Cibersegurança | Referência técnica para configuração segura de ambiente em nuvem

Veja a seguir algumas recomendações básicas para o uso seguro de nuvem considerando aplicações WEB. Tais recomendação baseiam-se em manter a tríade de *confiabilidade, disponibilidade e integridade*:

- Criar uma VPC (*virtual private cloud*), usando duas zonas geográficas distintas, com três subredes em cada uma.
- Para cada zona, gerar uma subrede pública e duas privadas:
  - *na subrede pública, utilizar o load balance;*
  - *nas redes privadas, utilizar em uma o servidor de aplicação e em outra o de banco de dados, utilizando um serviço de banco de dados relacional.*
- Inserir grupos de segurança gerenciando o acesso do fluxo. A aplicação, somente na porta 443 do load balance; já o banco, somente na porta a partir da aplicação.
- Para acesso remoto às máquinas, utilizar um servidor bastião se for Linux, ou um remote desktop gateway se for Windows na rede pública com IPs específicos de acesso.
- Para que as máquinas da rede privada tenham acesso à Internet, colocar um nat gateway.
- Caso seja acesso só interno, normalmente, avalia-se a VPN IPSec.
- É sempre importante ligar as ferramentas de logs de acesso, reconfiguração e performance dos ativos em nuvem.
- Recomenda-se, junto aos logs das máquinas, utilizar um repositório além do próprio HD delas.
- Criar snap shots das máquinas e banco de dados.
- Implementar mecanismo de deploy automatizado por devops.
- Criar e manter técnicas de autoscaling.
- Por fim, recomenda-se serviços de borda, para aumentar segurança.