# **DP201 - Designing an Azure Data Platform Solution**

## Lab 4 – Azure Security Design Considerations

**Exercise 1**

**Task 1: Defence in depth approach**

Use the table below to document the security requirements for AdventureWorks. You can use requirements as identified from the AdventureWorks case study. You should also suggest security requirements that are missed but should be considered to ensure that AdventureWorks has proper security coverage.

|  |  |
| --- | --- |
| Requirement  **Disponibilidade** – Serviço disponível somente ao professional autorizado;  **Confidencialidade** – Acesso restrito. Acesso aos recursos estritamente necessários;  **Integridade** – Prevenção de alterações não autorizadas; | Defence in Depth Category  **Opções**: Data, Applications, VM/compute, Networking, Perimeter, Policies & access e Physical security |
| Acesso ao SQL DW permitido somente à profissionais autorizados | Data Application, Perimeter e Policies & access |
| Bicicletas com conexões seguras (telemetria) – Somente profissionais autorizados e aplicativos autorizados pela AdventureWorks tem acesso aos dados | Data, Applications, Networking, Policies & access e Physical security. |
| Criptografia dos dados da social media | Data, Applications, Networking, Policies & access |
| Gestão de acessos à plataforma da Cloud – Roles, RBAC | Applications, VM/compute, Networking, Perimeter, Policies & access e Physical security |
| Governança dos dados – Definição da criticidade dos dados, GDPR, confidencialidade, dados sensíveis e etc | Data, Applications, Policies & access e Physical security. |
| Gestão da Segurança da Cloud – IP, NAT, Firewall e etc |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |