1. Sobre las actividades de cambios a los programas

1.1. Se carece del registro en el Sistema HelpDesk de 10 requerimientos de cambio y 3 aprobaciones de pase a producción, realizado por los usuarios finales

Posterior a la revisión realizada sobre una muestra de 30 cambios implementados en los sistemas SAP, GAD y ADRYAN, se identificaron las siguientes observaciones:

- No se evidenciaron 10 tickets de requerimiento de cambio, registrados por parte del usuario final, en el sistema de HelpDesk.

Sistema	Nro. Ticket TI
SAP	37013
SAP	37635
SAP	39159
SAP	44428
SAP	40081
SAP	40487
SAP	45256
SAP	45311
SAP	46152
GAD	46154

- No se cuenta con el sustento de la aprobación para el pase a producción, registrados por parte del usuario final, en el sistema de HelpDesk.

Sistema	Nro. Ticket TI
SAP	45216
SAP	45311
GAD	46154

Esta situación implica el riesgo de realizar cambios inadecuados y no autorizados debidamente por los usuarios finales, lo cual podría incurrir en cambios que no se encuentren alineados a los objetivos del negocio.

Se recomienda monitorear y formalizar el registro de los requerimientos y aprobaciones del usuario final sobre los cambios trabajados por sistemas dentro del "Procedimiento de atención de requerimientos".

2. Sobre los accesos a datos y programas

2.1. Se identificaron cuentas de personal cesado que permanecen activas en el Sistema ERP SAP.

Durante la revisión identificamos cuentas de usuarios de personal cesado, según el reporte de cese emitido por Recursos Humanos, que permanecen activos en el sistema SAP, tales como:

Código empleado	Descripción	Unidad organigrama	Fecha de Cese	Módulo SAP
795835	Bochelli, Andrea	LOGISTICA	09/01/2009	Order Management
795842	Boyle, Susan	LOGISTICA	09/01/2009	Order Management
795455	Riu, Andre	CONTABILIDAD	31/03/2009	General Ledger

Esta situación incrementa el riesgo de accesos no autorizados al sistema, mediante el uso de cuentas de personal cesado que se mantienen activas, después de su fecha de cese. El impacto asociado al riesgo identificado, dependerá de los permisos relacionados a los accesos asignados a cada una de las cuentas.

Se recomienda realizar un seguimiento sobre la desactivación de dichas cuentas de usuarios en el Sistema SAP y realizar un monitoreo continuo sobre las cuentas de usuario de personal cesado.

2.2. Se identificaron tickets que no registraron el formato respectivo para realizar el alta y baja de cuentas de usuarios en el sistema de HelpDesk

Durante la revisión de los usuarios se identificó que varios tickets de atención no adjuntan el formato respectivo para dar de alta o baja de acceso a los usuarios. Se identificaron los siguientes casos:

Código empleado	Descripción	Tipo de Acceso	Ticket
123	NOLBERTO SOLANO	Alta	44263
456	JOSE ANTONIO CROSILLAT	Alta	29755
789	JOSE FRANCISCO CROUSILLAT	Alta	40778
101	TEOFILO CUBILLAS	Alta	43634
321	HAMILTON PRADO	Alta	39506
451	DIONISIO ROMERO	Baja	46310
215	CESAR CUETO	Baja	47616
787	FRANCISCO PIZARRO	Baja	26200

Las situaciones anteriormente mencionadas incrementan el riesgo de otorgar acceso a personal no autorizado por los usuarios propietarios de los Sistemas de Información (documento “DOCSIS001 Propietarios Sistemas de Información”), quienes son los únicos autorizados, de acuerdo al documento “PROSIS025 Mantenimiento de Usuarios de Sistemas de Información”.

Se recomienda establecer un control para asegurar la adecuada gestión de accesos a las aplicaciones y recursos de red, cumpliendo con los procedimientos “DOCSIS001 Mantenimiento de Usuarios de Sistemas de Información” y “PROSIS025 Mantenimiento de Usuarios de Red” establecido por la compañía.

2.3. Existen 7 personas de la compañía de Outrsourcing con privilegios de administrador para las bases de datos del SAP, GAD y ADRYAN.

Durante la revisión de las bases de datos del SAP, GAD y Adryan, se identificó que existen 7 operadores de la compañía de Outsourcing con privilegios de administrador (DBA), los cuales son:

1. Leonel Messi
2. Diego Maradona
3. Juan Veron
4. Carlos Alvarez
5. Jorge Benvides
6. Magaly Medina
7. Miguel Barraza

Esta situación implica un alto riesgo de modificación no autorizada de información para las bases de datos del SAP, GAD y ADRYAN; así como la falta de identificación de las actividades realizadas por cada operador, por el uso compartido de las cuentas de acceso para la administración de la base de datos.

Se recomienda evaluar la definición de cuentas diferentes para cada operador del Outsourcing y definir a los operadores que deben de contar con el perfil administrador, a fin de delimitar el acceso y puedan cumplir con las funciones establecidas de DBA.

3. Sobre las actividades de desarrollo de programas

3.1 Se carece de una adecuada gestión de comunicación sobre las actividades realizadas en el proyecto de automatización de captura de información, así como de la documentación utilizada en el proyecto.

Durante nuestra revisión, se observaron las siguientes situaciones sobre la gestión del proyectos de automatización de captura de información:

- No se evidenciaron las actas de reunión que sustenten la comunicación de las actividades realizadas en el proyecto, ya que tan sólo se evidenciaron las actas de reunión hasta el mes de Abril 2009, habiendo culminado el proyecto en Febrero 2010.
- Se observó el uso de dos formatos diferentes de actas de reunión, no siguiendo lo estandarizado por la metodología de proyectos de LA COMPAÑIA, que figura en los anexos del documento.

Esta situación implica el riesgo de no evidenciar los acuerdos y decisiones relevantes que afecten la ejecución del proyecto. Asimismo, la falta de estandarización de documentos implica la falta de monitoreo sobre el uso apropiado de los formatos definidos por la metodología de proyectos de LA COMPAÑIA.

Se recomienda establecer en cada proyecto una frecuencia fija para llevar a cabo las reuniones de coordinación, registro y comunicación de las actas correspondientes. Así como también, establecer el control sobre la documentación elaborada para los proyectos de LA COMPAÑIA, a fin de cumplir con la "Metodología de Gestión de Proyectos" definida por la compañía.

4. Revisiones de Seguridad Base de Datos y Sistema Operativo

Sistema ADRYAN

4.1 No se registran los eventos de auditoría de la base de datos Oracle del sistema de Planillas ADRYAN

Durante nuestra revisión, verificamos que la base de datos que almacena la información del Sistema ADRYAN tiene la opción de registro de auditoría "audit_trail" en true, sin embargo, se observa las siguientes situaciones:

- No se encuentran definidos los valores a ser auditados para todas las cuentas de usuarios
- No se encuentra definido el registro de operaciones sensibles en los objetos de la base de datos, como DROP TABLE, CREATE TABLE, SELECT TABLE, entre otros.
- No registra los intentos de inicio de sesión exitosos y fallidos en la tabla DBA_AUDIT_SESSIONS.

Esta situación implica el riesgo de no poder identificar actividades no autorizadas realizadas en la base de datos.

Se recomienda evaluar la habilitación de los parámetros de auditoría o activaciones de comandos que permitan el registro de actividades relacionadas con accesos, eliminaciones, modificaciones a las tablas principales que se realizan a la base de datos del Sistema ADRYAN.

4.2 Se identificó que los parámetros de contraseña del sistema operativo Windows 2000 del servidor de base de datos del Sistema ADRYAN, no se encuentran alineados con las políticas de contraseñas establecidas por la compañía.

Durante nuestra revisión, se observó que los valores de los parámetros de contraseña, configurados en el servidor de la base de datos del ADRYAN no se encuentran alineados a lo definido en la "Norma sobre definición de contraseñas" de la compañía.

Parámetro	Norma	Configuración Servidor
Intentos fallidos	>=3	>5
Historial de la contraseña	5	10
Máximo tiempo de antigüedad	**60**	**30**

La falta de configuración de los dos primeros parámetros de la tabla según la norma, implica el riesgo de accesos no autorizados por la vulnerabilidad de las contraseñas o mediante el uso de contraseñas más factibles de identificar por la reutilización de las mismas.

Se recomienda alinear los parámetros configurados en el servidor del ADRYAN hacia lo definido en las políticas de seguridad de la empresa. Respecto al parámetro de "máximo tiempo de antigüedad" de contraseña, tiene como valor asignado en el servidor 30 días; mientras que la política indica 60 días. A pesar que la regla en el servidor es más fuerte; se recomienda evaluar si dicha configuración está acorde a las necesidades de la compañía.

4.3 La cuenta "administrador" del sistema operativo Windows 2000 del aplicativo ADRYAN, no ha sido renombrada.

Durante nuestra revisión validamos que la cuenta con privilegios de administración del sistema operativo Windows ("Administrator") no ha sido renombrada. Esta cuenta administra todos los recursos y configuraciones del sistema operativo del servidor que soporta el sistema de Planillas.

Esta situación incrementa el riesgo de realizar intentos de accesos utilizando la cuenta de "administrador" por personal no acreditado, lo que podría llevar a realizar cambios no autorizados.

Se recomienda adicionar en la "Norma sobre definición de contraseñas" una sección que incluya el procedimiento de cambios de contraseña para las cuentas con privilegios de administración que considere:

- Periodicidad del cambio de contraseña
- Responsable de ejecutar el cambio.
- Complejidad de contraseña
- Método de cambio (manual o automático).

5. Revisión de Seguridad del módulo Administrator del Sistema ERP SAP:

5.1. No se han activado logs de auditoría en el Sistema SAP.

Durante la revisión de configuración de logs de auditoría, se identificó que no se han activado logs de auditoría para la aplicación SAP.

Esta situación incrementa el riesgo de no detectar cambios críticos en la configuración o a nivel transaccional del sistema.

Se recomienda evaluar la implementación de logs de auditoría tales como el reporte "Signon Audit Forms" y realizar revisiones periódicas sobre los resultados de éstos, con el objetivo de identificar situaciones irregulares.

5.2. Se carece de una política de administración de contraseñas que aplique para el ERP SAP.

Durante la revisión de configuración de contraseñas se identificó que no se ha establecido la activación de los siguientes parámetros de contraseñas.

- Historial de contraseñas.
- Complejidad de contraseñas.
- Máximo número de intentos fallidos.

La situación mencionada, incrementa el riesgo de vulnerabilidad de las cuentas de usuario del SAP, ya que la falta de lineamientos de seguridad sobre las contraseñas podría ocasionar el uso de contraseñas que no sean lo suficientemente robustas y en consecuencia podría existir una mayor probabilidad que personal no autorizado pueda acceder a dichas cuentas.

Se recomienda añadir una sección en las políticas de contraseñas de usuarios, donde se definan los parámetros de contraseñas específicos para cuentas del sistema SAP y para las aplicaciones en general.

5.3. No se ha configurado la opción de "Sequential Numbering" en el Sistema SAP.

Durante la revisión de las configuraciones del SAP se verificó que la opción "Sequential Numbering", la cual está referida a la secuencia numérica que deben tener todos los documentos que se ingresan en el SAP, se ha configurado con el valor "Parcialmente usado".

La situación mencionada incrementa el riesgo de omitir las reglas de correlatividad y registrar documentos duplicados, lo cual conllevaría a una inadecuada administración de los mismos y posibles registros erróneos de información en las áreas comerciales o financieras.

Se recomienda evaluar la configuración del campo "Sequential Numbering" de acuerdo a las necesidades que se presenten en el flujo del negocio para los procesos administrativos, comerciales y financieros.