

MEMORANDO



OCI

20171350249593

Al responder cite este número

FECHA: Bogotá D.C., octubre 19 de 2017

PARA: **Yaneth Rocío Mantilla Barón**
Directora General

DE: Jefe Oficina de Control Interno

REFERENCIA: Informe Auditoría SIG - Tecnologías de Información y Comunicación

Respetada Doctora Yaneth Rocío:

En cumplimiento del Decreto 648 de 2017 y el Decreto Distrital 215 de 2017 con relación al destinatario principal de los informes de auditoría, seguimientos y evaluaciones, estamos remitiendo el informe de la auditoría interna al Sistema Integrado de Gestión – SIG, correspondiente al proceso de Tecnologías de Información y Comunicación, liderado por la Subdirección General de Gestión Corporativa.

El trabajo fue realizado en desarrollo del Plan de Acción de la Oficina de Control Interno para la vigencia 2017 y como parte del proceso de mejoramiento continuo, busca que se implementen las acciones correctivas y preventivas a las recomendaciones, No conformidades y observaciones presentadas, de las cuales destacamos:

- En el Subsistema de Gestión de Seguridad de la Información no están documentadas las oportunidades, así como el plan de tratamiento de las mismas, de acuerdo a lo establecido normativamente.
- No se da cumplimiento a lo establecido en el procedimiento Gestión de tecnologías de la información y comunicación, respecto al registro de la información en el formato de control de la capacidad de los recursos de TI.
- No se cuenta con controles para asegurar y salvaguardar la información crítica de los procesos., de acuerdo con los mecanismos definidos por proceso de Tecnologías de Información y Comunicación.
- No se cumplen los lineamientos para la gestión de activos de información en la entidad, fijados en el procedimiento de “Gestión de tecnologías de información y comunicación”.

A continuación presentamos el detalle de la evaluación realizada:

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**

MEMORANDO



OCI

20171350249593

Al responder cite este número

INFORME DE AUDITORÍA

Proceso	Fecha de corte	Tipo de auditoría
Gestión de Tecnologías de Información y Comunicación	2 de octubre de 2017	SIG

I. OBJETIVO:

Verificar el grado de cumplimiento y/o conformidad del proceso auditado, según los requisitos de Calidad, Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información, definidos en la NTC GP 1000:2009, la NTC ISO 9001:2008, la NTC ISO 14001:2004, la NTC OHSAS 18001:2007 y la NTC ISO IEC 27001:2013 respectivamente, asegurando el cumplimiento de los requisitos del cliente, legales aplicables y propios de la Entidad, como base de la mejora continua del mismo.

II. ALCANCE:

Aplica al proceso de Gestión de Tecnologías de Información y Comunicación, con base en los requisitos establecidos en la NTC GP 1000:2009, la NTC ISO 9001:2008, la NTC ISO 14001:2004, la NTC OHSAS 18001:2007 y la NTC ISO IEC 27001:2013 y aplicables en los manuales, guías, procedimientos, registros, formatos y demás documentos del proceso que sirvan de criterio evaluable.

Los aspectos a verificar comprenderán las actividades desarrolladas por el proceso durante el periodo del 1° de agosto de 2016 al 31 de Julio de 2017, desde la definición del direccionamiento estratégico de tecnologías de la información y la comunicación, hasta la evaluación del proceso y materialización de las acciones de mejora.

III. CRITERIOS DE LA AUDITORÍA: Requisitos de norma definidos en:

- NTC GP 1000:2009,
- NTC ISO 9001:2008,
- NTC ISO 14001:2004,
- NTC OHSAS 18001:2007,
- NTC ISO IEC 27001:2013.

Documentación perteneciente al proceso auditado:

- CP-TI-01 Caracterización de Proceso Gestión de Tecnologías de la información.
- Manuales, procedimientos, guías y demás documentación del proceso.

2

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



BOGOTÁ
MEJOR
PARA TODOS

MEMORANDO



OCI

20171350249593

Al responder cite este número

- Matriz de Riesgo Institucional
- Normograma del Proceso
- Planes de mejoramiento
- Matriz de activos de información
- Cuadro mando de indicadores

IV. EQUIPO AUDITOR Y FECHAS:

Auditor Líder Nombre: Héctor Pulido Moreno	Dependencia-Cargo: Profesional Especializado – Oficina de Control Interno
Equipo Auditor: Wilson Guillermo Herrera Reyes Sayda Ochica Vargas	Dependencia-Cargo: Profesional Especializado – Oficina de Control Interno Profesional Universitario – Dirección Técnica de Procesos Selectivos
Líder Responsable Proceso: Nombre, Cargo y Dependencias: Carlos Humberto Moreno Bermúdez – Subdirector General de Gestión Corporativa	Líder operativo: Nombre, cargo y dependencia. Salvador Mendoza Suarez – Director Técnico Administrativo y Financiero. Leydy Yohana Pineda Afanador - Subdirectora Técnica de Recursos Tecnológicos.
Informe Distribuido a: Dirección General, Subdirección General de Gestión Corporativa, Dirección Técnica Administrativa y Financiera y Subdirección Técnica de Recursos Tecnológicos.	

Reunión de Apertura			Ejecución de la Auditoría		Reunión de Cierre		
Día:	Mes:	Año:	Desde:	Hasta:	Día:	Mes:	Año:
12	09	2017	12/09/2017	02/10/2017	02	10	2017

V. DESARROLLO DE LA AUDITORÍA:

Para la evaluación del proceso se inició con el levantamiento de información y planeación de la auditoría, análisis de la información y documentación implementada para verificar el grado de cumplimiento de la documentación aplicable al proceso, en materia de caracterización, planes, programas, procedimientos, guías, instructivos, normograma, y demás documentación en el marco del SIG.

3

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**

MEMORANDO



OCI

20171350249593

Al responder cite este número

El trabajo en campo se ejecutó, mediante la aplicación del plan de auditoría y de las listas de verificación Integrada para las normas de Calidad, Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información teniendo como base los requisitos establecidos en la matriz “Requisitos SIG vs Procesos” y el Anexo C (informativo) “Correspondencia entre la NTC-OHSAS 18001:2007, la NTC-ISO 14001:2004 y la Norma Técnica de Calidad en la Gestión Pública, contenido en la edición oficial de la NTCGP 1000:2009, publicada por el Icontec y lo establecido en el documento base del Sistema de Gestión de Seguridad de la Información “Declaración de Aplicabilidad” adoptado en 2015, como instrumento para obtener información y evidencia sobre las actividades evaluadas.

La auditoría se realizó en las instalaciones del Instituto de Desarrollo Urbano IDU de la sede de la calle 22 N° 6 - 27, pisos 3 y 4, para lo cual se desarrollaron entrevistas, verificando la información suministrada, aplicando pruebas de auditoría para las siguientes actividades:

1. Levantamiento de información relacionada con:
 - a) Información de la caracterización del proceso, procedimientos, formatos y mapas de riesgos relacionada con el proceso auditado.
 - b) Matriz de activos de información del proceso.
 - c) Indicadores de gestión del cuadro de mando con fecha de corte 30 de junio de 2017, ubicado en el mapa de procesos del proceso de planeación estratégica.

2. Trabajo en campo:
 - a) Entrevistas: Se realizaron entrevistas con los servidores vinculados al proceso.
 - b) Se inspeccionaron las áreas físicas donde se desarrolla la parte administrativa del proceso, ubicadas en la sede de Principal, piso 3° y Piso 4°.
 - c) Se realizó inspección visual al centro de cómputo ubicado en la sede principal piso 4°.

De forma paralela, durante las entrevistas se verificó la aplicación de las directrices de los Subsistemas de Gestión de la Calidad (SGC), Subsistema de Gestión Ambiental (SGA), Subsistema de Gestión de Seguridad y Salud en el Trabajo (SST) y Subsistema de Gestión de Seguridad de la Información (SGSI), con base en los requisitos establecidos en las normas NTC ISO 9001:2008, NTC ISO 14001:2004, NTC OHSAS 18001:2007 y la NTC ISO IEC 27001:2013, adoptadas por el IDU con la Resolución número 002305 de 2017, las cuales hacen parte del alcance de ésta auditoría.

4

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**

MEMORANDO



OCI

20171350249593

Al responder cite este número

La evaluación se realizó aplicando el ciclo PHVA y las recomendaciones de auditoría establecidos en la Norma NTC ISO 19011:2012, así mismo, se dio cumplimiento a las actividades programadas y a las fechas establecidas dentro del plan de auditoría, de acuerdo con el objetivo y actividades previstas en el mismo.

El presente informe fue comentado el 2 de octubre de 2017, con la Subdirectora Técnica de Recursos Tecnológicos y servidores designados para atender la reunión de cierre, para lo cual se elaboró el acta correspondiente.

VI. CONCLUSIONES:

Los servidores pertenecientes al proceso, estuvieron atentos a los requerimientos del equipo auditor, mostrando disponibilidad en el suministro de la información solicitada.

Es necesario que desde el Subsistema de Seguridad de la Información se establezcan estrategias, para que los demás procesos den aplicación a los controles establecidos en el documento FO-TI-27 “Declaración de aplicabilidad (DDA) para seguridad de la información”.

Derivado de la evaluación al proceso, se debe considerar el registro de las solicitudes SAM con proveedores externos de servicios, en el sistema de información ARANDA.

Mediante la auditoría realizada al proceso de Gestión de Tecnologías de Información y Comunicación, se logró evaluar el cumplimiento de los requisitos aplicables definidos en la NTC GP 1000:2009, NTC ISO 9001:2008, NTC ISO 14001:2004, NTC OHSAS 18001:2007 y NTC ISO IEC 27001:2013, de acuerdo con las directrices de Calidad, Gestión Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información, verificando la aplicación de las directrices por parte de los servidores en el desarrollo de sus funciones, concluyendo que el proceso es conforme con los requisitos del Sistema Integrado de Gestión, encontrando no conformidades y oportunidades de mejora para el proceso evaluado.

VII. RECOMENDACIONES OBSERVACIONES Y/O NO CONFORMIDADES

Los hallazgos identificados relacionados con directrices o actividades propias de los Subsistemas del SIG determinados en el alcance, han sido asignados como no conformidades al Subsistema correspondiente, para la formulación de la acción correctiva y como observación para el proceso donde fue identificado.

5

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**

MEMORANDO



OCI

20171350249593

Al responder cite este número

N°	Ref.	RECOMENDACIÓN	DESCRIPCIÓN DE LA OBSERVACION Y/O NO CONFORMIDAD
ASPECTO			
1	NC1	<p>Revisar y actualizar la metodología institucional de riesgos, asegurando:</p> <p>a.) Identificar los dueños de los riesgos y obtener de éstos, la aprobación del plan de tratamiento de riesgos y la aceptación de los riesgos residuales.</p> <p>b.) Asegurar que la declaración de aplicabilidad para tratamiento de riesgos, sea socializada y divulgada, para fortalecer el conocimiento y apropiación de objetivos de control y controles transversales y específicos a cargo de los procesos de la entidad, frente al Sistema de Gestión de Seguridad de la Información.</p>	<p>Solicitada y verificada información sobre riesgos y oportunidades del proceso, se observan las siguientes situaciones, las cuales evidencian que no se encuentra implementado el requisito 6.1 "Acciones para tratar riesgos y oportunidades" de la norma NTC ISO IEC 27001:2013:</p> <ol style="list-style-type: none"> 1. La metodología de riesgos que aplica la entidad, conforme al Manual de Administración del Riesgo V6.0, no cumple lo establecido en el numeral 6.1.2 Valoración de riesgos de la seguridad de la información (NTC ISO IEC 27001:2013) en cuanto a c.2) "identificar a los dueños de los riesgos". 2. La metodología de riesgos mencionada, no cumple lo establecido en el numeral 6.1.3 Tratamiento de riesgos de la seguridad de la información (NTC ISO IEC 27001:2013) literal f) en cuanto a "obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información". 3. La Declaración de Aplicabilidad, que corresponde al requisito 6.1.3 (d) "Tratamiento de riesgos de la seguridad de la información", no fue socializada de acuerdo a lo informado por el proceso TICs, lo cual impacta de manera amplia la implementación efectiva del SGSI, al

6

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 - 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195





MEMORANDO



OCI

20171350249593

Al responder cite este número

			<p>no ser conocida, interiorizada y apropiada por la organización.</p> <p>Dado los requisitos, alcances y especificidades, el plan de tratamiento de riesgos del proceso TICS, no cumple todos los parámetros que exige la norma NTC ISO IEC 27001:2013.</p> <p>Lo anterior genera un incumplimiento del numeral 6.1 Acciones para tratar riesgos y oportunidades, de la norma NTC ISO IEC 27001:2013, por el cual se debe <i>“determinar riesgos y oportunidades que es necesario tratar con el fin de a) asegurar que se logren los resultados previstos, b) prevenir o reducir efectos indeseado”</i>.</p>
2	NC2	<p>Dar cumplimiento al procedimiento PR-TI-16 Gestión de capacidad y disponibilidad, a fin de cumplir el objetivo del procedimiento.</p>	<p>Verificada la actividad No. 9 - Gestión de capacidad y disponibilidad definida en la caracterización del proceso, se evidencia el incumplimiento al procedimiento PRTI16 Gestión de capacidad y disponibilidad, actividad 1.1.6.6 Calcular reservas de requerimientos, al no diligenciar el formato FO-TI-30 Control de capacidad de los recursos de TI, de acuerdo a lo establecido en el procedimiento, afectando el numeral 4.1 Requisitos Generales”, de la NTC GP 1000:2009 y NTC ISO 9001:2008, literal c) <i>“determinar los criterios y los métodos necesarios para asegurarse de que tanto la operación como el control de los procesos sean eficaces”</i>.</p>
3	NC3	<p>Dar cumplimiento a la Declaración de aplicabilidad (DDA) para seguridad de la información, adoptada por el</p>	<p>Al solicitar al proceso TICs los controles adoptados y/o los registros que acrediten la entrega y recibo de los módulos del sistema de información</p>

MEMORANDO



OCI

20171350249593

Al responder cite este número

		<p>IDU en el documento FO-TI-27, como instrumento operativo para el control A.14.2.9 "Prueba de aceptación de sistemas".</p>	<p>ZIPA, que están en producción, asociados a la gestión de desarrollo realizada para los procesos de Ejecución de Obras y de Conservación de la Infraestructura, se suministró un Acta de Reunión del 4 de abril de 2017, cuyo contenido no corresponde al control asociado, ni al formato FO-TI-27 "Declaración de aplicabilidad para seguridad de la información", adoptado para realizar la entrega por parte de la STRT y la aceptación por parte de las áreas que van a utilizar el aplicativo ZIPA.</p> <p>Ésta situación refleja el incumplimiento del requisito 4.2.4 Control de registros, que establece "...los registros son un tipo especial de documento y se establecen para proporcionar evidencia de la conformidad con los requisitos así como de la operación eficaz, eficiente y efectiva del sistema de gestión de la calidad deben controlarse..." de la norma NTC GP 1000:2009 y NTC-ISO 9001:2008.</p> <p>De igual manera, se afecta el cumplimiento del objetivo de control A.14.2.9 "Prueba de aceptación de sistemas" correspondiente al subsistema de gestión de seguridad de la información en su requisito 6.1.3 (d) de la norma NTC ISO IEC 27001:2013.</p>
<p style="text-align: center;">4</p>	<p style="text-align: center;">NC4</p>	<p>Dar cumplimiento y realizar seguimiento a la implementación de los puntos de control establecidos en el procedimiento "PR-TI-04 Gestión de Desarrollo de TI".</p>	<p>Se evidencia que no se cumple el procedimiento "PR-TI-04 Gestión de Desarrollo de TI" en lo que corresponde a los puntos de control de las actividades 1.1.6.18 realizar pruebas de aceptación; 1.1.6.28 Entregar solución</p>

MEMORANDO



OCI

20171350249593

Al responder cite este número

			<p>TI; 1.1.6.37 Formato lista de chequeo para la aceptación; 1.1.6.38 Formato Acta aceptación de producto, lo que afecta el cumplimiento del objetivo de control A 14.2.9 "Prueba de aceptación de sistemas" correspondiente al NTC-ISO-IEC 27001 en su requisito 7.5.3 Control de la información documentada, en relación con su "...c. <i>distribución, acceso, recuperación y uso; d) almacenamiento y preservación, f) retención y disposición</i>".</p>
5	NC5	<p>Asegurar la implementación de acuerdos de confidencialidad en los contratos a cargo de los procesos del Instituto, con el fin de garantizar la seguridad de la información, para las relaciones con los proveedores, según las políticas definidas por el SGSI.</p>	<p>En reuniones realizadas con los líderes de proceso se evidenció que no se tiene conocimiento de la aplicación del formato FO-TI04 Acuerdo de confidencialidad con terceros, ni en qué momento se debe diligenciar.</p> <p>Adicionalmente, resultado de auditoría interna realizada a procesos como Planeación Estratégica, Factibilidad de Proyectos, Gestión Ambiental, Calidad y SST, se encontró que no se está implementando este formato, para asegurar un acuerdo de confidencialidad con terceros y tampoco se está contemplando una cláusula de confidencialidad en los contratos a cargo de dichos procesos.</p> <p>Bajo esta situación se presenta incumplimiento al requisito 6.1.3 Tratamiento de riesgos de la seguridad de la información de la norma NTC ISO IEC 27001:2013, requisito 6.1.3 literal d) declaración de aplicabilidad, control A.6.1.5 Seguridad de la información en la gestión de proyectos y de las políticas de control para la Seguridad de la</p>

MEMORANDO



OCI

20171350249593

Al responder cite este número

			Información, definidas en el artículo decimo de la Resolución Interna 34217 de 2015, en relación con la <i>“política de seguridad de la información para las relaciones con proveedores”</i> .
6	NC6	Asegurar el recibo, administración, almacenamiento y custodia adecuada de los activos de información de cada uno de los procesos del Instituto, dando cumplimiento a lo definido en el procedimiento PR-TI-13 Gestión de activos de información.	De acuerdo con el procedimiento PR-TI-13 Gestión de Activos de Información, numeral 2, la SGGC es la responsable de la consolidación del inventarios de activos y por medio de sus dependencias brindará el apoyo necesario para asegurar que los activos de información de todos los procesos se encuentren identificados y controlados adecuadamente, situación que no se ha cumplido, ya que como resultado se observa que el inventario publicado en el portal Web es de 27/12/2016 y no se corresponde con el inventario publicado en la intranet, proceso gestión TICs, situación que se ratificó al verificar el listado de activos de información de los procesos objeto de la auditoría interna SIG, que no ha sido actualizado cada cuatro meses según lo indica el procedimiento, razón por la cual aparecen usuarios y custodios que ya no pertenecen al proceso, afectando el cumplimiento del requisito NTC ISO IEC 27001:2013, requisito 6.1.3 literal d) declaración de aplicabilidad, control A.8.1.1 Inventario de activos, relativo a <i>“Recibo, administración, almacenamiento y custodia adecuada de los activos de información del proceso”</i> .
7	NC7	Socializar el alcance de la metodología de backups con los líderes de procesos, que en el desarrollo de sus actividades tienen alta dependencia del	Resultado de la auditoría interna SIG, se evidenció que el personal es consciente de la información crítica que maneja y, de manera independiente ejecuta acciones para salvaguardar su

MEMORANDO



OCI

20171350249593

Al responder cite este número

		<p>componente tecnológico, garantizando la seguridad de la información, frente a potenciales fallas temporales o permanentes.</p>	<p>información, como por ejemplo, subir sus archivos al Drive, guardar la información en dispositivos de seguridad personales, mantener carpetas personales en sus equipos, pero no tiene conocimiento de la frecuencia, el mecanismo, ni el alcance de las copias de seguridad, según las directrices establecidas por el SGSI, lo cual afecta el cumplimiento del numeral A.12.3.1 Respaldo de la información de la NTC-ISO 27001:2013, relativo a <i>“la verificación de los controles y actividades que realiza el proceso para respaldar la información crítica y sensible de su gestión”</i>.</p>
<p style="text-align: center;">8</p>	<p style="text-align: center;">01</p>	<p>Revisar los indicadores fijados por las dependencias involucradas en el proceso, a fin de fijar unidad de criterio en la medición.</p>	<p>Revisados los indicadores del proceso TICS, reportados en el Tablero de Mando publicado por la OAP, con corte al 30 de junio de 2017, se identifica que su formulación atendió a un enfoque funcional por áreas, toda vez que por ejemplo, el indicador 50512 Lineamientos para el Plan de Modernización de infraestructura tecnológica del IDU, formulado por la SGGC, se ha desplegado con indicadores de seguimiento casi iguales a cargo de la DTAF 5157 Plan de Modernización Tecnológica definido, o el indicador del líder operativo 53613 Nivel de modernización física en el componente de TI, lo cual indica que sobre el mismo proyecto cada líder (SGGC, DTAF y STRT) tiene definido un indicador que apunta al mismo tema.</p> <p>Con lo anterior, se podría afectar el cumplimiento de la norma NTC GP 1000:2009 y NTC ISO 9001:2008,</p>

MEMORANDO



OCI

20171350249593

Al responder cite este número

			requisito 8.2.3 Seguimiento y medición de los procesos en cuanto a la <i>“aplicación de métodos apropiados para el seguimiento, y la medición de los procesos.”</i>
9	O2	Revisar el contenido del formato de reporte de Activos de información - Índice información clasificada y reservada, publicado en el portal Web de la Entidad, a fin de dar alcance de lo observado.	<p>Revisado el formato de reporte de <i>“Activos de información - Índice información clasificada y reservada”</i>, publicado en el portal Web de la Entidad, se observa información no coherente con lo solicitado:</p> <p>a. En la columna <i>“Fundamento Jurídico”</i>, se cita una referencia reglamentaria (interna), aun cuando de acuerdo con lo señalado en el artículo 40 del Decreto 103 de 2015, ésta debe ser una disposición legal.</p> <p>b. Igualmente se debe aclarar el texto citado en la columna <i>“Excepción”</i>, de acuerdo con el Decreto ya citado, ya que no es clara la identificación de la excepción que cobija la calificación de información reservada o clasificada.</p> <p>Lo anterior podría estar generando un presunto incumplimiento de orden legal a la Ley 1712 de 2014.</p>
10	O3	Revisar y si es necesario aclarar las responsabilidades de los diferentes actores en la gestión de activos de información en la Entidad.	Revisado el procedimiento PR-TI-13 gestión de activos de información, se establece la responsabilidad de la gestión de los activos de información en cabeza de la SGGC, se indica la periodicidad de revisión, pero no se establece claramente las responsabilidades de los diferentes actores en el cumplimiento del orden normativo fijado en la ley 1712 de 2014 ley de transparencia, NTC-ISO-IEC 27001, requisito 6.1.3 literal d)

12

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



MEMORANDO



OCI

20171350249593

Al responder cite este número

			declaración de aplicabilidad, control A.8.1.1 Inventario de activos, ocasionando un presunto incumplimiento a lo requerido.
--	--	--	---

Convenciones:

O: Observación (requiere Acción Preventiva).

NC (No conformidad): Requiere Acción correctiva/o corrección para los casos de auditorías del SIG.

VIII. BALANCE AUDITORÍA

BALANCE DE AUDITORÍA		
Proceso, proyecto, Procedimiento Evaluado	Total No conformidades	Total observaciones
Gestión de Tecnologías de Información y Comunicación	7	3

IX. FORTALEZAS:

- El proceso cuenta con un Plan Estratégico de Tecnologías de la Información y las Comunicaciones, que garantiza el direccionamiento a la STRT en el cumplimiento de sus objetivos y funciones.
- Para el seguimiento a la gestión del proceso, la STRT cuenta con una herramienta tecnológica que le permite realizar el registro de las actividades realizadas y mantener el control del seguimiento de acuerdo a lo planeado.
- Los servidores de la STRT reconocen y aplican las directrices de los sistemas de gestión de calidad, ambiental, seguridad y salud en el trabajo y seguridad de la información en el ejercicio de sus funciones.
- El equipo de servidores y contratistas en virtud de sus funciones y obligaciones contractuales estuvieron siempre atentos para atender los requerimientos y coadyuvar en el cumplimiento de los objetivos de la auditoría al proceso.

El resultado de la evaluación corresponde al análisis de una muestra, por tal motivo es responsabilidad del proceso, efectuar una revisión de carácter general sobre los temas y aspectos evaluados, con el fin de generar mejoras en la particularidad del proceso.

13

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**

MEMORANDO



OCI

20171350249593

Al responder cite este número

Es necesario a partir de los hallazgos evidenciados, que el líder del proceso formule un plan de mejoramiento a partir de un análisis de causas, generando las correcciones, las acciones correctivas, preventivas y/o de mejora para subsanar la raíz de las deficiencias encontradas, conforme a lo establecido en el procedimiento PR-MC-01 FORMULACIÓN, MONITOREO Y SEGUIMIENTO A PLANES DE MEJORAMIENTO INTERNO Y POR PROCESOS, ubicado en la intranet, en la siguiente ruta:

[http://intranet/manualProcesos/Mejoramiento Continuo/03 Procedimientos/PRMC01 FORMULACION MONITOREO SEGUIMIENTO A PLANES DE MEJORAMIENTO INTERNO Y O POR PROCESOS V 3.0.pdf](http://intranet/manualProcesos/Mejoramiento%20Continuo/03%20Procedimientos/PRMC01_FORMULACION_MONITOREO_SEGUIMIENTO_A_PLANES_DE_MEJORAMIENTO_INTERNO_Y_O_POR_PROCESOS_V_3.0.pdf)

Para diligenciar el formato de Plan de Mejoramiento, es necesario diligenciar previamente uno de los instrumentos de análisis de causas que se encuentran en la intranet tales como: lluvia de ideas, diagrama causa efecto y los cinco porqués, los cuales pueden ubicarse en la siguiente ruta:

[http://intranet/Mapa procesos/IntenasMain/evaluacionMejora/MejoraContinuo.asp](http://intranet/Mapa_procesos/IntenasMain/evaluacionMejora/MejoraContinuo.asp)

De acuerdo con lo establecido en el procedimiento PR-MC-01 Formulación, monitoreo y seguimiento a planes de mejoramiento interno y/o por procesos, se cuenta con ocho (8) días hábiles para la presentación del plan de mejoramiento resultado de la evaluación.

Cualquier aclaración al respecto con gusto será suministrada.

Cordialmente,

Luis Antonio Rodriguez Orozco

Jefe Oficina de Control Interno

Firma mecánica generada en 19-10-2017 03:21 PM

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 - 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Instituto de Desarrollo Urbano

MEMORANDO



OCI

20171350249593

Al responder cite este número

cc Salvador Mendoza Suarez - Dirección Técnica Administrativa y Financiera
cc Leydy Yohana Pineda Afanador - Subdirección Técnica de Recursos Tecnológicos
cc Carlos Humberto Moreno Bermudez - Subdirección General de Gestión Corporativa
cc Isauro Cabrera Vega - Oficina Asesora de Planeación

Elaboró: Oficina De Control Interno

15

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 106583 de diciembre 10 de 2014

Calle 22 No. 6 - 27 o Calle 20 No. 9 – 20
Código Postal 110311
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195



**BOGOTÁ
MEJOR
PARA TODOS**