Confidencialidad (Confidentiality)

Garantiza que la información solo sea accesible por personas autorizadas, asi mismo evita que datos sensibles sean vistos por usuarios no autorizados.

Ejemplos:

Uso de contraseñas seguras y autenticación de dos factores.
Cifrado de datos (por ejemplo, HTTPS o cifrado de archivos).
Control de acceso a archivos o sistemas.

2. Integridad (Integrity)

Asegura que la información no sea alterada o manipulada sin autorización, además los datos deben mantenerse exactos y completos.

Ejemplos:

Uso de hashes o firmas digitales para verificar que un archivo no fue modificado.
Control de versiones y auditorías de cambios.
Políticas que eviten la corrupción de datos o modificaciones indebidas.

3. Disponibilidad (Availability)

Garantiza que la información y los sistemas estén accesibles cuando los usuarios autorizados la necesiten. No sirve tener datos seguros si no se pueden usar cuando se requieren.

Ejemplos:

Copias de seguridad (backups).
Servidores redundantes y planes de recuperación ante desastres.
Protección contra ataques de denegación de servicio (DDoS).