**Integridad**

El término integridad de datos se refiere la correctitud y completitud de la información en una base de datos. Cuando los contenidos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes. Una de las funciones importantes de un DBMS relacional es **preservar** la integridad de sus datos almacenados en la mayor medida posible.

Las restricciones de integridad las podemos agrupar en **cuatro** grupos:

**a) Integridad del dominio:** La integridad de dominio es la validez de las restricciones que debe cumplir una determinada columna de la tabla.

-Datos Requeridos: establece que una columna tenga un valor no NULL. Se define efectuando la declaración de una columna es NOT NULL cuando la tabla que contiene las columnas se crea por primera vez, como parte de la sentencia CREATE TABLE.

-Chequeo de Validez: cuando se crea una tabla cada columna tiene un tipo de datos y el DBMS asegura que solamente los datos del tipo especificado sean ingresados en la tabla.

**b) Entidad:** Son reglas de integridad que aplican a la totalidad de los registros de la tabla, como un conjunto. Por ejemplo: Si validamos que el valor de un campo no se repita, estamos diciendo que solo un registro puede tener un determinado valor en ese campo. Como reglas de este nivel tenemos el PRIMARY KEY y el UNIQUE INDEX.

**c) Referencial:** asegura la integridad entre las llaves foráneas y primarias (relaciones padre/hijo). Existen cuatro actualizaciones de la base de datos que pueden corromper la integridad referencial:

-La inserción de una fila hijo se produce cuando no coincide la llave foránea con la llave primaria del padre.

-La actualización en la llave foránea de la fila hijo, donde se produce una actualización en la clave ajena de la fila hijo con una sentencia UPDATE y la misma no coincide con ninguna llave primaria.

-La supresión de una fila padre, con la que, si una fila padre -que tiene uno o más hijos- se suprime, las filas hijos quedarán huérfanas.

-La actualización de la clave primaria de una fila padre, donde si en una fila padre, que tiene uno o más hijos se actualiza su llave primaria, las filas hijos quedarán huérfanas.

**d) Del usuario:** Se refiere a restricciones programadas por el usuario utilizando herramientas como los “Triggers” y “Procedimiento almacenados”.

**Seguridad**

Un buen entorno de seguridad para Sql Server se fundamenta en la creación de conjunto de políticas y procedimientos orientados a garantizar la protección de los datos. Estos procedimientos deben trabajar los siguientes aspectos:

-La información es accedida solo por los usuarios autorizados.

-El almacenamiento de los datos es seguro.

-El tránsito de los datos es seguro.

-La data es recuperable.

**PRINCIPIOS DE SEGURIDAD**

Los principios de seguridad proporcionan la base sobre la cual se fundamentan todas las soluciones de seguridad. A continuación, una lista de algunos principios recomendados:

***-Comienza con un buen diseño.*** Debemos implementar sistemas que sean “Seguros por

defecto”. Sistemas que estén abiertos para recibir y aceptar cualquier cambio necesario en

característica o funcionalidades. Debemos trabajar sobre un diseño apropiado de la

infraestructura de red.

***-Confía, pero vigila.*** Aunque tengamos previstos ataques o amenazas conocidos debemos

protegernos contra los ataques que aún no conocemos. Tecnologías como Antivirus y Antispyware

puede ayudar.

***-Defensa a fondo (Defense-in-Depth***). Nunca debemos confiarnos en una sola solución de

seguridad. Por ejemplo, no debemos confiar solo en el Firewall para protegernos de ataques por

internet. No debemos confiar solo en el Active Directory para protegernos de ataques internos.

Por el contrario, debemos considerar una seguridad basada en niveles:

o Sensibilización de usuarios

o Seguridad en el cliente

o Seguridad en la red

o Seguridad en el servidor

o Seguridad perimetral

***- Menor privilegio***. Por defecto solo con lo indispensable.

o Sensibilización de usuarios

o Seguridad en el cliente

o Seguridad en la red

o Seguridad en el servidor

o Seguridad perimetral

**ASPECTOS DE SEGURIDAD EN LA ARQUITECTURA DE SQL SERVER**

Para conocer el modo de operar de la seguridad en SQL server se debe de conocer los siguientes aspectos:

• ***Autenticación***. Determinar la identidad del usuario.

• ***Autorización***. Determinar a qué objetos o funciones tiene acceso.

• ***Integridad***. Asegurar que la información no se modifique en el transito (Firma digital).

• ***Privacidad***. Asegurar que la información solo puede ser leída por el destinatario ( Cifrado).

**Disponibilidad de los datos**

**Alta Disponibilidad (High Availability)**

Se refiere al protocolo seguido para garantizar la continuidad del sistema. Que ese tiempo de inactividad (Downtime) sea el mínimo permitido. El tiempo de inactividad puede ser **planificado**: se refiere a interrupciones lógicas y por lo regular programadas, cosas aplicar actualizaciones, cambio de alguna configuración que requiera reinicio del sistema, etc. y **no** **planificado**: se refiere a interrupciones caudadas por imprevistos como son los errores de Software o Hardware, etc.

Todo sistema de tener un acuerdo de servicio (SLA) que defina el tiempo que el sistema debe estar en línea. Sistema de bajo criticidad puede ofrecer una disponibilidad de 8x5 (8 días por 5 horas). En sistemas críticos el nivel de servicio puede ser de 24/7 los 365 días del año (24\*365). La siguiente formula nos permite calcular la disponibilidad del sistema:

Disponibilidad = ((A-B) /A) \* 100%

Donde: A = Horas comprometidas. Eje: 24\*365 = 8,760 horas/año

B = Downtime durante las horas compromietidas. Eje: 15 horas por fallas de discos, 9 por mantenimientos = 24.

Entonces: D = ((8760-24) /8760 \* 100 = 99.726%

**Niveles de Alta Disponibilidad**

**Convencional**: 90% de disponibilidad. La continuidad e integridad no son un tema crítico. Servidor tradicional con técnicas de recuperación y copias de seguridad.

**Media (High Reliable):** 95% de disponibilidad. Se pueden tolerar algunas interrupciones, pero la integridad es un tema crítico. Se utilizan esquema de protección transaccionales.

**Alta disponibilidad:** 99% de disponibilidad. Se soportan interrupciones muy breves. Se utilizan esquema de protección transaccional y recuperación automática. Resistente a fallas. 99.9% de disponibilidad. El sistema debe trabajar sin interrupciones en horario laboral. Se utilizan esquemas de “mirroring” y “Clustering”.

**Tolerancia a fallas:** 99.99% de disponibilidad. El procesamiento es continuo y la recuperación ante fallas es transparente al usuario. Se utilizan esquemas de duplicidad y redundancia.

**Tolerancia a desastres:** 99.999% (los cinco 9s). Disponibilidad en todo momento. Recuperación transparente, incluso ante desastre naturales o humanos. Se utilizan todos los esquemas anteriores, con duplicidad extra.

**Técnicas de Alta Disponibilidad**

Se refiere a los procedimientos o prácticas que permiten que un sistema no deje de estar en funcionamiento y accesible en ningún momento o que ese tiempo de inactividad sea de un porcentaje de tiempo realmente mínimo. También nos referimos a estas técnicas como “soluciones de alta disponibilidad”. Algunas técnicas que ayudan en el proceso de proveer alta disponibilidad en las bases de datos son las siguientes:

-**Replicación**: permite la copia automática de data perteneciente a objetos seleccionados de la base de datos hacia otros servidores locales o remotos.

**-Espejos (Mirroring):** permite tener una copia exacta de nuestra base de datos en otro servidor.

**-Clustering**: es una agrupación de sistemas o componentes (Hardware o Software) que trabajan de forma combinada, como si fuera uno solo, con el objetivo de ofrecer rendimiento, escalabilidad, pero también alta disponibilidad.