Corporación Autónoma
Regional del Valle del Cauca

MEMORANDO

0120 - 794552018

PARA:	Ing. Diego Alexander Millán Londoño – Jefe Gestión de tecnologías de Información.
DE:	Jefe Oficina de Control Interno
ASUNTO:	Informe final de auditoria - Gestión de tecnologías de Información.
CIUDAD Y FECHA:	Cali Octubre 26 de 2018.

En cumplimiento del programa de auditoria 2018, se realizó la Auditoria Interna integral al proceso de Gestión de tecnologías de la Información, por lo anterior me permito enviarle el Informe Final producto de dicha auditoria, a fin de que se establezcan por parte del Líder y/o responsables del proceso de manera conjunta, las acciones correctivas y/o oportunidades de mejora necesarias para subsanar las no conformidades detectadas y atender las recomendaciones planteadas, en un plazo no mayor a diez (10) días hábiles, contados a partir del recibo de la presente comunicación.

Se recomienda al proceso de Gestión de tecnologías de Información identificar las causas que originaron la materialización de riesgos en el proceso, con base en factores internos o externos a la entidad, ya que la ocurrencia de estos, pueden afectar los logros de los objetivos del proceso y de la organización.

Por lo anterior, es pertinente efectuar la formulación de acciones para las oportunidades de mejora en procura, de fortalecer la cultura de control.

Agradezco su colaboración

Cordialmente,

BECQUI PAOLA ORDOÑEZ GARCIA

Anexos: Informe Final de Auditoria (4 folios)

Copia digital: Rubén Darío Materon Muñoz – Director General
Luis Guillermo Parra Suarez – Director Técnico de la Dirección de Planeación
Jaime Alberto Escudero - Coordinador del grupo Gestión Ambiental y Calidad.

Proyecto: Diego Fernando Arboleda Garcia.
Archívese en: 0120-061-008-0720-2018

INFORME FINAL DE AUDITORÍA

Corporación Autónoma Regional del Valle del Cauca

Fecha de Auditoría: 19, 20 Y 21 de septiembre de 2018.	Auditor Líder : Diego Fernando Arboleda Garcia
Proceso / Servicio: CP.0720 de Gestión de tecnologías de la Información.	Equipo Auditor: Abg .Diego Fernando Arboleda Garcia – Ing. Diana Maria Rodriguez – Apoyo Revisoría Fiscal.
Objetivo: Verificar y evaluar el cumplimiento de los controles internos del proceso CP.0720 de Gestión de tecnologías de la Información.	Alcance: Verificar el cumplimento de las acciones correctivas y oportunidades de mejora y el seguimiento al Plan de Mejoramiento de la CGR.
Programa de Trabajo	
Día 1: Revisión de no conformidades – Oportunidades de Mejora, Planes de mejoramiento.	Proceso: Gestión de tecnologías de la Información.
Día 2: Revisión de no conformidades – Oportunidades de Mejora, Planes de mejoramiento.	Proceso: Gestión de tecnologías de la Información.
Día 3: Revisión de recomendaciones planteadas por la Revisoría Fiscal en su informe de auditoría anterior.	Proceso: Gestión de tecnologías de la Información.

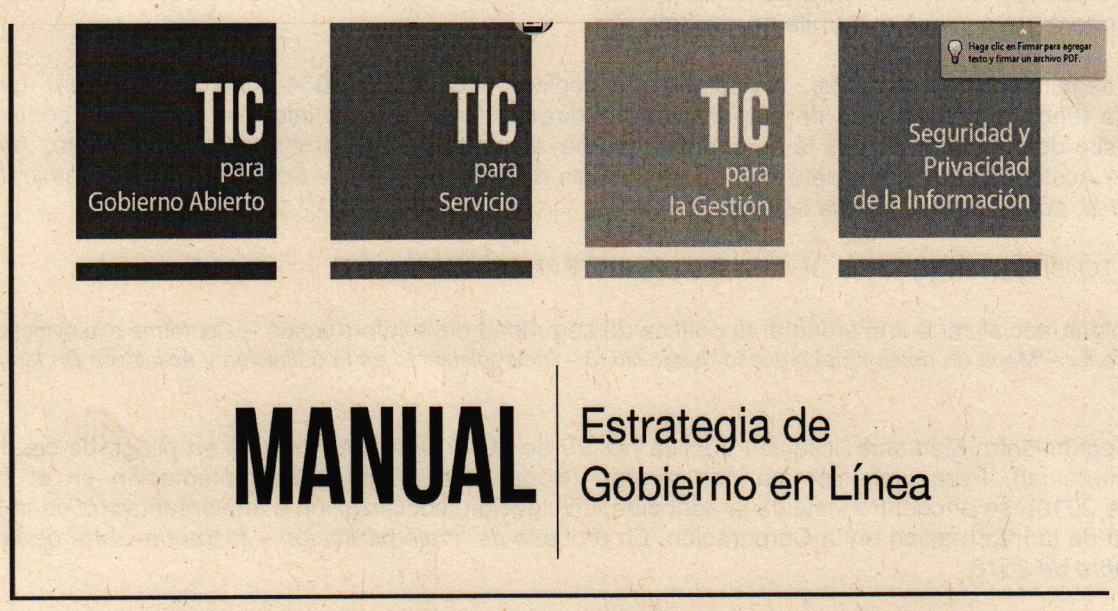
Principales Situaciones Detectadas:

Se realizó seguimiento a las Dos no conformidades encontradas en la Auditoria Anterior realizada en noviembre del 2017 y a las oportunidades de mejora así:

NO CONFORMIDADES AUDITORIA 2017.

1- Se mantiene la no conformidad de vigencias anteriores - No existe un plan estratégico de TI a través del cual se articule el cumplimiento de la líneas de acción de la Corporación.

Estado del seguimiento: La OTI ha venido revisando la información de GEL (Gobierno en línea) y los lineamientos del Ministerio de las tecnologías de la información (G-ES-06 guía como estructurar plan estratégico de tecnologías de Información PETI), con el propósito de estructurar el PETI de la Corporación.



Se solicitó por parte del líder auditor actas de reuniones internas mediante las cuales se evidenciara el adelanto de estas actividades y no fueron aportadas por el Proceso Auditado. *Se mantiene la no conformidad – continua abierta - fecha de cierre de la acción 31 de diciembre de 2018.*

2- Dentro de la revisión documental del contrato 601 de 2013 – Software financiero licitación Pública No. 27 de 2013. No se evidencio dentro del expediente contractual memorando mediante el cual se solicita la autorización al Director General para iniciar el trámite de contratación.

Estado del seguimiento: se solicita revisar otro expediente contrato el 634-2016, para validar que este efectivamente tenga el memorando de autorización del director General para iniciar el trámite de contratación, con el propósito de constatar de que la no conformidad haya sido tratada y corregida posteriormente, mediante el proceso de Acciones de Mejora para que no se vuelvan a repetir a futuro. – *Se evidenció el tratamiento de la no conformidad, por la tanto la misma se cierra.*

SEGUIMIENTO OPORTUNIDADES DE MEJORA PLANTEADAS POR LA OTI.

1- Adoptar, divulgar, socializar e implementar la política de seguridad de la información – *Conforme a lo evidenciado en la auditoria anterior – Mapa de riesgos del proceso riesgo No. 3 – Incumplimiento en la definición y aplicación De las políticas de T.I*

Estado del seguimiento: Mediante licitación pública No. 29 de 2018. Actualmente está en pliego de condiciones (fase precontractual). Para ejecución en dos meses. (Sería para iniciar la implementación en el mes de noviembre de 2018), se encuentra incluida la adopción, divulgación, socialización e implementación de la Política de Seguridad de la Información en la Corporación. *En proceso de implementación – fecha de cierre de la acción 31 de diciembre de 2018.*

2- Elaborar y diligenciar una encuesta para medir la satisfacción de usuarios con relación al servicio que presta la mesa de ayuda. *Conforme a lo evidenciado en la auditoria anterior – en el contrato de mesa de ayuda No. 634 de 2016 contempla la realización de una encuesta de servicios con el fin de medir la satisfacción de los usuarios internos.*

Estado del seguimiento: No se evidencio encuesta realizada por el contratista para medir la satisfacción de usuarios con relación al servicio que presta la mesa de ayuda. *Fecha de cierre de la acción 31 de diciembre de 2017 – no se cumplió con la oportunidad de mejora planteada.*

3- La definición de las acciones planteadas en el manejo de riesgos, para evitar su materialización, se establecerán con la elaboración del PETI, para su posterior implementación. *Conforme a lo evidenciado en la auditoria anterior – en la caracterización del proceso de Tecnologías de la Información, en las actividades del planear actividad No. 3 define que se debe generar el Plan Estratégico de T.I.*

Estado del seguimiento: Se está adelantando la contratación mediante licitación pública No. 29 de 2018. Actualmente está en pliego de condiciones (fase precontractual). Para ejecución en dos meses. Se iniciaría la implementación en el mes de noviembre de 2018, mediante la ejecución de este contrato se ejecutaría la acción. *Fecha de cierre de la acción 31 de diciembre de 2018.*

4- Socializar a los servidores públicos involucrados, de acuerdo a su posición técnica o administrativa, con relación a las guías enviadas al proceso Gestión de Calidad - *Guías remitidas a Calidad: modificar e inhabilitar cuentas de usuario en la red corporativa, creación de usuarios para acceso a los aplicativos corporativos y la Guía copia de seguridad informática.*

Estado del seguimiento: Mediante memorando No. 0130-681712018 del 18 de septiembre de 2018, dirigido a la Dirección de Planeación, se solicitó la revisión y análisis de los formatos: Guía crear, modificar e inhabilitar cuentas de usuario en la red corporativa, creación de usuarios para acceso a los aplicativos corporativos y la Guía copia de seguridad informática.

Se está adelantando la contratación mediante licitación pública No. 29 de 2018. La socialización será realizada por el contratista elegido dentro de la licitación en mención. Se iniciaría la implementación en el mes de noviembre de 2018, mediante la ejecución de este contrato se ejecutaría la acción.

5- Revisar y socializar los nuevos procedimientos para los integrantes del equipo de trabajo de la Oficina de Tecnologías de la Información.

Estado del seguimiento: se verifico la información de la socialización y se evidenciaron listados de asistencia de las socializaciones realizadas el día 1 de junio de 2018. *(Se cierra la Oportunidad de mejora estipulada por el área)*

6- Revisar periódicamente las tablas de retención documental del proceso.

Estado del seguimiento: se evidencio Acta de reunión Interna elaborada por el área mediante la cual se realizó la revisión de las tablas de retención documental del proceso y se evidencio la necesidad de la creación de una serie documental para archivar los registros del sistema de gestión de calidad. *(Se cierra la Oportunidad de mejora estipulada por el área)*

7- Apoyar a las demás áreas de la Corporación en la implementación de acciones conjuntas para dar cumplimiento a la Ley 1581 de 2012, por medio de la cual se dictan disposiciones generales para la protección de datos personales. Áreas Involucradas: Atención al ciudadano, Gestión de Talento humano, Asesoría y Representación jurídica, recursos físicos, Gestión Financiera.

Estado del seguimiento: Dentro de la licitación pública No. 29 de 2018, Se incluyó la definición de políticas y mecanismos para la implementación de la Ley 1581 de 2012. *(En proceso de implementación - fecha de cierre de la acción 31 de diciembre de 2018).*

SEGUIMIENTO PLAN DE MEJORAMIENTO

- En lo relacionado con el seguimiento y avance del Plan de Mejoramiento presentado a la CGR en lo referente a los hallazgos Nos. 7 y 14 se propuso la siguiente acción de mejora: " *Realizar la integración entre los aplicativos ARQ Comercial y ARQ documental",* al momento de la auditoria, el Jefe la oficina de Tecnologías de la Información manifestó lo siguiente:

El proceso de integración entre el sistema de información documental y el sistema de información comercial se desarrollará en tres puntos (generación de factura, validación de pago y creación cuenta), para cada uno de los trámites ambientales que aplique. En tal sentido, se tienen los siguientes avances:

Ya se encuentra listo y en fase de pruebas el desarrollo del componente de integración entre los dos sistemas que permite generar facturas de evaluaciones para derechos ambientales desde el flujo del trámite en la actividad Generar Factura.

Ya se encuentra listo y en fase de pruebas el desarrollo del componente de integración entre los dos sistemas que permite la validación de pago respectivo en el sistema comercial de la factura de evaluación generada desde el trámite del derecho ambiental.

La integración entre ambos sistemas de información para permitir la creación de cuentas de concesiones en el sistema comercial a partir del trámite de derechos ambientales, se encuentra en etapa de análisis y definición con los funcionarios de la Corporación. Sin embargo, a nivel de desarrollo se tiene el diseño de las formas para recepción de los datos necesarios para la creación de las cuentas. Es importante mencionar que este punto también abarca integración con el sistema de información de seguimiento a derechos ambientales SIPA.

No Conformidades

1- Se mantiene la no conformidad de vigencias anteriores - No existe un plan estratégico de TI a través del cual se articule el cumplimiento de la líneas de acción de la Corporación.

2- Elaborar y diligenciar una encuesta para medir la satisfacción de usuarios con relación al servicio que presta la mesa de ayuda. *Conforme a lo evidenciado en la auditoria anterior – en el contrato de mesa de ayuda No. 634 de 2016 contempla la realización de una encuesta de servicios con el fin de medir la satisfacción de los usuarios internos. – no s evidencio encuesta.*

Conclusiones

- En el seguimiento del Plan de Mejoramiento presentado a la CGR, al momento de la auditoria, se evidenció un avance en el cumplimiento de las acciones planteadas por el proceso, al cumplimiento de la meta ésta podría impactar positivamente en el manejo de la información oportuna, contribuyendo al cumplimiento de la misión, visión y objetivos institucionales. – *Lo anterior será objeto de seguimiento por parte de la Oficina de Control Interno.*

- Mediante memorando No. 0130-681712018 del 18 de septiembre de 2018, dirigido a la Dirección de Planeación, se solicitó revisión y análisis de los formatos: Guía crear, modificar e inhabilitar cuentas de usuarios en la red corporativa, creación de usuarios para acceso a los aplicativos corporativos y la Guía copia de seguridad informática. - *La Oficina de Tecnologías de la Información se encuentra en trámite de cumplimiento de la oportunidad de mejora, la cual será objeto de seguimiento por parte de la Oficina de Control Interno.*

- Teniendo en cuenta que el proceso realizó acciones de mejora, el líder del proceso debe asegurarse que las mismas se cumplan y se desarrollen dentro de las fechas estipuladas por el área, con el fin de completar el ciclo del planear, hacer verificar y actuar.

- Se recomienda al Líder del proceso documentar mediante los formatos de calidad establecidos, las reuniones internas mediante las cuales se adelantan actividades que conlleven a dar cumplimiento a las acciones de mejora y demás actividades propias del proceso, para con esto ayudar a mantener la confiabilidad, trazabilidad y facilidad para la consulta de la información.

- Dentro del seguimiento realizado por la firma Gonzalo Millan C y Asociados S.A en la auditoria se evidencio que a la fecha del seguimiento el proceso de licitación pública 029 de 2018, se encuentra en la fase precontractual. Por lo que no se logra evidenciar la implementación de las acciones. Y la clasificación de los riesgos continúa igual, hasta que finalice la ejecución del contrato.

- En lo relacionado con el cumplimiento de la Ley 1581 de 2012 Tratamiento de protección de datos, La Corporación debe iniciar a la brevedad posible la implementación de acciones que le permitan dar cumplimiento a la Ley 1581 de 2012 del tratamiento de datos personales. En este proyecto se deben involucrar todas las áreas

que realicen tratamiento de datos personales (Talento Humano, Atención al ciudadano, Contabilidad) con apoyo de las áreas Jurídica y Tecnologías de la Información.

- De conformidad a las recomendaciones realizadas por la Oficina de Control interno en el memorando No. 0120-98702018 del 13 de febrero de 2018, mediante el cual se da alcance a la evaluación de la dependencia, la OTI ha implementado las recomendaciones dadas por la oficina de control interno, con el fin de fortalecer y dinamizar el diligenciamiento oportuno y la utilización de los aplicativos en la Corporación.

- El proceso CP.0720 Gestión de Tecnologías de la información para las Dos No conformidades producto de la auditoría realizada en septiembre de 2017, formulo dos acciones correctivas, de las cuales una (1) se cierra y otra continua abierta, porque la fecha de cierre de la acción es diciembre 31 de 2018.

- En las oportunidades de mejora el proceso formulo 7 acciones de las cuales al momento del desarrollo de la auditoria se evidencio el cumplimiento de Dos (2), una (1) cumplida parcialmente, Tres (3) en proceso de implementación con cierre al 31 de diciembre de 2018 y una (1) acción no cumplida la cual pasa a ser no conformidad.

Información Adicional

SEGUIMIENTO Y RECOMENDACIONES REALIZADAS POR LA REVISORÍA FISCAL COMO APOYO TÉCNICO.

1- Política de seguridad de la información

- ✓ La Alta Dirección debe proveer los recursos para la implementación de la política de seguridad de la información y comunicar a todos los empleados y partes interesadas pertinentes.

2- Tratamiento de datos personales, implementación de acciones que le permitan dar cumplimiento a la Ley 1581 de 2012.

- ✓ La Corporación debe iniciar a la brevedad posible la implementación de acciones que le permitan dar cumplimiento a la Ley 1581 de 2012 del tratamiento de datos personales.
- ✓ En este proyecto se deben involucrar todas las áreas que realicen tratamiento de datos personales (Gestión Humana, Atención al ciudadano, Contabilidad) con apoyo de las áreas Jurídica y Tecnologías de la Información.

3- Acuerdos de confidencialidad de la información.

- ✓ Establecer acuerdos de confidencialidad de la información para todos los funcionarios de la Corporación.
- ✓ A pesar de que el Jefe de la Oficina de Tecnologías de la Información remitió comunicado al área administrativa y a la oficina Asesora de jurídica mediante memorando 0130-624552017, como responsables de la implementación de los acuerdos de confidencialidad en los contratos laborales. A la fecha no se evidencia implementación de dichos acuerdos.

4- Pérdida de Confidencialidad de la Información

- ✓ Fortalecer la documentación actual con respecto a la definición de perfiles en los diferentes sistemas de información de la Corporación, y los niveles de autorización.
- ✓ En la guía documentada se establece que la responsabilidad de la solicitud de la creación de los usuarios es del Director y/o Jefe de la Oficina. Sin embargo está pendiente el proceso de aprobación, socialización e implementación de la guía.
- ✓ Revisar periódicamente las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.
- ✓ Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

5- No se observa copia de seguridad de las configuraciones de los dispositivos de red y seguridad de la

Corporación.

- ✓ No se presenta avance al respecto, de esta recomendación. Por pate del Jefe de la oficina se sustenta que es responsabilidad de open group como proveedor de la solución y administrador de los dispositivos de red, y que contractualmente debe garantizar la continuidad de operación de los dispositivos (disponibilidad).
- ✓ Además se cuenta con un proceso de contratación en licitación pública para mejorar la infraestructura y fortalecer la solución de backup.

6- La Corporación no cuenta con ambientes de pruebas para validar la integridad de la información incluida en las copias de seguridad de la información. No se registran las validaciones realizadas a la información incluida en las copias de seguridad.

- ✓ No se cuenta con una ambiente de pruebas, ni infraestructura. Se está adelantando el proceso de contratación del servicio de administración de la base de datos, ya que internamente no se cuenta con el conocimiento para hacer el montaje de la base de datos.

7- Solicitar a los proveedores que cuentan con contraseñas de administración de dispositivos de red, seguridad, aplicaciones, bases de datos y/o servicios informáticos, realizar entrega formal en sobre sellado, o en herramientas informáticas de gestión de contraseñas, la entrega de las contraseñas.

- ✓ El Jefe de tecnologías de la información tiene bajo su recaudo y custodia en sobres sellados las contraseñas de administración de dispositivos de red, seguridad, aplicaciones, bases de datos y/o servicios informáticos.

8- No se realiza análisis de vulnerabilidades de los sistemas de información que están en uso - Pérdida de Disponibilidad.

- ✓ Se incluyó dentro de la licitación pública 029 de 2018, un análisis de vulnerabilidades 15 activos internos y 5 externos.
- ✓ Se incluyó dentro de la licitación pública 029 de 2018, que el proveedor debe presentar el análisis de las vulnerabilidades identificadas y definir las remediaciones necesarias.

9- Desarrollar y ejecutar un plan para la gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades e incidentes de seguridad.

- ✓ Se incluyó dentro de la licitación pública 029 de 2018, la gestión de parches de seguridad para los sistemas operativos de servidores y clientes.

10- Establecer una política formal y adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

- ✓ Dentro de la licitación pública se establece la implementación de una herramienta DLP, direccionada a la implementación en 30 equipos.

11- Establecer un protocolo para seleccionar, proteger y controlar los datos utilizados para realizar pruebas de los diferentes sistemas de información.

- ✓ La licitación pública 029 de 2018 incluye un punto para la documentación de políticas y procedimientos de seguridad.

12- Desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.

- ✓ A pesar de que en el proceso de implementación del SGSI se incorpora un análisis de riesgos de los activos de información, que pueden ser insumo para la definición del DRP, es necesario estructurar un documento detallado para establecer las acciones que deben implementarse por parte de la Corporación ante la materialización de una situación adversa.
- ✓ La definición del DRP incluye la definición de tiempos de recuperación y restauración, la priorización de los servicios, y la definición de los recursos necesarios (infraestructura, humano, económicos) para

garantizar la continuidad de la operación. - *Sin Implementar.*

13- El Datacenter ubicado en las instalaciones de la Corporación no cumple con algunas condiciones definidas en las mejores prácticas para la seguridad física del mismo.

- ✓ Por parte de un tercero se realizó un diagnóstico al datacenter en el que se establecieron oportunidades de mejora, como retirar el icopor y aislamiento de las redes eléctricas, instalación de sensores y sistemas de detección de incendios, sin embargo a la fecha no se han contratado las soluciones - *Sin Implementar*

14- Definir e implementar mecanismos de seguridad adicionales, para aquellos equipos en los que se realizan transacciones de banca en línea

- ✓ La licitación pública 029 de 2018 incluye el análisis de riesgos del proceso financiero que es el responsable de la realización de las transacciones de banca en línea, mediante este se pretende establecer controles a la medida de la Corporación para prevenir pérdida económica por riesgos asociados a ataques informáticos - *En proceso de Implementación.*

Lista de distribución del informe

Rubén Darío Materon Muñoz – Director General.
Diego Alexander Millan – Jefe Oficina de TI.
Luis Guillermo Parra Suarez – Director Técnico.
Jaime Alberto Escudero Jiménez – Coordinador del grupo Gestión Ambiental y Calidad.

Nombre y Firma auditor Líder

DIEGO FERNANDO ARBOLEDA GARCIA.