RETOS EN SEGURIDAD DE BASES DE DATOS

Fred Pinto PhD
fpinto@asesoftware.com

Asesoftware Ltda

OBJETIVOS

Ilustrar los retos en seguridad de bases de datos que nos plantean las nuevas regulaciones.

EL PROBLEMA

- ***Bases de datos que son el eje de operación de las organizaciones y son objeto de riesgo***

- ***Regulaciones que exigen proteger la información***

- ***Metodologías para el desarrollo de controles que debemos adoptar***

- ***Herramientas para implementar controles que no sabemos utilizar***

REGULACIONES Y MARCOS DE GESTIÓN DE IT Y SEGURIDAD

- ***Circular 052***
- ***Circular 014***
- ***Sarbanes Oxley***
- ***PCAOB***
- ***HIPAA(Health Insurance Portability and Accountability Act)***
- ***GLBA (Gramm LeachBliley Act)***
- ***PCI DSS (Payment Card Industry Data Security Act)***
- ***ISO 17799***
- ***COBIT***
- ***ITIL***
- ***…***

EXIGENCIAS DE LAS REGULACIONES

- ***Planes de continuidad de los sistemas de información***
- ***Autenticación de quienes acceden a la información***
- ***Trazabilidad sobre consultas y cambios***
- ***Desarrollo de controles***
- ***Cuentas individuales***
- ***Confidencialidad de la información***
- ***Separación de roles***
- ***Restricción al uso de cuentas privilegiadas***
- ***Cifrado de la información***
- ***Buenas prácticas de gestión de IT(Gestión de incidentes, problemas, cambios, versiones, ….)***
- ***…***

IMPLICACIONES PARA LA GESTIÓN DE BD

- ***Gestión de usuarios***
- ***Autenticación en entornos multicapa***
- ***Separación de responsabilidades y blindaje contra usuarios internos***
- ***Auditoría***
- ***Administración de cambios***
- ***Monitoreo y gestión de problemas***
- ***Disponibilidad***

GESTIÓN DE CUENTAS

•Utilización de cuentas únicas para todos los usuarios (en particular los dba)
•Políticas corporativas de gestión de claves (gestión centralizada de cuentas)

Implicaciones:
•los dba deben tener cuentas particulares!
•deben los usuarios web ser usuarios de la bd?
•centralización en la gestión de cuentas

ASIGNACIÓN DE ACCIONES

- ***Las acciones en la BD deben ser asignables a un usuario***
- ***Que va en contra de esto?***
  - ***Gestión de usuarios en sistemas multicapa (frecuentemente se utiliza un usuario genérico en la BD para atender las solicitudes WEB).***
  - ***Los nombres y claves de los usuarios que ejecutan procesos en lote están "alambrados" en el código***
  - ***Los DBA comparten el uso de cuentas privilegiadas de BD.***
  - ***Las cuentas genéricas de la BD no se aseguran.***

ASIGNACIÓN DE ACCIONES

- *Que hacer en entornos multicapa donde se utiliza conexión genérica a la BD?*
  - *Delegar parte de la responsabilidad a la aplicación:*
    - *Exigir que la auditoría de aplicación deje trazas identificando los usuarios*
    - *Utilizar la auditoría de BD pero exigir que la aplicación configure variables de contexto que luego son registradas en la auditoría de la BD para identificar al usuario.*
  - *Si la aplicación no admite mayores cambios:*
    - *Validar el posible uso de conexiones con usuarios proxy. Se conecta a la BD el usuario WEB, pero se registra que representa a cierto usuario final en un momento dado. De esta forma la auditoría de BD asigna las acciones al usuario final.*

ASIGNACIÓN DE ACCIONES

- ***Que hacer con la autenticación para procesos en lote?***
  - ***El desarrollador típicamente coloca nombre y clave en los fuentes o los lee de un archivo que no tiene mayor protección.***
  - ***Utilizar autenticación por SO. Requiere blindar el uso de la cuenta de SO!.***
  - ***Almacenar usuario y clave en archivos protegidos por certificados. La aplicación solo referencia el repositorio de claves y los certificados, el sistema de autenticación de la base de datos hacer el resto del trabajo.***
  - ***Habilitar reconocimiento del servidor desde donde se ejecutan los procesos en lote.***

SEPARACIÓN DE RESPONSABILIDADES

- ***No utilizar "súper-usuarios" de la BD en tareas del día a día***
- ***Las cuentas dueñas de los esquemas no deben ser utilizadas para la ejecución de la aplicación***
- ***Las responsabilidades de los DBA deben estar claramente delimitadas***
- ***Los DBA no deben tener privilegios para modificar o leer información de la aplicación***
- ***Los privilegios de cada involucrado deben estar en los niveles más bajos necesarios***
- ***Los desarrolladores no deben tener acceso al entorno de producción***
- ***La actividad de SO que afecta la BD debe estar restringida y auditada***

SEPARACIÓN DE RESPONSABILIDADES

- ***El control de usuarios privilegiados resulta uno de las exigencias más complicadas de implementar en los diferentes motores de BD.***
- ***Como evitar:***
  - ***Que el DBA lea tablas de la aplicación?***
  - ***Como limitar sus privilegios sin limitar su capacidad de gestión de la BD?***

BLINDANDO LA BD

Tradicionalmente los súper-usuarios del motor de BD eran "todo poderosos" y poco controlados.
Las regulaciones exigen limitar poderes y controlar acciones.
Los diferentes vendedores de BD empiezan a ofrecer herramientas que blindan la base de datos desde el interior. Las características que debemos buscar en dichas herramientas son:

- ***Posibilidad de auditar las acciones del DBA y que este no pueda manipular las trazas de auditoría***

- ***Permitir configurar alarmas para identificar comportamiento malicioso***

- ***Proteger la información de las aplicaciones de los ojos del DBA***

- ***Permitir configurar diferentes tipos de DBA con responsabilidades limitadas (dba_backups, dba_usuarios, dba_aplicacion, dba_auditor) con responsabilidades limitadas estableciendo un equilibrio de poderes***

AUDITORÍA Y DESARROLLO DE CONTROLES

Elementos comunes en diferentes regulaciones

- ***Entender y documentar procesos***
- ***Comunicar***
- ***Monitorear cumplimiento***

Requerimientos de auditoría

- ***Acceso a información sensitiva***
- ***Cambios a esquemas***
- ***Cambios a datos***
- ***Errores relacionados con seguridad***
- ***Cuentas, roles y permisos***

AUDITORÍA Y CONTROLES

A tener en cuenta:

- ***No basta activar la auditoría***
- ***La auditoría puede impactar el desempeño***
- ***Los controles y en particular la auditoría deben estar alineados con los objetivos del negocio…***

AUDITORÍA Y CONTROLES

- ***Como desarrollar los controles?***
  En el caso más general COSO provee una metodología para identificar los controles.
  En el caso de TI COBIT identifica controles más concretos.

AUDITORÍA Y CONTROLES-COSO

- ***COSO: Committee of Sponsoring Organizations of the Treadway Commission***
- ***COSO: Marco para la gestión de controles***

COSO: CONCEPTOS CLAVE

- ***El control interno es un proceso. Una herramienta para lograr un fin***
- ***El control interno involucra personas***
- ***Se debe esperar del control interno una confiabilidad razonable y no absoluta***
- ***El control interno debe estar orientado al logro de una serie de objetivos***

COSO: CONTROL INTERNO

- **CONTROL INTERNO: PROCESO PROMOVIDO POR LOS ADMINISTRADORES Y DISEÑADO PARA TENER UNA CONFIANZA RAZONABLE EN EL LOGRO DE OBJETIVOS:**
- ***Alineación con objetivos estratégicos***
- ***Efectividad y eficiencia de las operaciones***
- ***Confiabilidad de los reportes de los sistemas***
- ***Cumplimiento de leyes y regulaciones***

COSO: COMPONENTES

- ***Ambiente interno***
- ***Formulación de objetivos***
- ***Identificación de eventos***
- ***Diagnóstico de riesgos***
- ***Respuesta a los riesgos***
- ***Actividades de control***
- ***Información y comunicación***
- ***Monitoreo***

COSO: COMPONENTES

- ***Ambiente interno***
- ***Formulación de objetivos***
- ***Identificación de eventos***
- ***Diagnóstico de riesgos***
- ***Respuesta a los riesgos***
- ***Actividades de control***
- ***Información y comunicación***
- ***Monitoreo***

COBIT

- ***DOMINIOS***
  - ***Planeación***
  - ***Adquirir e implementar***
  - ***Operar y soportar***
  - ***Monitorear y evaluar***

COBIT

PLANEACIÓN

- PO1 Define a Strategic IT Plan and direction
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

COBIT

ADQUIRIR E IMPLEMENTAR

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredit Solutions and Changes

COBIT

OPERAR Y SOPORTAR

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

COBIT

MONITOREAR Y EVALUAR

ME1	***Monitor and Evaluate IT Processes***
ME2	***Monitor and Evaluate Internal Control***
ME3	***Ensure Regulatory Compliance***
ME4	***Provide IT Governance***

CIRCULAR 014

CONTROL INTERNO

- ***Eficiencia***
- ***Prevención de fraudes***
- ***Gestión de riesgos***
- ***Confiabilidad y oportunidad de la información***
- ***Cumplimiento de regulaciones***

ELEMENTOS

- ***Ambiente de control***
- ***Gestión de riesgos***
- ***Actividades de control***
- ***Información y Comunicación***
- ***Monitoreo***
- ***Evaluación independiente***

AREAS

- ***Gestión contable***
- ***Gestión de tecnología***

OTROS ASPECTOS

- ***Departamento de Gestión***
- ***Gestión de los datos***

CIRCULAR 014-Normas para gestión IT

Plan estratégico de tecnología.
Infraestructura de tecnología.
Relaciones con proveedores.
Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
Administración de proyectos de sistemas.
Administración de la calidad.
Adquisición de tecnología.
Adquisición y mantenimiento de software de aplicación.
Instalación y acreditación de sistemas.
Administración de cambios.
Administración de servicios con terceros.
Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
Continuidad del negocio.
Seguridad de los sistemas.
Educación y entrenamiento de usuarios.
Administración de los datos.
Administración de instalaciones.
Administración de operaciones de tecnología.
Documentación.

CIRCULAR 014

- ***Circular 014-Seguridad***

Autorización, autenticación y control de acceso.

Identificación de usuarios y perfiles de autorización los cuales deberán ser otorgados de acuerdo con la necesidad de tener y necesidad de conocer.

Manejo de incidentes, información y seguimiento.

Prevención y detección de código malicioso, virus, entre otros.

Entrenamiento de usuarios.

Administración centralizada de la seguridad

CIRCULAR 014

- ***Circular 014-Administración de datos***
  - ***•Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos.***
  - ***•Verificar la exactitud, suficiencia y validez de los datos de transacciones que sean capturados para su procesamiento (generados por personas, por sistemas o entradas de interface).***
  - ***•Preservar la segregación de funciones en el procesamiento de datos y la verificación rutinaria del trabajo realizado. Los procedimientos deberán incluir controles de actualización adecuados, como totales de control "corrida a corrida" y controles de actualización de archivos maestros.***
  - ***•Establecer procedimientos para que la validación, autenticación y edición de los datos sean llevadas a cabo tan cerca del punto de origen como sea posible.***
  - ***•Definir e implementar procedimientos para prevenir el acceso a la información y software sensitivos de computadores, discos y otros equipos o medios, cuando hayan sido sustituidos o se les haya dado otro uso. Tales procedimientos deberán garantizar que los datos marcados como eliminados no puedan ser recuperados por cualquier individuo interno o tercero ajeno a la entidad.***
  - ***•Establecer los mecanismos necesarios para garantizar la integridad continua de los datos almacenados.***
  - ***•Definir e implementar procedimientos apropiados y prácticas para transacciones electrónicas que sean sensitivas y críticas para la organización, velando por su integridad y autenticidad.***
  - ***•Establecer controles para garantizar la integración y consistencia entre plataformas.***

REQUERIMIENTOS DE AUDITORIA EN BD

- ***Auditar acceso a datos sensitivos(Select)***
- ***Auditar modificaciones a esquemas(DDL: Create, Drop, Alter, …)***
- ***Auditar cambios a datos(DML: Insert, Update, Delete)***
- ***Excepciones de seguridad(Logins fallidos, errores)***
- ***Modificaciones a cuentas & privilegios(Grant, Revoke)***

REQUERIMIENTOS DE AUDITORIA EN BD

- ***Auditar acceso a datos sensitivos(Select)***
- ***Auditar modificaciones a esquemas(DDL: Create, Drop, Alter, …)***
- ***Auditar cambios a datos(DML: Insert, Update, Delete)***
- ***Excepciones de seguridad(Logins fallidos, errores)***
- ***Modificaciones a cuentas & privilegios(Grant, Revoke)***
- ***Controlar las acciones de usuarios privilegiados***
- ***Considerar la amenaza interna: conexiones a BD por fuera de la aplicación o desde el mismo servidor***

OTROS REQUERIMIENTOS

Protección de las trazas

- ***Protección de los DBA y otros usuarios privilegiados***
- ***Consolidación de trazas de diferentes sistemas***

Análisis de las trazas

- ***Reportes***
- ***Alertas***

Controlar acciones de usuarios privilegiados

QUE PREGUNTAS HAY QUE RESPONDER

- ***Quien?***
- ***Cuando?***
- ***Con que programa?***
- ***Donde?***
- ***Que SQL?***
- ***Fue exitoso?***
- ***Como cambiaron los datos?***

QUE TABLAS AUDITAR

- **Auditar todas las acciones?**
  - **Demasiado costoso**
  - **Demasiada información no es realmente información**
- **Aplicar COSO**
  - **Objetivos del negocio**
  - **Riesgos**
  - **Vulnerabilidades**
  - **Controles. Entre otros**
    - **Auditoría de BD. Nivel de detalle depende de los objetivos de control.**
    - **Limitar acciones en la BD**
    - **Generar alertas para comportamiento anómalo**
  - **Evaluar periódicamente**

COMO AUDITAR

- ***Alternativas***
  - ***Auditoría de la aplicación***
    - ***No detecta actividad externa a la aplicación***
  - ***Auditoría nativa de la BD***
    - ***Posible impacto en desempeño(los motores han evolucionado para reducir este impacto)***
  - ***Herramientas que interceptan los llamados a la BD en la red***
    - ***No detectan actividad desde el servidor***
- ***Como gestionar las trazas de auditoría***
  - ***Diferentes regulaciones exigen centralizar las trazas.***
  - ***Diferentes herramientas recolectan las trazas de auditoría y las almacenan en repositorios independientes de las bases de datos auditadas***

COMO AUDITAR

- ***Alternativas***
  - ***Auditoría de la aplicación***
    - ***No detecta actividad externa a la aplicación***
  - ***Auditoría nativa de la BD***
    - ***Posible impacto en desempeño(los motores han evolucionado para reducir este impacto)***
  - ***Herramientas que interceptan los llamados a la BD en la red***
    - ***No detectan actividad desde el servidor***
- ***Como gestionar las trazas de auditoría***
  - ***Diferentes regulaciones exigen centralizar las trazas.***
  - ***Diferentes herramientas recolectan las trazas de auditoría y las almacenan en repositorios independientes de las bases de datos***

HERRAMIENTAS PARA GESTIÓN DE TRAZAS

- ***Que características buscar?***
  - ***Integración de trazas de diferente motores de BD e instancias en repositorio seguro***
  - ***Integración con el "blindaje" de la BD***
  - ***Utilización de la auditoría nativa de la BD con bajo impacto en el desempeño***
  - ***Gestión de los niveles de auditoría en la BD***
  - ***Configuración de reglas para detectar comportamiento anómalo***
  - ***Configuración de alertas***
  - ***Integración con un sistema de WorkFlow para gestión de incidentes***
  - ***Integración con un sistema de gestión de riesgos y controles***

RESUMEN

- ***Hemos enfatizado los siguientes retos propuestos por las regulaciones***
  - ***Trazabilidad de las acciones en BD***
  - ***Blindaje de la BD***
  - ***Desarrollo y gestión de controles dentro del marco de alguna metodología***
  - ***Utilización de la auditoría como base para la implementación de controles***
  - ***Gestión de trazas de auditoría con herramientas que apoyen la implementación de controles***

PREGUNTAS