The write up assignment

Pamela davis

02/08/26

The CIA Triad is a foundational framework in cybersecurity that guides how information and systems are protected. According to the Chai article, the triad consists of confidentiality, integrity, and availability, each representing a core security goal. Confidentiality focuses on ensuring that sensitive information is only accessible to authorized individuals, often through tools such as encryption, passwords, and access controls. Integrity ensures that data remains accurate, complete, and unaltered unless changed by authorized users; mechanisms like hashing, checksums, and audit logs help detect unauthorized modifications. Availability ensures that systems and data are accessible to authorized users when needed, which is supported through backups, redundancy, system maintenance, and protections against attacks such as denial-of-service. Together, these three principles help organizations balance security with usability and reliability.

Authentication and authorization are closely related to security concepts but serve different purposes. Authentication is the process of verifying the identity of a user or system and answers the question, “Who are you?” Common examples include logging in with a username and password, using multi-factor authentication, or scanning a fingerprint or face ID. Once authentication is successful, authorization determines what actions or resources the authenticated user is permitted to access, answering the question, “What are you allowed to do?” For example,

after logging into a company network, an employee may be authorized to access general work files but restricted from viewing payroll or administrative data. In a school system, a student may be authenticated to access the portal but authorized only to view their own grades. In short, authentication confirms identity, while authorization controls permissions, and both are essential components of effective cybersecurity aligned with the CIA Triad.