1.INFORME Nº: 16	PROCESO/DEPENDENCIA
	GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN

2. FECHA: 7 de Julio al 27 de Agosto de 2015

3. PROCESO / ACTIVIDAD AUDITADA:

Garantizar el funcionamiento de la plataforma de Tecnología de Información y Comunicaciones (TICS) y lo relacionado con la Seguridad Informática de acuerdo con las políticas de la Entidad y las normas legales vigentes.

4. EQUIPO AUDITOR:

Rocio Pedrozo (Líder)

5. OBJETIVO:

Constatar que las actividades desarrolladas en el proceso cumplan con los criterios de auditoria definidos en el ítem anterior, con el fin de validar su adecuado funcionamiento, de manera que permita contribuir a la mejora continua del Sistema de Gestion Integrado, el Sistema de Control Interno y la Gestión Institucional.

6. ALCANCE DE LA AUDITORIA:

Aplica a todas las actividades del Proceso de Gestión de Infraestructura y Tecnologías de Información y a las dependencias que participan en el, para el periodo comprendido entre el 1 de Diciembre de 2014 y la fecha de la auditoria. Para el desarrollo de esta auditoría se aplicarán las normas de auditoria generalmente aceptadas en Colombia y la validación y análisis se hará por prueba selectiva y/o muestreo. No obstante se podrán incorporar hechos adicionales que se evidencien en la auditoría y que estén por fuera del periodo definido en el alcance, hechos que quedarán habilitados para el informe.

7. PERSONAL ENTREVISTADO:

Jorge Bernardo Gómez, Héctor Gerardo Guerrero, Julio Roberto Romero, Francisco Arguello Zuta, Gerardo Enrique Reyes, Camilo León, Leonor León, Jeny Shirley Diaz Gonzalez y Andersón López Cruz Peñaloza

8. ASPECTOS FUERTES:

1. Receptividad a las observaciones realizadas en el desarrollo de la auditoria, encaminadas a fortalecer la mejora continua en la Gestión Institucional.

9. OBSERVACIONES

1. Revisada la caracterización del proceso auditado se observa que si bien la Entidad ha desarrollado planes de acción encaminados a la implementación de la gestión del servicio de TI basado en las mejores prácticas ITIL, esto no se ve reflejado dentro de la caracterización del mismo, al no encontrarse procedimientos documentados orientados a la gestión de las buenas prácticas en la Entidad, que permita garantizar un mejor servicio a los usuarios internos y externos.

1.INFORME N°: 16

PROCESO/DEPENDENCIA
GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN

2. FECHA: 7 de Julio al 27 de Agosto de 2015

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Plan de Acción	1. Durante el desarrollo de la auditoria, el equipo auditor evidenció que la Entidad para el año 2015 estructuró un Proyecto o Plan de Acción denominado "Implementación Política Gobierno en Línea – GEL", sin embargo, éste no se encuentra desagregado para cada uno de los componentes articulados en el Decreto 2573 de 2014 y en el Manual de Gobierno en Línea (GEL), donde se identifique cada una de las actividades a realizar, asignación de responsables, metas y plazos. Situación que impide realizar un adecuado seguimiento a la ejecución y al cumplimiento de dicho plan. Adicionalmente, se evidenció que la Entidad aún no cuenta con un equipo de trabajo asignado para desarrollar cada una de las actividades de la Estrategia de Gobierno en Línea, situación que podría poner en riesgo el cumplimiento de los plazos establecidos en el Art. 10 del citado Decreto.					Elemento: Planes, Programas y Proyectos 1.2.1		Art. 5 Decreto 2573 de 2014
Plan de Mejoramiento	2. El plan de mejoramiento estructurado por el proceso auditado para la vigencia 2014, con ocasión del informe de auditoría de la Oficina de Control Interno, determinó en su no conformidad No. 2 "*El equipo auditor pudo evidenciar que existen documentos dentro de la caracterización del proceso auditado, que se encuentran desactualizados según prueba selectiva realizada sobre estos así: procedimiento GINF-PR-006 GESTIÓN DE CAMBIOS, Guía GINF-G-005 PLAN DE RECUPERACIÓN ANTE DESASTRES -DRP*". Así las cosas, analizada la información para el periodo definido dentro del alcance de esta auditoria, se evidenció que las acciones tomadas para eliminar esta no conformidad no fueron eficaces, por cuanto aún persiste la desactualización generalizada en la documentación que hace parte de este proceso, como por ejemplo dentro del contenido del procedimiento se citan formatos que no corresponden a la codificación, se nombran plataforma tecnológica (servidores, Bases de Datos) que ya no están en servicio en la Entidad.	Numeral 4.1.c y Numeral 8.5.2				Elemento: Planes de Mejoramiento por proceso.		

1.INFORME Nº: 16	PROCESO/DEPENDENCIA	2. FECHA: 7 de Julio al 27 de Agosto de 2015
	GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN	

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Puesta en Producción de Aplicativos	3. En la Página Web de la Entidad se encuentran servicios publicados con errores de funcionamiento, como lo evidenció el equipo auditor así: • Servicio "Peticiones, Quejas y Reclamos (PQRS)": Al ingresar por las opciones de "Informe Transparencia al Ciudadano" e "informes", al generar cualquier reporte de éstos, aparece el siguiente mensaje: "*Error al convertir el tipo de datos nvarchar a datetime*" y no muestra información. Cabe mencionar que este servicio se encuentra en producción desde el 2013. • Servicio "Sistema de Información General de Sociedades": Al ingresar a esta opción despliega al lado izquierdo de la pantalla un submenú con las siguientes opciones: Listas, Bibliotecas, Videos y Ministerio Comercio Al acceder a cada uno de estos link, muestra librerías de SharePoint, que no tiene relación con la consulta realizada.				A.14.2.9		GINT-PR-003 Adquisición e Implementación de Sistemas de Información 2.3	
	4. El procedimiento interno "*Adquisición e Implementación de Sistemas de Información GINT-PR-003*", dentro de su esquema tiene como punto de control, realizar pruebas finales de la solución antes de su paso a producción, para ello cuenta con el formato "*GINT-F-006 Lista de Chequeo Pruebas Finales Sistemas de Información*", diseñado para tal fin. El equipo auditor evidenció que dicha lista de chequeo no es utilizada por el Ingeniero de Sistemas designado para realizar las pruebas.						GINT-PR-003 Adquisición e Implementación de Sistemas de Información 3	
	5. Al realizar un análisis de documentos radicados en el aplicativo Post@l, el equipo auditor evidenció que desde el Grupo de Sistemas y la Dirección de Informática y Desarrollo se crearon registros de pruebas en la Base de Datos de Producción de dicho aplicativo, pruebas estas, que se deben realizar en ambientes diferentes al de producción. Al momento de la auditoria, estos registros aún no han sido anulados en el Post@l. Como en los siguientes casos: Radicados: 2014-01-073238, 2014-01-073240, 2014-01-088512, 2014-01-088518, 2014-01-088519, 2014-01-108321 y 2014-01-426946.				A.12.1.4		GINT-PR-003 Adquisición e Implementación de Sistemas de Información 2.8	

1.INFORME N°: 16

PROCESO/DEPENDENCIA
GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN

2. FECHA: 7 de Julio al 27 de Agosto de 2015

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Respaldo y Recuperación de Datos	6. Dentro del desarrollo de la auditoría, el equipo auditor evidenció que se realizan copias de respaldo a la información institucional; sin embargo, no se están realizando pruebas trimestrales de restauración de estas copias de seguridad, que garanticen que son confiables en caso de emergencia.				A.12.3.1		GINT-PR-001 Respaldo y Recuperación de Datos de la Infraestructura Tecnológica 2.9	
Desactualización Análisis de Impacto al Negocio (BIA)	7. El Análisis de Impacto al Negocio (BIA), documento estructurado en Febrero del año 2009, con el que soporta el Plan de Recuperación ante Desastres-DRP, donde están identificados los procedimientos, la Plataforma Crítica de la Entidad, es decir, sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son decisivos para soportar los procesos y servicios en caso de un incidente o desastre, no se encuentra ajustado a la actual plataforma tecnológica con que cuenta la Entidad, poniendo en riesgo la disponibilidad y la continuidad en la prestación de los servicios a usuarios internos y externos ante un posible evento de interrupción.	4.2.3 b)						
Alineación entre los documentos del proceso	8. Al realizar un análisis entre la Guía Plan de Recuperación ante Desastres GINT-G-005, y el Procedimiento Gestión al Plan de Recuperación ante desastres GINT-PR-005, el equipo auditor evidenció que éstos no se encuentran alienados con el Documento de Modelos del SGI GC-MO-001, lo que puede impactar con los roles y responsabilidades que deben cumplir ante un incidente o desastre. Adicionalmente se encontró debilidades en la Dirección de Informática y Desarrollo y en los grupos adscritos a ésta, en la socialización de los procedimientos, en los perfiles asignados y empoderamiento de los roles, responsabilidades y actividades que se deben surtir ante la ocurrencia de un evento que pueda impactar la continuidad del negocio. Situación que se vuelve crítica teniendo en cuenta que la Entidad en estos momentos no cuenta con un Centro de Cómputo Alterno, que permita recuperar los procesos soportados por TI.	4.2.3 b)						

1.INFORME Nº: 16	PROCESO/DEPENDENCIA	2. FECHA: 7 de Julio al 27 de Agosto de 2015
	GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN	

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Aplicación del Políticas	9. Al revisar el procedimiento que llevó a cabo la Entidad al conceder la modalidad de Teletrabajo a un funcionario de la Superintendencia de Sociedades, el equipo auditor evidenció que el oficial de seguridad de la información no fue requerido para aprobar el acceso a la plataforma tecnológica de servicios no publicados hacia redes externas, o que implicara la administración remota de la plataforma, conforme lo establece el Documento de Políticas del SGI. Lo anterior evidencia falta de controles y de comunicación entre las áreas involucradas.				A.14.1.1		GC-PO-001 Documento de Políticas del SGI 2.2.8 Política de Trabajo Remoto	
	10. Al Oficial de seguridad no se le envía para su custodia, las contraseñas impresas de super usuario, para cada uno de los sistemas de información que son críticos para la Entidad. Incumpliendo lo establecido en el Documento de Políticas del SGI.				A.14.1.1		GC-PO-001 Documento de Políticas del SGI 2.2.12 Política de uso de contraseñas	
Gestión de Incidentes y Mejoras en la Seguridad de la Información	11. Dentro de la Gestión de Incidentes de Seguridad de la Información que realiza la Entidad, el equipo auditor evidenció, que si bien es cierto, se registra y documenta el incidente de seguridad en la herramienta utilizada para tal fin (Service Manager), en la Entidad no existe un procedimiento documentado, donde establezca directrices de cómo abordar y gestionar los siguientes temas que contempla ISO:2701: A.16.1.2. Reporte de eventos de seguridad de la información. A.16.1.3. Reporte de debilidades de seguridad de la información. A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. A.16.1.5. Respuesta a incidentes de seguridad de la información. A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la Información. A.16.1.7. Recolección de evidencia.				A.16.1			

1.INFORME Nº: 16	PROCESO/DEPENDENCIA
	GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN

2. FECHA: 7 de Julio al 27 de Agosto de 2015

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Gestión de Cambios	12. Al revisar el procedimiento de Gestión de Cambios, que aplica la Entidad antes de poner en producción un sistema de información, servicio, Hardware y/o Software , entre otros, el equipo auditor evidenció que aun cuando se registran las peticiones de cambios en la herramienta Service Manager, ésta información no cumple con todas disposiciones descritas en el Procedimiento Gestion de Cambios GINT-PR-006, como en los casos CR6180 Instalación Botón PSE y CR6001 Actualización Sistema de Gestión Documental en Producción así. No se documentaron las reuniones del Comité de Cambios. No se Analizó riesgo/impacto de las Peticiones en el entorno de producción. No se documentaron las lecciones aprendidas. No se cerraron los casos. Adicionalmente se evidencia debilidad en cuanto a la asignación de roles y responsables de ejecutar las funciones que deben cumplir cada uno de los involucrados en la gestión de cambios.				A.12.1.2		GINT-PR-006 Gestion de Cambios	
Permisos sobre el Directorio Activo	13. Dentro del reporte de funcionarios registrados en el Directorio Activo de la Entidad, base de datos que permite almacenar información relativa a los recursos de red con el fin de facilitar su localización y administración, el equipo auditor evidenció que existen cuentas de usuarios que requieren ser depuradas, por cuanto se encontraron funcionarios categorizados dentro del grupo denominado "Coordinadores", que no ostentan dicho cargo, los cuales cuentan con privilegios como navegación sin restricción, acceso a redes sociales, entre otros. Situación encontrada en los siguientes casos: Paola Marcel Cañón Prieto, Laura Alejandra Medina Gonzalez, Nancy Arias Rodriguez, Edicsson de Armas Amaris, John Gabriel Espinosa Gómez, Stella Isabel Rodriguez Cortes, Aida Patricia Quiroga Montaña.				A.9.2.3		GINT-G-002 Guía: Gestión de Usuarios Plataforma Tecnológica 2.5	

1.INFORME Nº: 16	PROCESO/DEPENDENCIA
	GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACIÓN

2. FECHA: 7 de Julio al 27 de Agosto de 2015

10. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DEL HALLAZGO DETECTADO	NORMATIVIDAD						
		GP 1000	14001	18001	27001	MECI	REQUISITO INT	LEGALES
Plan de Mejoramiento	14. Al analizar el Plan de Mejoramiento estructurado por la Dirección de Informática y Desarrollo, producto de la auditoría realizada por la Oficina de Control Interno durante el año 2014, en busca de eliminar la no conformidad No. 3 así: " De la revisión realizada a la lista de funcionarios y/o contratistas con derechos de acceso a la Red Privada Virtual (VPN de acceso remoto) de la Entidad, el equipo auditor pudo evidenciar que falta depurar la información allí relacionada, por cuanto en ella aparecen contratistas que pese a tener la cuenta de acceso expirada, visualmente pareciera que tuvieran acceso a ella. Como es el caso de las cuentas analizadas aleatoriamente de los contratistas: Angela Bibiana Galindo, Claudia Juliana Naranjo, Daniel Espinoza, Nelson Ricardo Avendaño, Cristhian Caldas", el equipo auditor encontró durante el desarrollo de ésta auditoria, que la no conformidad persiste, por lo cual se establece que las acciones tomadas para eliminar esta no conformidad, no fueron eficaces. Aun cuando se depuró la información encontrada en la auditoria anterior, para esta vigencia se encontraron los siguientes registros: Carlos Francisco Ruiz Perdomo, Jairo Antonio Becerra Delgado, Angelica Martinez López, Fredy Aparicio Posada Tapasco, entre otros.	Numeral 4.1.c y Numeral 8.5.2				Elemento: Planes de Mejoramiento por proceso		

11. CONCLUSIÓN GENERAL

Las actividades auditadas del proceso de Gestión de Infraestructura y Tecnologías de Información se desarrollan conservando los parámetros establecidos para el cumplimiento del objetivo del proceso, en este sentido, el grado de conformidad del mismo cumple en términos generales con los criterios evaluados en la auditoria . No obstante lo anterior, se deben implementar las acciones preventivas a las observaciones y correctivas a las no conformidades detectadas, de manera que su implementación permita garantizar la mejora continua del proceso auditado y por ende la maduración del Sistema de Gestión Integrado, la Gestión Institucional y el Sistema de Control Interno.

De acuerdo con la estructura orgánica interna de la Dirección de Informática y Desarrollo, se sugiere efectuar un análisis de los roles, perfiles y funciones de cada uno de los funcionarios de las dependencias adscritas a ésta, de manera que permita diagnosticar y determinar si cuenta con las personas necesarias para administrar y gestionar los temas relacionados con TI.

12. FIRMAS:

WILMA ROCÍO PEDROZO ULLOA
NOMBRE Y FIRMA: DEL AUDITOR LIDER

ARNULFO SUAREZ PINZÓN
NOMBRE Y FIRMA: JEFE OFICINA CONTROL INTERNO