecedores . . . . .                          | 4        |
| 2.2.4 Recursos Humanos . . . . .                              | 4        |
| 2.2.5 Área de Segurança . . . . .                             | 5        |
| 2.2.6 Área Logística e Transporte . . . . .                   | 5        |
| 2.2.7 Área de Venda . . . . .                                 | 5        |
| 2.2.8 Marketing . . . . .                                     | 5        |
| 2.2.9 Área de Controlo de Qualidade . . . . .                 | 5        |
| 2.2.10 Apoio ao Cliente . . . . .                             | 5        |
| 2.2.11 Gestão de Stocks . . . . .                             | 5        |
| 2.2.12 Área E-Commerce . . . . .                              | 5        |
| <b>3 Infraestrutura Local</b>                                 | <b>6</b> |
| 3.1 Topologia da Rede Local . . . . .                         | 6        |
| 3.2 Servidores Existentes . . . . .                           | 7        |
| 3.2.1 DNS . . . . .   | 7        |
| 3.2.2 DHCP . . . . .  | 7        |
| 3.2.3 AD . . . . .  | 7        |
| 3.2.4 Servidor Página Web (SPW) . . . . .                     | 7        |
| 3.2.5 Gestor de Ficheiros (GP) . . . . .                      | 7        |
| 3.2.6 Servidor de IoT (IoT) . . . . .                         | 7        |
| 3.2.7 Servidor de Backup (Backup) . . . . .                   | 7        |
| 3.2.8 Servidor de Base de Dados (Base de Dados) . . . . .     | 8        |
| 3.2.9 Servidor de Atualizações (Atualizações) . . . . .       | 8        |
| 3.2.10 Servidor de Aplicações Comerciais (AC) . . . . .       | 8        |
| 3.2.11 Servidor de VoIP (VoIP) . . . . .                      | 8        |
| 3.2.12 Servidor de Impressão (Impressão) . . . . .            | 8        |
| 3.2.13 Servidor de Análise de Dados (Data) . . . . .          | 8        |
| 3.3 Limitações da Arquitetura Atual . . . . .                 | 9        |

|  |           |
|--|-----------|
| <b>4 Estratégia de Migração para a Cloud</b>             | <b>10</b> |
| 4.1 Recursos a Migrar para a Cloud . . . . .             | 10        |
| 4.2 Recursos a Manter Localmente . . . . .               | 11        |
| 4.3 Modelo de Cloud . . . . .                            | 12        |
| 4.4 Tipo de Serviço . . . . .                            | 13        |
| 4.4.1 Infrastructure as a Service (IaaS) . . . . .       | 13        |
| 4.4.2 Platform as a Service (PaaS) . . . . .             | 13        |
| 4.4.3 Software as a Service (SaaS) . . . . .             | 13        |
| 4.4.4 Relação com o Cenário . . . . .                    | 13        |
| <b>5 Arquitetura Cloud Proposta</b>                      | <b>14</b> |
| 5.1 Topologia da Rede com Cloud . . . . .                | 14        |
| <b>6 Produtos das Empresas AWS, Azure e Google Cloud</b> | <b>15</b> |
| 6.1 Computação . . . . .                                 | 15        |
| 6.2 Armazenamento de Objetos . . . . .                   | 15        |
| 6.3 Armazenamento de Ficheiros . . . . .                 | 16        |
| 6.4 Bases de Dados Relacionais . . . . .                 | 16        |
| 6.5 Bases de Dados NoSQL . . . . .                       | 17        |
| 6.6 Aplicações Comerciais . . . . .                      | 17        |
| 6.7 IoT . . . . .  | 18        |
| 6.8 Microserviços . . . . .                              | 18        |
| 6.9 Backup e Recuperação . . . . .                       | 19        |
| 6.10 Políticas de Segurança . . . . .                    | 19        |
| 6.11 Controlos de Acesso . . . . .                       | 20        |
| 6.12 Monitorização e Detecção de Ameaças . . . . .       | 20        |
| 6.13 Educação e Consciencialização . . . . .             | 21        |
| 6.14 Encriptação . . . . .                               | 22        |
| 6.15 Gestão de Chaves . . . . .                          | 23        |
| <b>7 Frameworks</b>                                      | <b>24</b> |
| 7.1 NIST CSF . . . . .                                   | 24        |
| 7.1.1 Relação com o Cenário . . . . .                    | 24        |
| 7.2 ISO/IEC 27001 . . . . .                              | 25        |
| 7.2.1 Relação com o Cenário . . . . .                    | 25        |
| 7.3 CIS Controls . . . . .                               | 26        |
| 7.3.1 Relação com o Cenário . . . . .                    | 26        |
| 7.4 COBIT . . . . .                                      | 27        |
| 7.4.1 Relação com o Cenário . . . . .                    | 27        |
| 7.5 MITRE ATT&CK . . . . .                               | 28        |
| 7.5.1 Relação com o Cenário . . . . .                    | 28        |

|  |           |
|--|-----------|
| <b>8 Matriz de Direito</b>                                     | <b>29</b> |
| 8.1 Grupos . . . . .   | 30        |
| <b>9 Firewall</b>  | <b>31</b> |
| 9.1 Microsoft Azure . . . . .                                  | 31        |
| 9.1.1 Tipo de Azure Firewall . . . . .                         | 31        |
| 9.1.2 Serviços a ser Protegidos pela Azure Firewall . . . . .  | 32        |
| 9.1.3 Ferramentas Azure a Implementar com Firewall . . . . .   | 32        |
| 9.2 AWS . . . . .  | 33        |
| 9.2.1 Tipo de AWS Firewall . . . . .                           | 33        |
| 9.2.2 Serviços a ser Protegidos pela AWS Firewall . . . . .    | 33        |
| 9.2.3 Ferramentas AWS a Implementar com Firewall . . . . .     | 34        |
| 9.3 Google Cloud Platform . . . . .                            | 34        |
| 9.3.1 Tipo de GCP Firewall . . . . .                           | 34        |
| 9.3.2 Serviços a ser Protegidos pela Firewall da GCP . . . . . | 35        |
| 9.3.3 Ferramentas GCP a Implementar com Firewall . . . . .     | 35        |
| <b>10 Resposta a Incidentes</b>                                | <b>36</b> |
| 10.1 Processo e Pessoas . . . . .                              | 36        |
| 10.2 Tecnologia . . . . .                                      | 39        |
| <b>11 Conclusão</b>  | <b>40</b> |
| <b>12 Anexos</b>   | <b>41</b> |

## Índice de Figuras

|    |   |    |
|----|---|----|
| 1  | Topologia Inicial . . . . .                               | 6  |
| 2  | Topologia de Rede na Cloud (Inicial) . . . . .            | 14 |
| 3  | Grupos - AWS . . . . .                                    | 41 |
| 4  | Utilizadores - AWS . . . . .                              | 42 |
| 5  | Exemplo de Utilizador - AWS . . . . .                     | 43 |
| 6  | Exemplo de Grupo - AWS . . . . .                          | 43 |
| 7  | Grupos - Azure . . . . .                                  | 44 |
| 8  | Grupo Específico - Azure . . . . .                        | 45 |
| 9  | Exemplo de Membros num Grupo - Azure . . . . .            | 45 |
| 10 | Exemplo de Users - Azure . . . . .                        | 46 |
| 11 | Exemplo de User Específico - Azure . . . . .              | 47 |
| 12 | Exemplo de Funções de Users - Azure . . . . .             | 47 |
| 13 | Exemplo de Redes Virtuais - Azure . . . . .               | 48 |
| 14 | Exemplo de Rede Virtual Específica - Azure . . . . .      | 49 |
| 15 | Exemplo de Sub-Redes - Azure . . . . .                    | 50 |
| 16 | Exemplo de Sub-Rede Específica - Azure . . . . .          | 51 |
| 17 | Exemplo de Tabela de Rotas - Azure . . . . .              | 52 |
| 18 | Exemplo de Sub-Redes na Tabela de Rotas - Azure . . . . . | 52 |
| 19 | Exemplo de Firewall - Azure . . . . .                     | 53 |
| 20 | Exemplo de Regras de Firewall - Azure . . . . .           | 53 |
| 21 | Exemplo de Uma Regra de Firewall - Azure . . . . .        | 54 |

## Índice de Tabelas

|    |   |    |
|----|---|----|
| 1  | Computação (Infraestrutura Base) . . . . .                    | 15 |
| 2  | Armazenamento de Objetos . . . . .                            | 15 |
| 3  | Armazenamento de Ficheiros . . . . .                          | 16 |
| 4  | Bases de Dados Relacionais . . . . .                          | 16 |
| 5  | Base de Dados NoSQL . . . . .                                 | 17 |
| 6  | Aplicações Comerciais (E-commerce) . . . . .                  | 17 |
| 7  | IoT . . . . .   | 18 |
| 8  | Microserviços . . . . .                                       | 18 |
| 9  | Backup e Recuperação . . . . .                                | 19 |
| 10 | Políticas de Segurança . . . . .                              | 19 |
| 11 | Controlos de Acesso . . . . .                                 | 20 |
| 12 | Monitorização e Detecção de Ameaças . . . . .                 | 20 |
| 13 | Educação e Consciencialização . . . . .                       | 21 |
| 14 | Encriptação . . . . .   | 22 |
| 15 | Gestão de Chaves na Cloud . . . . .                           | 23 |
| 16 | Matriz de Direito . . . . .                                   | 29 |
| 17 | Grupos para Implementação na Cloud . . . . .                  | 30 |
| 18 | Serviços a ser Protegidos - Azure Firewall Standard . . . . . | 32 |
| 19 | Ferramentas Azure a Implementar com Firewall . . . . .        | 32 |
| 20 | Serviços a ser Protegidos - Azure Firewall Standard . . . . . | 33 |
| 21 | Ferramentas AWS a Implementar com Firewall . . . . .          | 34 |
| 22 | Serviços a ser Protegidos - NGFW Padrão . . . . .             | 35 |
| 23 | Ferramentas GCP a Implementar com Firewall . . . . .          | 35 |

## 1 Introdução

No âmbito da unidade curricular de "Segurança em Cloud" foi solicitado o desenvolvimento de um relatório cujo objetivo é indicar o processo mais acertado à migração de uma infraestrutura de rede local para a Cloud, tendo como base o cenário hipotético previamente analisado na unidade curricular de "Segurança em Rede e Dispositivos IoT", um Supermercado com sede, sucursal e ambiente de trabalho remoto.

A infraestrutura do supermercado exige uma elevada disponibilidade, escalabilidade e segurança, face às tarefas críticas com que uma organização desta área tem que suportar como, getão de stocks, loja online, comunicação entre clientes e fornecedores, entre outros. No caso em questão, a migração para a cloud apresenta uma solução para modernizar e tornar mais robusta a infraestrutura da organização, garantindo fiabilidade nas operações e suporte a ambientes distribuídos.

Neste relatório, após a análise da infraestrutura local atual do supermercado, será apresentada a proposta de migração para a cloud, com as suas vantagens, identificação dos recursos a migrar, os serviços e os produtos mais adequados, fazendo uma comparação entre as plataformas *AWS*, *Azure* e *Google Cloud*. Posteriormente, serão abordados os modelos e serviços de segurança adequados à organização, de forma a serem também implementados.

## 2 Cenário Alvo

### 2.1 Descrição do Cenário e Estrutura Organizacional

Para o desenvolvimento deste projeto, é simulado um ambiente real, onde é feito um pedido, por parte de um supermercado fictício denominado "*Products A Lot*", que consiste na contratação de uma equipa com capacidades para implementar e configurar um sistema de rede, na Cloud, que ofereça segurança e eficiência para a sede desta empresa, uma sucursal e um ambiente remoto. O orçamento proposto pela empresa é ilimitado, isto é, devem ser tomadas as melhores e mais avançadas medidas para alcançar a robustez máxima do ambiente de rede.

A estrutura da organização vai ao encontro da descrição feita acima, onde é indicado que a empresa está subdividida em três secções, a sede, onde estão centralizados todos os componentes da empresa, a sucursal, que apesar de não conter os mesmos atributos que a sede, atua de forma independente e o ambiente remoto, onde colaboradores serão capazes de aceder aos recursos disponibilizados pela organização.

### 2.2 Áreas

No seguinte tópico serão tratadas as diferentes áreas que acompanham o cenário simulado e que vão ao encontro do supermercado, resumindo os objetivos de cada área, respetivamente, de forma sucinta.

#### 2.2.1 IT

Nesta área, serão geridas tarefas como gestão da infraestrutura de rede e servidores, monitorização e manutenção do sistema e controlo de acessos à rede.

#### 2.2.2 Administração

Área responsável pela gestão geral da empresa, incluindo a tomada de decisões estratégicas e também coordena operações financeiras, jurídicas e administrativas.

#### 2.2.3 Área de Fornecedores

Gere as relações com os fornecedores incluindo a negociação de preços e contratos e também garante que existe sempre stock no supermercado.

#### 2.2.4 Recursos Humanos

Gere o recrutamento, treino e desenvolvimento dos funcionários cuidando dos seus salários, benefícios e relações.

---

### 2.2.5 Área de Segurança

Monitoriza e protege os sistemas digitais implementando sistemas de vigilância, alarmes e políticas de acesso. Realiza também auditorias de segurança.

### 2.2.6 Área Logística e Transporte

Coordena a movimentação de mercadorias entre os fornecedores e as lojas gerindo frotas de veículos e armazéns e garantindo eficientemente a entrega pontual dos produtos encomendados.

### 2.2.7 Área de Venda

Faz o atendimento ao cliente garantindo que os produtos estejam bem apresentados e disponíveis para compra.

### 2.2.8 Marketing

Cria e desenvolve estratégias de marketing analisando o comportamento do consumidor para atrair mais clientes e aumentar as vendas através de publicidades, promoções e branding.

### 2.2.9 Área de Controlo de Qualidade

Garante que os produtos vendidos atendem os padrões de qualidade e segurança fazendo regularmente inspeções e testes às mercadorias.

### 2.2.10 Apoio ao Cliente

Responde a dúvidas, reclamações e pedidos dos clientes oferecendo também suporte pós-venda de forma a melhorar a experiência dos clientes.

### 2.2.11 Gestão de Stocks

Controla os níveis de stock nos armazéns e lojas e previne a falta ou até excesso de inventário.

### 2.2.12 Área E-Commerce

Gere a loja online do supermercado garantindo que a experiência de utilização do site incluindo a navegação e pagamento seja o melhor possível. Também coordena a logística de entrega dos pedidos online.

### 3 Infraestrutura Local

#### 3.1 Topologia da Rede Local

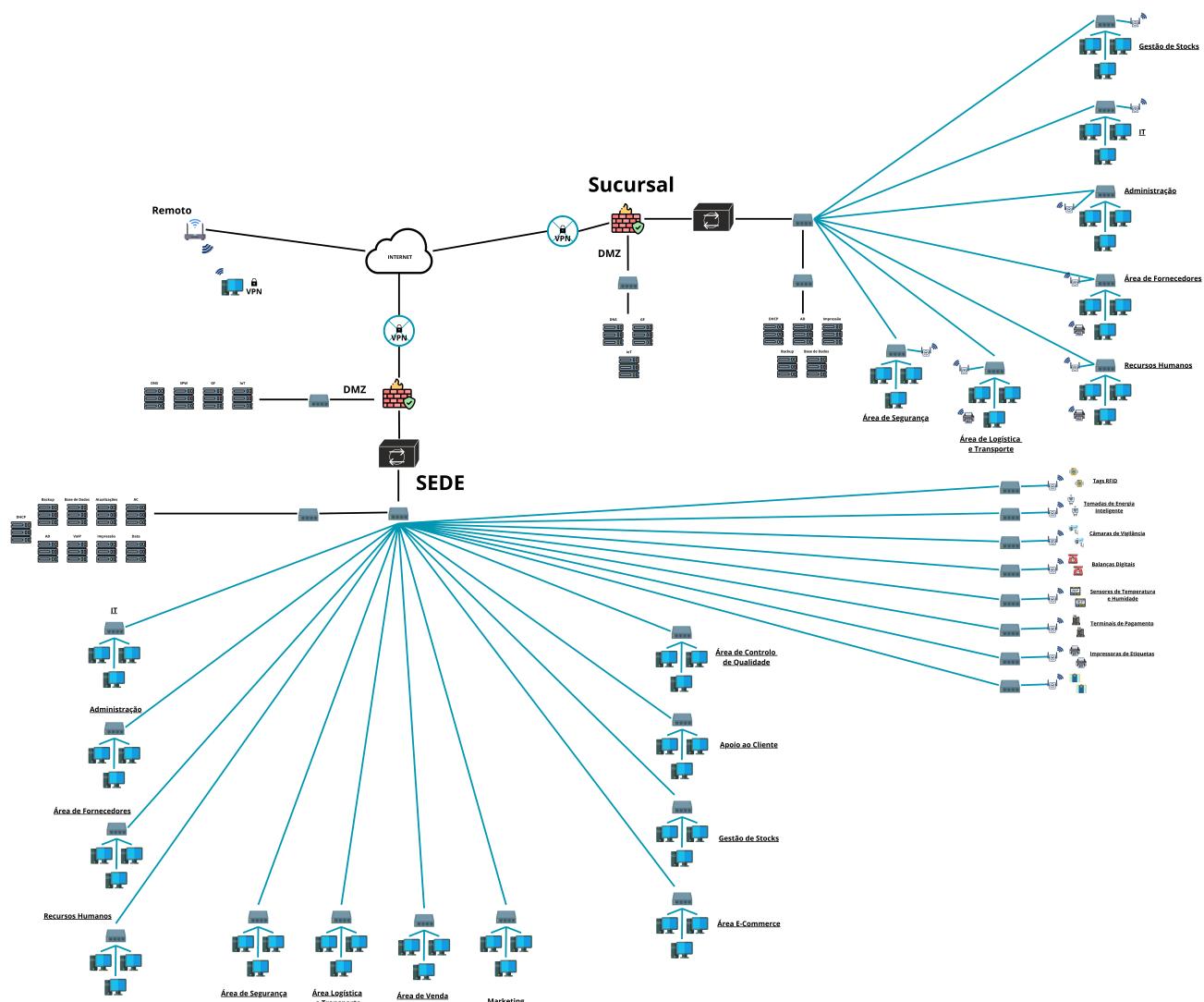


Figura 1: Topologia Inicial

## 3.2 Servidores Existentes

### 3.2.1 DNS

- Este servidor resolve os nomes de domínio nos endereços IP e vice-versa, o que facilita o acesso a sistemas internos e externos através do uso de nomes mais amigáveis e é essencial para a comunicação entre dispositivos na rede.

### 3.2.2 DHCP

- Automatiza a atribuição de endereços IP, máscaras de sub-rede, gateways e garante que dispositivos ligados à rede como terminais de ponto de venda, computadores, impressoras e dispositivos IoT recebam as configurações de rede sem intervenção manual

### 3.2.3 AD

- Centraliza a autenticação e autorização de utilizadores, dispositivos e serviços numa rede oferecendo diretórios para organizar e gerir recursos. Este servidor controla quem possa aceder a diferentes áreas da rede como ficheiros, sistemas ou aplicações específicas. Também implementa políticas de segurança como bloqueios de ecrã automáticos ou restrições de acesso a dispositivos USB.

### 3.2.4 Servidor Página Web (SPW)

- Serve para dar host a páginas web que são acessíveis internamente ou externamente e suporta sistemas internos acessíveis via web como intranet, ferramentas de gestão de stock ou relatórios de vendas.

### 3.2.5 Gestor de Ficheiros (GP)

- Armazena, organiza e distribui ficheiros numa rede o que facilita a partilha de documentos entre departamentos como por exemplo listas de stock, relatórios financeiros e políticas de RH.

### 3.2.6 Servidor de IoT (IoT)

- Faz a gestão de dispositivos IoT conectados na rede do supermercado assim como sensores de temperatura, câmeras de segurança, entre outros.

### 3.2.7 Servidor de Backup (Backup)

- Armazena cópias de segurança de dados críticos como ficheiros, bases de dados e configurações do sistema.

### 3.2.8 Servidor de Base de Dados (Base de Dados)

- Gere e armazena informações como dados de clientes.

### 3.2.9 Servidor de Atualizações (Atualizações)

- Centraliza e distribui atualizações de sistemas operativos e softwares.

### 3.2.10 Servidor de Aplicações Comerciais (AC)

- Serve para hospedar sistemas como software de gestão de stock, sistemas de ponto de venda, entre outros.

### 3.2.11 Servidor de VoIP (VoIP)

- Suporta comunicações telefónicas baseadas em IP o que reduzirá os custos de telecomunicação.

### 3.2.12 Servidor de Impressão (Impressão)

- Serve para centralizar a gestão de impressoras e consequentes filas de impressão.

### 3.2.13 Servidor de Análise de Dados (Data)

- Usado para processar grandes volumes de dados que posteriormente serão analisados para compreender o comportamento dos clientes e tendências atuais.

### 3.3 Limitações da Arquitetura Atual

Apesar de a arquitetura local do supermercado “Products A Lot” ter sido desenhada com foco na segurança e organização por áreas, a sua natureza apresenta diversas limitações face às exigências atuais a nível de escalabilidade e mobilidade. A infraestrutura depende fortemente de servidores físicos instalados localmente, o que implica custos elevados de manutenção, necessidade constante de atualizações de hardware e risco de falhas críticas por avarias ou desastres locais.

A escalabilidade da infraestrutura é limitada, tornando-se difícil responder rapidamente a picos de utilização, como em períodos promocionais. Além disso, o acesso remoto de colaboradores e a integração entre a sede, sucursal e ambiente remoto depende de VPNs e configuração manual, o que pode causar complicações operacionais.

Outra limitação significativa é a redundância de dados e continuidade do negócio. Apesar da existência de backups, o armazenamento local apresenta riscos de perda de dados em caso de falha física ou ciberataque.

Por fim, a capacidade de adotar novas tecnologias, como inteligência artificial, machine learning e análises preditivas de dados, está severamente condicionada pelas restrições de processamento e armazenamento locais, dificultando o processo inovativo.

## 4 Estratégia de Migração para a Cloud

### 4.1 Recursos a Migrar para a Cloud

Após analisar a infraestrutura local, foram identificados vários recursos críticos cuja migração para a cloud trará ganhos substanciais em termos de escalabilidade, desempenho, segurança e custo-benefício. Passamos a listar os recursos selecionados para a migração:

- **Servidor de Página Web (SPW)** - Hospedar este servidor na cloud garante alta disponibilidade, resposta rápida e melhor performance em acessos externos, especialmente no e-commerce.
- **Servidor de IoT** - A gestão centralizada e remota dos dispositivos IoT torna-se mais eficiente em ambientes cloud, permitindo também o uso de serviços analíticos em tempo real.
- **Servidor de Base de Dados** - A cloud permite escalabilidade automática, replicação geográfica e backups contínuos, garantindo integridade e disponibilidade dos dados críticos da operação.
- **Servidor de Análise de Dados (Data)** - Serviços cloud de Big Data e Business Intelligence são otimizados para grandes volumes de dados, permitindo análises avançadas com menor esforço técnico local.
- **Servidor de Backup** - A cloud proporciona armazenamento redundante, encriptação de dados e recuperação rápida em caso de falha, minimizando o risco de perda de informação.
- **Servidor de Aplicações Comerciais (AC)** - A migração permite maior flexibilidade no acesso remoto, atualizações automáticas e melhor integração com sistemas externos, como gateways de pagamento.

Esta seleção visa maximizar o valor obtido com a cloud, mantendo localmente os serviços mais sensíveis à latência ou dependentes de hardware físico específico.

## 4.2 Recursos a Manter Localmente

Apesar das vantagens evidentes da cloud, determinados serviços serão mantidos em infraestrutura local por razões de desempenho, latência, dependência de hardware específico ou criticidade operacional.

- **Servidor DHCP e DNS** - Estes serviços são essenciais para a comunicação e resolução interna de nomes e endereços IP. A sua presença local garante uma menor latência, autonomia em caso de falha de ligação à cloud e melhor desempenho na gestão de rede interna.
- **Servidor de Active Directory (AD)** - Devido à sua ligação direta com autenticação de utilizadores e dispositivos locais, manter o AD localmente assegura disponibilidade imediata e evita atrasos na autenticação.
- **Servidor de Impressão** - A proximidade física às impressoras e a frequência de uso local justificam a manutenção deste serviço no local, evitando complexidade desnecessária na gestão remota de filas de impressão.
- **Servidor de VoIP** - Embora seja possível fazer a migração para soluções cloud, o serviço VoIP pode apresentar latência e perdas de qualidade com dependência total da internet. Assim, opta-se por manter um servidor VoIP local com ligação redundante à internet.
- **Servidor de Gestão de Ficheiros (GF)** - Por se tratar de partilhas internas entre departamentos, manter o servidor local garante velocidade no acesso e menor dependência de conectividade externa.

Alguns recursos como o Servidor DHCP, DNS e AD podem permanecer num ambiente local ou híbrido, devido à ligação direta com serviços críticos da rede interna. Estes podem ser duplicados na cloud como redundância, tirando partido tanto do servidor local, como na cloud.

Assim sendo a combinação entre serviços locais e cloud forma um modelo híbrido que proporciona resiliência, segurança e flexibilidade, mantendo o controlo sobre os serviços críticos e sensíveis à latência enquanto se aproveitam os benefícios da escalabilidade da cloud.

### 4.3 Modelo de Cloud

Para o cenário do supermercado, foi adotado o modelo de cloud híbrida, combinando recursos locais com serviços em cloud, como AWS, Azure e Google Cloud.

Este modelo foi escolhido por oferecer um equilíbrio ideal entre controlo, desempenho e escalabilidade. A cloud pública será usada para hospedar serviços que exigem alta disponibilidade, como a loja online, análise de dados, backups e serviços IoT, beneficiando da automação e resiliência inerentes à infraestrutura dos principais fornecedores de cloud.

Ao mesmo tempo, a infraestrutura local será mantida para serviços essenciais que exigem baixa latência, controlo direto sobre dados ou que dependem de equipamentos físicos, como DHCP, AD, impressão e VoIP.

A abordagem híbrida permite ainda:

- Garantir continuidade operacional mesmo em caso de falha na ligação à internet;
- Reduzir custos com serviços que não exigem elasticidade;
- Cumprir requisitos de segurança e conformidade local (ex.: dados sensíveis não saem do perímetro físico);
- Evoluir gradualmente para maior adoção da cloud, sem interrupções.

Este modelo garante flexibilidade e escalabilidade progressiva, mantendo ao mesmo tempo o desempenho e a segurança dos sistemas críticos internos.

## 4.4 Tipo de Serviço

### 4.4.1 Infrastructure as a Service (IaaS)

A IaaS é fornece recursos básicos de infraestrutura como servidores, armazenamento e redes em máquinas virtuais. O utilizador é responsável por configurar e gerir o sistema operativo e aplicações.

### 4.4.2 Platform as a Service (PaaS)

O PaaS oferece uma plataforma completa para desenvolver, testar e executar aplicações, sem necessidade de gerir a infraestrutura subjacente.

### 4.4.3 Software as a Service (SaaS)

O SaaS aplica-se a software pronto a usar, acessível via internet (ex: e-mail), gerido totalmente pelo fornecedor. O utilizador apenas consome o serviço.

### 4.4.4 Relação com o Cenário

No nosso cenário iremos usar a migração para a cloud com base apenas no modelo IaaS, uma vez que o objetivo é manter a mesma estrutura de servidores que existia localmente, mas agora num ambiente de cloud. Assim, a organização mantém o controlo total sobre a sua infraestrutura mas com maior flexibilidade para aplicar configurações específicas, políticas de segurança personalizadas e integração com sistemas locais via VPN.

## 5 Arquitetura Cloud Proposta

### 5.1 Topologia da Rede com Cloud

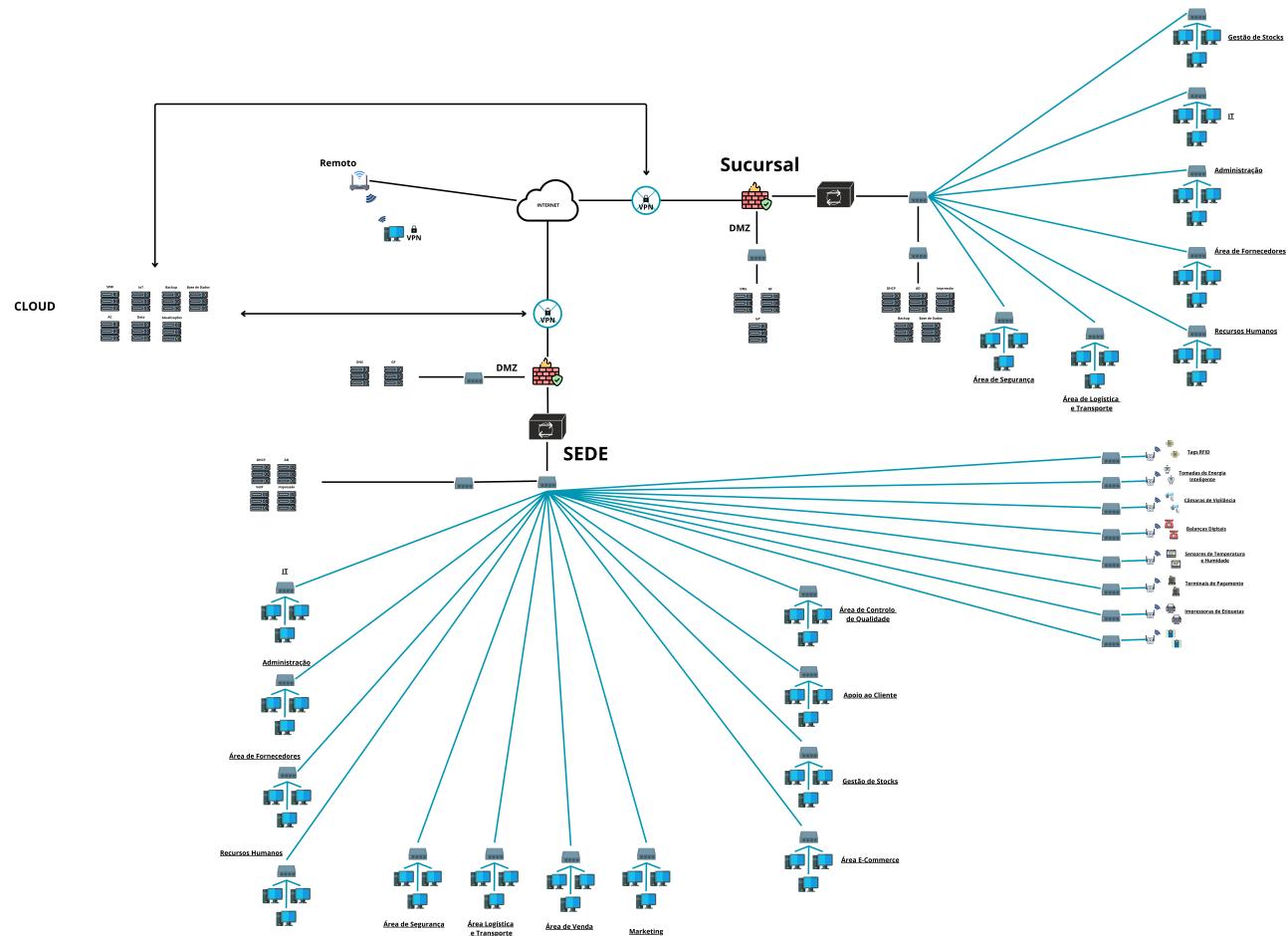


Figura 2: Topologia de Rede na Cloud (Inicial)

## 6 Produtos das Empresas AWS, Azure e Google Cloud

Neste tópico serão apresentados, através de uma lista, os produtos essenciais de acordo com o cenário em questão, das três empresas com serviços em Cloud, *Amazon Web Services*, *Microsoft Azure* e *Google Cloud Platform*.

### 6.1 Computação

| Provedor | Produto          | Vantagens   | Desvantagens  |
|----------|------------------|---|---|
| AWS      | EC2              | Ótima escalabilidade, flexibilidade e variedade de instâncias | Curva de aprendizagem elevada e preços complexos                              |
| Azure    | Virtual Machines | Integração com AD e fácil gestão                              | Baixa variedade de tipos de Virtual Machines e dependente da região onde atua |
| GCP      | Compute Engine   | Faturação ao segundo e excelente desempenho                   | Ecossistema mais limitado   |

Tabela 1: Computação (Infraestrutura Base)

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *Azure*, face à sua integração com *Active Directory* e suporte a ambientes híbridos, o que facilitaria na relação sede/sucursal. Este mesmo sistema poderia hospedar os sistemas de faturação e possíveis aplicações personalizadas da organização.

### 6.2 Armazenamento de Objetos

| Provedor | Produto       | Vantagens                                    | Desvantagens                          |
|----------|---------------|--|---------------------------------------|
| AWS      | S3            | Maturidade do Serviço e segurança do serviço | Custos adicionais face às requisições |
| Azure    | Blobs Storage | Integração com outros serviços Microsoft     | Regras pouco flexíveis                |
| GCP      | Cloud Storage | Performance elevada                          | Menor número de ferramentas           |

Tabela 2: Armazenamento de Objetos

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *AWS*, face à sua fiabilidade e robustez o que seria ideal para o armazenamento de imagens, documentos e backups para o supermercado.

### 6.3 Armazenamento de Ficheiros

| Provedor     | Produto     | Vantagens                              | Desvantagens                                 |
|--------------|-------------|--|--|
| <i>AWS</i>   | Amazon FSx  | Performance elevada                    | Configuração mais complexa                   |
| <i>Azure</i> | Azure Files | Integração nativa com Azure AD         | Limitações de performance em cargas elevadas |
| <i>GCP</i>   | Filestore   | Boa performance e configuração simples | Suporte limitado a protocolos                |

Tabela 3: Armazenamento de Ficheiros

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *Azure*, devido à permissão de mapeamento de unidades de rede nas virtual machines. No cenário, este produto substituiria o servidor de ficheiros do supermercado, permitindo aos departamentos aceder aos ficheiros partilhados de forma segura e sincronizada.

### 6.4 Bases de Dados Relacionais

| Provedor     | Produto      | Vantagens                                  | Desvantagens                             |
|--------------|--------------|--|--|
| <i>AWS</i>   | RDS          | Suporte a vários motores de bases de dados | Complexidade na configuração             |
| <i>Azure</i> | SQL Database | Integração com AD                          | Custo mais elevado em planos escaláveis  |
| <i>GCP</i>   | Cloud SQL    | Utilização simples                         | Suporta poucos motores de bases de dados |

Tabela 4: Bases de Dados Relacionais

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *AWS*, face à sua flexibilidade entre motores de bases de dados, alta disponibilidade e boa performance. Este serviço seria capaz de armazenar dados dos clientes, históricos de compras, inventário e faturação.

## 6.5 Bases de Dados NoSQL

| Provedor | Produto   | Vantagens                                    | Desvantagens   |
|----------|-----------|--|--|
| AWS      | DynamoDB  | Alta performance e escalabilidade automática | Modelo de dados rígido e custos imprevisíveis em grandes volumes |
| Azure    | Cosmos DB | Latência baixa e alta disponibilidade global | Custo elevado e complexidade de configuração inicial             |
| GCP      | Firestore | Simples e serverless                         | Menos controlo sobre desempenho                                  |

Tabela 5: Base de Dados NoSQL

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *AWS*, face à sua rapidez e escalabilidade. No cenário, este produto armazenaria os eventos dos dispositivos IoT em tempo real e poderia ser usado para sessões *guest* na loja online do supermercado.

## 6.6 Aplicações Comerciais

| Provedor | Produto           | Vantagens                                    | Desvantagens                              |
|----------|-------------------|--|---|
| AWS      | Elastic Beanstalk | Escalabilidade Automática e Simples de usar  | Pouco personalizável                      |
| Azure    | App Service       | Fácil de integrar e suporte nativo para .NET | Otimização dependente de boas práticas    |
| GCP      | App Engine        | Totalmente serverless                        | Pouco controlo sobre ambiente de execução |

Tabela 6: Aplicações Comerciais (E-commerce)

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *Azure*, isto se a organização tivesse aplicações desenvolvidas, principalmente, em *.NET* e utilizasse mais sistemas *Microsoft*. Este serviço hospedaria o site do supermercado.

## 6.7 IoT

| Provedor | Produto  | Vantagens                            | Desvantagens                       |
|----------|--|--------------------------------------|------------------------------------|
| AWS      | IoT Core   | Suporte MQTT e encriptação integrada | Curva de aprendizagem elevada      |
| Azure    | IoT Hub  | Boa política de dispositivos         | Preços elevados com cargas grandes |
| GCP      | Descontinuado o <i>Google Cloud IoT Core</i> e substituído pelo ClearBlade | —                                    | —                                  |

Tabela 7: IoT

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela AWS, face à sua robustez com os protocolos MQTT, TLS e HTTP e face à sua escalabilidade. No cenário, este produto garantiria a comunicação segura com sensores de temperatura, câmaras, terminais de pagamento e dispositivos inteligentes.

## 6.8 Microserviços

| Provedor | Produto | Vantagens                                 | Desvantagens   |
|----------|---------|---|--|
| AWS      | EKS     | Altamente escalável e suporte empresarial | Requer experiência com Kubernetes e complexidade de gestão inicial |
| Azure    | AKS     | Gestão automatizada de nós                | Tempos de arranque mais lentos                                     |
| GCP      | GKE     | Ótima performance e escalabilidade        | Curva de aprendizagem grande                                       |

Tabela 8: Microserviços

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela Azure, face à gestão automática de clusters. No cenário em questão, este produto seria ideal para gerir múltiplos pontos de venda (venda em reatalho).

## 6.9 Backup e Recuperação

| Provedor | Produto      | Vantagens                                | Desvantagens                          |
|----------|--------------|--|---------------------------------------|
| AWS      | AWS Backup   | Centralizado                             | Gestão requer componente mais técnica |
| Azure    | Azure Backup | Interface simples e recuperação granular | Custo elevado                         |
| GCP      | Backup & DR  | Integrado com Cloud SQL                  | Funcionalidades Limitadas             |

Tabela 9: Backup e Recuperação

Neste caso, para o cenário em questão, talvez a solução mais adequada seria a proposta pela *Azure*, face à sua simples configuração e suporte com máquinas virtuais. Relacionando com o cenário, este produto faria o backup automático dos servidores e garantiria uma recuperação fácil e rápida, caso necessário.

## 6.10 Políticas de Segurança

| Provedor | Produto                     | Vantagens  | Desvantagens   |
|----------|-----------------------------|--|--|
| AWS      | AWS Organizations           | Permite aplicar políticas a múltiplas contas e força regras de segurança | Curva de aprendizagem elevada e configuração complexa.             |
| Azure    | Azure Policy                | Criação de políticas de conformidade e avaliação contínua                | Requer conhecimento técnico avançado para criar políticas eficazes |
| GCP      | Organization Policy Service | Controla comportamentos nos projetos                                     | Interface menos intuitiva e funcionalidades mais limitadas         |

Tabela 10: Políticas de Segurança

## 6.11 Controlos de Acesso

| Provedor | Produto                    | Vantagens  | Desvantagens  |
|----------|----------------------------|--|---|
| AWS      | IAM                        | Controlo detalhado com políticas, suporte a MFA e integração com <i>Security Token Service</i> e <i>Single Sign-On</i> | Políticas podem ser complexas e difíceis de auditar manualmente |
| Azure    | Azure Active Directory B2C | Suporte a SSO, MFA, grupos e identidades híbridas  | Custo elevando para funcionalidades avançadas                   |
| GCP      | Cloud IAM                  | Gestão de permissões por função e projeto  | Menos detalhe em algumas permissões                             |

Tabela 11: Controlos de Acesso

## 6.12 Monitorização e Detecção de Ameaças

| Provedor | Produto                                 | Vantagens  | Desvantagens  |
|----------|---|--|---|
| AWS      | GuardDuty + CloudTrail + CloudWatch     | Detecção baseada em inteligência de ameaças; Integração com logs e alertas; Análise comportamental | Pode gerar falsos positivos; Requer detalhe para alertas eficazes |
| Azure    | Microsoft Defender for Cloud + Sentinel | Detecção de ameaças em tempo real; Correlação de eventos com MITRE ATT&CK                          | Custo Elevado   |
| GCP      | Security Command Center + Cloud Logging | Visibilidade centralizada  | Funcionalidades avançadas requerem versão mais custosa            |

Tabela 12: Monitorização e Detecção de Ameaças

## 6.13 Educação e Consciencialização

| Provedor | Produto                                   | Vantagens  | Desvantagens   |
|----------|---|--|--|
| AWS      | AWS Skill Builder + Well-Architected Tool | Cursos técnicos e de boas práticas em segurança e arquitetura cloud e gratuito em grande parte | Foco técnico e não cobre campanhas de consciencialização organizacional    |
| Azure    | Microsoft Learn                           | Plataforma educativa com <i>kits</i> prontos para sensibilização interna                       | <i>Toolkit</i> depende de iniciativa da organização e não é automatizado   |
| GCP      | Google Cloud Skills Boost                 | Formação técnica e prática com laboratórios hands-on, baseado em desafios reais                | Foco no utilizador técnico, sem módulos empresariais de consciencialização |

Tabela 13: Educação e Consciencialização

## 6.14 Encriptação

| Provedor | Produto  | Vantagens  | Desvantagens  |
|----------|--|--|---|
| AWS      | Amazon EBS Encryption / Amazon S3 Server-Side Encryption (SSE) | Encriptação automática em volumes e objetos e integração com outros serviços AWS                                     | Pode exigir configuração adicional para integração com outras aplicações e custos adicionais em algumas opções      |
| Azure    | Azure Disk Encryption, Azure Storage Service Encryption        | Suporte nativo para BitLocker e DM-Crypt, integração com Azure VM e Blob, encriptação transparente para o utilizador | Menor controlo sobre os parâmetros avançados de encriptação, limites em performance de discos com encriptação ativa |
| GCP      | Google Cloud Skills Boost                                      | Encriptação automática por padrão, simplicidade na gestão e baixa latência de leitura/escrita                        | Menor personalização dos mecanismos de encriptação e menos opções de configuração comparado com o AWS               |

Tabela 14: Encriptação

## 6.15 Gestão de Chaves

Nesta secção, revela-se a importância da gestão de chaves num ambiente em cloud, principalmente para cenário em questão. Dados pessoais, inventário, transações financeiras, backups e comunicações entre dispositivos IoT são o tipo de dados sensíveis que esta solução procura proteger.

A gestão de chaves procura permitir encriptar dados em repouso ou em trânsito, controlar quem pode usar as chaves e auditar o uso das mesmas.

| Provedor     | Produto                     | Vantagens   | Desvantagens   |
|--------------|-----------------------------|---|--|
| AWS          | AWS Key Management Service  | Integração com IoT e Alta escalabilidade  | Custos elevados e Gestão detalhada exige conhecimento técnico    |
| Azure        | Azure Key Vault             | Permite rotação automática  | Mais controlos avançados requerem o uso de políticas específicas |
| Google Cloud | Google Cloud Key Management | Integração com Cloud Storage e Suporte a chaves geridas pelo cliente ou Google; API simples | Algumas funcionalidades requerem uma versão mais dispendiosa     |

Tabela 15: Gestão de Chaves na Cloud

## 7 Frameworks

Nesta secção, o objetivo será descrever a importância da aplicação dos diferentes controlos, propostos pelas cinco *frameworks* de segurança abordadas para este cenário.

### 7.1 NIST CSF

A *NIST CSF* (*National Institute of Standards and Technology - Cybersecurity Framework*), é uma referência central desenvolvida visando gerir e reduzir riscos associados à cibersegurança. Esta *framework* tem como principais áreas de Identificar, Proteger, Detetar, Responder e Recuperar.

#### 7.1.1 Relação com o Cenário

No contexto do supermercado a aplicação da NIST permite estabelecer uma estrutura clara e eficaz da gestão da segurança da informação com base no ambiente híbrido adotado. A *framework* em questão permite mitigar riscos operacionais e garantir que os sistemas são resilientes, dando suporte a operações como e-commerce, pontos de venda, gestão de stock e dispositivos IoT.

De modo a dar a entender a relação desta *framework* com o cenário, são apresentadas as principais ações associadas a cada uma das cinco funções da NIST.

- **Identificar** - Mapeamento de ativos críticos como por exemplo servidores em cloud, além de análise de risco contínua para cada componente migrado para a cloud.
- **Proteger** - Implementação de políticas de controlo de acesso, encriptação de dados sensíveis e uso de firewalls cloud para a proteção de sistemas críticos. Aplicação de políticas de backups automáticos e segmentação de redes.
- **Detetar** - Monitorização contínua com ferramentas SIEM, com base em indicadores de compromisso. Integração com modelos como o MITRE ATT&CK para deteção de táticas conhecidas.
- **Responder** - Desenvolvimento de planos de resposta a incidentes que envolvem dados de clientes ou interrupção de serviços essenciais, incluindo contacto com fornecedores de cloud.
- **Recuperar** - Definição de estratégias de recuperação de sistemas através de snapshots, recuperação automatizada de backups e failover para garantir a continuidade dos serviços durante um incidente ou desastre.

Desta forma, a NIST proporciona uma abordagem sistemática e adaptável que são pontos essenciais para garantir a segurança e continuidade dos serviços digitais no cenário em questão, mantendo também a confiança dos clientes e a integridade das operações da organização.

## 7.2 ISO/IEC 27001

A *ISO/IEC 27001* é uma norma que procura padronizar a gestão da segurança da informação. Deste modo, foca-se em ajudar as organizações a proteger os seus ativos de informação, como dados dos clientes, documentos, sistemas e comunicações da organização, através de um Sistema de Gestão de Segurança da Informação (SGSI).

O principal foco desta *framework* baseia-se na tríade da cibersegurança, sendo esta, a **Confidencialidade, Integridade e Disponibilidade**.

### 7.2.1 Relação com o Cenário

Na relação com o cenário esta framework pode ser aplicada como uma base para a gestão da segurança da informação, trazendo benefícios diretos nas vertentes a seguir representadas:

- **Política de Segurança** - Estabelecimento de políticas de segurança claras e obrigatórias para todas as áreas, garantindo a gestão de forma adequada da informação crítica da organização.
- **Gestão de Riscos** - Identificação e avaliação de riscos associados aos sistemas migrados para cloud e definição de planos de tratamento adequados, incluindo mitigação, aceitação ou transferência de risco.
- **Controlo de Acessos** - Definição de regras de controlo de acessos com base na necessidade funcional, tanto para ambientes cloud como para a infraestrutura local.
- **Conformidade e Auditoria** - Criação de processos para auditorias internas regulares e controlo documental, essenciais para manter a conformidade com a norma e demonstrar boas práticas a clientes e parceiros.
- **Melhoria Contínua** - Adoção do ciclo PDCA (*Plan-Do-Check-Act*) para garantir que os mecanismos de segurança se mantêm eficazes e em evolução, conforme surgem novas ameaças ou alterações na infraestrutura.

Com isto a organização garante uma abordagem estruturada e reconhecida internacionalmente para a gestão da segurança da sua informação, o que é fundamental num ambiente de trabalho híbrido onde existem tanto recursos locais como em cloud.

## 7.3 CIS Controls

A *CIS Controls* (*Center of Internet Security Controls*), é uma *framework* que consiste em 18 controlos de segurança práticos, criados com o intuito de ajudar as organizações a detetar, proteger e responder a ameaças. Estes controlos são atualizados de modo a manterem-se alinhados com as ameaças emergentes do dia-a-dia, na área da cibersegurança.

### 7.3.1 Relação com o Cenário

Na existência de coabitAÇÃO de servidores tanto locais como na cloud os CIS Controls são relevantes na medida que oferecem ações concretas e facilmente implementáveis que fortalecem a segurança da infraestrutura híbrida.

- **Inventário e Controlo de Ativos** - Aplicação de controlos para manter um registo atualizado dos ativos locais e na cloud, de forma a garantir que apenas sistemas autorizados estão ativos.
- **Configuração Segura de Sistemas e Cloud** - Adoção dos *CIS Benchmarks* específicos para plataformas cloud, assegurando que as máquinas virtuais, bases de dados e servidores de aplicações são lançados com configurações seguras por padrão.
- **Gestão de Contas e Privilégios** - Estabelecimento de controlo rigoroso sobre contas de utilizador e privilégios administrativos, aplicando o princípio do menor privilégio tanto localmente como na cloud.
- **Gestão de Vulnerabilidades** - Uso de ferramentas automáticas para identificar e corrigir vulnerabilidades nos sistemas cloud, com base nos controlos CIS.
- **Monitorização Contínua** - Implementação de soluções de monitorização de logs e alertas, permitindo a deteção rápida de comportamentos anómalos ou acessos indevidos.

A adoção dos CIS Controls proporciona uma base técnica sólida, eficiente e compatível com os recursos da organização, facilitando a proteção da infraestrutura cloud.

## 7.4 COBIT

A **COBIT** (*Control Objectives for Information and Related Technologies*) é uma *framework* de governança e gestão de TI, que abrange também a segurança cibernética. Esta referência fornece um conjunto de práticas e estruturas para garantir a segurança e confiabilidade dos sistemas de informação.

### 7.4.1 Relação com o Cenário

O COBIT acaba por desempenhar um papel essencial na governança da mitigação para a cloud assim como na gestão estratégica da segurança da informação.

- **Alinhamento com os Objetivos do Negócio** - O COBIT permite garantir que a adoção de soluções cloud e medidas de segurança não são decisões isoladas da equipa de IT, mas sim parte de um plano alinhado com a visão estratégica do supermercado.
- **Gestão de Riscos de IT** - Apoia na identificação, avaliação e resposta a riscos tecnológicos, incluindo aqueles relacionados com disponibilidade de serviços cloud, conformidade legal e continuidade de negócio.
- **Monitorização de Desempenho** - Define indicadores de desempenho e conformidade para serviços migrados para a cloud, como uptime do site, tempos de resposta de APIs e eficácia dos backups automáticos.
- **Responsabilidades Claras** - Ajuda a distribuir responsabilidades entre as várias áreas da organização, definindo papéis de decisão e controlo sobre os ativos digitais.
- **Otimização de Recursos** - Apoia a gestão de recursos tecnológicos e humanos de forma eficaz, com o objetivo de evitar duplicações de sistemas, controlando custos com serviços cloud e promovendo a inovação de forma sustentável.

No cenário em questão a aplicação do COBIT proporciona um modelo de governança estruturado que é essencial para garantir que a transição para a cloud é segura, eficiente e integrada com os objetivos de negócio da organização.

## 7.5 MITRE ATT&CK

A *MITRE ATT&CK* é uma *framework* que contém o conhecimento base de táticas e técnicas utilizadas pelos atacantes. Atua fornecendo uma matriz detalhada de técnicas de ataque, fornecendo às organizações, formas sobre como atuam os atores maliciosos.

### 7.5.1 Relação com o Cenário

A aplicação do MITRE ATT&CK permite detetar e responder a comportamentos maliciosos com maior precisão, otimizando a postura de segurança da organização, sobretudo em ambientes onde coexistem infraestruturas locais e em cloud.

- **Criação de Casos de Uso no SIEM** - Com base nas técnicas da matriz ATT&CK, é possível configurar regras de deteção em ferramentas SIEM para identificar atividades anómalas, como movimentos laterais entre máquinas virtuais ou tentativas de acesso a contas privilegiadas.
- **Proteção da Infraestrutura Cloud** - Técnicas como *Valid Accounts* (*T1078*) ou *Credential Dumping* (*T1003*) são aplicáveis ao contexto cloud do supermercado, permitindo que sejam monitorizadas tentativas de acesso indevido à base de dados ou ao portal de e-commerce.
- **Análise de Comportamento em IoT** - A ATT&CK for Enterprise inclui técnicas associadas a exploração de dispositivos IoT. Isso permite detetar comportamentos anómalos em sensores, câmaras ou leitores RFID que fazem parte da logística e controlo de qualidade.
- **Simulação de Ataques** - Com base nas técnicas da ATT&CK, podem ser realizados exercícios de *red teaming* ou testes de penetração simulando ataques realistas para validar a eficácia dos controlos implementados.
- **Apoio à Resposta a Incidentes** - Durante uma resposta a incidente, a identificação de técnicas específicas permite mapear o progresso do atacante, prever próximos passos e aplicar medidas de contenção mais eficazes.

A utilização do MITRE ATT&CK fornece à equipa de segurança do supermercado uma abordagem tática e orientada por inteligência, permitindo melhorar significativamente as capacidades de deteção e resposta a ataques nos seus ambientes híbridos.

## 8 Matriz de Direito

| Serviço / Acesso                 | Admin TI | Infra Cloud | Gestor Loja | Operador POS | Técnico IoT | Analista Dados | RH | Util. Comum | Auditor |
|----------------------------------|----------|-------------|-------------|--------------|-------------|----------------|----|-------------|---------|
| Servidor DNS                     | G        | G           | X           | X            | X           | X              | X  | X           | L       |
| Servidor DHCP                    | G        | G           | X           | X            | X           | X              | X  | X           | L       |
| Active Directory                 | G        | G           | G           | X            | X           | X              | G  | X           | L       |
| Servidor Web                     | G        | G           | L           | L            | L           | L              | L  | L           | L       |
| Gestor de Ficheiros              | G        | G           | C/E/L       | X            | X           | L              | L  | L           | L       |
| Servidor IoT                     | G        | L           | X           | X            | G           | X              | X  | X           | L       |
| Servidor de Backup               | G        | G           | X           | X            | X           | X              | X  | X           | L       |
| Base de Dados Comercial          | G        | G           | L           | X            | X           | L              | X  | X           | L       |
| Servidor de Atualizações         | G        | G           | X           | X            | A           | X              | X  | X           | L       |
| Aplicações Comerciais (ERP, POS) | G        | L           | U/A         | U            | X           | L              | L  | X           | L       |
| Servidor VoIP                    | G        | L           | U           | U            | U           | U              | U  | U           | L       |
| Servidor de Impressão            | G        | L           | U           | U            | X           | U              | U  | U           | L       |
| Análise de Dados                 | G        | L           | L           | X            | X           | G              | X  | X           | L       |

Tabela 16: Matriz de Direito

### Legenda:

- **G** – Gestão completa (configuração, manutenção e permissões)
- **C** – Criar (ficheiros ou dados)
- **E** – Editar (modificar dados existentes)
- **L** – Ler (acesso de leitura/consulta)
- **U** – Utilizar (executar funcionalidade, sem alterar dados)
- **A** – Atualizar (aplicar atualizações técnicas)
- **X** – Sem acesso

## 8.1 Grupos

| Grupo de Acesso Cloud  | Perfis Incluídos   | Serviços Acedidos   |
|------------------------|--|---|
| TI-Admin               | Administrador de Sistemas, Gestor de Segurança de Infraestrutura, Técnico de Redes | Todos os serviços críticos: DNS, DHCP, AD, ERP, IoT, BD, backups, atualizações, firewall, gestão de cloud |
| Infraestrutura Cloud   | Gestor de Infraestrutura Cloud, Administrador de Backups                           | Gestão de VMs, redes, backups, firewall, armazenamento, logging, segurança cloud                          |
| TI-IoT                 | Técnico IoT  | Servidor IoT, atualizações de dispositivos, comunicação com sensores                                      |
| Gestão-Operações       | Gestor de Loja, Assistente de Operações, Supervisor de Ecommerce                   | Aplicações comerciais (ERP/POS), relatórios de vendas, gestão de ficheiros                                |
| Vendas-POS             | Operador POS, Formador POS   | POS, impressão de talões, comunicações VoIP   |
| Analistas-Dados        | Analista de Dados  | BI, base de dados, dashboards internos, leitura de ficheiros  |
| Recursos Humanos (RH)  | RH, Técnico de Formação  | Aplicações comerciais, documentos de RH, relatórios internos, ficheiros partilhados                       |
| Utilizadores Comuns    | Utilizador Comum, Colaborador Remoto   | Intranet, impressão, email corporativo, pasta pessoal de ficheiros  |
| Auditória / Compliance | Auditor  | Logs, métricas, relatórios de acesso, firewalls, eventos cloud  |

Tabela 17: Grupos para Implementação na Cloud

## 9 Firewall

Assim como na infraestrutura local, a migração da rede do supermercado para a cloud também necessita da implementação de mecanismos de segurança robustos para garantir a integridade, confidencialidade e disponibilidade dos serviços da organização. Deste modo, a implementação de *firewalls* no ambiente *cloud* é crucial.

Tal como numa infraestrutura local, as *firewalls* na *cloud* também desempenham um papel de proteção contra acessos indevidos, ataques internos ou externos e permitem ainda uma segmentação segura das redes, dentro da infraestrutura. Aquilo que distingue as *firewalls* em *cloud* das locais é a sua gestão, como serviços, por parte das plataformas de *cloud* pública, que apresenta uma alta disponibilidade e escalabilidade.

Para o cenário em questão, a implementação das *firewalls* em *cloud* procuram filtrar o tráfego entre as redes virtuais da organização e proteger as aplicações web contra ataques ou acessos indevidos. Esta abordagem procura complementar com as necessidades da organização, que envolvem a interligação entre a sede, sucursal e trabalhadores remotos, sistemas de pontos de venda, aplicações comerciais, sensores IoT e agora, armazenamento em *cloud*.

Assim como todos os pontos abordados no relatório, este tópico irá apontar os recursos mais relevantes ao cenário do supermercado das três soluções de *cloud* existentes, *Microsoft Azure*, *AWS* e *Google Cloud Platform*.

### 9.1 Microsoft Azure

#### 9.1.1 Tipo de Azure Firewall

Numa análise comparativa entre os tipos de *firewalls* que a *Microsoft Azure* oferece, entende-se que a solução mais viável ao cenário do supermercado é o **Azure Firewall Standard**, pois numa relação entre custo e funcionalidades, é a proposta mais completa, visto que a diferença para o **Azure Firewall Premium** é a falta de inspeção a tráfego encriptado (TLS), algo que o cenário não prioriza.

### 9.1.2 Serviços a ser Protegidos pela Azure Firewall

De modo a apoiar a decisão pela *Azure Firewall Standard*, é apresentada uma tabela abaixo com os serviços que se procuram proteger com a aquisição deste serviço e a sua aplicação prática no contexto do cenário.

| Serviço a ser Protegido  | Aplicação Prática                              |
|--------------------------|--|
| VMs, POS e Base de Dados | Controlar Comunicações entre Sub-redes         |
| Armazenamento            | Bloquear Acessos Externos à Base de Dados      |
| Dispositivos IoT         | Isolar Dispositivos IoT da Rede Administrativa |
| Acesso Remoto            | Utilizar Regras SNAT/DNAT                      |
| Aplicações Web           | Proteger contra Ataques                        |
| Backups                  | Garantir que Backups estão Seguros             |

Tabela 18: Serviços a ser Protegidos - Azure Firewall Standard

### 9.1.3 Ferramentas Azure a Implementar com Firewall

| Ferramentas Azure         | Função   |
|---------------------------|--|
| Azure Firewall Standard   | Controlo do Tráfego entre sub-redes e internet |
| Azure Firewall Manager    | Gestão de Políticas                            |
| Azure Application Gateway | Protecção das Aplicações Web                   |
| Azure DDoS Protection     | Mitigação de Ataques                           |
| Network Security Groups   | Controlos por Sub-redes                        |
| Route Tables              | Definir que Tráfego passa pela firewall        |
| Azure Monitor             | Análise e Registo de Tráfego                   |

Tabela 19: Ferramentas Azure a Implementar com Firewall

## 9.2 AWS

### 9.2.1 Tipo de AWS Firewall

Após a comparação dos serviços oferecidos pelas diferentes *firewalls* por parte da AWS, optou-se por selecionar o serviço *AWS Network Firewall*. A selecção deste produto focou-se nas diversas funcionalidades que oferece, como é o exemplo da integração nativa com *VPCs*.

No cenário do supermercado, a escolha deste serviço servirá de apoio para o controlo das comunicações internas entre as diferentes sub-redes da organização. O apoio dado na área de configuração de políticas é também uma vantagem deste serviço.

### 9.2.2 Serviços a ser Protegidos pela AWS Firewall

De modo a apoiar a decisão pela *AWS Network Firewall*, é apresentada uma tabela abaixo com os serviços que se procuram proteger com a aquisição deste serviço e a sua aplicação prática no contexto do cenário.

| Serviço a ser Protegido | Aplicação Prática                              |
|-------------------------|--|
| VMs, ERP e POS          | Controlar Zonas Críticas                       |
| Armazenamento           | Bloquear Acessos Externos à Base de Dados      |
| Dispositivos IoT        | Isolar Dispositivos IoT da Rede Administrativa |
| Acesso Remoto           | Utilizar Regras SNAT/DNAT                      |
| Aplicações Web          | Proteger contra Ataques                        |
| Backups                 | Garantir que Backups estão Seguros             |

Tabela 20: Serviços a ser Protegidos - Azure Firewall Standard

### 9.2.3 Ferramentas AWS a Implementar com Firewall

| Ferramentas AWS      | Função   |
|----------------------|--|
| AWS Network Firewall | Controlo do Tráfego entre sub-redes e internet |
| AWS Firewall Manager | Gestão de Políticas                            |
| AWS WAF              | Proteção de APIs e Loja Online                 |
| AWS Shield           | Mitigação de Ataques                           |
| Security Groups      | Regras de Acesso                               |
| Network ACLs         | Regras Stateless Complementares                |
| CloudWatch Logs      | Análise de Tráfego e Eventos de Segurança      |

Tabela 21: Ferramentas AWS a Implementar com Firewall

## 9.3 Google Cloud Platform

### 9.3.1 Tipo de GCP Firewall

Com base no mesmo princípio de seleção usado para os fornecedores anteriores, foi selecionado o serviço *Padrão de NGFW do Cloud*, no lugar do mais avançado, *NGFW para empresas de nuvem*, pois a diferença entre os mesmos não justifica um investimento maior nesta altura, face ao cenário do supermercado em questão. O complemento deste serviço com outros de proteção e monitorização adequam-se mais ao cenário.

No cenário do supermercado, a escolha deste serviço servirá de apoio para o controlo das comunicações internas entre as diferentes sub-redes da organização. O apoio dado na área de configuração de políticas é também uma vantagem deste serviço.

### 9.3.2 Serviços a ser Protegidos pela Firewall da GCP

De modo a apoiar a decisão pelo serviço *Padrão de NGFW do Cloud*, é apresentada uma tabela abaixo com os serviços que se procuram proteger com a aquisição deste serviço e a sua aplicação prática no contexto do cenário.

| Serviço a ser Protegido | Aplicação Prática                                   |
|-------------------------|---|
| ERP e POS               | Controlar Tráfego entre Sub-redes de Venda e Gestão |
| Dispositivos IoT        | Isolar Dispositivos IoT da Rede Administrativa      |
| Loja Online             | Proteger contra Ataques                             |
| Acesso Remoto           | Garantir Acesso Seguro à Infraestrutura             |
| Backups                 | Garantir que Backups estão Seguros                  |

Tabela 22: Serviços a ser Protegidos - NGFW Padrão

### 9.3.3 Ferramentas GCP a Implementar com Firewall

| Ferramentas GCP      | Função                                   |
|----------------------|--|
| NGFW Padrão do Cloud | Regras de Firewall e Controlo de Tráfego |
| Google Cloud Armor   | Proteção para Apps e APIs Web            |
| AWS WAF              | Proteção de APIs e Loja Online           |
| AWS Shield           | Mitigação de Ataques                     |
| HTTPS Load Balancer  | Proteção do Tráfego na Loja Online       |
| IAM                  | Controlar Acesso Remoto                  |

Tabela 23: Ferramentas GCP a Implementar com Firewall

## 10 Resposta a Incidentes

Com a migração de alguns serviços críticos para a cloud, o supermercado passa a depender de um ambiente digital altamente dinâmico e exposto a novas ameaças. Nesse contexto, a resposta a incidentes torna-se um pilar fulcral da estratégia de segurança, principalmente quando os incidentes em cloud tendem a propagar-se mais rapidamente e a envolver múltiplos componentes distribuídos.

Ao contrário dos ambientes locais, a cloud exige que a resposta a incidentes seja automática, escalável e integrada com os serviços nativos dos fornecedores cloud. A rápida deteção, contenção eficiente e a recuperação imediata são essenciais para garantir que interrupções, acessos indevidos ou até mesmo perda de dados não comprometam o funcionamento dos sistemas. Além disto, num ambiente cloud, a responsabilidade pela segurança é partilhada entre o provedor e a organização, sendo que embora a infraestrutura física seja protegida pela cloud, a configuração de permissões, monitorização de acessos e resposta a incidentes continua a ser da responsabilidade do supermercado.

Com base nisso, é necessário definir um plano de resposta a incidentes específico para o ambiente cloud que seja baseado em três eixos, sendo eles o processo, pessoas e tecnologia, de forma a garantir uma abordagem coordenada, eficiente e alinhada com as boas práticas de cibersegurança.

### 10.1 Processo e Pessoas

A resposta a incidentes em cloud no cenário do supermercado "Products A Lot" exige um processo estruturado, baseado em seis fases (segundo o NIST SP 800-61 Rev. 2), e articulado com as responsabilidades reais dos perfis definidos na organização. Esta relação entre processo e pessoas garante que cada tipo de incidente em serviços cloud migrados (como base de dados, SPW, IoT e backup) seja tratado por quem tem as permissões adequadas, conforme definido na matriz de direito.

- **Preparação**

**Objetivo:** Estabelecer os mecanismos de prevenção, deteção e reação a incidentes nos serviços cloud.

**Responsáveis:**

- **Admin Sistemas** – configura alertas, logging e permissões nas máquinas virtuais na cloud.
- **Gestor de Loja** – valida o impacto dos serviços cloud na operação (e-commerce, POS).
- **Técnico IoT** – prepara monitorização para os dispositivos ligados ao servidor IoT na cloud.

- **Deteção e Análise**

**Objetivo:** Identificar rapidamente anomalias nos sistemas cloud e classificá-las.

**Responsáveis:**

- **Admin Sistemas** – consulta logs das instâncias cloud e valida alertas.
- **Técnico IoT** – analisa tráfego ou comportamento irregular nos sensores integrados na cloud.

- **Contenção**

**Objetivo:** Isolar sistemas ou componentes afetados para limitar o impacto do incidente.

**Responsáveis:**

- **Admin Sistemas** – isola VMs ou containers afetados, revoga acessos temporariamente.
- **Gestor de Loja** – comunica a suspensão temporária de serviços às equipas de operação.
- **Técnico IoT** – coopera na remoção de dispositivos em potencial risco.

- **Erradicação**

**Objetivo:** Eliminar o vetor de ataque e restaurar configurações seguras.

**Responsáveis:**

- **Admin Sistemas** – repõe serviços com base em snapshots seguros ou recriação de instâncias.
- **Técnico IoT** – reconfigura dispositivos afetados ou remove firmware comprometido.
- **Analista de Dados** – verifica integridade dos dados restaurados após o incidente.

- **Recuperação**

**Objetivo:** Retomar a operação normal de forma segura.

**Responsáveis:**

- **Admin Sistemas** – reativa serviços migrados (SPW, BD, backups) e testa conectividade.
- **Gestor de Loja** – valida que os sistemas de vendas estão totalmente funcionais.
- **Analista de Dados** – confirma a continuidade dos relatórios e dashboards operacionais.

- **Lições Aprendidas**

**Objetivo:** Rever o incidente e implementar melhorias.

**Responsáveis:**

- **Admin Sistemas** – documenta falhas técnicas e propõe atualizações de segurança.
- **Gestor de Loja** – avalia impacto do incidente no negócio e comunica com as áreas envolvidas.
- **RH (Recursos Humanos)** – pode intervir em campanhas internas de formação ou sensibilização, se a origem do incidente estiver relacionada com erro humano.

## 10.2 Tecnologia

Embora a resposta a incidentes dependa fortemente de processos bem definidos e de uma equipa capacitada, esta também está diretamente relacionada com as ferramentas tecnológicas disponíveis no ambiente cloud. No nosso cenário do supermercado a utilização de soluções específicas dos fornecedores cloud permite uma deteção mais rápida, uma contenção automatizada e uma recuperação mais eficiente dos serviços migrados para a cloud.

Abaixo são apresentadas as principais tecnologias aplicáveis ao contexto do cenário:

- **Monitorização e Deteção de Ameaças**

- **AWS GuardDuty, Azure Defender for Cloud, Google SCC** – Deteção de comportamentos anómalos e chamadas suspeitas.
- **CloudTrail / Log Analytics / Cloud Logging** – Recolha e análise detalhada dos logs de atividade nos recursos migrados.

- **Resposta Automatizada**

- **AWS Systems Manager, Azure Logic Apps + Playbooks** – Automatização de tarefas de contenção, como isolamento de instâncias, revogação de chaves ou aplicação de regras de firewall.

- **Recuperação e Continuidade**

- **Snapshots Automáticos e Backup Services** – AWS Backup, Azure Backup, GCP Backup & DR - permitem a rápida recuperação dos servidores afetados, garantindo a integridade dos dados e a continuidade das operações.

- **Gestão de Acessos e Autenticação**

- **IAM com MFA (Multi-Factor Authentication)** – Gestão detalhada de permissões e autenticação forte para reduzir o risco de movimentação lateral em caso de incidente.
- **Azure Active Directory B2C** – Integração com autenticação cloud, com suporte para Single Sign-On e políticas adaptáveis de acesso.

- **Gestão de Chaves e Encriptação**

- **AWS KMS, Azure Key Vault, Google Cloud KMS** – Gestão e rotação segura de chaves de encriptação para proteger dados sensíveis em repouso e em trânsito.

## 11 Conclusão

Com a redação deste relatório, foi possível apresentar uma estratégia detalhada para a migração da infraestrutura do cenário em questão, no caso, supermercado, para a cloud, assegurando a continuidade das operações e o reforço da sua segurança, face ao atingido na fase anterior com a estruturação da rede local. Partindo de uma análise à infraestrutura local, identificaram-se os principais serviços a migrar, assim como os que deverão permanecer no local, promovendo uma abordagem híbrida eficiente e de acordo com o cenário.

A escolha do modelo **IaaS** revelou-se a mais adequada, dado o objetivo de manter o controlo direto sobre a configuração e gestão dos servidores, replicando na cloud a estrutura da rede já existente, ganhando vantagem em termos de flexibilidade, escalabilidade e robustez. Foram ainda considerados os principais fornecedores de cloud (AWS, Azure e GCP), identificando os produtos mais adequados para cada componente do sistema, tendo em conta critérios técnicos e a sua relação com o cenário em questão.

Adicionalmente, abordaram-se aspectos fundamentais da segurança na cloud, como políticas de acesso, monitorização, firewall, gestão de chaves e resposta a incidentes, garantindo a proteção dos dados e serviços da organização. A implementação de frameworks como a NIST, ISO 27001, CIS Controls, COBIT e MITRE ATT&CK fortaleceu ainda mais a abordagem adotada, assegurando o alinhamento com boas práticas e padrões estipulados internacionalmente.

A estruturação de grupos de acesso, a matriz de direitos e os controlos de segurança propostos permitem garantir um modelo de gestão robusto e adaptado à realidade do supermercado, com foco na proteção dos ativos digitais e na garantia da continuidade do negócio.

Em suma, este trabalho representa, não apenas uma proposta técnica de migração, mas uma visão de segurança e gestão eficaz em ambientes cloud.

Como maiores obstáculos aliados à realização deste projeto, destacam-se a seleção dos produtos dos diferentes fornecedores, devido ao pouco conhecimento desta área e soluções disponíveis, o desenvolvimento da matriz de direito e dos respetivos grupos e consequentemente a sua aplicação prática nas plataformas dos fornecedores, visto ter sido a primeira interação dos elementos do grupo com estas tecnologias.

## 12 Anexos

### Anexo 1 - Configuração User Groups AWS

| User groups (9) <small>Info</small> |                                      |           |                      |                   |
|-------------------------------------|--------------------------------------|-----------|----------------------|-------------------|
|                                     | Group name                           | ▲   Users | ▼   Permissions      | ▼   Creation time |
| <input type="checkbox"/>            | <a href="#">Analistas-Dados</a>      | 1         | <span>Defined</span> | 28 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Auditoria</a>            | 1         | <span>Defined</span> | 26 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Gestao-Operacoes</a>     | 3         | <span>Defined</span> | 30 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Infraestrutura-Cloud</a> | 2         | <span>Defined</span> | 32 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Recursos-Humanos</a>     | 2         | <span>Defined</span> | 27 minutes ago    |
| <input type="checkbox"/>            | <a href="#">TI-Admin</a>             | 3         | <span>Defined</span> | 35 minutes ago    |
| <input type="checkbox"/>            | <a href="#">TI-IoT</a>               | 1         | <span>Defined</span> | 31 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Utilizadores-Comuns</a>  | 2         | <span>Defined</span> | 27 minutes ago    |
| <input type="checkbox"/>            | <a href="#">Vendas-POS</a>           | 2         | <span>Defined</span> | 29 minutes ago    |

Figura 3: Grupos - AWS

| Users (17) <a href="#">Info</a>  |   |   |      |   |               |
|--|---|---|------|---|---------------|
| An IAM user is an identity with long-term credentials that is used to interact with AWS in an account. |   |   |      |   |               |
| <input type="text"/> <a href="#">Search</a>  |   |   |      |   |               |
| <input type="checkbox"/>   | User name                                       | ▲ | Path | ▼ | Groups ▾      |
|  |   |   |      |   | Last activity |
| <input type="checkbox"/>   | <a href="#">Administrador-de-Backups</a>        | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Administrador-de-Sistemas</a>       | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Analista-de-Dados</a>               | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Assistente-de-Operacoes</a>         | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Auditor</a>                         | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Colaborador-Remoto</a>              | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Formador-POS</a>                    | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Gestor-de-Infraestrutura-Cloud</a>  | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Gestor-de-Loja</a>                  | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Gestor-de-Seguranca-de-Infra...</a> | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Operador-POS</a>                    | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">RH</a>                              | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Supervisor-de-Ecommerce</a>         | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Tecnico-de-Formacao</a>             | / |      | 1 | -             |
| <input type="checkbox"/>   | <a href="#">Tecnico-de-Redes</a>                | / |      | 1 | -             |

Figura 4: Utilizadores - AWS

## SRDIoT

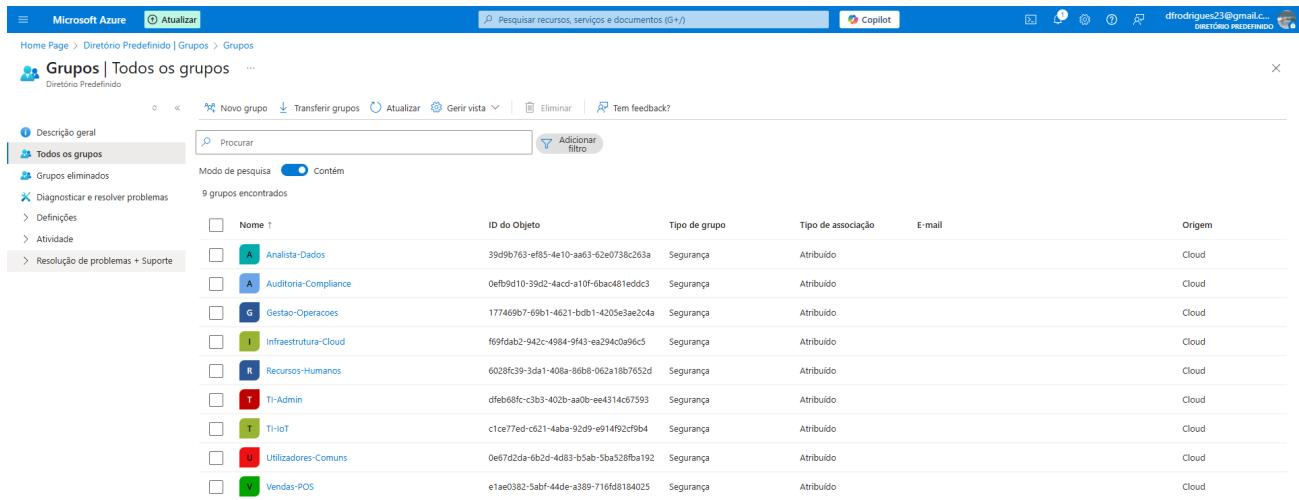
The screenshot shows the AWS IAM User configuration for 'Assistente-de-Operacoes'. It includes sections for Summary, Permissions policies (3), and Groups (1). The user has ARN arn:aws:iam::065932174201:user/Assistente-de-Operacoes, was created on June 12, 2025, at 21:26 (UTC+01:00), and has disabled console access. It lists three attached policies: AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess, and PowerUserAccess, all associated with the group 'Gestao-Operacoes'. The 'Permissions' tab is selected.

Figura 5: Exemplo de Utilizador - AWS

The screenshot shows the AWS IAM Group configuration for 'Gestao-Operacoes'. It includes sections for Summary, Users (3), and Permissions. The group has ARN arn:aws:iam::065932174201:group/Gestao-Operacoes, was created on June 12, 2025, at 21:18 (UTC+01:00), and contains three users: 'Assistente-de-Operacoes', 'Gestor-de-Loja', and 'Supervisor-de-Ecommerce'. The 'Users' tab is selected.

Figura 6: Exemplo de Grupo - AWS

## Anexo 2 - Configuração User Groups Azure



The screenshot shows the Microsoft Azure portal interface for managing user groups. The top navigation bar includes 'Microsoft Azure' and 'Atualizar'. The search bar says 'Pesquisar recursos, serviços e documentos (G+ /)'. The top right shows the user's email (dfrodrigues23@gmail.com) and a 'Copilot' icon. Below the header, the URL is 'Home Page > Diretório Predefinido > Grupos > Grupos'. The main title is 'Grupos | Todos os grupos' under 'Diretório Predefinido'. The left sidebar has links for 'Descrição geral', 'Todos os grupos' (selected), 'Grupos eliminados', and 'Diagnosticar e resolver problemas'. The main content area shows a table of 9 groups found, with columns for 'Nome', 'ID do Objeto', 'Tipo de grupo', 'Tipo de associação', 'E-mail', and 'Origem'. Each group entry includes a checkbox, a color-coded icon, and the group name.

| Nome  | ID do Objeto                          | Tipo de grupo | Tipo de associação | E-mail | Origem |
|---|---------------------------------------|---------------|--------------------|--------|--------|
| <span style="color: blue;">A</span> Analista-Dados        | 39d9b763-ef85-4e10-aa63-62e0738c263a  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: blue;">A</span> Auditoria-Compliance  | 0efb9d10-39d2-4acd-a10f-6bac481edd3   | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: green;">G</span> Gestao-Operacoes     | 177469b7-69b1-4621-bdb1-4205e3ae2c4a  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: green;">I</span> Infraestrutura-Cloud | f69fdab2-942c-4984-9f43-ea294c0a96c5  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: blue;">R</span> Recursos-Humanos      | 6028fc39-3da1-408a-86b8-062a188b7852d | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: red;">T</span> Ti-Admin               | dfeb68fc-c3b3-402b-aa0b-ee4314c67593  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: yellow;">T</span> Ti-IoT              | c1ce77ed-c621-4aba-92d9-e914f92cf9b4  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: red;">U</span> Utilizadores-Comuns    | 0e67d2da-6b2d-4d83-b5ab-5ba528fba192  | Segurança     | Atribuído          |        | Cloud  |
| <span style="color: green;">V</span> Vendas-POS           | e1ae0382-3abf-44de-a389-716fd8184025  | Segurança     | Atribuído          |        | Cloud  |

Figura 7: Grupos - Azure

## SRD IoT

The screenshot shows the Microsoft Azure Groups page for the 'Vendas-POS' group. The top navigation bar includes 'Microsoft Azure', 'Atualizar', 'Copilot', and a search bar. The left sidebar has sections like 'Descrição geral', 'Diagnosticar e resolver problemas', 'Gerir', 'Propriedades', 'Membros', 'Proprietários', etc. The main content area displays the group's name 'Vendas-POS' with a green 'V' icon, its description 'Grupo que faz a gestão das Vendas e Pontos de Venda na Cloud', and various properties: Tipo de associação (Atribuído), Origem (Cloud), Utilizador(es) (1), Grupo(s) (0), Dispositivo(s) (0), Outro(s) (0). Below this are three cards: 'Associações a grupos' (0), 'Proprietários' (0), and 'Número total de membros' (1).

Figura 8: Grupo Específico - Azure

The screenshot shows the Microsoft Azure Groups page for the 'Vendas-POS' group, specifically the 'Membros' tab. The top navigation bar and sidebar are similar to Figure 8. The main content area shows a table of members: 1 membro do grupo encontrado. The member listed is 'Operador POS' (Utilizador), with ID 'cbc3b149-3b21-42f0-9aa3-1ecb6e2e27e6'. There are buttons for 'Adicionar membros', 'Operações em massa', 'Atualizar', 'Gerir vista', and 'Remover'.

Figura 9: Exemplo de Membros num Grupo - Azure

## Anexo 3 - Configuração Users Azure

| Nome a apresentar                 | Nome principal de utilizador | Tipo de utilizador | Sincronização | Identidades               | Nome da empresa | Tipo de criação |
|-----------------------------------|------------------------------|--------------------|---------------|---------------------------|-----------------|-----------------|
| AD Admin de Sistemas              | Admin de Sistemas            | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| AD Analista de Dados              | Analista-Dados@...           | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| A Auditor                         | Auditor@dfrodrig...          | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| DR Daniel Rodrigues               | dfrodrigues23_gm...          | Membro             | Não           | MicrosoftAccount          |                 |                 |
| GD Gestor de Infraestrutura Cloud | Gestor-Infraestrutu...       | Membro             | Não           | dfrodrigues23@gmail.on... | Products a Lot  |                 |
| GL Gestor de Loja                 | Gestor-de-Loja@...           | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| OP Operador POS                   | Operador-POS@...             | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| RH Recursos Humanos               | Recursos-Humano...           | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| TI Técnico IoT                    | Tecnico-IoT@dfro...          | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |
| UC Utilizadores Comuns            | Utilizadores-Com...          | Membro             | Não           | dfrodrigues23@gmail.on... | Products A Lot  |                 |

Figura 10: Exemplo de Users - Azure

## SRD IoT

Figura 11: Exemplo de User Específico - Azure

Figura 12: Exemplo de Funções de Users - Azure

## Anexo 4 - Configuração Rede Virtual Azure

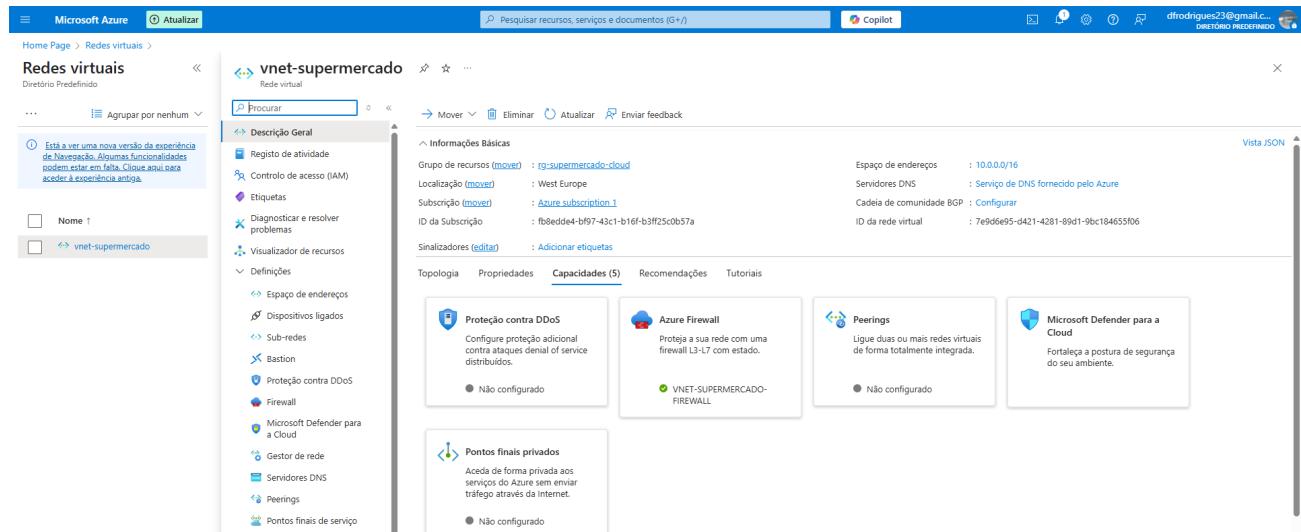


Figura 13: Exemplo de Redes Virtuais - Azure

**vnet-supermercado | Sub-redes**

| Nome                | IPv4        | IPv6 | IPs disponíveis | Delegado a | Grupo de segu... | Tabela de rotas |
|---------------------|-------------|------|-----------------|------------|------------------|-----------------|
| AzureFirewallSubnet | 10.0.0.0/26 | -    | 56              | -          | -                |                 |
| sub-rede-rh         | 10.0.2.0/24 | -    | 251             | -          | nsg-rh           |                 |
| sub-rede-iot        | 10.0.3.0/24 | -    | 251             | -          | nsg-iot          |                 |
| sub-rede-db         | 10.0.4.0/24 | -    | 251             | -          | nsg-db           |                 |
| sub-rede-pos        | 10.0.1.0/24 | -    | 251             | -          | nsg-pos          |                 |

Figura 14: Exemplo de Rede Virtual Específica - Azure

## Anexo 5 - Configuração Sub-Redes Azure

The screenshot shows the Azure portal's 'Sub-redes' (Sub-nets) page for the 'vnet-supermercado' virtual network. The left sidebar lists various networking resources like Bastion, Firewall, and Peering. The main area shows a table of sub-nets:

| Nome                | IPv4        | IPv6 | IPs disponíveis | Delegado a | Grupo de segu... | Tabela de rotas |
|---------------------|-------------|------|-----------------|------------|------------------|-----------------|
| AzureFirewallSubnet | 10.0.0.0/26 | -    | 56              | -          | -                | -               |
| sub-rede-rh         | 10.0.2.0/24 | -    | 251             | -          | nsg-rh           | -               |
| sub-rede-iot        | 10.0.3.0/24 | -    | 251             | -          | nsg-iot          | -               |
| sub-rede-db         | 10.0.4.0/24 | -    | 251             | -          | nsg-db           | -               |
| sub-rede-pos        | 10.0.1.0/24 | -    | 251             | -          | nsg-pos          | rt-pos-fire...  |

Figura 15: Exemplo de Sub-Redes - Azure

The screenshot shows the Azure portal interface for managing a virtual network. On the left, the navigation pane is visible with options like 'Redes virtuais', 'Agrupar por nenhum', and a note about a new navigation experience. The main area displays the 'vnet-supermercado | Sub-redes' page. A table lists existing subnets: 'AzureFirewallSubnet' (IPv4: 10.0.0.0/26), 'sub-rede-rh' (IPv4: 10.0.2.0/24), 'sub-rede-iot' (IPv4: 10.0.3.0/24), 'sub-rede-db' (IPv4: 10.0.4.0/24), and 'sub-rede-pos' (IPv4: 10.0.1.0/24). The right side shows the 'Editar sub-rede' (Edit subnet) dialog for 'sub-rede-pos'. It includes sections for 'IPv4' (with 'Incluir um espaço de endereços IPv4' checked, setting 'Endereço inicial' to 10.0.1.0 and 'Tamanho' to /24 (256 endereços)), 'IPv6' (disabled), 'Sub-rede privada' (disabled), and 'Segurança' (with 'NAT Gateway' set to 'Nenhum'). Buttons for 'Guardar' (Save) and 'Cancelar' (Cancel) are at the bottom.

Figura 16: Exemplo de Sub-Rede Específica - Azure

## Anexo 6 - Configuração Tabela de Rotas Azure

**Descrição geral**

- Grupo de recursos (mover) : rg-supermercado-cloud
- Localização : West Europe
- Subscrição (mover) : Azure subscription 1
- ID da Subscrição : fb8edde4-fbf7-43c1-b16f-b3ff25cb57a
- Etiquetas (editar) : Adicionar etiquetas

**Definições**

| Nome            | Prefixo de endereço | Tipo do próximo salto | Endereço IP do próximo salto |
|-----------------|---------------------|-----------------------|------------------------------|
| rt-via-firewall | 0.0.0.0/0           | Aplicação virtual     | 10.0.0.4                     |

**Subredes**

| Nome         | Intervalo de endereços | Rede virtual      | Grupo de segurança |
|--------------|------------------------|-------------------|--------------------|
| sub-rede-pos | 10.0.1.0/24            | vnet-supermercado | nsgr-pos           |

Figura 17: Exemplo de Tabela de Rotas - Azure

**Descrição geral**

| Nome         | Intervalo de endereços | Rede virtual      | Grupo de segurança |
|--------------|------------------------|-------------------|--------------------|
| sub-rede-pos | 10.0.1.0/24            | vnet-supermercado | nsgr-pos           |

Figura 18: Exemplo de Sub-Redes na Tabela de Rotas - Azure

## Anexo 7 - Configuração Firewall Azure

**Informações Básicas**

|                              |                                   |
|------------------------------|-----------------------------------|
| SKU                          | : Standard (alterar)              |
| Sub-rede                     | : AzureFirewallSubnet             |
| IP público                   | : vnet-supermercado-firewall      |
| IP privado                   | : 10.0.0.4                        |
| Sub-rede de gestão           | :                                 |
| IP de gestão público         | :                                 |
| Intervalos IP Privados       | : Gerido por Política de Firewall |
| Route Server (pré-visualiz.) | : Adicionar                       |

**Firewall policy**

Visit Azure Firewall Manager at the link below to edit the Firewall Policy on this firewall.

|                        |  |
|------------------------|--|
| Policy                 | vnet-supermercado-firewall-policy (change) |
| Auto-learn IP Prefixes | Disabled                                   |

**Rules**

|                   |                          |
|-------------------|--------------------------|
| DNAT rules        | 0 rules in 0 collections |
| Network rules     | 1 rule in 1 collection   |
| Application rules | 1 rule in 1 collection   |

Figura 19: Exemplo de Firewall - Azure

| Name          | Type                        | Priority | Rules | Inherited from |
|---------------|-----------------------------|----------|-------|----------------|
| default-group | Rule collection group       | 100      | 2     | ...            |
| iot           | Network rule collection     | 101      | 1     | ...            |
| pos           | Application rule collection | 102      | 1     | ...            |

Figura 20: Exemplo de Regras de Firewall - Azure

The screenshot shows the Microsoft Azure portal interface for managing a firewall policy. The left sidebar navigation includes Home Page, Redes virtuais, vnet-supermercado | Firewall, vnet-supermercado-Firewall, and vnet-supermercado-firewall-1. Under Rules, Coleções de regras is selected, showing sub-options: Regras DNAT, Regras de rede, and Regras de Aplicações. The main content area is titled "vnet-supermercado-firewall-policy | Coleções de regras". It displays a table of rule collections:

| Name          | Type                        |
|---------------|-----------------------------|
| default-group | Rule collection group       |
| iot           | Network rule collection     |
| pos           | Application rule collection |

A modal window titled "Editar coleção de regras" is open, showing configuration details for the "iot" collection:

- Nome: iot
- Tipo de coleção de regras: Rede
- Prioridade: 101
- Ação de coleção de regras: Permitir
- Grupo de coleções de regras: default-group

The "Regras" section lists a single rule:

| Nome *             | Tipo de origem | Origem                 | Protocolo * | Portas de Destino * | Tipo de Destino * | Destino *            |
|--------------------|----------------|------------------------|-------------|---------------------|-------------------|----------------------|
| block-iot-internet | Endereço IP    | 10.0.3.0               | Any         | *                   | Endereço IP       | 0.0.0.0              |
|                    | Endereço IP    | *.192.168.10.1, 192... |             | 0 selecionado       | Endereço IP       | *.10.0.1.10.1.0/1... |

Figura 21: Exemplo de Uma Regra de Firewall - Azure