Superintendencia de Sociedades	SUPERINTENDENCIA DE SOCIEDADES	Codigo:EC-F-003
	SISTEMA DE GESTIÓN INTEGRADO	Fecha: 29-03-2011
	PROCESO: EVALUACIÓN Y CONTROL	Version 005
	FORMATO: INFORME DE AUDITORIA - SEGUIMIENTO	Pagina 1 de 5

PROCESO/DEPENDENCIA	
1.INFORME Nº: 15	GESTIÓN DE INFRAESTRUCTURA Y LOGISTICA

2. FECHA: DICIEMBRE 13 DE 2011

3. PROCESO / ACTIVIDAD AUDITADA:
Proceso de Infraestructura y Logistica

4. EQUIPO AUDITOR:
Rocio Pedroza Ulloa (Lider)
Miguel Dario Quintana Sanchez

5. OBJETIVO:

Constatar que las actividades desarrolladas en el proceso de Infraestructura y Logistica, cumplan con los criterios de auditoria (NTCGP1000:2009, ISO 27001:2005, MECI, Requisitos Legales aplicables y Requisitos de la Organización)

6. ALCANCE DE LA AUDITORIA:
Aplica a todas las actividades del proceso

7. PERSONAL ENTREVISTADO
Ing. Juan Pablo Buitrago Ruge - Director de Informática y Desarrollo
Ing. Jaime Orlando Rincon Peñuela (Coordinador Grupo de Sistemas)
Ing. Francisco Javier Lara (Lider Centro de Computo)
Ing. Gerardo Enrique Reyes
Ing. Claudia Patricia Castillo
Ing. Jorge Bernardo Gomez
Ing. Daniel Barragan
Arq. Juan Esteban Rojas - Coordinador Grupo Administrativo

8. ASPECTOS FUERTES:

La Dirección de Informática y Desarrollo está trabajando en la renovación y modernización de la plataforma tecnologica, para fortalecer los esquemas de seguridad y garantizar la disponibilidad y continuidad de la prestación de los servicios.

Disposición, colaboración y entrega de información parte de los auditados durante el desarrollo de esta auditoria.

9. OBSERVACIONES	NORMATIVIDAD					REFERENCIACIÓN
	GP 1000	27001	MECI	REQUISITO INTERNO	LEGALES	FOLIO No.
Revisado los indicadores que se llevan en el proceso auditado, se observa que estos son de ejecución y miden la eficiencia, eficacia y efectividad, dejando de lado la implementacion de otros indicadores importantes que incluyen variables de costo y tiempo, a manera de ejemplo • Recursos: Como talento humano • Cargas de trabajo: Como estadisticas y metas que se tengan para un periodo determinado, y el tiempo y número de personas requeridas para realizar una actividad • Resultados: Como Compañias atendidas, oficios respondidos, ejecucion del cronograma, etc. • Productividad: Como casos atendidos por profesionales, solicitudes procesadas por persona, llamadas atendidas. • Satisfacción del usuario: Como el número de quejas recibidas, resultados de las encuestas, utilización de procesos participativos y visitas. • Calidad del servicio: Como tiempos de respuesta al usuario, capacidad para acceder a una instancia, racionalizacion de tramites.	Numeral 8.2.3 Seguimiento y medición de los procesos y 8.4 Análisis de datos NTCGP 1000:2009		Numeral 2.1.4 Indicadores MECI 1000:2005			

Superintendencia de Sociedades	SUPERINTENDENCIA DE SOCIEDADES	Codigo:EC-F-003
	SISTEMA DE GESTIÓN INTEGRADO	Fecha 29-03-2011
	PROCESO: EVALUACIÓN Y CONTROL	Version 005
	FORMATO: INFORME DE AUDITORIA - SEGUIMIENTO	Pagina 1 de 5

PROCESO/DEPENDENCIA	
1.INFORME Nº: 15	GESTION DE INFRAESTRUCTURA Y LOGISTICA

2. FECHA: DICIEMBRE 13 DE 2011

3. PROCESO / ACTIVIDAD AUDITADA:
Proceso de infraestructura y Logistica

9. OBSERVACIONES	NORMATIVIDAD					REFERENCIACIÓN
	GP 1000	27001	MECI	REQUISITO INTERNO	LEGALES	FOLIO No
DIRECCIÓN DE INFORMATICA Y DESARROLLO **Plan de Acción:** Revisado el servidor Superscan en la carpeta de. año 2011 para el proceso auditado, se encontro que el objetivo estrategico No. 3 "*Actualizar e integrar la plataforma tecnológica, adecuar la infraestructura física y optimizar los procesos para mejorar la prestacion del servicio el suministro de información y la comunicacion interna y externa*". requiere para su desarrollo de siete (7) estrategias, cinco (5) planes y siente (7) entregables de acuerdo al documento consolidado de la planeación estratégica para el año 2011. Revisada la información sobre la ejecución de los planes de acción, se encontró que hay tres (3) planes en ejecucion y no se evidencian planes para las estrategias. 1. *Fortalecer y sensibilizar en riesgos y seguridad informática, y 2. implementar las políticas de gobierno en línea, a través de la mejora de los servicios tecnológicos*.	Numeral 8.2.3 NTCGP 1000:2009					
No se puede evidenciar la integracion de los sistemas de información con que cuenta la Entidad.				Numeral 2.2 del Procedimiento GINF-PR-003 "Procedimiento de Adquisicion e implementacion de Sistemas de nformacion".		

10. RECOMENDACIONES

DIRECCIÓN DE INFORMATICA Y DESARROLLO

Es conveniente que las actividades documentadas en los planes de acción que no se cumplieron en su totalidad, sean retomadas para el siguiente año, con el fin de alcanzar el objetivo propuesto. ejemplo Plan de Contingencia Informatico Fase I – contratacion especializada para la construcción del Datacenter, actividad en la cual se ha presentado retrasos y evidenciamos que a la fecha 12 de diciembre de 2011 no se ha realizado el contrato.

Pese a que existe un Plan de Mantenimiento Preventivo y Correctivo para los equipos que conforman la Plataforma Tecnologica de la Entidad para el año 2011, es necesario que se le haga un monitoreo constante y una actualizacion permanente, para poder realizar planes de contingencia en el momento en que sea necesario.

Mantener actualizado el inventario de la plataforma tecnologica con lo que reporta el aplicativo STONE, teniendo en cuenta que esta informacion debe salir de una sola fuente de información y tiene que ser homogénea.

Crear un canal mas directo y efectivo con los grupos e Intendencias Regionales, para conocer las necesidades de información de cada uno de ellos y poder mejorar la gestión.

Realizar depuración del servidor de comunicaciones, teniendo en cuenta que en el momento de la auditoria se encontraron extensiones activas de exfuncionarios, como en el caso de: Ruth Garzón, Omaira Delgado Evangelina Otero.

Llevar una relacion detallada de los equipos que se encuentran en garantia o con mantenimiento vigente, para tener información exacta.

Reforzar la socializacion de cada uno de los Procedimientos, Guias, Manuales, Formatos y temas de interes, en especial aquellos en los que se involucran a los funcionarios como parte activa del proceso y que pueda poner en riesgo la norma, desarrollo de las tareas que realizan, como en el caso del procedimiento de Respaldo y Recuperación de Datos.

GRUPO ADMINISTRATIVO

En el desarrollo de la auditoria el dia 30 de noviembre de 2011, se identifico en el formato GINF-F-016 "Control de Ingreso a Instalaciones", que tres funcionarios ingresaron a la entidad a las 8:00 a.m., e inmediatamente diligenciaron la hora de salida 5:00 p.m., por lo anterior se recomienda ejercer mas control por el grupo administrativo para evitar que esto siga sucediendo.

Superintendencia de Sociedades	SUPERINTENDENCIA DE SOCIEDADES	Codigo:EC-F-003
	SISTEMA DE GESTIÓN INTEGRADO	Fecha: 29-03-2011
	PROCESO: EVALUACIÓN Y CONTROL	Version 005
	FORMATO: INFORME DE AUDITORIA - SEGUIMIENTO	Pagina 1 de 5

1.INFORME Nº: 15

PROCESO/DEPENDENCIA
GESTION DE INFRAESTRUCTURA Y LOGISTICA

2. FECHA: DICIEMBRE 13 DE 2011

3. PROCESO / ACTIVIDAD AUDITADA
Proceso de Infraestructura y Logistica

11. HALLAZGOS

ACTIVIDAD	DESCRIPCIÓN DE LA NO CONFORMIDAD DETECTADA	NORMATIVIDAD					REFERENCIACION
		GP 1000	27001	MECI	REQUISITO INT	LEGALES	FOLIO No
DIRECCIÓN DE INFORMATICA Y DESARROLLO							
Planes de Mejoramiento	Al revisar el Plan de mejoramiento de año 2010 definido para el hallazgo número 11 *"Existen servidores que soportan bases de datos de alto impacto para la Entidad que a la fecha de la auditoria, no se les ha programado ni realizado un mantenimiento preventivo, como es el caso de los SERVIDORES DELL DS 4300 (SAN), LTO 3583 (Libreria), AIX 550 "* se evidencio que las acciones tomadas para eliminar la no conformidad en el año 2010 no fueron eficaces. Por cuanto al validar la información para el año 2011, se encontro que no se cuenta con un contrato de mantenimiento preventivo y correctivo vigente, la los mismos servidores, 814 computadores, 17 scanners y 41 impresoras.	Numeral 6.3.b y Numeral 8.5.2 NTCGP 1000:2009	Numeral A.8.2.4 ISO 27001:2006	Componente de información. elemento sistema de información. Elemento: Planes de mejoramientos por proceso	Numeral 2.6 del Procedimiento GINF-PR-002 "Mantenimiento Preventivo, Soporte Técnico y mantenimiento correctivo de la infraestructura Tecnológica".		
Módulo Administrador de usuario	El aplicativo Baranda Virtual Coactiva no cuenta con un módulo administrador de usuarios que permita crear, modificar o asignar permisos a un determinado funcionario; tarea que realiza una persona que no pertenece a área de desarrollo poniendo en riesgo el sistema de información.	Numeral 7.5.3 NTCGP 1000:2009			Numera 2.9 del Procedimiento GINF-PR-003 "Adquisicion e Implementacion de Sistemas de Informacion		
Planes de Mejoramiento	Al evaluar el Plan de Mejoramiento de año 2010 definido para el hallazgo número 14 *"No se evidencia en la caracterización del proceso ninguna actividad relacionada con la aplicación de la Encuesta Interna de Satisfaccion formato GINF-F-007"*, se evidenció que las acciones tomadas para eliminar la no conformidad no fueron eficaces. Por cuanto al validar la información para el periodo 2011, se encontro que tampoco se aplicó la encuesta para el año 2010 y aún no se ha aplicado para el año 2011".	Numeral 4.1.c y Numeral 8.5.2 NTCGP 1000:2009		Elemento. Planes de mejoramientos por proceso			
Revisión técnica de las aplicaciones	Se constató que existen funcionalidades en la parte privada de la página intranet de la entidad, como por ejemplo las opciones de "inventario a mi cargo", " Mi crédito de Vivienda" ; que dejaron de funcionar despues de una actualización y migracion a un nuevo servidor. No se revisó, ni se realizaron las pruebas necesarias por parte del área de sistemas, para asegurar su correcto funcionamiento.		A.15.1.4 ISO 27001:2006		Numeral 3.4. de la Guia GINF-G-008 "Administracion Técnica de la Infraestructura Tecnologica"		
Control de procesamiento interno	Durante el desarrollo de la auditoria se evidencio que al aplicativo SIGS se le hacen actualizaciones desde linea de comando para solucionar problemas como por ejemplo: actualizar campos, sincronizar etapa en el proceso, eliminar registros, cambiar la dependencia. Situación que pone en riesgo la integridad de la información en el sistema .		A.12.2.2 ISO 27001:2006				

Superintendencia de Sociedades	SUPERINTENDENCIA DE SOCIEDADES	Codigo:EC-F-003
	SISTEMA DE GESTIÓN INTEGRADO	Fecha: 29-03-2011
	PROCESO: EVALUACIÓN Y CONTROL	Versión 005
	FORMATO: INFORME DE AUDITORIA - SEGUIMIENTO	Pagina 1 de 5

1.INFORME Nº: 15

PROCESO/DEPENDENCIA
GESTION DE INFRAESTRUCTURA Y LOGISTICA

2. FECHA: DICIEMBRE 13 DE 2011

3. PROCESO / ACTIVIDAD AUDITADA:
Proceso de Infraestructura y Logistica

ACTIVIDAD	DESCRIPCION DE LA NO CONFORMIDAD DETECTADA	NORMATIVIDAD					REFERENCIACION
		GP 1000	27001	MECI	REQUISITO INT	LEGALES	FOLIO No.
Protección de los datos y privacidad de la información personal	El 30 de Marzo del presente año, la Dirección de informatica y desarrollo envió un correo electrónico con la cuenta "Webmaster@supersociedades.gov.co" a cada uno de los funcionarios de la Entidad, donde se anexaba un link para acceder al Certificado de Ingresos y Retenciones correspondiente al año 2010, sin tomar las medidas necesarias para asegurar la proteccion, la privacidad de la informacion personal y la seguridad de los datos.		A.12.5.2 ISO 27001:2006				
Planes de Mejoramiento	Al revisar el plan de mejoramiento del año 2010 definido para el hallazgo numero 10 *"No se estan monitoreando los logs de los servidores con que cuenta la entidad"* se constato que las acciones tomadas para eliminar la no conformidad no fueron eficaces. Por cuanto al validar para el periodo 2011 el monitoreo a los logs estos no se estan realizando de acuerdo al procedimiento Gestion de Logs y Registro de Auditoria	Numeral 8.5.2 NTCGP 1000:2009		Elemento: Planes de mejoramientos por proceso	Procedimiento GINF-PR-007 "Gestion de Logs y Registros de Auditoria"		
pruebas de vulnerabilidad de la plataforma tecnológica	La entidad no ha realizado la revision de manera independiente de las pruebas de vulnerabilidad de la plataforma tecnológica.		A.6.1.8 de la ISO 27001:2006		Numeral 2.5 de la Guia GINF-G-008 "Administracion Tecnica de la Infraestructura Tecnológica".		
Custodia de las copias de Respaldo	Hace más de un mes que no se entregan las copias de respaldo que contiene información institucional para la custodia por parte del contratista , teniendo en cuenta que el contrato esta vencido en tiempo, pero existe un saldo en dinero, que esta pendiente por resolver.				Numeral 2.6 del Procedimiento GINF-PR-001 "Respaldo y Recuperación de Datos".		
GRUPO ADMINISTRATIVO							
Contro: Solicitud Fotocopias	El equipo auditor encontro que se está incumpliendo el procedimiento para solicitar fotocopias reglamentado en la Resol 500-003189 del 2004, dificultando la verificacion de la cantidad de copias utilizadas contra la lectura de los contadores de las fotocopiadoras.				Articulo 4, Parágrafos 1 y Parágrafo 3 de la Resolucion 500-003189 de 2004		
Control de Ingreso a las Instalaciones	Se constato que para el Control de Ingreso a las instalaciones (formato GINF-F-016) en Bogotá, se esta utilizando la version 001 y al consultar en la intranet ya está vigente la version 002 de este formato.	Numeral 4.2.3 Control de documentos NTCGP 1000:2009					

Superintendencia de Sociedades	SUPERINTENDENCIA DE SOCIEDADES	Codigo EC-F-003
	SISTEMA DE GESTIÓN INTEGRADO	Fecha: 29-03-2011
	PROCESO: EVALUACIÓN Y CONTROL	Versión 005
	FORMATO: INFORME DE AUDITORIA - SEGUIMIENTO	Pagina 1 de 5

1.INFORME Nº: 15

PROCESO/DEPENDENCIA
GESTION DE INFRAESTRUCTURA Y LOGISTICA

2. FECHA: DICIEMBRE 13 DE 2011

3. PROCESO / ACTIVIDAD AUDITADA:
Proceso de Infraestructura y Logística

12. CONCLUSION GENERAL

Pese a que en el proceso auditado se encuentran no conformidades, se determina que el grado de conformidad del sistema cumple en términos generales con los criterios evaluados en la auditoria. No obstante se deben estructurar acciones que eliminen las no conformidades detectadas, de tal manera que su implementación contribuya a la mejora continua del proceso

13 FIRMAS:

P/

ROCIO PEDROZO ULLOA
AUDITOR LIDER
OFICINA DE CONTROL INTERNO

JUAN PABLO MARIN ECHEVERRY
LIDER DEL PROCESO DE GESTIÓN DE INFRAESTRUCTURA Y LOGISTICA
FIRMA DEL LIDER DEL PROCESO AUDITADO