UNIVERSIDAD DEL SURESTE: DE LA FRONTERA COMALAPA.

DOCENTE: Ing. Berning Eduardo Aguilar Córdoba.

ASIGNATURA: Base de datos “II”.

ALUMNO: Ramiro Gerardo Resendíz Valdéz.

CUATRIMESTRE: Octavo (8vo).

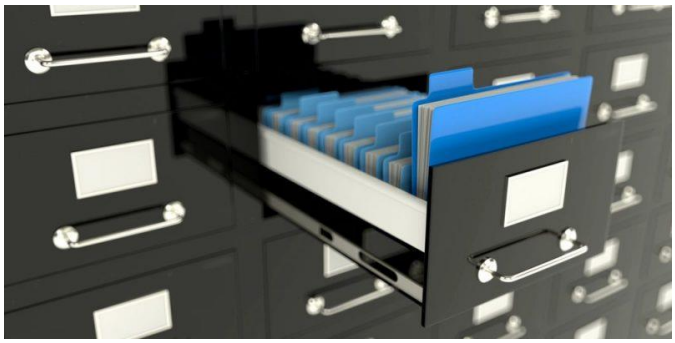
CARRERA: Ingeniería en sistemas computacionales.

GRUPO: ISC13SDC0220-A.

UNIDAD: Primera (1ra).

TRABAJO: Ensayo de la unidad uno a la tres de la antología.

FECHA DE ENTREGA: 09/Abril/2023.



Unidad I.

Una transacción es una colección de acciones con transformaciones consistentes. La base de datos es en un estado consistente si obedece todas las restricciones de integridad definidas. Por supuesto, debe asegurarse de que la base de datos nunca entre en el estado Sin embargo, durante la ejecución de la transacción, la base de datos asegurar que la base de datos vuelva a un estado consistente cuando el transacción. Transparencia adecuada de acciones concurrentes a bases de datos y otras bases de datos. Un lado que es lo suficientemente transparente en su manejo de las fallas que puede hacer. Una transacción es una colección de acciones que resultan en una transformación consistente de la base de datos. La base de datos es. Por supuesto, debe asegurarse de que la base de datos nunca entre en el estado. Sin embargo, durante la ejecución de la transacción, la base de datos asegurar que la base de datos vuelva a un estado consistente cuando el transacción. Una de las misiones en la gestión de transacciones es ser transparente por un lado Mientras que las acciones concurrentes a la base de datos, Transparencia total en la gestión de los fallos que se pueden producir en la base de datos. Una versión simplificada de una reserva típica es condiciones para el cierre de transacciones. Las transacciones siempre terminan, incluso en caso de falla. Cuando termina la transacción. Si tiene éxito, se dice que la transacción está comprometida (se usa la terminología inglesa) Cuando no existe un término en español que refleje fácilmente el significado del término. Si una transacción se detiene sin completar sus tareas, la transacción. Cuando se aborta una transacción, se detiene su ejecución y todas sus acciones. La discusión en la sección anterior explica el concepto de transacciones. No se da ninguna justificación para afirmar que las transacciones son unidades de procesamiento consistente y confiable, seguir: Se refiere al hecho de que las transacciones se tratan como uno por lo tanto, tanto todas estas acciones de transacción. La atomicidad requiere que, si un transacción interrumpida por falla, los resultados parciales deben ser actividades relacionadas con el mantenimiento de la atomicidad de las transacciones en cancelación debido a un error de entrada, sobrecarga del sistema o consistencia. La consistencia de la transacción es solo suya. En otras palabras, la transacción es el programa correcto recuperar la base de datos de un estado consistente a otro con la misma cosa por lo tanto, la transacción no viola la prohibición. Integridad de una base de datos. Aislamiento. Las transacciones en curso no pueden revelar los resultados a las transacciones se ejecutan simultáneamente, el resultado debe ser el mismo igual que si se ejecutara secuencialmente (serialidad). Es la propiedad de la transacción la que asegura que una vez se realizan transacciones, los resultados son permanentes y no pueden ser será eliminado de la base de datos. Por lo tanto, el DBMS asegura que los

resultados de las transacciones sobrevivirán a las fallas del sistema. Aspecto motivador de la recuperación de bases de datos, que se relaciona con la forma restaurar la base de datos a un estado coherente en el que todas las acciones las transacciones pueden pertenecer a varias clases. Los conceptos básicos son los mismos para las diferentes clases, algoritmos y técnicas utilizadas. Agrupados por las siguientes dimensiones: En primer lugar, las transacciones se pueden realizar en transacciones que operan sobre datos distribuidos se conocen como transacciones distribuidas. El resultado de una transacción que realiza una confirmación de larga duración, la única manera para deshacer el efecto de una transacción realizada es a través de otro este tipo de transacción se conoce como transacción. Tiempo de duración. Teniendo en cuenta el tiempo transcurrido desde las transacciones pueden ser por lotes o en línea. Así como transacciones de corta y larga vida. Caracterizada por tiempos de respuesta muy cortos y por acceso parcial base de datos relativamente pequeña. El tipo de lote lleva un tiempo relativamente largo y accede principalmente datos. Estructura. Considerando la estructura que puede tener una transacción, no comprueba dos aspectos: si las transacciones pueden ser contenidas a su vez subtransacciones o secuencias de acciones de lectura y escritura en un solo sistema. Por el contrario, las fallas globales, afectan a varias -y casi siempre a todas- las transacciones que se estaban efectuando en el momento de la falla, por lo cual tienen implicaciones importantes en el sistema. Por ejemplo, interrupción del servicio eléctrico, estas afectan a todas Las transacciones que se estaban ejecutando pero no afectan a la base de datos. Además, puede ocurrir que sea necesario volver a ejecutar algunas transacciones que sí se realizaron con éxito antes de la falla pero cuyas modificaciones no lograron efectuarse sobre la base de datos porque no lograron ser transferidas de los buffers de la base de datos a la base de Datos física. La recuperación de una falla semejante implica en esencia cargar de nuevo la DB a partir de una copia de respaldo y utilizar después la bitácora para realizar de nuevo todas las transacciones terminadas desde que se hizo esa copia de respaldo. No hay necesidad de anular las transacciones inconclusas en el momento de la falla, porque por definición todas las modificaciones de esas transacciones ya se anularon de todas maneras. Por ejemplo una falla en el controlador de disco o un aterrizaje de cabeza en el disco, estas fallas sí causan daños a la base de datos o a una porción de ella y afecta, al menos, a las transacciones que están haciendo uso de esa porción. La Recuperación de una falla semejante implica, en esencia, cargar de nuevo la base de datos a partir de una copia de respaldo y después utilizar la bitácora, o system log, para realizar de nuevo todas las transacciones terminadas desde que se hizo esa copia para respaldo. No hay necesidad de anular todas las transacciones inconclusas en el momento de la falla, porque esta se anula.

Unidad II.

Concurrencia se refiere al hecho de que los Sistemas Administradores de Base de Datos permiten que muchas transacciones accedan a una misma Base de Datos a la vez. Cuando existen varios usuarios intentando modificar los datos al mismo tiempo, se necesita establecer algún tipo de control para que dichas modificaciones de un usuario no interfieran en las de los otros, a este sistema se le denomina control de concurrencia. En este informe podremos ver algunos de los problemas que se presentan cuando la concurrencia no se controla y algunos de los mecanismos de bloqueo que nos permiten manejar la concurrencia en las transacciones. De esta manera, los sistemas de control de concurrencia deben garantizar la consistencia de transacciones que se ejecutan de manera concurrente. En el campo informático, el termino concurrencia se refiere a la capacidad de los Sistemas de Administración de Base de Datos, de permitir que múltiples procesos sean ejecutados al mismo tiempo, y que también puedan interactuar entre sí. Los procesos concurrentes pueden ser ejecutados realmente de forma simultánea, sólo cuando cada uno es ejecutado en diferentes procesadores. En cambio, la concurrencia es simulada si sólo existe un procesador encargado de ejecutar todos los procesos, simulando la concurrencia, ocupándose de forma alternada de uno y otro proceso a muy pequeños intervalos de tiempo. De esta manera simula que se están ejecutando a la vez. La multiprogramación, ya que el tiempo del procesador es compartido dinámicamente por varios procesos. Las aplicaciones estructuradas, donde la programación estructurada se implementa como un conjunto de procesos concurrentes. También se tiene que la misma estructura recién mencionada es utilizada en el diseño de los sistemas operativos, los cuales se implementan como un conjunto de procesos. Debido a que los procesos concurrentes en un sistema pueden interactuar entre otros también en ejecución, el número de caminos de ejecución puede ser extremadamente grande, resultando en un comportamiento sumamente complejo. Las dificultades asociadas a la concurrencia han sido pensadas para el desarrollo de lenguajes de programación y conceptos que permitan hacer la concurrencia más manejable. Existen tres formas en las que una transacción, aunque sea correcta por sí misma, puede producir una respuesta incorrecta si alguna otra transacción interfiere con ella en alguna forma. Consideremos que la transacción que interfiere también puede ser correcta; lo que produce el resultado incorrecto general es el intercalado sin control entre las operaciones de las dos transacciones correctas. En los ejemplos anteriores, los errores fueron causados por la ejecución intercalada de operaciones de transacciones diferentes. Los ejemplos no muestran todas las posibles formas en las que la ejecución de dos transacciones pueden interferir, pero sí ilustran dos de los problemas que surgen con

frecuencia debido a la intercalación. Para evitar estos problemas, se deben controlar las intercalaciones entre transacciones. El control de transacciones concurrentes en una base de datos brinda un eficiente desempeño del Sistema de Administración de Base de Datos, puesto que permite controlar la ejecución de transacciones que operan en paralelo, accediendo a información compartida y, por lo tanto, interfiriendo potencialmente unas con otras. El objetivo de los métodos de control de concurrencia es garantizar la no inferencia o la propiedad de aislamiento de transacciones que se ejecutan de manera concurrente. Los distintos objetivos atacan el problema garantizando que las transacciones se ejecuten en un plan que sea serializable, es decir, que el resultado sea equivalente a el resultante de ejecutar un plan en serie. El criterio de clasificación más común de los algoritmos de control de concurrencia es el tipo de primitiva de sincronización. Esto resulta en dos clases: aquellos algoritmos que están basados en acceso mutuamente exclusivo a datos compartidos y aquellos que intentar ordenar la ejecución de las transacciones de acuerdo a un conjunto de reglas. Un bloqueo en general es cuando una acción que debe ser realizada está esperando a un evento. Para manejar los bloqueos hay distintos acercamientos: prevención, detección, y recuperación. También es necesario considerar factores como que hay sistemas en los que permitir un bloqueo es inaceptable y catastrófico, y sistemas en los que la detección del bloqueo es demasiado costosa. En el caso específico de las bases de datos distribuidas usar bloqueo de recursos, peticiones para probar, establecer o liberar bloqueos requiere mensajes entre los manejadores de transacciones y el calendarizador. En sistemas operativos, el bloqueo mutuo es el bloqueo permanente de un conjunto de procesos o hilos de ejecución en un sistema concurrente que compiten por recursos del sistema o bien se comunican entre ellos. A diferencia de otros problemas de concurrencia de procesos, no existe una solución general para los interbloqueos. Todos los interbloqueos surgen de necesidades que no pueden ser satisfechas, por parte de dos o más procesos. En la vida real, un ejemplo puede ser el de dos niños que intentan jugar al arco y flecha, uno toma el arco, el otro la flecha. Ninguno puede jugar hasta que alguno libere lo que tomó. En el siguiente ejemplo, dos procesos compiten por dos recursos que necesitan para funcionar, que sólo pueden ser utilizados por un proceso a la vez. El primer proceso obtiene el permiso de utilizar uno de los recursos. Las reglas básicas para manejar los bloqueos son: transacciones distintas no pueden tener acceso simultáneamente a un elemento (lectura-escritura o escritura-escritura), y una vez se libere un bloqueo no se puede pedir otro, es decir, los bloqueos de la transacción crecerán mientras no libere ninguno y luego de liberar alguno solo puede liberar los demás. Antes de implementar un algoritmo de control de concurrencia 2PL es necesario considerar. Distintos factores como cuál es la unidad.

Unidad III.

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida. Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización. Hoy en día, organizaciones de todo el mundo invierten fuertemente en la tecnología de información relacionada con la ciberdefensa con el fin de proteger sus activos críticos: su marca, capital intelectual y la información de sus clientes. Ingeniería de la seguridad de datos. Pensar en seguridad de datos y construir defensas desde el primer momento es de vital importancia. Los ingenieros de seguridad tienen como objetivo proteger la red de las amenazas desde su inicio hasta que son confiables y seguras. Los ingenieros de seguridad diseñan sistemas que protegen las cosas correctas de la manera correcta. Encriptación. Si la ingeniería de seguridad de datos protege la red y otros activos físicos como servidores, computadoras y bases de datos, la encriptación protege los datos y archivos reales almacenados en ellos o que viajan entre ellos a través de Internet. Las estrategias de encriptación son cruciales para cualquier empresa que utilice la nube y son una excelente manera de proteger los discos duros, los datos y los archivos que se encuentran en tránsito a través de correo electrónico, en navegadores o en camino hacia la nube. En el caso de que los datos sean interceptados, la encriptación dificulta que los hackers hagan algo con ellos. Detección de intrusión y respuesta ante una brecha de seguridad. Si en la red ocurren acciones de aspecto sospechoso, como alguien o algo que intenta entrar, la detección de intrusos se activará. Los sistemas de detección de intrusos de red supervisan de forma continua y pasiva el tráfico de la red en busca de un comportamiento que parezca ilícito o anómalo y lo marcan para su revisión. Los NIDS no sólo bloquean ese tráfico, sino que también recopilan información sobre él y alertan a los administradores de red. Pero a pesar de todo esto, las brechas de seguridad siguen ocurriendo. Es por eso que es importante tener un plan de respuesta a una violación de datos. Hay que estar preparado para entrar en acción con un sistema eficaz. Ese sistema se puede actualizar con la frecuencia que se necesite, por ejemplo, si hay cambios en los componentes de la red o surgen nuevas amenazas que deban abordarse. Firewall. ¿Cómo mantener a visitantes no deseados y software malicioso fuera de la red? Cuando estás conectado a Internet, una buena manera de asegurarse de que sólo las personas y archivos adecuados están recibiendo nuestros datos es mediante firewalls: software o hardware

diseñado con un conjunto de reglas para bloquear el acceso a la red de usuarios no autorizados. Análisis de vulnerabilidades. Los hackers suelen analizar las redes de forma activa o pasiva en busca de agujeros y vulnerabilidades. Los analistas de seguridad de datos y los profesionales de la evaluación de vulnerabilidades son elementos clave en la identificación de posibles agujeros y en cerrarlos. Pruebas de intrusión. El análisis de vulnerabilidad también puede incluir deliberadamente investigar una red o un sistema para detectar fallos o hacer pruebas de intrusión. Es una excelente manera de identificar las vulnerabilidades antes de tiempo y diseñar un plan para solucionarlas. Hay una línea aún más holística de defensa que se puede emplear para mantener los ojos en cada punto de contacto. Es lo que se conoce como Información de Seguridad y Gestión de Eventos . SIEM es un enfoque integral que monitoriza y reúne cualquier detalle sobre la actividad relacionada con la seguridad de TI que pueda ocurrir en cualquier lugar de la red, ya sea en servidores, dispositivos de usuario o software de seguridad como NIDS y firewalls. Los sistemas SIEM luego compilan y hacen que esa información esté centralizada y disponible para que se pueda administrar y analizar los registros en tiempo real, e identificar de esta forma los patrones que destacan. Internet en sí mismo se considera una red insegura, lo cual es algo que puede asustar cuando nos damos cuenta que actualmente es la espina dorsal de muchas de las transacciones de información entre organizaciones. Para protegernos de que, sin darnos cuenta, compartamos nuestra información privada en todo Internet, existen diferentes estándares y protocolos de cómo se envía la información a través de esta red. Las conexiones cifradas y las páginas seguras con protocolos HTTPS pueden ocultar y proteger los datos enviados y recibidos en los navegadores. Para crear canales de comunicación seguros, los profesionales de seguridad de Internet pueden implementar protocolos TCP/IP y métodos de encriptación como Secure Sockets. Detección de amenazas en punto final. Se pueden prevenir ataques de ransomware siguiendo buenas prácticas de seguridad, como tener software antivirus, el último sistema operativo y copias de seguridad de datos en la nube y en un dispositivo local. Sin embargo, esto es diferente para organizaciones que tienen múltiple personal, sistemas e instalaciones que son susceptibles a ataques. Los usuarios reales, junto con los dispositivos que usan para acceder a la red , suelen ser el eslabón más débil de la cadena de seguridad. Prevención de pérdida de datos. Dentro de la seguridad de punto final hay otra estrategia de seguridad de datos importante: la prevención de pérdida de datos . Esencialmente, esto abarca las medidas que se toman para asegurar que no se envían datos confidenciales desde la red, ya sea a propósito, o por accidente y la gestión de identidad acceso (abreviado: IAM o IdAM) es un modo de saber quién es un usuario y qué tiene permiso.