

Para : AUDITORIA INTERNA
De : DPTO. DE AUDITORIA DE GESTION TECNICA
Ref. : REMITIR INFORME FINAL N° 06/DAGT-AI/2019
Fecha : 28/06/2019.

INFORME FINAL N° 06/DAGT-AI/2019

1. ANTECEDENTES:

El presente trabajo fue realizado desde el 30 de Mayo al 27/Junio/2019, en cumplimiento a la Orden de Trabajo N° 32/AI/19 de fecha 29/05/2019 correspondiente al Plan de Trabajo Anual de la Auditoría Interna.

2. ALCANCE:

La auditoría fue realizada de acuerdo a las funciones y responsabilidades conferidas por la norma que regula las funciones de la instancia de auditoría y otras disposiciones legales concordantes y aplicables al sector público.

Nuestra labor fue realizada conforme lo establece el manual de auditoría gubernamental. La verificación comprendió las actividades relacionadas a la aplicación de los procedimientos establecidos por parte de los encargados de las distintas áreas, en base a pruebas selectivas.

El presente informe surge como resultado de la aplicación de procedimientos de control y del análisis de los documentos proveídos a los auditores. La ejecución y formalización de las operaciones examinadas son de exclusiva responsabilidad de los funcionarios del área auditada.

Nuestro trabajo no incluye una revisión detallada e integral de todas las operaciones, por lo tanto, el presente informe no se puede considerar como exposición de todas las deficiencias existentes o de todas las medidas que podrían adoptarse para corregirlas.

3. OBJETIVOS:

- 3.1 Identificar los roles habilitados y las operaciones permitidas por cada rol.
- 3.2 Identificar los usuarios habilitados y la correspondencia entre los roles asignados y las funciones de las dependencias en las que prestan servicio.
- 3.3 Verificar la documentación de habilitación de acceso y operaciones de usuarios.
- 3.4 Verificar los procedimientos de seguridad existentes para la gestión de acceso y operaciones del sistema.
- 3.5 Verificar la existencia de archivos de auditoría y el modo en que estos se encuentran implementados (aplicativo, base de datos).
- 3.6 Verificar si se realizan operaciones por fuera del aplicativo y la existencia de procedimientos de autorización para estas tareas.

4. TRABAJOS REALIZADOS

- 4.1 Auditoría en las oficinas de los involucrados de la Gerencia de Tecnología de Información.

✓ Departamento de Sistemas

- ✓ Departamento de Calidad Informática.
- ✓ División Recursos TI.
- ✓ Sección Base de Datos.

- 4.2 Elaboración y firma del acta de los empleados participantes de esta auditoría.
4.3 Análisis de los documentos obtenidos y emisión de los hallazgos establecidos

5. DESARROLLO DEL INFORME:

La Auditoría Interna procede a la identificación de los diferentes tipos de observaciones y para el mismo se utilizará el código "H" para los Hallazgos, el código "CI" para las observaciones de Control Interno y "R" para las recomendaciones.

6. SITUACIONES OBSERVADAS:

6.1 IDENTIFICACION DE LOS ROLES HABILITADOS Y LAS OPERACIONES PERMITIDAS PARA CADA ROL.

6.1.1 USUARIOS CON ROL DE DBA

Usuario	Rol	Estado
ROMASILV	DBA	Activo
SCOREDB	DBA	Inactivo
SIRD	DBA	Activo
RAMIBERN1	DBA	Activo
BILLING	DBA	Activo

(CI) se observan 4 usuarios activos con privilegio de administrador (DBA).

(R) Se recomienda a la Gerencia de TI limitar controlar y formalizar la asignación y uso de este privilegio. Dado que se trata del máximo nivel de privilegios, se deberá restringir su utilización a lo estrictamente necesario para cumplir con su función administradora.

Descargo de la Sección Base de Datos – Div. Recursos TI.

Los Usuarios con ROLES "DBA" fueron cambiados los roles de los siguientes usuarios:

- ROMASILV= DBA, encargada de la Sección Base de Datos, sigue con el mismo ROL
- SIRD=DBA, cambiado por el ROL SIRD_NEW_BILL
- RAMIBERN1= DBA, funcionario de la Sección Base de Datos, cambiado por el ROL = R_DBA_NEW_BILL
- BILLING= DBA, es el owner (propietario de la BD), pues todos objetos le pertenecen a este usuario, otro usuario puede tener acceso a estos objetos siempre y cuando el usuario BILLING se los otorgue.



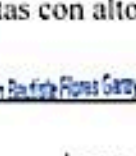
Opinión del Equipo Auditor

De la evaluación del descargo, esta Auditoría ha tomado conocimiento de los cambios realizados, sin embargo mantiene su observación con relación a la formalización y control de la función.

6.1.2 ROLES CON MULTIPLES PRIVILEGIOS DE SISTEMA Y DE OBJETOS

Rol/Usuario	Observación	Asignado al Rol/Usuario	Usuarios
BILL_DML_TABLAS_PEDIDAS	Permisos de objeto (insert, update, delete) sobre múltiples tablas.	R_DBA_NEW_BILL	
BILL_SELECT_TABLAS_COMPLETO	Permisos de objeto select sobre múltiples tablas y permisos de objeto (insert, update, delete) sobre las tablas: MVTOCTAS, INSTALACIONES, CLIENTES_RETIRADOS.	R_DBA_NEW_BILL	SINCBILL, CABAGABR, ESTAENJO, ESPINORM
R_COPACO_CONSULTA	Permisos de objeto (insert, update, delete) sobre múltiples tablas.	No asignado	No asignado
R_COPACO_DML	Privilegios de sistema (Delete any table, insert any table, select any sequence, select any table, update any table). Además del rol resource.		BILL_DS BILLING
R_DBA_NEW_BILL	Múltiples roles. Permisos de objeto (insert, update, delete) sobre múltiples tablas.		BILL_DS RAMIHECT PISTRICA OLAVJOSE DUARNOEM GONZVIVI ESTAENJO VAZQMARI ORTEAGUS MAREJORG ALMILOUR ARIAJORG GUANFABI FLORLILI IRRAJOSE MEDIMARI
R_DBA_BILL	Múltiples roles. Permisos de objeto (insert, update, delete) sobre múltiples tablas.	No asignado	No asignado

(CI) se observan varios roles con múltiples privilegios de sistema y objetos asignados a usuarios u otros roles. El rol R_COPACO_DML asignado a los usuarios BILL_DS y BILLING cuentan con altos privilegios de sistema.

(R) Se recomienda a la Gerencia de TI verificar los privilegios asignados a usuarios y roles, a efectos de asegurar que cuenten con los privilegios mínimos para cumplir a cabalidad sus tareas. La concesión de privilegios de usuarios y roles debe enmarcarse en lo establecido en la Política de Seguridad de Sistemas de Información (Administración de Privilegios).

Descargo de la División de Recursos TI.

No se realizó descargo con relación a la observación.

Opinión del Equipo Auditor

Se mantiene la observación y recomendación.

6.1.3 USUARIOS CON ROLES DE ADMIN OPTION

Usuario/Rol	Usuario/Rol	Admin Option
BILL_DS	R_COPACO_DML	YES
BILLING	R_COPACO_DML	YES
BILLING	DBA	YES

(CI) Se observan roles con altos privilegios, que cuentan con la posibilidad de ceder los privilegios obtenidos a otros usuarios o roles.

(R) Se recomienda a la Gerencia de TI identificar y revocar la posibilidad de cesión de privilegios de sistemas entre roles o usuarios.

Descargo de la Div. Recursos TI.

Usuarios con ROLES de Admin Option: BILL_DS, y BILLING; el acceso a estos usuarios genéricos, están restringidos por sus respectivas contraseñas encriptadas, cuyo encargado sería la Div. Mantenimiento de Sistemas, evitando de esa manera posibles manipulaciones de otorgar ROLES a otros usuarios.

Opinión del Equipo Auditor

De la evaluación del descargo, esta Auditoría mantiene su observación y recomendación.

6.1.4 ROLES NO ASIGNADOS A USUARIOS U OTROS ROLES

Rol
BILL_ACCESO_FACT
BILL_ADMINISTRATIVA_ADMIN_RECA
BILL_ADMIN_BILLING
BILL_ADMIN_CTASOFICIALES
BILL_AGREGAR_SIMCARD
BILL_ANULAR_PAGO
BILL_ASIGNAR_CREDITO
BILL_CAJERO_ADMIN

BILL_CAJERO_COBRADOR
BILL_CAJERO_SUPERVISOR
BILL_CALL_CENTER_SUPERVISION
BILL_CALL_CENTER_VOX
BILL_COMERCIAL_ADMIN_CLIENTES
BILL_COMERCIAL_CLIENTES_CORP
BILL_COMERCIAL_CONSULTA
BILL_COMERCIAL_OPER_CLIENTES
BILL_CONTABILIDAD_COMP
BILL_DISTRIBUCION_FACTURA
BILL_FACTURACION_ADELANTADA
BILL_FRACC_EXCEPCIONAL
BILL_PAGO_A_CUENTA
BILL_REPORTA_AUDITORIA
BILL_REPORTA_COBRANZAS
BILL_REPORTA_COMERCIAL
BILL_REPORTA_CONTABLES
BILL_REPORTA_FACTURACION
BILL_REPORTA_PLANTAEXTERNA
BILL_REPORTA_TOTAL
BILL_TECNICA_ADMIN_COMANDO
BILL_TECNICA_ADMIN_MEDIACION
BILL_TECNICA_ADMIN_PEXTERNA
BILL_TECNICA_COMANDOS
BILL_TECNICA_CONSULTA
BILL_TECNICA_CONSULTA_COMANDO
BILL_TECNICA_OPER_COMANDO
BILL_TECNICA_OPER_PEXTERNA
BILL_TECNOLOGIA_ADMIN_GENERAL
BILL_TECNOLOGIA_ADMIN_PROCESOS
BILL_TECNOLOGIA_DEBITO_MANUAL
R_COPACO_CONSULTA
R_DBA_BILL

(CI) Se observan roles que no se encuentran asignados a ningún usuario o rol. Algunos de ellos como R_COPACO_CONSULTA y R_DBA_BILL cuentan con altos privilegios de sistema.

(R) Se recomienda a la Gerencia de TI identificar y verificar los roles definidos y no asignados a usuarios y determinar la necesidad de mantenerlos o eliminarlos.

Descargo de la Div. Recursos TI

El listado de ROLES que aparece en la impresión, son ROLES de la Aplicación, es decir SI son asignados a los usuarios en el momento de logearse, de modo que el Sistema BOSS, pueda habilitar o deshabilitar los formularios (ventanas), según el ROL asignado.

En cuanto a los 2 últimos roles = R_COPACO_CONSULTA y R_DBA BILL, estos SI son Roles que NO están asignados a ningún usuario, pero en algún momento lo estuvieron por ello NO se pueden eliminar, tampoco deshabilitar ya que los ROLES solo se pueden Asignar y Revocar.

Opinión del Equipo Auditor

De la evaluación del descargo, esta Auditoria mantiene su observación y recomendación con relación a los 2 últimos roles mencionados.

6.1.5 USUARIOS CON IDENTIFICADORES GENERICOS

Usuario/Rol
APP_COPACO
BILL_DS
APP_TEMBIAPO
BILLING

(CI) Se observan usuarios con identificadores genéricos.

(R) Se recomienda a la Gerencia de TI utilizar identificadores únicos para usuarios, que permitan identificar las acciones realizadas por los mismos. En caso de requerir la utilización de identificadores compartidos, formalizarlos y justificarlos debidamente. Los accesos a sistemas, datos y servicios de información deben enmarcarse en lo establecido en la Política de Seguridad de Sistemas de Información (Administración de Accesos de Usuarios).

Descargo del Dpto. de Sistemas

Con base a esta recomendación, desde el Departamento Sistemas informamos que, de acuerdo al tipo de arquitectura utilizado para el desarrollo de softwares, se pueden tener conexiones en "dos capas" (Cliente / Servidor), o en "n capas" (Cliente / Servidor App / Servidor BD); como la tendencia para el desarrollo de softwares desde principios del nuevo milenio está orientada a objetos, los nuevos proyectos adquiridos o desarrollados in house en la Compañía, están fundamentados en dicho modelo, por tanto eso implica que se utilice un agrupamiento de conexiones (connection pool), con lo cual se hace mucho más eficiente el uso de recursos de hardware disponibles, ya que las conexiones, generalmente se mantienen abiertas el tiempo que dura la ejecución del programa y sólo son cerradas al finalizar el trabajo de la aplicación con la base de datos. Estas especificaciones técnicas, también obran en las documentaciones provistas por responsables de la Facultad Politécnica, quienes son los fabricantes puntuales del Sistema BOSS. Por otro lado, se exponen puntualmente las asociaciones de cada usuario genérico con su aplicación informática correspondiente:

APP_COPACO : Usuario genérico utilizado en el connection pool a la base de datos de: COPACO App Móvil para Clientes y Prospectos de la Compañía.

BILL_DS: Usuario genérico utilizado en el connection pool a la base de datos de BOSS (Business Operational Support System).

APP_TEMBLAPO : Usuario genérico utilizado en el connection pool a la base de datos de COPACO App Móvil para Técnicos de Cuadrillas de la Compañía.

BILLING: Usuario propietario (owner) del schema del Sistema BOSS (Business Operational Support System).

Así también se informa, que se disponen y quedan registradas todas las cuentas de usuarios nominales de cada empleado que se conectan e inician sesión en la base de datos del Sistema BOSS, tanto desde la interface de usuario, como así también cuando se accede en forma directa a la base de datos, las cuales quedan plasmadas en las pistas de auditoría del citado sistema en producción comercial.

Opinión del Equipo Auditor

De la evaluación del descargo, esta Auditoría mantiene su observación y recomendación.

6.2 CORRESPONDENCIA DE LOS ROLES ASIGNADOS Y LAS FUNCIONES DEL USUARIO.

La habilitación de acceso y operaciones de usuarios se realiza mediante el formulario GTI-01-E, en el cual se especifican las funciones a asignar y deben contar con la autorización del Jefe Inmediato. Sin embargo, según indica el Jefe de Dpto. de Calidad Informática, no siempre la asignación del rol está relacionada al cargo que ocupa cada empleado de la Compañía. Ej. Un Jefe de Distrito muchas veces debe gestionar tareas administrativas, comerciales, técnicas y otras donde la Compañía lo requiera, debido generalmente a la escases de recursos humanos, por lo que se le asignan varias funciones al mismo usuario.

Descargo del Dpto. de Calidad Informática

En el Acta de Reunión de fecha 11/06/2019 en base a la Orden de Trabajo N° 32/A1/2019, se hizo la siguiente consulta Imprimir las funciones de usuarios del Sistema Boss, y la respuesta completa descrita a continuación. "Con respecto a este pedido, el plan de carreras no está definido en la Compañía, por lo que las funciones no están contempladas en el módulo de Nómina del Sistema Administrativo Financiero y Contable (S.A.F.), dicho módulo provee la información para la creación de usuarios y asignación de roles en los Sistemas Corporativos. Cabe mencionar, que no siempre la asignación del rol está relacionada al cargo que ocupa cada empleado en la Compañía. Ejemplo: El jefe de Distrito muchas veces debe gestionar tareas administrativas, comerciales, técnicas y otras donde la Compañía lo requiera, debido generalmente a la escasez de recursos humanos. "Se hace la aclaración que actualmente se otorga el usuario y rol al empleado; de acuerdo a las funciones y/o tareas descritas en el Formulario GTI-01-E de Acceso a los Sistemas Informáticos de la Compañía, disponible en el Portal Corporativo (Intranet), también se tiene en consideración la dependencia en la cual el empleado presta servicio, si es administrativo, comercial o técnico, para la asignación de los roles en los Sistemas Corporativos. El ejemplo que se citó, sobre todo en el interior de país, contamos con casos

excepcionales donde el jefe de Distrito por falta de personales para la distribución de tareas, se le otorga perfil tanto administrativo, comercial y técnico, en una manera de brindar una buena atención y respuestas inmediatas a los reclamos y solicitudes de nuestros clientes.

6.3 CONTROL DE LOS PROCEDIMIENTOS DE SEGURIDAD EXISTENTES PARA LA GESTIÓN DE ACCESO Y OPERACIONES DEL SISTEMA

Los procedimientos de seguridad de acceso y operaciones del sistema se encuentran enmarcados en el documento formalizado denominado “Política de Seguridad de Sistemas de Información”(Comité de Seguridad de la Información Memorandum N° 361 P/2005), cuyo objetivo es “Implementar las medidas de seguridad comprendidas en esta Política, proteger los recursos de información de la compañía y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información”.

6.4 VERIFICACION DE LA EXISTENCIA DE ARCHIVOS DE AUDITORIA Y EL MODO EN QUE ESTOS SE ENCUENTRAN IMPLEMENTADOS

La auditoría del sistema se encuentra implementada a nivel de tablas mediante triggers que registran las modificaciones y borrados de registros.

(CI) A nivel de base de datos, se encuentran implementada la auditoria nativa de Oracle solamente sobre la tabla de Pagos.

(R) Se recomienda evaluar e implementar la auditoria de la base de datos nativa de Oracle para aquellas tablas sensibles del sistema. Para el caso de las tablas de auditoria generadas mediante triggers, se deberá asegurar que ningún usuario posea la posibilidad de realizar cambios sobre las mismas

Descargo de la Div. Recursos TI

En cuanto a la implementación de la Auditoria del Motor de Oracle sobre otras tablas, implicaría utilización de más Recursos de la BD, esto se debería consensuar con el Soporte de la BD., de manera que No exista una afectación en el rendimiento del Sistema BOSS.

En cuanto a las tablas de Auditoria afectadas por triggers, los permisos sobre estos triggers, solo tienen accesos a ellos los usuarios con perfil DBA, quedando de igual manera en las propiedades del trigger registrado la fecha si hubiera alguna modificación, como prueba de su edición.

Opinión del Equipo Auditor

De la evaluación del descargo, esta Auditoria mantiene su observación y recomendación.



Juan Bautista Flores Garay

6-5 VERIFICACION DE LAS OPERACIONES POR FUERA DEL APLICATIVO Y LA EXISTENCIA DE PROCEDIMIENTOS DE AUTORIZACIÓN PARA ESTAS TAREAS.

(II) Se ha observado que existen situaciones donde se realizan modificaciones de tablas por fuera del aplicativo (BOSS), como por ejemplo: cuando se solicita actualizar el tipo de crédito para una cuenta, se realiza a través de un script que realiza dicha modificación. La autorización es solicitada por el programador responsable a su jefe directo a través de correo electrónico.

(R) La Gerencia de Tecnología de Información debe asegurarse que todas las operaciones necesarias para el normal funcionamiento del sistema se realicen desde el aplicativo. En caso de requerirse, por alguna razón justificada, la modificación de tablas por fuera del mismo, ésta deberá ser tratada como evento específico y formalizada por escrito en un documento de autorización por parte del Propietario de datos.

Descargo del Dpto. Sistemas

Se informa que las modificaciones realizadas eventualmente, no corresponden a transformaciones a nivel de tablas de base de datos (DDL), sino que a registros o filas (DML) que están almacenadas en ellas. De acuerdo al procedimiento vigente en la Gerencia de T.I., para atender este tipo de casos, exige que el usuario solicitante del cambio utilice el Formulario Electrónico a través de la Intranet (GTI-SAT), el cual, para que pueda ser ejecutado por un responsable de la Gerencia de T.I., debe estar debidamente autorizado por el Jefe Inmediato del solicitante; todos estos trámites deben ser gestionados a través de la Intranet.

No siempre es recomendable que desde la interface de usuario (BOSS), se lleven a cabo modificaciones en los valores de los registros, debido a que los estados de los procesos pueden estar comprometiendo seriamente la situación de todo el negocio, pudiendo inclusive dejar inconsistentes los datos. Si bien existen algunos valores que pueden ser modificados posterior a confirmaciones o anulaciones, las mismas deben ser siempre bien analizadas y respaldadas con motivos suficientemente comprobables para evitar dichas inconsistencias. Actualmente en la Gerencia de T.I., un equipo de trabajo de técnicos expertos está trabajando en la elaboración de un procedimiento, que formalice este tipo de situaciones de acuerdo a los eventos que se puedan presentar.

Así también, informamos sobre nuestra predisposición para recibir, aceptar y adoptar las recomendaciones señaladas, las cuales hallamos muy oportunas.

Opinión del Equipo Auditor


De la evaluación del descargo, esta Auditoría mantiene su observación y recomendación.



Lic. Juan Bautista Flores Jarey



Lic. Juan Bautista Flores Garay
Auditor Actuante



Abog. Silvia Jiménez Olmedo
Encargada de Despacho
Dpto. Auditoría de Gestión Técnica