Juan David Páez Olivares
20231020028

Task 2: What is a Database Backup and what policies are recommended to manage them?

In today's day and age, data is the foundation of many businesses and systems, and the way it is managed is critical to keeping organizations afloat, which is why backups and complete database recovery systems are created.

Any organization that uses personal and other sensitive data must have a strong, tested plan for bussiness continuity in the event of a disaster or cyberattack. Losing access or control of data for an extended period of time will disrupt operations, lead to financial losses, and damage an organization's reputation. Recovering from a tarnished reputation can be costly and time-consuming.

A failure that compromises data can be caused by a hardware failure, due to wear, physical damage or some other factor that causes the hardware to fail, it can also be due to a software failure, where different vulnerabilities are compromised that can compromise the information within specialized software for data management, and lastly and most common, human error, where an incorrect configuration can cause a failure of the two previous types.

Data management also means protecting people's privacy, protecting against breaches, and complying with regulations and standards such as the European Union's General Data Protection Regulation (GDPR), the United states' Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security standard (PCI DSS).