



**AUDITORÍA INTERNA DE GESTIÓN
PROCESO GESTIÓN TIC's**

**PROCEDIMIENTO
GTI-PRC05 "CONTROL DE ELEMENTOS DE TI"**

Agosto 4 de 2016

Apreciado Ingeniero

Mauricio Velásquez Mesa, Coordinador GIT de Apoyo Informático

El Grupo Interno de Trabajo (GIT) de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones, los Decretos 1537 de 2001, 019, 2482 y 2641 de 2012 y 943 del 21 de mayo de 2014; así como los lineamientos establecidos en la nueva Guía de Auditoría para Entidades Públicas del DAFP, y las Resoluciones CGN 328 de 2005 y 203 de 2015, tiene como función realizar la evaluación independiente al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar el cumplimiento y la efectividad de la gestión institucional y de los objetivos de la entidad, produciendo recomendaciones para asesorar al representante legal en busca del mejoramiento continuo.

En cumplimiento al Programa General de Auditorías aprobado el 24 de febrero de 2016, por el Comité de Coordinación del Sistema de Control Interno, este GIT adelantó la Evaluación al Procedimiento GTI-PRC05 “Control de Elementos de TI”, del proceso Gestión TIC’s, a fin de conocer el grado de cumplimiento de las actividades establecidas para su desarrollo y elevar las recomendaciones que sean necesarias en ejercicio del mejoramiento continuo, lo cual redundará en el cumplimiento de los Objetivos Estratégicos de la Entidad.

Los procedimientos de auditoría se realizaron sobre la base de pruebas selectivas; un procedimiento de esta naturaleza, no puede identificar todas las desviaciones de control, sino solamente aquellas que estén presentes dentro de la muestra evaluada.

Este informe fue presentado en mesa de trabajo del 8 de agosto de 2016 para la suscripción del respectivo plan de mejoramiento; por tanto es importante que se termine de diligenciar el formato “CYE04-FR-01 Plan de Mejoramiento”, el cual debe ser remitido por correo electrónico a más tardar el 12 de agosto de 2016.

Cordialmente,

MARITZA VELANDIA CARDOZO
Coordinador GIT de Control Interno

C. C.: Dr. Pedro Bohórquez Ramírez - Contador General de la Nación

Proyectó: José Leonardo Buitrago
Revisó: Maritza Velandía Cardozo

Tabla de Contenido

Objetivos y Alcance.....	4
Evaluación de Controles.....	5
Conclusión.....	9
Informe Detallado.....	10

OBJETIVO




Evaluar el cumplimiento de la normatividad legal vigente y la gestión del procedimiento GTI-PRC05 “Control de Elementos de TI” del proceso Gestión TIC’s en la Contaduría General de la Nación; así como, la efectividad de los controles, los indicadores y riesgos.

ALCANCE


El GIT de Control Interno, evaluará el cumplimiento de las normas vigentes y los lineamientos descritos en el procedimiento GTI-PRC05 “Control de Elementos de TI” del proceso Gestión TIC’s para la vigencia 2015 y lo corrido de 2016, lo anterior, mediante la verificación de los registros de cada una de las actividades allí descritas, así como de la administración de los riesgos y los indicadores asociados al procedimiento.

EVALUACION DE CONTROLES


De conformidad con los resultados obtenidos, en el siguiente cuadro se presenta la metodología de evaluación con sus respectivos comentarios para la adecuada comprensión y correcta implementación del plan de mejoramiento, de acuerdo con la clasificación:

	<p>INADECUADO</p> <p>En los procedimientos y pruebas de auditoría, se evidencia que existe un bajo grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero son muy vulnerables y deben ser objeto de intervención o ajustes que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.</p>
	<p>ADECUADO CON OPORTUNIDAD DE MEJORA</p> <p>En los procedimientos y pruebas de auditoría, se evidencia que existe un grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero presentan oportunidades de mejora que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.</p>
	<p>SATISFACTORIO</p> <p>En los procedimientos y pruebas de auditoría, se evidencia que existe un alto grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando.</p>


1. Matriz de riesgos del proceso

Actividades de Control	Evaluación del Control	Observaciones
Identificación, valoración, medición, controles y seguimiento.		<p>Los riesgos del proceso no se encuentran actualizados y aunque se han realizado algunas modificaciones, éstas se encuentran pendientes de aprobación por parte de la oficina de planeación para su posterior adopción.</p> <p>De igual manera se debe reconocer y dar el respectivo tratamiento, al potencial riesgo de "violación del derecho de autor", causado por aplicaciones que requieren el debido licenciamiento y que hoy día son posibles de instalar en algunos equipos de la entidad sin autorización.</p>


2. Indicadores

Actividades de Control	Evaluación del Control	Observaciones
Implementación, seguimiento y análisis.		<p>Se deben desarrollar actividades que propendan por el análisis, estudio y aplicabilidad de las mejores prácticas en la construcción de indicadores, teniendo en cuenta aspectos como la tipología, medidas de desempeño, así como referentes comparativos; lo anterior con el objetivo de contar con herramientas que faciliten la medición y control de las actividades críticas que exclusivamente pertenezcan al procedimiento.</p>


3. Normatividad relacionada

Actividades de Control	Evaluación del Control	Observaciones
Aplicabilidad de la normatividad y directrices vigentes.		


4. Especificaciones técnicas contratadas

Actividades de Control	Evaluación del Control	Observaciones
Recibidos a satisfacción; especificaciones del producto coincidentes con las estipuladas en el contrato.		


5. Licenciamiento, facturación e ingreso a almacén

Actividades de Control	Evaluación del Control	Observaciones
Legalidad, cubrimiento, vigencia y trazabilidad de los documentos.		Debilidades de control y seguimiento, toda vez que se evidenció la instalación de programas que aunque son de libre uso y distribución, no contaban con el análisis de riesgo y su respectiva autorización.

6. Equipos obsoletos y ciclo de vida de medios y licencias

Actividades de Control	Evaluación del Control	Observaciones
Seguimiento, evaluaciones técnicas y reintegros a almacén.		

7. Control de préstamos de medios, manuales y licencias

Actividades de Control	Evaluación del Control	Observaciones
Registros en la bitácora general, fichas de control y devoluciones.		

CONCLUSIÓN

El GIT de Control Interno concluye que el proceso de Gestión TIC's cumple con el procedimiento documentado GTI-PRC05 "Control de Elementos de TI", existiendo varios aspectos susceptibles de mejora que deben ser identificados y ajustados de acuerdo con las observaciones y recomendaciones establecidos en el presente informe.

Dada la importancia que tienen los riesgos y los indicadores como mecanismos de medición y control en la gestión del procedimiento, se les debe dar un tratamiento prioritario al interior del proceso, los cuales ameritan ser revaluados y ajustados para su fortalecimiento y así cumplir con los objetivos institucionales de la CGN.

Así mismo, es importante anotar la cordialidad y disponibilidad para atender esta auditoría durante su etapa de ejecución, evidenciándose el compromiso con el Programa General de Auditorías vigencia 2016, aprobado por la alta dirección.

1. Matriz de riesgos del proceso

Una vez detectadas las falencias técnicas en la aplicación SIGI, las cuales impiden el acceso amplio y suficiente a toda la información actualizada y relacionada con los riesgos, el GIT de Control Interno se abstiene de consultar dicha fuente como referente para realizar cualquier tipo de comparación o análisis.

OBSERVACIÓN

Vía correo electrónico se solicitó información sobre la gestión de riesgos asociados al procedimiento, en respuesta, el auditado informó que el único riesgo relacionado es: “deficiencia en la prestación de servicios”, el cual es evaluado como extremo y se controla por medio de la asignación apropiada de recurso técnico y humano; el registro de esta actividad se realiza en el aplicativo para la gestión de requerimientos CA Service Desk.

De igual manera, comunicó que los riesgos del proceso no se encuentran actualizados y que aunque se han realizado algunas modificaciones, éstas se encuentran pendientes de aprobación por parte de la oficina de planeación para su posterior adopción.

RECOMENDACIÓN

De acuerdo a la metodología establecida por el MECI, y para no afectar el nivel de riesgo de la entidad, se deben desarrollar estrategias que aseguren el estudio y aplicabilidad de las mejores prácticas en la identificación, valoración, medición y seguimiento de los riesgos asociados al procedimiento, teniendo en cuenta aspectos como el contexto estratégico, las clases de riesgos y la valoración de los controles; lo anterior con el objetivo de contar con herramientas que mitiguen el impacto de errores en las actividades críticas del procedimiento como son: asegurar la recepción de las especificaciones técnicas contratadas y la completitud del licenciamiento, contar con las autorizaciones técnicas para la baja de equipos y administrar el préstamo de elementos de TI.

De igual manera se debe reconocer y dar el respectivo tratamiento, al potencial riesgo de “violación del derecho de autor”, causado por aplicaciones que requieren el pago del debido licenciamiento y que hoy día son posibles de instalar en algunos equipos de la entidad sin autorización ni control por parte del GIT de Apoyo Informático.

2. Indicadores

Una vez detectadas las falencias técnicas en la aplicación SIGI, las cuales impiden el acceso amplio y suficiente a toda la información actualizada y relacionada con los indicadores, el GIT de Control Interno se abstiene de consultar dicha fuente como referente para realizar cualquier tipo de comparación o análisis.

Vía correo electrónico se solicitó información sobre el seguimiento de los indicadores asociados al procedimiento; ante lo cual el auditado informó que éste se basa en la “Satisfacción a Usuarios - Mesa de Servicios” para realizar las actividades de medición y análisis correspondientes; el registro de esta actividad se realiza en el aplicativo para la gestión de requerimientos CA Service Desk.

OBSERVACIÓN

Se evidenció que en el Cuadro de Mando Integral publicado en la página web de la entidad, existe un indicador llamado “Satisfacción de Usuario de Mesa de Servicios”, el cual es de tipo efectividad, de periodicidad mensual, evaluado en promedio al 97.7% para los últimos quince (15) meses, soportado en la ejecución de actividades que se efectúan al interior del procedimiento, pero también en acciones pertenecientes a otros procesos que nada tienen que ver con el mismo, tal como se muestra en la siguiente imagen.

Fecha de solucion	Fecha de cierre	Resumen	Descripcion
01/06/2016 10:02:26	07/06/2016 10:02:26	solicito ayuda de soporte para convertir archivos de pdf a w...	solicito ayuda de soporte para convertir archivos de pdf a word
01/06/2016 7:49:35	06/06/2016 17:00:00	solicito actualizar formularios del b.d.me.	solicito actualizar formularios del b.d.me.
01/06/2016 8:23:58	07/06/2016 8:23:58	Consulta sobre la capacitacion que realizar el día de maña...	Consulta sobre la capacitacion que realizar el día de mañana 2 de junio en bogotá
01/06/2016 8:25:50	07/06/2016 8:25:50	Usuaría solicita al analista asignado al municipio de la Vic...	Usuaría solicita al analista asignado al municipio de la Victoria Caldad
01/06/2016 8:31:58	07/06/2016 8:31:58	Tengo bloqueado el chip local	Tengo bloqueado el chip local
01/06/2016 8:45:00	07/06/2016 8:45:01	no puedo actualizacion de formularios	no puedo actualizacion de formularios
01/06/2016 8:46:10	07/06/2016 8:46:10	no puedo actualizacion de formulario	no puedo actualizacion de formulario
24/06/2016 8:26:28	30/06/2016 8:26:28	Para actualizar formularios del BDME que no he podido	Para actualizar formularios del BDME que no he podido
24/06/2016 8:25:43	30/06/2016 8:25:43	Solicita clave web	Solicita clave web
21/06/2016 10:52:08	27/06/2016 10:52:08	Jairo Garcia teléfono 8898477 solicita al analista por req...	Jairo Garcia teléfono 8898477 solicita al analista por requerimiento enviado
01/06/2016 9:13:29	07/06/2016 9:13:29	Restablecer contraseña del equipo de computo Doris Arrieta Teléfono 3132096900 solicita al analista	Solicito establecer contraseña del equipo de computo del usuario rpolanco
01/06/2016 10:56:29	07/06/2016 10:56:30	Doris Arrieta Teléfono 3132096900 solicita al analista	Doris Arrieta Teléfono 3132096900 solicita al analista
01/06/2016 10:02:50	07/06/2016 10:02:49	mi telefono no timbra, estoy ubicada en el 6 piso	mi telefono no timbra, estoy ubicada en el 6 piso
01/06/2016 10:32:04	07/06/2016 10:32:04	llama asistente cárdenas asistente de la contadora para con...	llama asistente cárdenas asistente de la contadora para consultar sobre resolucion de encargos fiduciarios, se le envio la resolucion 423 de 2011
01/06/2016 10:00:53	07/06/2016 10:00:53	Solicita ayuda para diligenciar el formulario del BDME que n...	Solicita ayuda para diligenciar el formulario del BDME que nop se deja
01/06/2016 10:02:22	07/06/2016 10:02:23	no puedo ingresar al computador	no puedo ingresar al computador
01/06/2016 16:44:24	07/06/2016 16:44:24	Asistencia Técnica Contable	Ángela Granados tel 3132065128 solicita que lo comuniquen con su analista Juan Jaramillo.
01/06/2016 10:20:10	07/06/2016 10:20:10	Para actualizar formualrios del BDME	Para actualizar formualrios del BDME
01/06/2016 10:27:56	07/06/2016 10:27:56	Capacitación	Yésica Castrillón tel. 324 82 31/30 (6) Pereira solicita que se le informen los lugares en dónde se van a realizar las capacitaciones de Barranquilla, Medellín y Bogotá en el mes de junio de 2016.

RECOMENDACIÓN

Se deben desarrollar actividades que propendan por el análisis, estudio y aplicabilidad de las mejores prácticas en la construcción de indicadores, teniendo en cuenta aspectos como la tipología, medidas de desempeño, así como referentes comparativos; lo anterior con el objetivo de contar con herramientas que faciliten la medición y control de las actividades críticas que exclusivamente pertenezcan al procedimiento.

3. Derechos de Autor – Normatividad Externa

La CGN tiene un software para generar el reporte de inventario través de la red de datos generado por el GIT de Apoyo Informático, con base en este informe y los licenciamientos vigentes y emitidos por las casas desarrolladoras o comercializadoras; se comprobó la pertinencia y legalidad de las aplicaciones implementadas en la entidad; lo anterior con el fin de evaluar la aplicabilidad de la normatividad legal vigente al procedimiento objeto de esta auditoría. A continuación se enuncian los aspectos más relevantes:

En relación con la Ley 23 de 1982 y la Ley 44 de 1993, se observó el cumplimiento en lo que tiene que ver con las disposiciones generales y más específicamente en lo estipulado sobre la ejecución, distribución y difusión de cualquier elemento sujeto del derecho de autor.

Se evidenció la observancia del Decreto 1360 de 1989 en cuanto a las disposiciones aplicables al soporte lógico “software”, no solamente en lo relacionado con la protección del derecho de autor sino en lo que dicta el derecho común.

La aplicabilidad de la Circular 01 de 2000 emitida por la U. A. E. Dirección Nacional de Derecho Autor se evidenció especialmente en lo que estipula el numeral 7° del artículo 2°, el cual manifiesta: “En materia de utilización de programas de computador (software), las sociedades deben contar con las respectivas licencias de uso para el número de equipos de computador permitidos por la licencia. Los usos o explotación de los programas deben ser no más que los autorizados expresamente en el contrato de licencia de uso y la licencia debe estar vigente al momento de la utilización de los programas;”

El resultado es satisfactorio

4. Cumplimiento de las especificaciones técnicas contratadas

Dentro del proceso de auditoría se evaluó el cumplimiento del procedimiento en relación a que cada elemento de TI adquirido cuente con el correspondiente recibido a satisfacción; también se comprobó que las especificaciones del producto coincidieran con las solicitadas en el proceso contractual, a continuación se enuncian los aspectos más relevantes:

El consolidado de adquisiciones de elementos de TI para la vigencia 2015 y lo corrido de 2016 presenta un total de diecisiete (17) productos, clasificados de la siguiente manera:

ESPECIALIDAD	NUMERO DE ELEMENTOS ADQUIRIDOS
Licenciamiento	6
Hardware	5
Mantenimiento de equipos	2
Seguridad de acceso	2
Renta de equipos	1
Almacenamiento	1
TOTAL	17

Se realizó una visita al GIT de Apoyo Informático donde se revisaron las carpetas en físico y se observó la completitud en la documentación de los recibidos a satisfacción y su alineación a las especificaciones técnicas incluidas en los procesos de adquisición tal como se muestra a continuación:

OBJETO: Adquisición de una impresora Matriz de Punto para la UAE Contaduría General de la Nación.
 CLÁUSULA SEGUNDA. OBLIGACIONES: Para La ejecución del presente contrato las obligaciones del CONTRATISTA frente a LA U.A.E CONTADURÍA GENERAL DE LA NACIÓN serán las siguientes: A) OBLIGACIONES ESPECÍFICAS:

Item	Requerimientos Mínimos Obligatorios
1.	ALCANCE: Impresora Matriz de Punto.
2.	ESPECIFICACION DE PRODUCTO Y/O SERVICIO
2.1	TIPO DE IMPRESIÓN: Punto
2.2	VELOCIDAD DE IMPRESIÓN: - Borrador de alta velocidad 347 cps (10 cpi) 357 cps (12 cpi) 390 cps (15 cpi) - Borrador de alta velocidad condensado: 383 cps (17 cpi) 298 cps (20 cpi) - Borrador: 260 cps (10 cpi) 312 cps (12 cpi) 223 cps (15 cpi) - Borrador condensado: 222 cps (17 cpi) 260 cps (20 cpi) - Borrador con énfasis: 130 cps (10 cpi)
2.3	- MEMORIA: 128KB PARALELA Y USB
2.4	- IMPRESORA CARTUCHOS: Cinta LX-350
2.5	CONECTIVIDAD: Cable USB
2.6	OTROS: • Duración de cinta de impresión: 4.0 millones de caracteres • Buffer de entrada: 128KB • Conectividad: Cable Paralelo • Tipo de cinta, estándar Negro • Método de impresión: Matriz de puntos de impacto en serie, 9 agujas
3.	GARANTIA: 12 Meses.

MINISTERIO DE HACIENDA
 CONTADURÍA GENERAL DE LA NACIÓN
 TODOS POR UN NUEVO PAÍS
 PAZ EQUIDAD EDUCACIÓN

CONSTANCIA DE RECIBO A SATISFACCIÓN

Nombre del contratista e identificación (Cédula o NIT)
 P&S TECNOLOGIA NIT 900.769.586-1

Orden No. 17 Fecha: 16/05/2016 Plazo: Un (1) mes
 Valor total del contrato \$ 918.000,00 Registro Presupuestal No. 36316 del 16/05/2016
 Póliza No. Aprobación Póliza
 No. Factura: 10 Fecha: 20/05/2016 Valor \$ 918.000,00

Objeto: Adquisición de una impresora Matriz de Punto para la UAE Contaduría General de la Nación.

Este certificado corresponde al 01 de 01

Porcentaje Ejecutado en el Periodo: 100,0%
 Porcentaje de Ejecución Acumulada: 100,0%

Documentos que soportan el servicio prestado: Factura de Venta No. 10, Certificación de Parafiscales y entrada a almacén.

Cumplimiento del Servicio: El contratista cumplió con el objeto del contrato.

Observaciones:

Dado en Bogotá, D.C., en las instalaciones de la U.A.E. Contaduría General de la Nación, a los 1 días del mes de Julio del año 2016.

Expedido por el supervisor,

Mauricio Velásquez Meza
 MAURICIO VELÁSQUEZ MEZA
 Coordinador GIT de Apoyo Informático

"Cuentas Claras, Estado Transparente"

Calle 95 No. 15 - 56 Código Postal: 110221 PBX (57 1) 492 6400
 www.contaduria.gov.co E-mail: contactenos@contaduria.gov.co
 Bogotá D.C. - Colombia

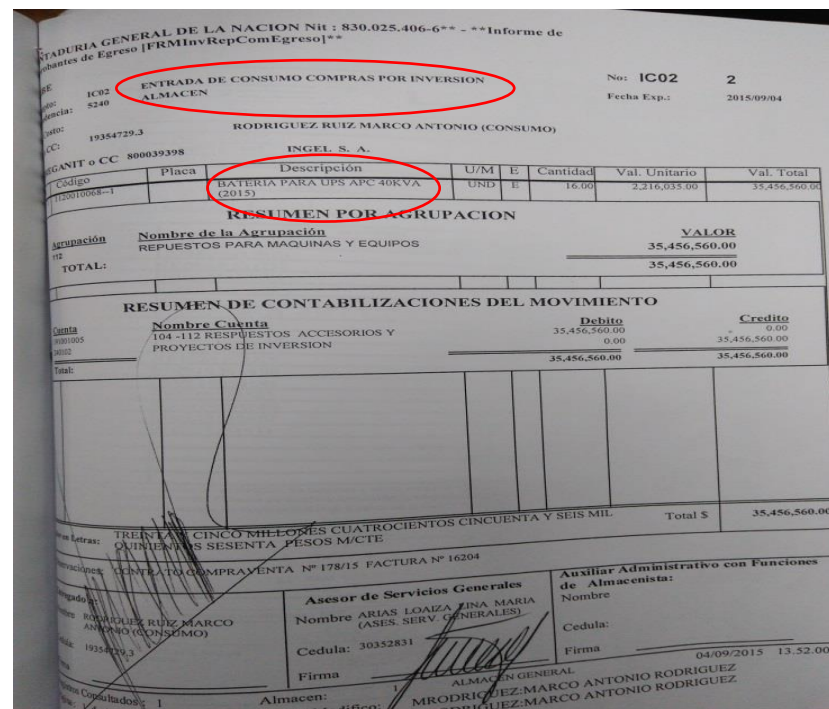
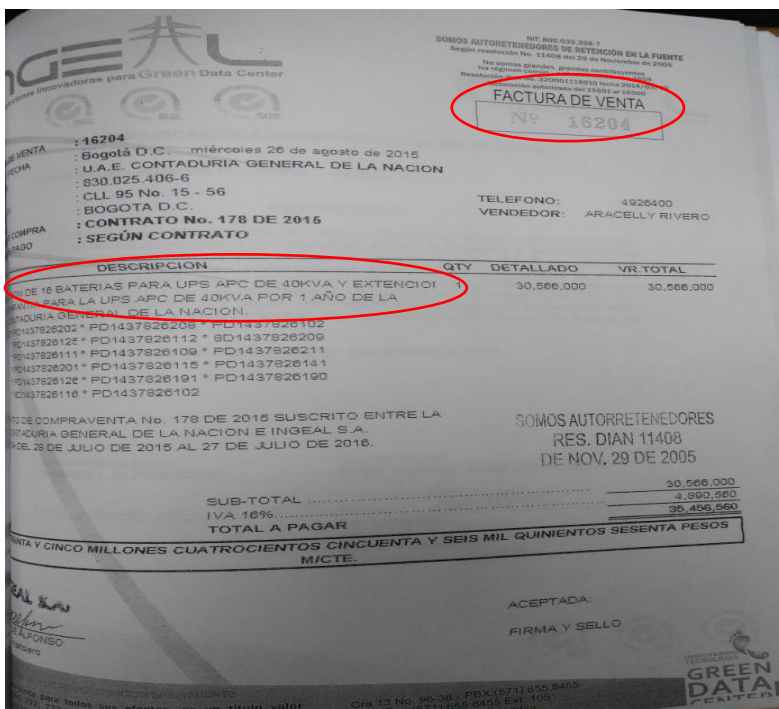


El resultado es satisfactorio.

5. Licenciamiento, facturación e ingreso a almacén

5.1 Elementos de TI

En el desarrollo de este punto se observó la existencia, completitud y trazabilidad de los documentos que demuestran la existencia del producto, la facturación por parte del proveedor y el correspondiente ingreso a almacén de cada elemento de TI adquirido durante las vigencias auditadas como se puede evidenciar en las siguientes imágenes:





5.2 Software Base

Dada la importancia, se indagó por el licenciamiento del software que soporta la plataforma misional y las aplicaciones más representativas de la entidad, como son: el sistema CHIP (Consolidador de Hacienda e Información Pública), el BDME (Boletín de Deudores Morosos del Estado), el Geoportal (Sistema de Información Geográfico), las interfaces WEB (Página WEB e Intranet), entre otros, y se observó el cubrimiento de éstas incluso hasta el 30 de junio del año 2017.

5.3 Software de Gestión

Con el ánimo de asegurar que los equipos de la entidad se encuentren libres de aplicaciones que no estén relacionadas con el quehacer institucional y en cumplimiento de las disposiciones que dicta la “Política de Seguridad de la Información”, se revisó el inventario de software generado por el GIT de Apoyo Informático, en el cual se observaron debilidades de control y seguimiento, toda vez que se evidenció la instalación de programas que aunque son de libre uso y distribución, no contaban con el análisis de riesgo y su respectiva autorización; a continuación se mencionan los aspectos más relevantes:

OBSERVACIÓN

- De doscientos cincuenta y dos (252) equipos asignados a los servidores públicos, treinta y uno (31) contenían aplicaciones que no estaban claramente relacionadas con el quehacer institucional; de igual manera, en estos últimos se evidenciaron setenta y un (71) instalaciones de aplicaciones no autorizadas.
- Se observó, por tanto, el incumplimiento de los literales “d”, “f” y “k” del numeral 6.2 de la Política de Seguridad de la Información, lo cual aumenta el potencial riesgo de afectación de la infraestructura tecnológica por diferentes amenazas como virus, software malicioso, spyware, etc.
- Los controles y seguimientos aplicados para evitar la instalación de aplicaciones sin autorización en los equipos de la entidad, fueron insuficientes e inefectivos, toda vez, que aunque se cuenta con un inventario detallado de todas las instalaciones por equipo, no se observaron acciones de mitigación.

RECOMENDACIÓN

Se deben ejecutar acciones correctivas inmediatas que aseguren la desinstalación de las aplicaciones que no estén autorizadas por el GIT de Apoyo Informático en los equipos de la entidad; de igual manera, se deben aplicar configuraciones a nivel de red y de dominio que impidan la descarga e instalación de cualquier tipo de software no autorizado; así como, fomentar la cultura de autoprotección informática.

6. Seguimiento a equipos obsoletos y ciclo de vida de medios y licencias

En relación con el ciclo de vida de los medios y licencias se observó que los elementos de TI dados de baja durante las vigencias auditadas son los siguientes:

ESPECIALIDAD	NUMERO DE ELEMENTOS DADOS DE BAJA
Equipos activos de red	26
Servidores IBM 550	5
Unidades de almacenamiento	2
Manejadoras de aire acondicionado	2
Condensadoras de aire acondicionado	2
TOTAL	37

Durante el proceso auditor se pudieron observar las evaluaciones técnicas de obsolescencia y reintegro al almacén, así como el respectivo seguimiento en el formato creado para tal fin.

El resultado es satisfactorio

7. Control de préstamos de medios, manuales y licencias

Para asegurar el control de préstamos de medios, manuales y licencias realizados por el proceso Gestión TIC's, se verificaron los registros en la bitácora general y en la ficha de control, observando coherencia entre éstos documentos. De igual manera, se evidenció que durante las vigencias evaluadas se realizaron veinticinco (25) préstamos, veintiuno (21) ya han sido retornados y cuatro (4) aún están en poder de los solicitantes. En la mayoría de los casos se requieren elementos de hardware como portátiles, cámaras y discos duros; a nivel de software son los sistemas operativos los más demandados.

El resultado es satisfactorio