Auditoría de BBDD: Caso práctico

11 de mayo 2023

Hemos visto la importancia de los datos en las organizaciones. La inconsistencia, pérdida de datos o fuga de información puede tener implicaciones nefastas en las empresas. La auditoría de BBDD trata de asegurar a las empresas la integridad y seguridad de sus datos. Existen diferentes metodologías, técnicas y herramientas que los auditores pueden utilizar al hacer auditorías de BBDD.

Supongamos el siguiente caso de estudio. La gestoría GEST-VAL se dedica a realizar trámites tributarios, como la presentación de distintos impuestos en la administración pública fiscal. Actualmente, cuenta con los siguientes trabajadores:

- Marta: dueña de GEST-VAL, realiza cualquier trámite (de impuestos, facturación, y gestión comercial)
- Sara: administrativa, se encarga de los impuestos
- Ana: administrativa, se encarga de la facturación a los clientes
- Roberto: comercial, se encarga de capturar clientes para la empresa, los da de alta, gestiona su información de cliente, …

Los sistemas que utiliza la empresa son los siguientes:

- Una aplicación para la gestión del pago de impuestos.
- Una aplicación para la gestión de los clientes.
- Una aplicación para la facturación a los clientes.

Todas las aplicaciones se componen de cliente web/móvil y backend-base de datos. Los backend de las aplicaciones se ejecutan en un servidor en la misma máquina. Las 3 aplicaciones utilizan la misma base de datos ORACLE, pero cada una utiliza unos datos específicos. Las tablas de la base de datos son:

- Cliente, datos de los clientes como nombre, dni, dirección, teléfono, mail, descripción, …
- Pago fiscal, datos sobre pagos tributarios realizados por un cliente, como fecha, cantidad, modelo, referencia, comentarios,….
- Factura, datos sobre facturas a clientes, como fecha, cantidad, iva, descripción,...
- Detalle factura, datos sobre las líneas de una factura, como concepto, descripción, cantidad,…

Vamos a utilizar la propuesta metodológica que se presenta en [1] para realizar una auditoría de BBDD a esta empresa. La Tabla 1 muestra las actividades requeridas para una auditoría según esta metodología.

Ejercicio propuesto

El ejercicio consiste en que instanciéis las actividades **de 1 a 6** propuestas en la Tabla 1 para el caso de estudio. Para ello, debéis plantear en cada actividad qué acciones concretas realizaríais y adelantar los resultados que se pueda. Por ejemplo, en la actividad 4 "*Analizar la información encontrada y definir los controles existentes en el sistema de información y en la base de datos*", no podéis hacer la actividad, pero sí plantear qué controles sobre la BD esperáis que haya en la empresa.

Tabla 1. Actividades auditoría de BBDD

1	*Plan de Auditoria Preliminar*	- Conformar el grupo de trabajo que realizara la Auditoria de Base de Datos - Estimar el tiempo necesario para realizar la auditoria.
2	*Levantamiento de la información de la organización*	- Levantamiento de la información sobre el estado actual y características de la organización, infraestructura, recursos humanos y técnicos, procesos de negocio y sistemas de información que lo soportan - Diseño de flujograma de procesos de negocio - Realizar ficha técnica de los sistemas de información que soporta los negocios
3	*Definición de objetivos y alcance de la auditoría de la BD*	- Seleccionar objetivos principales de la auditoría - Definir el alcance de la auditoria de BD
4	*Evaluación de sistemas de control interno*	- Analizar la información encontrada y definir los controles existentes en el sistema de información y en la base de datos.
5	*Análisis de riesgos en las BBDD*	- Determinar a qué amenazas se encuentra expuesta la BD - Determinar qué salvaguardas hay disponibles y qué tan eficaces son frente al riesgo - Estimar el impacto de un riesgo
6	*Diseño de pruebas de auditoria de BD*	- Elaboración de procedimientos de auditoria de BD para cada control a evaluar
7	Ejecución de las pruebas de auditoría	
8	Evaluación de los resultados de las pruebas de auditoría	
9	Elaboración del informe con los resultados de la auditoría	
10	Seguimiento a las observaciones de auditoría de BD	

Referencias.

[1] JHON ALEXANDER LOPEZ y ANDRES FABIAN ZULUAGA TAMAYO. Metodología para el Control de Riesgos para la Auditoría de Bases de Datos. Trabajo de Tesis. UNIVERSIDAD TECNOLÓGICA DE PEREIRA. 2013

1 *Plan de Auditoria preliminar*
2 *Levantamiento de la información de la organización*
3 *Definición de objetivos y alcance de la auditoría de la BD*
4 *Evaluación de sistemas de control interno*
5 *Análisis de riesgos en la BD*
6 *Diseño de pruebas de auditoria de BD*