

## LABORATORIO 2

Héctor Díaz Camacho

1.

- **Confidenciales:** Es el aseguramiento a la protección sobre la información o datos sensibles contra accesos no autorizados, es decir, solamente las personas que están autorizadas tengan el acceso.
- **Integridad:** Es asegurar que la información sea precisa confiable y segura, que no sea modificada o alterada, es decir la protección contra la modificación no autorizada de los datos.
- **Disponibilidad:** Es garantizar que la información, los datos o recursos estén disponibles a la hora de necesitarlos, esto lleva a recurrir en métodos o estrategias ante fallos o ataques para mantener los recursos disponibles.

2.

Ejemplo de Confidencialidad: A la hora de registrar datos sensibles en la base de datos, los sistemas y la base de datos, deben guardar dichos datos de forma encriptada, para que los datos no entendibles a la hora de una persona sin autorización tenga acceso a los registros, también al navegar por el se debe tener en cuenta los protocolos seguros, por ejemplo, “HTTPS”, “SSH”, “SFTP”, entre otros.

Ejemplo de Integridad: Hoy en día encontramos varias maneras de probar la integridad ya sea de datos, información o archivos, por ejemplo paginas importantes que generan descargas de archivos esenciales, tienden a entregar un hash para que lo compares con las descarga realizada para evitar ataques como MIM.

Ejemplo de disponibilidad: Al manejar una empresa que maneja gran cantidad de solicitudes en el sistema o tiene una infraestructura de red amplia, se debe tener en cuenta el manejo ya sea varios routers o switches que se presten como respaldo o soporte a la hora de fallos o ataques para prevenir fallas en la comunicación y mantener alta disponibilidad de los recursos.

3.

La triada CID se complementan entre si, ya que por ejemplo, tiene acceso a datos de autenticación donde deben ser modificadas, podría loguearse en el sistema y modificar información, afectando la integridad de la información, o un fallo del sistema que afecte la disponibilidad de información, puede aprovecharse un atacante para también realizar un MiTM u otro ataque como phishing para tener información sensible

### **Reflexión:**

- Para una empresa de salud debe tenerse muy en cuenta los tres conceptos de la triada CID, ya que cada concepto es fundamental para mantener eficacia y eficiencia en los objetivos de la empresa de salud, ya que cualquier falla en uno de estos conceptos, pueden recurrir a consecuencias graves y hasta penales.
- La implementación de estos conceptos se basan en los métodos o procesos que se manejan, por ejemplo una empresa con recursos limitados, en la parte de confidencialidad debe tener en cuenta buenas practicas para encriptación de datos en sus software, para la integridad protocolos de manejo de datos y archivos así evitando la utilización de recursos externos y en la Disponibilidad el uso de UPC, la buena configuración de routers o el análisis del lugar donde manejan el sistema, por ejemplo en la nube.