“Año de la recuperación y consolidación de la economía peruana“

UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA”

ESCUELA PROFESIONAL “INGENIERÍA DE SISTEMAS Y COMPUTACIÓN”

Cátedra: Base de datos II

Catedrático: Fernandez Bejarano Raul Enrique

Estudiante: Egoavil Machado Jesus Miguel

HUANCAYO PERÚ

Módulo 4: Seguridad en SQL Server

Subtemas: Seguridad básica, protección de datos y prevención de ataques

Introducción a la seguridad en SQL Server

- Conceptos de seguridad básicos: Protección de la confidencialidad, integridad y disponibilidad de los datos.
- Autenticación y autorización:

  - Autenticación: Verifica la identidad (Windows o SQL Server login).

  - Autorización: Controla el acceso a los objetos.
- Roles y permisos:

  - Asignación de roles fijos o definidos por el usuario.

  - Permisos para ejecutar acciones específicas.

Protección de datos

- Cifrado de datos: Protege los datos sensibles mediante técnicas de cifrado (columnas, backups).
- Controles de acceso: Configuración de permisos estrictos por usuario o rol.
- Auditoría de seguridad: Registro de eventos y actividades para detectar accesos indebidos.

Prevención de ataques

- Vulnerabilidades comunes en SQL Server:

  - Inyección SQL

  - Accesos no autorizados

  - Configuración insegura

- Medidas de protección contra ataques:

  - Aplicar actualizaciones y parches

  - Configurar firewalls

  - Uso de conexiones seguras (SSL/TLS)

- Plan de respuesta a incidentes: Procedimientos para actuar en caso de un ataque o vulneración.

Conclusión

- La seguridad en SQL Server debe ser:
- • Proactiva: Prevenir antes que ocurran ataques.
- • Integral: Proteger el acceso, los datos y la infraestructura.
- • Monitoreada: Revisar continuamente las configuraciones y actividades.