UNIDAD DE AUDITORÍA INTERNA

Informe de Auditoría Nº 27/18

Gestión de Bases de Datos

INFORME DE AUDITORÍA Nº 27/2018[1]
Gestión de Bases de Datos

Índice

[1] Auditores intervinientes: [redacted]

INFORME DE AUDITORIA Nº 27/2018
Gestión de Bases de Datos

I. INFORME EJECUTIVO

1. Objeto de la Auditoría

Evaluar la gestión de las bases de datos, la administración de los motores/gestores que las soportan, analizando los procedimientos de diseño, interrelación, el establecimiento de controles, la administración de la seguridad, y las garantías de resguardo y recupero.

Adicionalmente, se evaluará la aplicabilidad de cada uno de los nueve Objetivos Estratégicos establecidos en los lineamientos del planeamiento 2018, y de corresponder, se verificará su grado de cumplimiento.

2. Alcance

Comprende el análisis de los gestores de bases de datos del Organismo, la administración de seguridad conjuntamente con las garantías de funcionamiento, realizando las tareas de acuerdo con las Normas de Auditoría Gubernamentales para las actividades de Tecnología de la Información (TI).

Complementariamente, y en consonancia a los lineamientos SIGEN para el año 2018, en caso de corresponder se verificará el grado de cumplimiento de los siguientes Objetivos Estratégicos: 1) Relevamiento del estado de aplicación de sistemas normalizados de gestión; 2) Responsabilidad social; 3) Responsabilidad ambiental; 4) Costos de la “no calidad”; 5) Corrupción cero; 6) Matriz legal; 7) Identificación de centros de responsabilidad de procesos; 8) Construcción de programas de incentivos a la productividad; 9) Procesos de innovación en los territorios.

3. Observaciones, recomendaciones, opinión del auditado y comentario de la UAI

Mediante Nota de la Dirección Nacional Asistente de Sistemas de Información, Comunicación y Calidad “NO-2018-66643857-APN-DNASICYC#INTA”, se recibió respuesta al presente informe, transcribiéndose a continuación las observaciones más relevantes con sus respuestas:

Observación N° 1:
El Organismo no tiene definido su diccionario de datos corporativo, en donde se establezcan las pautas de diseño homogéneas de las diferentes bases, ni un repositorio de la documentación de las bases de datos. Tampoco se estableció la responsabilidad del rol DBA (Administrador de bases de datos), que tenga injerencia en los aspectos de diseño, técnicos, legales y calidad de los datos, se aclara que una parte de este rol lo cumplía una consultora hasta septiembre de 2018.

Recomendación:
Se debe definir el diccionario de datos corporativo del Organismo, en donde se fijen los procedimientos relacionados con cada una de las actividades, las pautas de diseño y de gestión de los datos (gestores y base de datos). Adicionalmente se debe asignar el rol de DBA, para que se puedan llevar a cabo las cuestiones planteadas. Informar a esta UAI las acciones y plazo de regularización.

Opinión del auditado:
Parcialmente de acuerdo.
Hasta principios del 2018 la Gerencia de Informática no tenía injerencia directa sobre el desarrollo de las aplicaciones disponibles que le fueron delegadas.
En relación con la administración de los datos de cada base, cabe señalar que la responsabilidad primaria sobre la administración de estas bases de datos fue del equipo competente del área responsable de la aplicación y esta Gerencia brindo las condiciones de infraestructura y conectividad para su alojamiento.
Requerir hoy el diccionario de datos como requisito para su alojamiento implicaría sacar de línea muchas de las aplicaciones existentes en producción, destacando que esta decisión excede lo meramente técnico y entendemos, debe ser analizado por más de un área de competencia (DGA, GGI, GI y otras áreas dueñas de cada aplicación) para determinar plazos y formas de regularización de tal requerimiento. Además, debe ser elevado al Comité de Seguridad Informatica para su conocimiento y consideración.
En relación con el rol DBA, que hoy es compartido en la GI por distintos perfiles y que se considera estratégico y necesario, debemos señalar que lamentablemente, a pesar de los esfuerzos, la dificultad presupuestaria y de contratación que tiene el INTA, sumado el nivel de remuneración de mercado respecto del escalafón interno para este tipo de recurso, imposibilitaron la cobertura de esa posición necesaria.
Elevaremos esta recomendación a la DNA de Organización y Desarrollo del Potencial Humano para que se proceda en ese sentido.
Elevaremos, también, la necesidad presupuestaria para cubrir los costos de capacitación de los recursos propios de la GI, en esta temática de DBA.
Teniendo en cuenta la gran cantidad de aplicaciones legadas, el crecimiento constante de informatización de procesos y de digitalización de información, y considerando la cantidad de recursos de la GI, es imposible y no sería deseable, la homogeneización completa de BD de las aplicaciones. Buscamos mantener ciertos estándares de cara al futuro y en función de la actualización y reemplazo de los aplicativos iremos modificando el escenario actual. Es económica y técnicamente inviable realizarlo de otra manera en este contexto.
Es estrategia de esta DNA y de la GI, la constitución de repositorios (DataWarehouse) oficiales del Organismo para la consolidación de las entidades principales, aportados por cada sistema de gestión y así también sus registros históricos, de forma tal de que se constituya como repositorio principal de consumo y explotación de datos validados de los procesos internos de cada área de competencia. Esta tarea comenzó a planificarse en la segunda mitad del año 2018 con varias reuniones de integración en la que participaron todas las direcciones de la sede central.

A tales efectos ya está en construcción el repositorio DataWarehouse integrado de RRHH, DGA y Cartera de proyecto 2013, actualmente en una base de datos intermedia (staging), con procesos implementados que integran cronológicamente los datos de las respectivas bases de datos productivas.
La integración final en el DW pretende homogenizar el repositorio y garantizar la integridad de los datos para consumo y explotación para los distintos sistemas y reportes.

PLAZO DE REGULARIZACIÓN: como se indicó elevaremos para consideración del Comité de SI la propuesta del plan de integración final del repositorio como así también el procedimiento escrito para la realización de estas integraciones y la construcción de la documentación derivada. Se formalizará, también, los pedidos para cubrir el puesto crítico de DBA y el pedido de recursos presupuestarios para la capacitación del personal propio.

Comentario de la UAI:
Si bien el auditado expresó las consecuentes acciones a encarar, pero al no haber indicado el plazo de regularización ni iniciado su cronograma de tarea, la observación se categoriza como **Sin Acción Correctiva Informada** hasta que se se remita documentación respaldatoria de la realización de las acciones propuestas.

Observación N° 2
La asignación de los permisos sobre las bases de datos y sus gestores se realiza otorgando a los administradores de los sistemas, usuarios con amplios privilegios (db_owner" o "GRANT ALL privileges") que permitirían el acceso al ambiente de producción. Destacándose además los casos particulares de las bases de datos de la Gerencia de Procesos y Calidad, de la DNA OyPH y de la DGA.

Recomendación:
Como primera medida se debe articular con el Responsable de Seguridad Informática la definición de los tipos de permisos a otorgar para el ambiente de producción sobre los gestores y las bases de datos, de manera tal que exista una adecuada separación de ambientes. Posteriormente, revisar los permisos otorgados y comenzar un proceso de actualización de acuerdo a lo que se definió.

Adicionalmente, la Gerencia de Informática conjuntamente con el Responsable de Seguridad Informática deben definir la estrategia de utilización y resguardo de los usuarios administradores de los gestores de base de datos. Informar a esta UAI las acciones y plazo de regularización.

Opinión del auditado:
parcialmente de acuerdo.
Efectivamente, estos usuarios con privilegios son requeridos por las áreas mencionadas para la gestión de sus respectivas Bases de Datos. Cabe aclarar que, en ningún caso, los usuarios designados en cada área poseen los mismos roles en otras bases de datos, quedando circunscriptos a los permisos de sus propias bases de datos.

Esta práctica se corresponde con la necesidad de dar respuesta a un requerimiento recibido, basado en una necesidad operativa de las áreas mencionadas y del organismo.
Procederemos a tomar contacto con la DGA, DNA de Organización y Desarrollo del Potencial Humano y la DNASICyC para establecer en conjunto un plan de adecuación que segregue los niveles de acceso en este ambiente productivo de estas bases de datos, acorde a las necesidades y posibilidades de estas áreas involucradas, tratando de evitar la salida de estas aplicaciones de producción.
Por tratarse de aplicativos críticos para el funcionamiento actual del INTA, presentaremos al Comité de Seguridad de la Información el plan acordado con cada área para su consideración, aprobación e implementación. Esta última acción sujeta a la posibilidad de contar con el recurso especializado para la gestión y administración de las Bases de Datos.

Comentario de la UAI:
Si bien el auditado expresó las consecuentes acciones a encarar, pero al no haber indicado el plazo de regularización ni iniciado su cronograma de tarea, la observación se categoriza como **Sin Acción Correctiva Informada** hasta que se se remita documentación respaldatoria de la realización de las acciones propuestas.

4. Conclusión

Del relevamiento de bases de datos del Organismo realizado por la Gerencia de Informática se desprenden varios de los temas observados, entre los que se destaca la asignación de privilegios y la dispersión en la responsabilidad en la administración de las mismas.

De acuerdo a lo evaluado de la Gestión de las Bases de Datos en el Organismo, se entiende que las cuestiones operativas planteadas son de compleja solución, ya que involucran a varios sectores y en algunos casos demandaría la realización de importantes erogaciones.

Sin embargo, se considera oportuno la propuesta de involucrar a todos los actores necesarios del Organismo y con ello, planificar la adecuación del ambiente de producción tendiente a mejorar el esquema de seguridad y a mantener una adecuada segregación de funciones, tal como lo definen las normas de control interno.

Además, es necesario indicar que el mantenimiento de los servidores y el sistema de backup de las bases es adecuado.

CABA, 21 de diciembre de 2018.

II. INFORME ANALÍTICO

1. Objeto de la Auditoría

Evaluar la gestión de las bases de datos, la administración de los motores/gestores que las soportan, analizando los procedimientos de diseño, interrelación, el establecimiento de controles, la administración de la seguridad, y las garantías de resguardo y recupero.

Adicionalmente, se evaluará la aplicabilidad de cada uno de los nueve Objetivos Estratégicos establecidos en los lineamientos del planeamiento 2018, y de corresponder, se verificará su grado de cumplimiento.

2. Alcance

Comprende el análisis de los gestores de bases de datos del Organismo, la administración de seguridad conjuntamente con las garantías de funcionamiento, realizando las tareas de acuerdo con las Normas de Auditoría Gubernamentales para las actividades de Tecnología de la Información (TI).

Complementariamente, y en consonancia a los lineamientos SIGEN para el año 2018, en caso de corresponder se verificará el grado de cumplimiento de los siguientes Objetivos Estratégicos: 1) Relevamiento del estado de aplicación de sistemas normalizados de gestión; 2) Responsabilidad social; 3) Responsabilidad ambiental; 4) Costos de la “no calidad”; 5) Corrupción cero; 6) Matriz legal; 7) Identificación de centros de responsabilidad de procesos; 8) Construcción de programas de incentivos a la productividad; 9) Procesos de innovación en los territorios.

3. Tarea realizada

El trabajo se orientó a verificar los aspectos funcionales de la administración de los gestores de bases de datos, analizar el universo de las bases, la asignación de permisos y las garantías de continuidad.

Además, el trabajo incluye análisis de la documentación, verificación de implementación de procedimientos y controles.

4. Marco de referencia

4.1. Análisis de Auditoría

Relevamiento

Mediante Nota UAI N° 335/18 (NO-2018-57391481-APN-UAI%INTA), esta Unidad de Auditoría Interna (UAI) solicitó a la Gerencia de Informática (GI), información y documentación a fin de realizar el trabajo de campo de auditoría.

La GI informó que existen 141 Bases de Datos Institucionales, acorde al relevamiento que efectuó. De ese universo se desprende que alrededor de 80 bases tienen estructuras predefinidas y fijas establecidas por los aplicativos o sistemas.

Desde la información suministrada se identificaron 4 centros de cómputos, de los cuales 3 se encuentran en predios del INTA y el restante es el Data Center de la empresa Telecom, cuya distribución se expone en el Cuadro N° 1.

Cuadro N° 1: Centros de Cómputos del Organismo

Centro de Computo	Cantidad de Base de Datos
Data Center Telecom (TECO)	70
Centro de Cómputos Edificio Calle Chile	57
Centro de Cómputos CNIA	8
Centro de Cómputos Edificio Calle Rivadavia	6
Total	141

Fuente: Elaboración propia a partir de datos de la GI

Los gestores de bases de datos que se implementaron en el ambiente de producción en el Organismo se distribuyen de acuerdo a lo expuesto en el Cuadro N° 2:

Cuadro N° 2: Bases de datos INTA por Gestores

Gestor de Bases de Datos	Cantidad Bases de Datos
Microsoft SQL Server	69
MySQL	40
Microsoft Exchange 2016	24
PostgreSQL	8
Total	141

Fuente: Elaboración propia a partir de datos de la GI

Adicionalmente, del relevamiento se desprenden que los servidores (físicos, virtuales, rancher, etc.) que tiene instalados estos gestores ascienden a 39, excluyendo de este análisis los servidores relacionados con el correo electrónico Institucional “Microsoft Exchange 2016” por ser un producto que soporta una tarea específica.

Gestores MySQL

Los gestores MySQL instalados son los denominados “de código abierto” y de acuerdo al relevamiento se distribuyen de siguiente forma (Cuadro N° 3):

Cuadro N° 3: Versiones de Gestores MySQL

Versión	Cantidad	Lanzamiento
5.0.x	2	2005
5.1.x	3	2008
5.5.x	13	2010
5.6.x	1	2012
5.7.x	1	2015
mariadb 10.1.23	1	2017

Fuente: Elaboración propia a partir de datos de la GI

Según lo que figura en la página Web oficial de MySQL, la última versión estable que se permite descargar es la 8.0.13 (lanzada en el 2018). De acuerdo a los Gestores MySQL implementados en el Organismo se desprende que las versiones instaladas están desactualizadas y que en la mayoría de los casos ya no cuenta con soporte por parte del proveedor. Por lo expuesto, se debería tender a la actualización y estandarización de estos gestores utilizando versiones más actualizadas de forma tal que facilite su administración y la optimización de las mejoras en la calidad de servicio de los mismas.

Gestores Microsoft SQL Server

Los gestores SQL Server instalados en el ambiente de producción tienen la siguiente distribución de versiones (Cuadro N° 4):

Cuadro N° 4: Versiones de Microsoft SQL

Versión	Cantidad	Lanzamiento
MSSQL - SQL Server 2005 SP4	3	2010
MSSQL - SQL Server 2008 R2	4	2010
MSSQL - SQL Server 2014 SP2	4	2016
MSSQL - Express	1	S/D

Fuente: Elaboración propia a partir de datos de la GI

Al igual que sucede con MySQL las versiones instalados de Microsoft SQL Server están desactualizadas. De acuerdo a lo expuesto en la Web oficial de Microsoft, la última versión de este producto es “SQL Server 2017”, sin embargo, a diferencia de los otros gestores, para su actualización es necesario, como primera medida la adquisición de las licencias respectivas.

Gestores PostgreSQL

En el Centro de cómputos del Centro Nacional de Investigaciones Agropecuarias (CNIA), se instalaron 3 gestores “Postgresql+Postgis” siendo un módulo que añade soporte de objetos geográficos a la base de datos PostgreSQL, convirtiéndola en una base de datos para Sistema de Información Geográfica. Por lo descripto, es una versión específica para el funcionamiento de los sistemas relacionados.

Adicionalmente, en el Centro de Cómputos de INTA de calle Chile se encuentran instalados los siguientes gestores:

- PostgreSQL 8.4.20: Usado por “Comdoc” sistema que fue reemplazado y solo puede funcionar para consultas históricas.
- PostgreSQL 9.5.7: Una base de datos de una aplicación referida a buenas prácticas en lechería.
- PostgreSQL 9.1.13: Servidor de intercambio archivos para el personal del Organismo.

Es de señalar que los gestores ubicados en el CNIA tienen un uso específico y particular, y las otras versiones de este gestor no pertenecen a sistemas críticos.

Equipo de Gestión

El personal de la Gerencia de Informática que administra los gestores y otorgar permisos sobre las bases de datos se compone de 4 agentes (1 Planta Permanente, 1 Planta No Permanente y 2 contratos INTA). Es necesario aclarar que los integrantes del equipo no dedican exclusivamente su tiempo laboral para estas tares ya que tienen la responsabilidad de la realización de otras actividades.

De acuerdo a lo manifestado, las actividades relacionadas con gestores y bases de datos son registrados en el sistema de tickets Institucional “ServiceDesk Plus”, sin embargo, no se obtuvo el reporte pertinente que corrobore esta tarea.

Administración de Permisos

Los permisos con privilegios de administración sobre los gestores de bases de datos los tienen los integrantes del grupo que gestiona los mismos, sin embargo, los usuarios administradores no están resguardados en un repositorio seguro.

El personal de la GI administra todos los servidores y los gestores de bases de datos, con la salvedad de los ubicados en el centro de cómputos del CNIA los cuales son administradas por personal de esa sede. Otro caso particular se da con las bases de recursos humanos en donde el sector de la Dirección Nacional Asistente de Organización y Desarrollo del Potencial Humano (DNA OyPH) que administra estos sistemas tienen el usuario administrador del gestor con todos sus privilegios.

De los reportes de asignación de permisos sobre las principales bases de datos, se observa que los usuarios otorgados tienen asignados los perfiles de “db_owner” (MSSQL) o “GRANT ALL privileges” (MySQL), que de acuerdo al tipo de gestores le confiere privilegios íntegros sobre las bases de datos. Estos usuarios son utilizados por las aplicaciones, sin embargo, los responsables podrían utilizarlos para acceder directamente a los registros de las bases.

De lo expuesto, y teniendo en cuenta que estos usuarios los tienen los administradores de los sistemas, las bases de datos quedan expuestas a riesgos

potenciales que se registren accesos a las bases de datos en el ambiente de producción, y no quedar registradas pistas de las acciones realizadas en los sistemas.

Adicionalmente, a la base de datos del sistema de procesos “PectraBPMSuite”, gestionada por la Gerencia de Procesos y Calidad, se le definieron usuarios con una gran cantidad de privilegios (por ejemplo, el usuario iwfadmin tiene los perfiles public, db_accessadmin, db_backupoperator, db_datareader, db_datawriter, db_ddladmin, db_denydatareader, db_denydatawriter, db_owner y db_securityadmin), y en las bases del sistema de e-SIGA, gestionado por la Dirección General de Administración (DGA), se otorgaron permisos para varios usuarios.

Por otro lado, la GI no cuenta con registros de los permisos otorgados, ya que esta tarea mayormente fue realizada antes de la puesta en producción del sistema de tickets Institucional.

Por lo expuesto, se deben analizar los permisos otorgados con el responsable de Seguridad Informática a fin de establecer claramente el tipo de privilegios a otorgar. Además, se deben realizar acciones para que se favorezca la separación de ambientes y se establezcan controles que minimicen los riesgos de que ocurra algún tipo de inconveniente.

Diccionario de Datos Corporativos

El diseño de las bases de datos en la Organización no se funda en un modelo de arquitectura de la información, en donde los datos se organicen eficientemente y de manera homogénea, garantizando su disponibilidad, en concordancia con las necesidades operativas de las diferentes áreas del Organismo. Este modelo de arquitectura debe documentarse y mantenerse actualizado en un diccionario de datos corporativo.

Lo antes descripto se debe a que no se cuenta con reglas establecidas y que son varios los sectores (GI, de Calidad y Procesos, DGA, DNA OyPH, entre otros) que gestionan sus bases de datos, no habiendo una coordinación Institucional que tenga la responsabilidad de organizar el diseño.

Por lo expuesto, es necesario el establecimiento del perfil DBA (Administrador de Bases de Datos) que asuma la responsabilidad de los aspectos técnicos, tecnológicos y legales de las bases de datos, y, asimismo, establezca criterios para garantizar la calidad de datos.

Ambiente de Producción

Como si indicó anteriormente, no existe una adecuada separación de ambientes en los centros de cómputos, ni segregación de funciones, ya que de acuerdo a los privilegios otorgados a los administradores/desarrolladores de los sistemas estos podrían acceder a las bases de datos de producción por fuera de la aplicación.

Es necesario que se implemente una adecuada separación de ambientes que incluya los accesos a los gestores de bases de datos, se revisen los privilegios otorgados y se implementen controles para que sólo se pueda acceder a los datos desde las aplicaciones y se registren pistas de las acciones realizadas.

Documentación

La Gerencia de Informática no cuenta con procedimientos documentados para la configuración de los gestores de base de datos, ni la administración de la asignación de permisos sobre los mismos.

Por otro lado, los Diagramas de Entidad Relacional (DER) de las diferentes bases de datos las poseen los sectores que desarrollan sus aplicativos, contando la Gerencia de Informática sólo con los DER de las bases en que su personal intervino en el diseño. Adicionalmente no se definió un repositorio único de los mismos.

Asistencia técnica - Base de Datos

Según el relevamiento efectuado se constató que de febrero a septiembre del 2018 se contó con los servicios de la Consultora Dthink SRL disponiendo de 60 horas mensuales de consultoría, y que por falta de presupuesto se discontinuó.

De acuerdo a lo informado la Consultora intervino, entre otros, en los siguientes proyectos:

.

- Data Warehouse del INTA.
- Integración con Integration Services (desde bases de producción) de varias bases de datos para la construcción de modelos de Analisys Services.
- Integración de información del sitio Bandas Horarias con Buxis y Relojes Biométricos.
- Participación en el armado del repositorio de información de RRHH.
- Trabajó en la integración de información meteorológica del Instituto de Clima y Agua para el proyecto de Plataforma Agropecuaria (pia.inta.gob.ar).
- Optimización “queries” sobre el funcionamiento de las aplicaciones.

Logs y pistas de auditorias

El registro de logs y/o pistas de auditorías es realizado por los diferentes sistemas y controlado por sus administradores.

No obstante, cada gestor de bases de datos genera su propios logs, los cuales, por la complejidad y el esfuerzo que demandaría no se analizan, salvo que ocurra alguna contingencia.

Para disminuir los riesgos de que ocurran de estas contingencias, como ya se mencionó, es necesario mejorar y controlar el otorgamiento de permisos.

Relacionamiento

Al no contar con un sector que asuma el rol de DBA, las bases de datos se relacionan con web service (conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones) elaborados por cada administrador.

Resguardo y Recupero

De acuerdo a lo informado y relevado en informes anteriores, para el resguardo de los datos se definieron rutinas automáticas, con un proceso de verificación continua.

Sin embargo, aún no se obtuvo el reporte detallado y actualizado que verifique la inclusión de los gestores, las bases de datos, especificando tipo de backup y periodicidad.

El Organismo aún no definió su plan de recupero, por consiguiente, de llegarse a necesitar que se restaure alguna base de datos en el ambiente de producción se realizaría manualmente y sin los controles formales que deberían estar definidos. Este tema fue observado en el informe de auditoría N° 112/12 Observaciones 1 y 3, las cuales se encuentran pendientes de regularización.

4.2. Objetivos estratégicos

Se realizó el relevamiento de los 9 objetivos estratégicos incluidos en los Lineamientos para el Planeamiento UAI 2018, emitidos por la Sindicatura General de la Nación, surgiendo el siguiente resultado:

Cuadro N° 5 – Objetivos Estratégicos

Objetivo Estratégico	Aplica	Cumple	Comentarios
1) Relevamiento del estado de aplicación de sistemas normalizados de gestión	SI	NO	No se utilizan normas o estándares ISO.
2) Responsabilidad social	NO		
3) Responsabilidad ambiental	NO		
4) Costos de la “no calidad”	NO		
5) Corrupción cero	NO		
6) Matriz legal	SI	Parcialmente	No se definieron los aspectos legales sobre la registración de las bases de datos.
7) Identificación de centros de responsabilidad de procesos	SI	Parcialmente	La gestión de permisos no se basa en un proceso formal.
8) Construcción de programas de incentivos a la productividad	NO		
9) Constituir una adecuada Unidad de Vinculación tecnológica de INTA	NO		

5. Observaciones, recomendaciones, opinión del auditado y comentario de la UAI

Mediante Nota de la Dirección Nacional Asistente de Sistemas de Información, Comunicación y Calidad “NO-2018-66643857-APN-DNASICYC#INTA”, se recibió

respuesta al presente informe, transcribiéndose a continuación las observaciones con sus respuestas:

Observación N° 1:
El Organismo no tiene definido su diccionario de datos corporativo, en donde se establezcan las pautas de diseño homogéneas de las diferentes bases, ni un repositorio de la documentación de las bases de datos. Tampoco se estableció la responsabilidad del rol DBA (Administrador de bases de datos), que tenga injerencia en los aspectos de diseño, técnicos, legales y calidad de los datos, se aclara que una parte de este rol lo cumplía una consultora hasta septiembre de 2018.

Recomendación:
Se debe definir el diccionario de datos corporativo del Organismo, en donde se fijen los procedimientos relacionados con cada una de las actividades, las pautas de diseño y de gestión de los datos (gestores y base de datos). Adicionalmente se debe asignar el rol de DBA, para que se puedan llevar a cabo las cuestiones planteadas. Informar a esta UAI las acciones y plazo de regularización.

Opinión del auditado:
Parcialmente de acuerdo.
Hasta principios del 2018 la Gerencia de Informática no tenía injerencia directa sobre el desarrollo de las aplicaciones disponibles que le fueron delegadas.
En relación con la administración de los datos de cada base, cabe señalar que la responsabilidad primaria sobre la administración de estas bases de datos fue del equipo competente del área responsable de la aplicación y esta Gerencia brindo las condiciones de infraestructura y conectividad para su alojamiento.
Requerir hoy el diccionario de datos como requisito para su alojamiento implicaría sacar de línea muchas de las aplicaciones existentes en producción, destacando que esta decisión excede lo meramente técnico y entendemos, debe ser analizado por más de un área de competencia (DGA, GGI, GI y otras áreas dueñas de cada aplicación) para determinar plazos y formas de regularización de tal requerimiento. Además, debe ser elevado al Comité de Seguridad Informatica para su conocimiento y consideración.
En relación con el rol DBA, que hoy es compartido en la GI por distintos perfiles y que se considera estratégico y necesario, debemos señalar que lamentablemente, a pesar de los esfuerzos, la dificultad presupuestaria y de contratación que tiene el INTA, sumado el nivel de remuneración de mercado respecto del escalafón interno para este tipo de recurso, imposibilitaron la cobertura de esa posición necesaria.
Elevaremos esta recomendación a la DNA de Organización y Desarrollo del Potencial Humano para que se proceda en ese sentido.
Elevaremos, también, la necesidad presupuestaria para cubrir los costos de capacitación de los recursos propios de la GI, en esta temática de DBA.
Teniendo en cuenta la gran cantidad de aplicaciones legadas, el crecimiento constante de informatización de procesos y de digitalización de información, y considerando la cantidad de recursos de la GI, es imposible y no sería deseable, la homogeneización completa de BD de las aplicaciones. Buscamos mantener ciertos estándares de cara al futuro y en función de la actualización y reemplazo de los

aplicativos iremos modificando el escenario actual. Es económica y técnicamente inviable realizarlo de otra manera en este contexto.
Es estrategia de esta DNA y de la GI, la constitución de repositorios (DataWarehouse) oficiales del Organismo para la consolidación de las entidades principales, aportados por cada sistema de gestión y así también sus registros históricos, de forma tal de que se constituya como repositorio principal de consumo y explotación de datos validados de los procesos internos de cada área de competencia. Esta tarea comenzó a planificarse en la segunda mitad del año 2018 con varias reuniones de integración en la que participaron todas las direcciones de la sede central.
A tales efectos ya está en construcción el repositorio DataWarehouse integrado de RRHH, DGA y Cartera de proyecto 2013, actualmente en una base de datos intermedia (staging), con procesos implementados que integran cronológicamente los datos de las respectivas bases de datos productivas.
La integración final en el DW pretende homogenizar el repositorio y garantizar la integridad de los datos para consumo y explotación para los distintos sistemas y reportes.

PLAZO DE REGULARIZACIÓN: como se indicó elevaremos para consideración del Comité de SI la propuesta del plan de integración final del repositorio como así también el procedimiento escrito para la realización de estas integraciones y la construcción de la documentación derivada. Se formalizará, también, los pedidos para cubrir el puesto crítico de DBA y el pedido de recursos presupuestarios para la capacitación del personal propio.

Comentario de la UAI:
Si bien el auditado expresó las consecuentes acciones a encarar, pero al no haber indicado el plazo de regularización ni iniciado su cronograma de tarea, la observación se categoriza como **Sin Acción Correctiva Informada** hasta que se se remita documentación respaldatoria de la realización de las acciones propuestas.

Observación N° 2
La asignación de los permisos sobre las bases de datos y sus gestores se realiza otorgando a los administradores de los sistemas, usuarios con amplios privilegios (db_owner" o "GRANT ALL privileges") que permitirían el acceso al ambiente de producción. Destacándose además los casos particulares de las bases de datos de la Gerencia de Procesos y Calidad, de la DNA OyPH y de la DGA.

Recomendación:
Como primera medida se debe articular con el Responsable de Seguridad Informática la definición de los tipos de permisos a otorgar para el ambiente de producción sobre los gestores y las bases de datos, de manera tal que exista una adecuada separación de ambientes. Posteriormente, revisar los permisos otorgados y comenzar un proceso de actualización de acuerdo a lo que se definió.

Adicionalmente, la Gerencia de Informática conjuntamente con el Responsable de Seguridad Informática deben definir la estrategia de utilización y resguardo de los

usuarios administradores de los gestores de base de datos. Informar a esta UAI las acciones y plazo de regularización.

Opinión del auditado:
parcialmente de acuerdo.
Efectivamente, estos usuarios con privilegios son requeridos por las áreas mencionadas para la gestión de sus respectivas Bases de Datos. Cabe aclarar que, en ningún caso, los usuarios designados en cada área poseen los mismos roles en otras bases de datos, quedando circunscriptos a los permisos de sus propias bases de datos.
Esta práctica se corresponde con la necesidad de dar respuesta a un requerimiento recibido, basado en una necesidad operativa de las áreas mencionadas y del organismo.
Procederemos a tomar contacto con la DGA, DNA de Organización y Desarrollo del Potencial Humano y la DNASICyC para establecer en conjunto un plan de adecuación que segregue los niveles de acceso en este ambiente productivo de estas bases de datos, acorde a las necesidades y posibilidades de estas áreas involucradas, tratando de evitar la salida de estas aplicaciones de producción.
Por tratarse de aplicativos críticos para el funcionamiento actual del INTA, presentaremos al Comité de Seguridad de la Información el plan acordado con cada área para su consideración, aprobación e implementación. Esta última acción sujeta a la posibilidad de contar con el recurso especializado para la gestión y administración de las Bases de Datos.

Comentario de la UAI:
Si bien el auditado expresó las consecuentes acciones a encarar, pero al no haber indicado el plazo de regularización ni iniciado su cronograma de tarea, la observación se categoriza como **Sin Acción Correctiva Informada** hasta que se se remita documentación respaldatoria de la realización de las acciones propuestas.

Observación N° 3
Teniendo en cuenta los gestores de bases de datos instalados en los 4 centros de cómputos informados, se observan distintas versiones de un mismo producto, los que en su mayoría están desactualizados y sin soporte oficial. Adicionalmente, no se definió un standard de configuración de los mismos.

Recomendación:
Definir un standard de configuración para los gestores de mayor uso (MMSQL y MySQL), para facilitar su administración, y con ello, planificar la actualización y unificación de los mismos con versiones más actuales. Informar a esta UAI las acciones y plazo de regularización.

Opinión del auditado:
parcialmente de acuerdo.
Esta situación sobre la existencia de diferentes versiones de los productos de BD y que algunos estén sin actualización, responde a lo referido anteriormente sobre el legado de las aplicaciones alojadas en los Data Center.

Cambiar o migrar las versiones de los motores de base de datos no es inocuo y debe ser analizado particularmente con cada dueño de la aplicación, para evitar salidas de funcionamiento o comportamientos inesperados.
Somos conocedores de esta situación y es intención mantener las versiones actualizadas de los productos sobre todas las aplicaciones críticas, para lo cual también elevaremos al Comité de SI el estado y versiones de los motores de las aplicaciones principales, para el análisis y la determinación formal del plan de adecuación.

Comentario de la UAI:
Si bien el auditado expresó las consecuentes acciones a encarar, pero al no haber indicado el plazo de regularización ni iniciado su cronograma de tarea, la observación se categoriza como **Sin Acción Correctiva Informada** hasta que se se remita documentación respaldatoria de la realización de las acciones propuestas.

Observación N° 4
Si bien la asistencia técnica del grupo de la GI que administra las bases de datos, registra en el sistema de tickets Institucional las incidencias, no se pudo acceder al informe detallado de las mismas que verifique fehacientemente esta tarea.

Adicionalmente, aunque se comprobó que el proceso de resguardo se realiza con rutinas automáticas, no se pudo obtener el informe detallado sobre el esquema de resguardo que incluya a todos los gestores y sus bases de datos.

Recomendación
La Gerencia de Informática debe remitir un reporte detallado de los incidentes cargados en el sistema Institucional relacionados con la gestión de las bases de datos que realizan, y además, el reporte sobre el proceso de resguardo de las bases que verifique la inclusión de los gestores, las bases de datos, especificando tipo de backup y periodicidad.

Opinión del auditado:
De Acuerdo.
En relación con las incidencias atendidas en la GI, por el tema Bases de Datos, se detallan los ticket's recibidos y atendidos en el curso el año (Adjunto reporte pdf – TicketsBD.pdf)

Nro Ticket	Tema
118631	Portal caído por SQL
113852	TABLAS BORRADAS DE SQL
113512	Actualización de la copia de Base de datos en server
113338	PostgreSQL en Report Server (Producción)
108904	Reiniciar server SQL ucsqlcluster11\pectrapre
101789	Caído sql nuevamente, ahora BD BPMSUITE
96522	Caída sql WF producción
96148	Backup de la Base de Datos Renpre

Sobre el proceso de resguardo, en el cuadro adjunto se detallan las actividades que se realizan (adjuntoimágenes de pantalla)

Rutinas de back up				
Nombre del job	Tipo	Dias	Hora	Retención
Consulta_SQL_FULL	FULL	Lunes a Viernes	01:30	4 semanas
KODOS_SQL_FULL (4 instancias)	FULL	Lunes a Viernes	17:30	4 semanas
UCCluster01.iNTA.AR (Pectra)	FULL	Lunes a viernes, y domingos	00:30	4 semanas
UCCluster02.iNTA.AR (PectraPre)	FULL	Lunes a viernes, y domingos	00:30	4 semanas
UCDBSERVER003s_Huella	FULL	Lunes a Viernes	11:30 y 21:30	4 semanas
Snorky (4 instancias)	FULL	Lunes a Viernes	01:00	4 semanas
UCDBSERVER002 (3 INSTANCIAS)	FULL	Lunes a Viernes	20:30	4 semanas
Protection Group – SharePoint Producción	FULL	Lunes a Viernes		
Esiga				
Base de datos (1)	FULL	4 veces x día	01, 09, 12 y 18 hs	15 días
App (2)	FULL	Domingo		15 días
(1) El Back Up se resguarda en disco en el Data Center de Telecom.				
(2) Se toma el Back Up desde un server del Data Center				

Comentario de la UAI:
De acuerdo a lo expresado por el auditado y a la documentación presentada, se considere **REGULARIZADA** la observación.

6. Conclusión

Del relevamiento de bases de datos del Organismo realizado por la Gerencia de Informática se desprenden varios de los temas observados, entre los que se destaca la asignación de privilegios y la dispersión en la responsabilidad en la administración de las mismas.

De acuerdo a lo evaluado de la Gestión de las Bases de Datos en el Organismo, se entiende que las cuestiones operativas planteadas son de compleja solución, ya que involucran a varios sectores y en algunos casos demandaría la realización de importantes erogaciones.

Sin embargo, se considera oportuno la propuesta de involucrar a todos los actores necesarios del Organismo y con ello, planificar la adecuación del ambiente de producción tendiente a mejorar el esquema de seguridad y a mantener una adecuada segregación de funciones, tal como lo definen las normas de control interno.

Además, es necesario indicar que el mantenimiento de los servidores y el sistema de backup de las bases es adecuado.

CABA, 21 de diciembre de 2018.