INFORME DE AUDITORÍA A LA ADMINISTRACION DE LAS BASES DE DATOS EN AMBIENTE PRODUCTIVO

Contenido

Objetivo

- Comprobar los niveles de seguridad y control de acceso definidos en las bases de datos, con el fin de identificar oportunidades de mejora para que se implementen planes de acción que mitiguen los riesgos observados.
- Verificar distribución, integridad, conservación y transporte de la información en las base de datos.
- Evaluar el nivel de servicio y soporte tecnológico con que cuenta la las bases de datos para su disponibilidad y funcionalidad.

Alcance

La evaluación a la administración de la bases de datos, se realiza a la bases datos (Misional e Icfesdb) instaladas en el ambiente de producción, a los recursos de apoyo disponibles para la operación, conservación y mantenimiento de la información allí contenida, teniendo en cuenta las disposiciones normativas y las mejores prácticas para el manejo de esta información. La revisión se realiza del 10 de mayo de 2016 al 14 de junio de 2016.

Metodología

Durante la auditoría se desarrollaron:

- Recolección de información en la fuente (solicitud) y acceso a la base de datos de producción
- Análisis de información recibida.
- Reuniones con el responsable de la administración de la bases de datos.

Información Solicitada

Con el fin de realizar la labor inicial se solicitó:

INFORMACIÓN SOLICITADA	ÁREA GENERADORA DE INFORMACIÓN
Distribución de la BDD; modelo entidad relación de las BDD productivas; roles y privilegios; usuarios de servidores (funciones asignadas); reportes de seguridad imperva. Acuerdos niveles de servicio del procedimiento H4.P.2.; solicitudes de actualización de bases de datos-formato H4.2.F01; Log o trazabilidad del control de cambios del transporte o despliegue realizado a las BDD; Reporte de mantenimiento de las BDD realizado por el proveedor; lista de migración de datos por actividades de las pruebas definidas en calendario; Lista de tablas sensibles objeto de trazabilidad; listado de los valores de parámetros en la BDD;	Subdirección de Información

Desarrollo de Auditoría

Con base en la información recolectada y las entrevistas efectuadas se realizaron las siguientes actividades:

- Análisis y evaluación de la información suministrada, arriba enunciada, y entrevista realizada al administrador de la base de datos , los cuales proporcionaron datos para la revisión, así mismo y determinaron elementos (tareas, información) de apoyo a la evaluación.
- Análisis de información de la base de datos puesta en producción.

- Evaluación de los resultados realizados a las pruebas funcionales del software.

Resultados

De la revisión realizada a las bases de datos de producción, se observó la siguiente situación:

<u>Controles de acceso y usuarios base de datos:</u>

Comprende verificación a la administración de usuarios, autenticación y permisos en la base de datos.	
Observación y Recomendación	1. En el reporte log "Auditoria Misional" del sistema de seguridad "Imperva" se observa que la cuenta de usuario "arquitectos", la cual tiene acceso para administrar (recursos, objetos, integridad, ajustes) la base de datos Prisma, es utilizada por los usuarios: "aarboleda", "varanda", "lbenavides", "jdiaz", "smeza", sin cumplir con el criterio de uso personal de las cuentas de usuario y password. *<u>Recomendación</u>* *Las contraseñas son de uso personal e intransferible, no se deben compartir con ninguna persona. Luego es necesario reconsiderar el uso compartido que tiene el usuario genérico "arquitectos" y asignar uno específico para cada usuario, de tal manera que se reconozca el propietario de la cuenta, de acuerdo con lo definido en la política de base de datos en cuanto a la seguridad de los usuarios de las bases de datos* 2. Además, de la revisión a los roles con privilegio, opción de administración "WITH ADMIN_OPTION", los cuales permite borrar,

insertar crear llaves de referencia, crear triggers, actualizar datos y ejecutar procedimientos, se evidencio que no menos de cuatro cuentas de usuario, independientemente de los que lo requieren, tienen habilitados los parámetros de administración:

Usuario	Rol	Adm
Arquitectos	ROL_ORGANIZACIONES;ROL_MINISTERIOEDUCACION, ROL_DIVISIONPOLITICA, ROL_DIRECTORIOUNICO ROL_PIR,ROL_PARAMETROS, ROL_DISCAPACITADOS, ROL_RESULTADOS, R_NSM_CONSULTALK, ROL_ARMADO, ROL_CITACION, ROL_APROVISIONAMIENTO, ROL_PERSONAS, ROL_USUARIOS, ROL_CALIFICACION_DML, ROL_CALIFICACION, ROL_INSCRIPCION, ROL_RECAUDO, ROL_ENCUENTASYFORMULARIOS, ROL_RESULTADOS_DML, ROL_ZINTERNO, ROL_INSTRUMENTOS, ROL_SOPORTEINTERNO, ROL_TEMPORALES, ROL_MATRICULADO, ROL_SOLICITUDES, CONNECT, RESOURCE.	Si
Jdiaz	ROL_ZINTERNO, ROL_CITACION, ROL_DIVISIONPOLITICA, ROL_PERSONAS, ROL_SOLICITUDES, ROL_APROVISIONAMIENTO, ROL_DIRECTORIOUNICO, ROL_PIR, ROL_RESULTADOS, ROL_CALIFICACION_DML, ROL_SOPORTEINTERNO, ROL_TEMPORALES, ROL_ARMADO, R_NSM_CONSULTALK, ROL_MATRICULADO, CONNECT, ROL_INSCRIPCION, ROL_PARAMETROS, ROL_CALIFICACION, ROL_ENCUENTASYFORMULARIOS, ROL_ORGANIZACIONES, ROL_RECAUDO, ROL_RESULTADOS_DML, ROL_DISCAPACITADOS, ROL_MINISTERIOEDUCACION, ROL_USUARIOS, RESOURCE.	Si
Varanda	ROL_RESULTADOS, ROL_CITACION, ROL_INSCRIPCION, ROL_PIR, ROL_SOPORTEINTERNO, ROL_ARMADO, ROL_CLASIFICACION, ROL_ENCUENTASYFORMULARIOS, ROL_MATRICULADO, ROL_PARAMETROS, ROL_TEMPORALES, ROL_DISCAPACITADOS, ROL_DIVISIONPOLITICA, ROL_MINISTERIOEDUCACION, ROL_ORGANIZACIONES, ROL_APROVISIONAMIENTO, ROL_INSTRUMENTOS, ROL_RECAUDO, ROL_USUARIOS, ROL_CALIFICACION, CONNECT, ROL_DIRECTORIOUNICO, ROL_ZINTERNO, ROL_SOLICITUDES, ROL_PERSONAS.	Si

	- De la revisión a la lista de roles, se encontró que al usuario "Jvargas" sin tener función de administración, se le permite administrar la base de datos. -crear, eliminar y/o modificar archivos de la base de datos (create table, create any table; drop any table; alter any table). *<u>Recomendación</u>* *La cantidad de usuarios con privilegios super usuario o administrador del sistema operativo que soporta la base de datos debe ser limitada (máximo dos usuarios). Se debe evaluar la cantidad de usuarios que utilizan estos privilegios y corregir su asignación.* 3. Se encontró que el usuario "Jmelendez" se encuentra activo en la base de datos, la cual correspondió a un contratista que prestó servicios de administración de base de datos. *<u>Recomendación</u>* *Cuando un usuario no se esté utilizando por un periodo de 30 días se debe bloquear. Se recomienda validar permanentemente las cuentas de usuario para bloquear los que se ausentan y/o retiran del Instituto, a fin de cumplir la política. Para los contratos con terceros "Contratistas", informar de manera oportuna a través de la mesa de ayuda, cualquier novedad, terminación anticipada o prórroga, para garantizar el adecuado mantenimiento de las cuentas de usuarios.* *Igualmente, en la creación de usuarios se debe definir la vigencia, en especial para el control de usuarios que son contratistas.*

4. En la revisión realizada a los perfiles de usuario de la base de datos "Misional", se observó que los siguientes perfiles, no limitan los parámetros para el manejo de password, lo que puede exponer la seguridad de las cuentas de usuarios, por ejemplo:

Perfiles	Parámetro	Observación
Prueba_icfes Sysman Arquitectos(1 usuario) Misional (28 usuario) Monitoring Profile (1 usuario) Default (32 usuario)	Password_life_time	Se permite utilizar la contraseña sin límite de uso.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile (1 usuario) Default(32 usuario)	Password _reuse_time	Se permite utilizar una misma contraseña en cualquier momento.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile (1 usuario) Default(32 usuario)	Password_reuse_max	Se permite volver a utilizar una contraseña.
Prueba_icfes	Password_grace_time	El perfil no tiene límite periodo de gracia de no utilización en su inicio.

Recomendación

Es importante evaluar los valores que tienen los parámetros que administran seguridad y control en el manejo de password de usuario, de acuerdo con lo establecido en la política de base de datos, en cuanto a la seguridad de las contraseñas de las bases de datos

5. Se observan perfiles de usuario de la base de datos "Misional", para los cuales no hay limitante en la utilización de recursos del

sistema en la BDD, lo que puede afectar la adecuada utilización del sistema, por ejemplo:

Perfiles	Parámetro	Observación
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile (1 usuario) Default(32 usuario)	Composite_limite	No hay límite
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile Default(32 usuario)	Sessions_per_user	Límite de 180 sesiones para el perfil "prueba_icfes". No hay imite de sesiones para el resto de perfiles
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile (1 usuario) Default(32 usuario)	Cpu_per_session	Sin límite de Cpu por sesión.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring Profile (1 usuario) Default(32 usuario)	Cpu_per_call	Sin límite de Cpu por llamado.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring_ Profile (1 usuario) Default(32 usuario)	Logical_reads_per_session	Sin límite de lectura por sesión.
Arquitectos(1 usuario) Misional(28 usuario) Monitoring_ Profile Default(32 usuario)	Logical_reads_per_call	Sin límite de lectura por llamado.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring_ Profile (1) Default(32 usuario)	Idle_time	Los perfiles no tiene tiempo de inactividad.
Prueba_icfes Sysman Arquitectos(1 usuario) Misional(28 usuario) Monitoring_ Profile (1 usuario) Default(32 usuario)	Connect_time	Tiempo de conectividad ilimitada.

	<u>Recomendación</u> *Se hace necesario evaluar los criterios establecidos para el control y administración de los recursos del sistema que se asignan a los usuarios que acceden la base de datos, de acuerdo con lo establecido en la política de seguridad de la base de datos en cuanto a la realización de afinamientos para optimizar el rendimiento de la base de datos y garantizar el uso adecuado de los recursos.* 6. No hay declaraciones escritas de privilegios de acceso al sistema que se otorgan a los usuarios, en ella el funcionario responsable del manejo de la cuenta de usuario de la base de datos manifiesta, entiende y acepta las condiciones de acceso. *<u>Recomendación</u>* *Debe existir un sistema formal de registro/cancelación de usuario para acceso a las BD, aplicaciones y/o servicios. Debe entregarse a los usuarios una declaración escrita de sus privilegios, y se requiere que sea firmada por ellos de tal manera que entiendan cuáles son las condiciones de su acceso, de acuerdo con lo definido en la política de base de datos en cuanto a la seguridad de los usuarios de las bases de datos.*
Estándares y regulaciones - Política de Contraseñas – Seguridad de la Información v 1.1, H3.P1. - Política de Base de datos – Seguridad de la información v1.0, H3.P1 - Modelo de Gestión IT4 plus MINTIC, numeral 6.2.1.4 sistemas de almacenamiento. - Manual Gobierno en Línea: Información-Gestión de la calidad y de seguridad de los componentes de información.	

- ISO 27001:2012 Gestión de seguridad de la información, Anexo A.9 Control de acceso.

<u>Controles a la gestión de la base de datos:</u>

Incluye la gestión a las actividades que se realizan para administrar y controlar la operación sobre las bases de datos productivas.	
Observación - Recomendación	7. Se evidencia que no menos del 70% de las actividades registradas en log de trazabilidad del sistema de seguridad "Imperva" de febrero a mayo de 2016 sobre la operación de cambios en la base de datos no se encuentran reportadas en el listado control que administra los arquitectos de la base de datos. <u>Recomendación</u> *Evaluar que todo transporte de datos o estructura de software al ambiente de producción de la base de datos esté registrado en una bitácora confiable y segura que mantenga el control de toda la información autorizada que se despliega al ambiente.* 8. De la revisión al control de las solicitudes de actualización de base de datos que se lleva en el formato "H4.2.F01" para los 5 últimos meses, se evidenció que no se elaboró registro de novedades en la base de datos misional de producción. Únicamente se presentaron dos novedades de actualización para el ambiente icfes-interactivo (una del 19 de mayo de 2016 y otra del 10 de junio de 2016), los cuales no son consecuentes con el registro de trazabilidad del sistema de seguridad y monitoreo "Imperva" que solamente para el mes de

abril/016 reportó 3200 eventos en el ambiente de producción misional.

<u>Recomendación</u>
Propender por preservar un registro único y confiable que mantenga el control de información que ingresa a la base de datos.

9. De la revisión a los informes recibidos del proveedor UNE sobre el desempeño de las bases de datos Misional durante los periodos de marzo y mayo de 2016, se encontró que:
   - Se tiene uno objetos (archivos y/o procedimientos) que se encuentran inválidos en la base de datos que no han sido corregidos o regularizados, según el informe de mayo/2016 en su numeral "3. Esquema: Objetos inválidos".
   - Existen por lo menos de 162 constraints (restricciones) deshabilitadas que no han sido tratados y se encuentran relacionados en los informes de marzo y mayo de 2016.
   - En los informes se citan los siguientes usuarios con rol administrador de base de datos (DBA), cuya función debe ser evaluada:

Usuario	**Role**	**Opción de administración**	**Role por default**
Jchaves	DBA	No	Yes
Cdiazcat	DBA	Yes	Yes
Rman	DBA	No	Yes
Bfernandez	DBA	No	Yes
Dalvarfe	DBA	No	Yes
Jvelasquez	DBA	No	Yes
Mgonzalez	DBA	No	Yes

Ytorres	DBA	No	Yes

10. De la revisión a las actividades definidas para crear pistas de auditoría a los archivos (tablas) con información sensible de la base de datos, en el documento: "Plan General de Seguridad para Base de Datos", se evidenció que las siguientes tareas del año 2015 se encuentran en estado pendiente:

- Revisión y análisis de los datos arrojados por la auditoria periódica (17/08/2015).
- Auditoría a la creación de librería de comandos (library statements). (17/08/2015).
- Aseguramiento de los objetos de la base de datos. (tales como: tablas e índices no están operando en modo "NOLOGGING"). (17/08/2015).
- Revocar los privilegios de ejecución del rol público sobre los paquetes: UTL_FILE, UTL_SMTP, UTL_TCP, UTL_HTTP, DBMS_RANDOM, DBMS_LOB, DBMS_SQL, DBMS_SYS_SQL, DBMS_JOB, DBMS_BACKUP_RESTORE, DBMS_OBFUSCATION_TOOLKIT (17/08/2015).
- Respaldo del log y trazabilidad de operaciones de la base de datos. Se recomienda que todos los redo logs estén mirror on-line y que existan al menos 2 grupos de redo log (17/08/2015).
- En la capa de conexión a la base de datos activar el log de conexiones establecidas (17/08/2015)
- Establecer módulos de trazabilidad en las aplicaciones que se conectan a la base de datos para obtener información del usuario final que está accediendo a la base de datos (17/08/2015).

Recomendación

Evaluar las recomendaciones que efectúa el proveedor en sus informes periódicos en materia de

	distribución y seguridad de la base de datos para mejorar el desempeño y protección de los datos.
Estándares y regulaciones - Modelo de Gestión IT4 plus MINTIC, numeral 6.2.1.4 sistemas de almacenamiento. - Manual Gobierno en Línea: Información-Gestión de la calidad y de seguridad de los componentes de información. - ISO 27001:2012 Gestión de seguridad de la información, Anexo A.12.1.3 Gestión de capacidad	

Controles a documentación de la base de datos

La documentación proporciona entendimiento técnico, operativo, funcional y direccional que se da al proceso de la base de datos	
Observación - Recomendación	11. De la revisión al documento: "Plan General de Seguridad para Base de Datos", realizado en el segundo semestre de 2015, se observó que los resultados obtenidos de este plan no han sido incluidos o actualizados en un manual o procedimiento del proceso gestión de seguridad de la información. *Recomendación* *Es importante evaluar la actualización de los procedimientos, de tal manera que incluyan los mecanismos de control definidos en el plan de seguridad de base de datos (2015).* 12. Los procedimientos y documentos que detallan el proceso de gestión de seguridad de la información, no incluyen la descripción de las actividades que se realizan para el despliegue o transporte de datos y software de la base de datos en el servidor de la Nube, la cual muestra

	información de los aspirantes de pruebas por internet. *<u>Recomendación</u>* *Evaluar que en los manuales del proceso se incluya las actividades que permiten ejercer control sobre el transporte de datos y software en la base de datos Nube, la cual contiene información que se presenta a los usuarios por internet.* 13. No se ha formalizado el registro formato control que especifique los objetos (archivo y procedimientos) y componentes datos que se actualizan, modifican o eliminan en las bases de datos de producción. El procedimiento H4.P2 hace la descripción para la actualización de base de datos pruebas y desarrollo. *<u>Recomendación</u>* *Se requiere formalizar el log de trazabilidad, en lo posible automático, para tener registro de las operaciones que se realizan en las bases de datos de producción.*
Estándares y regulaciones - Política de Base de datos – Seguridad de la información v1.0 H3.P1 - Modelo de Gestión IT4 plus MINTIC, numeral 6.2.1.5 Sistema de bakcup. - ISO 27001:2013 Gestión de seguridad de la información, anexo A.12.3 copias de respaldo	

<u>Controles al plan de continuidad del servicio base de datos</u>

Las pruebas que se realizan al plan de continuidad, permite preparar a la institución para una emergencia, así como identificar problemas y fallas que se puedan tener con el plan, para su corrección oportuna.	
Observación - Recomendación	11. No se evidencia registro de pruebas realizadas a la continuidad de la operación de las bases de datos para mitigar eventualidades de interrupción que se puedan presentar en el data center del proveedor UNE. *Recomendación* *Coordinar junto con el proveedor TIGO-UNE, la programación de pruebas de funcionalidad de las bases de datos, en las cuales considere escenarios de continuidad de operación que realiza el Icfes.*
Estándares y regulaciones - Modelo de Gestión IT4 plus MINTIC, numeral 6.5.2.4 Gestión de continuidad. - ISO 22301:2012 Sistema de gestión de continuidad de negocio, numeral 8.5 Ejercicio y pruebas - *COBIT 5, proceso DSS04 Administración de la continuidad*	

Conclusiones

Como resultado de la evaluación realizada a la base de datos productiva, presentamos la siguiente conclusión:

- Se encuentran implementados niveles de seguridad para el acceso a las bases de datos productivas, sin embargo se observan algunas debilidades, como las arriba mencionadas, de administración de acceso a usuarios y de definición de parámetros de control de password y de recursos al sistema que afectan la protección de la información y requieren ser tratadas.

- Atender oportunamente los comentarios y recomendaciones que realiza el proveedor UNE en los informes mensuales y actualizar la

documentación establecida para el proceso de gestión de la información, en cuanto a la administración y seguridad de las bases de datos.

- Se tienen definidos procedimientos de réplicas automáticas de información de las bases de datos y procesos de respaldo de datos, no obstante no se han realizado pruebas de interrupción que constaten la continuidad de operación de las bases de datos.