Bogotá D.C. 22 de Mayo de 2016.

OCI-169- SNR2017

Ingeniero
Luis Emilio Romero Mogollón
Jefe (E) Oficina de Tecnologías de la Información
Ciudad

Asunto: Informe de Auditoría Interna de Gestión.

Respetado Ing. Romero Mogollón

La Oficina de Control Interno, con fundamento a las facultades otorgadas en la Ley 87 de 1993, realizó auditoría interna de gestión a la Oficina de Tecnologías de la Información a su cargo, en las que se identificaron siete (7) no conformidades y tres (3) Observaciones. A partir de la fecha, tendrá cinco (5) días hábiles para que presente por escrito la suscripción de las acciones del plan de mejoramiento respectivo.

Adjunto al presente el "Formato de Suscripción de Acciones a Plan de Mejoramiento Integrado" a fin de relacionar las acciones que conducirán a la eliminación de la causa raíz del Hallazgo, conforme a lo establecido en el procedimiento "AUDITORIAS INTERNAS INTEGRALES, DE CALIDAD Y DE GESTIÓN" que a la letra indica:

"1. Los hallazgos de la auditoría son incluidos en el formato "Suscripción de Acciones para Plan de Mejoramiento Integrado" (CIG-CIGPRO7FRO1) por proceso y enviado al líder del proceso auditado, para el planteamiento de las acciones que conduzcan a la eliminación de la causa raíz del hallazgo.
2. El líder de proceso coordinará junto con su equipo de trabajo el análisis de causas tendientes a subsanar los hallazgos de la auditoría, evitando toda demora injustificada. Se debe analizar las causas y documentar las acciones para eliminar el incumplimiento u observación presentada. Si se requiere asesoría para la elaboración del Plan de Mejoramiento será el líder del equipo auditor quien acompañará este ejercicio.
3. A partir de la fecha de recibido del informe de auditoría y el plan de mejoramiento, el responsable del proceso auditado en un término máximo de cinco (5) días hábiles enviará el plan en mención a la Oficina de Control Interno para su inclusión en el "Seguimiento a Planes de Mejoramiento Integrados" (CIG-CIGPRO7FRO1 V.2), quien le asignará el consecutivo correspondiente.
4. Si la Oficina de Control Interno, observa que las acciones planteadas no cumplen el propósito de eliminar la causa raíz devolverá el plan de mejoramiento y solicitará el replanteamiento de las mismas.

5. Al interior de cada proceso, el responsable realizará seguimiento mensual a las acciones del Plan de Mejoramiento para verificar su cumplimiento, contando con el facilitador del Sistema de Gestión de su área. La Oficina de Control Interno programará las visitas de seguimiento para que sean realizadas por los auditores calificados y verificar la realización de las acciones formuladas.
6. Cuando la Oficina de Control Interno lo indique, el grupo de auditores seleccionados realizará la verificación de la totalidad de las acciones planeadas con sus respectivas evidencias documentadas, la confirmación de la eficacia de las acciones y el cierre de las mismas. El Auditor reportará el resultado a la Oficina de Control Interno.
7. El Jefe de Control Interno presentará ante el Comité Directivo, cuando se requiera, las conclusiones de las auditorías para el análisis de las situaciones presentadas si fuera el caso. Así mismo, entregará copia a la Oficina Asesora de Planeación."

De igual manera y por tratarse de un proceso transversal en la entidad, se hace necesario que desde su jefatura se lidere e involucre a las dependencias que directamente se relacionan con las No Conformidades y Observaciones encontradas, con fin de suscribir conjuntamente las acciones de mejoramiento.

Cordialmente,

RITA CECILIA COTES COTES
Jefe Oficina de Control Interno de Gestión

Anexos: Folios

Proyectó: *Nayibe B.*

FORMATO INFORME AUDITORÍA DE GESTIÓN	
INFORMACIÓN GENERAL	
SNR - Dependencia	MACROPROCESO TECNOLOGÍAS DE LA INFORMACIÓN
Fecha de Auditoría:	12 al 16 de Diciembre de 2016 y Cierre de auditoría al 7 Feb/2017
Actividad:	Auditoría de Gestión
Responsable:	ING. LUIS ROMERO MOGOLLÓN
Objetivo de la auditoría:	Evaluar el Macroproceso Tecnologías de la Información en los procedimientos Administración del Hardware, Administración de Software, Supervisión y/o Interventoría de Contratos, Administración de Usuarios, Backup y protección de la Información. Así mismo, verificar el avance de Gobierno en Línea en el componente Seguridad y Privacidad de la Información; la implementación del SGSI y el mantenimiento de la NTCGP 1000:2009 y demás normatividad aplicable en el Nivel Central.
Alcance de la auditoría:	Del 1 de Enero al 30 de Noviembre de 2016
Requisitos:	Ley 594 de 2000, Ley 734 de 2002 - Código único Disciplinario, Artículo 34., MECI, NTCGP:1000, Documentación y registros del Macroproceso, Decreto 2573 de 2015, Matriz de Riesgos, Indicadores, Planes de mejoramiento y demás requisitos Legales aplicables al Macroproceso.
Auditor líder:	Luisa Nayibe Barreto López.
Equipo Auditor:	Luisa Nayibe Barreto López

A continuación, se presentan los resultados de la auditoría interna de Gestión realizada al Macroproceso de Tecnologías de la Información, con base en las verificaciones efectuadas a los criterios establecidos como referencia, de acuerdo con las muestras aleatorias simples seleccionadas y a los resultados de las entrevistas efectuadas a los funcionarios en desarrollo de las operaciones y actividades aplicables en la Oficina de Tecnologías de la Información.

MACROPROCESO TECNOLOGÍAS DE LA INFORMACIÓN

1- Verificación del cumplimiento al Plan Anual de Gestión

En desarrollo de la presente Auditoría se verificó el cumplimiento dado al Plan Anual de Gestión de Tecnologías de la Información, a través del cual se relacionaron las necesidades de actualización tecnológica de la SNR.

Para ello se tomó como muestra aleatoria las actividades establecidas para la Implementación del Sistema de Gestión de la Seguridad de la Información - SGSI, y específicamente las acciones 1 y 3 cuya fecha de entrega establecida es la que se relaciona a continuación

OBJETIVO ESTRATÉGICO	ACTIVIDAD	ACCIÓN	FECHA INICIO	FECHA FINAL
Mejorar la seguridad de la información administrada y producida por la entidad	1.- Implementar el Sistema de Gestión de la Seguridad de la Información (SGSI) en cumplimiento de los elementos transversales establecidos por el manual de implementación GEL	1. Divulgar la resolución que oficializa la implementación del SGSI.	abr-16	may-16
		3. Realizar campaña de sensibilización y divulgación del SGSI en todos los estamentos de la entidad.	abr-16	nov-16

Tabla No.1 – PAG OTI – 2016, Fuente: Pág. WEB

Como se puede observar en la tabla No.1, la ejecución de las acciones debían ser presentadas en los meses de Mayo y Noviembre de 2016, encontrándose que la OTI dio cumplimiento a las fechas establecidas, así:

- Mediante correo electrónico del 31 de Mayo de 2016 realizó la Divulgación de la Resolución No.4905/2016, por medio de la cual "*Se adopta el Sistema de Seguridad de la Información, para realizar el seguimiento de seguridad a nivel integral sobre procesos, procedimientos y sistemas de información*".

-En el mes de Octubre de 2016 y mediante correo electrónico, se observó que la OTI realizó la campaña de sensibilización y divulgación del ciclo PHVA del SGSI, con la finalidad de que este Sistema fuera conocido por los funcionarios y contratistas de toda la entidad.

Los anteriores elementos fueron establecidos en atención a los lineamientos generales contenidos en la Estrategia de Gobierno en Línea, a través de los cuales se busca la preservación de la confidencialidad, integridad y disponibilidad de la información, constituyéndose en la base sobre la que se cimienta la seguridad de la información en la SNR, como uno de los principales activos de la entidad.

- **Verificación al cumplimiento de la Resolución No.4905 de 2016, mediante la cual se realiza la adopción del Sistema de Gestión de Seguridad de la Información – S.G.S.I.**

El S.G.S.I. fue adoptado mediante Resolución No.4905 de 2016 expedida por la S.N.R., y para efectuar esta verificación se tomó como muestra algunos de los Artículos establecidos en ella, solicitando evidencias del cumplimiento dado a los mismos, encontrando lo siguiente:

1.1 Verificación al Art.12 de la Resolución 4905 de 2016:
Se solicitaron evidencias de las reuniones trimestrales instituidas en la Resolución No.4905 de 2016, Art.12 que establece: "***Reuniones***. *El comité Institucional de Desarrollo Administrativo deberá reunirse periódicamente cada tres (3) meses y en forma extraordinaria cuando se amerite. Previa convocatoria del Oficial de Seguridad y/o Profesional Asignado....* ***PARAGRAFO DOS***. *De cada una de las reuniones se levantará la respectiva acta, la cual deberá estar firmada por quien presida la reunión y el Oficial de Seguridad de la Información y/o Profesional Asignado, previa aprobación de los miembros participantes en la reunión. Las actas deben registrar los compromisos para hacer seguimiento y serán numeradas consecutivamente durante la vigencia anual.*"

Al respecto no se presentaron las evidencias del registro de estas reuniones.

Esta situación conlleva a generar el incumplimiento a lo señalado en el Art. 12 de la Resolución No. 4905.

Mediante correo electrónico del 9 de Febrero de 2017, la Oficina de Tecnologías de la Información –OTI, manifestó lo siguiente:
"Los temas de SGSI se desarrollaban por medio de las reuniones del Comité Directivo. Los temas tratados en Comité son adopción de políticas de tratamiento de datos, adopción del SGSI, aplicación de políticas en redes sociales, restricciones de navegación de sucursales, entre otros."

Una vez analizada la respuesta dada por la Oficina de Tecnologías y dado que no se presentaron evidencias de los registros llevados en las reuniones trimestrales establecidas mediante la Resolución, se mantiene la no conformidad por cuanto esta situación genera el incumplimiento a lo señalado en el Parágrafo 2 del Art.12, de la Resolución 4905 de 2016, así como a lo establecido en la norma NTC-ISO/IEC 27001, NUMERAL 4.3.3 – Control de Registros.

1.2 Similar situación se presenta con respecto a las evidencias (Actas y/o registros) de las reuniones bimestrales que fueron establecidas en el Manual del Sistema Gestión de Seguridad Información que establece en el numeral 8,3- Roles y Responsabilidades; 8.3.1-Comité de Seguridad: "*El Administrativo y Desarrollo de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO está conformado por los Directores, Coordinadores y Jefes de todas las dependencias de la Entidad incluyendo el Superintendente Delegado para Registro, Delegado para Notariado y Delegado de Tierras. Éste comité es el responsable de la centralización de todas las acciones relacionadas con la seguridad de la información, y para todos los efectos se reúne de manera periódica, mínimo cada dos (2) meses o cuando se presenten situaciones que así lo requieran."*

Ante esta situación la OTI informó mediante correo electrónico del 9 de Febrero de 2017, lo siguiente: *"Las reuniones establecidas por medio del manual como bimensuales, en la resolución se establecieron como trimestrales y se han desarrollado por medio del Comité Directivo. Por tal razón, la Oficina de Tecnologías actualizará el documento del Manual de Seguridad con la periodicidad de la resolución..."*

Por lo anterior, se mantiene la no conformidad con el fin de establecer las acciones de mejora en el mencionado Manual.

1.3 Revisión a lo establecido en la Resolución No.4905 de 2016, Art. 10 – *"La SUPERINTENDENCIA DE NOTARIADO Y REGISTRO contará con un Oficial de Seguridad y/o Profesional Asignado, quien lidera un grupo dedicado a la gestión de la seguridad de la información dentro de la Entidad."*

Al respecto no se presentaron evidencias de la asignación del Oficial de Seguridad y/o Profesional.

La OTI remitió la siguiente respuesta a éste numeral, mediante correo electrónico del 9 de Febrero de 2017: "*Teniendo en cuenta que se tiene un proceso de implementación del SGSI, de acuerdo a los plazos establecidos por Gobierno en Línea, La Oficina de Tecnologías en la reestructuración no logro contar con una coordinación para la seguridad de la información, por tanto, se cuenta con un profesional en calidad de apoyo para la implementación del sistema de gestión. Adicionalmente, las evidencias de las actividades realizadas durante el año 2016 se anexaron como soportes en el plan anual de gestión del año 2016.*"

Al respecto y dado que la Resolución No.4905 de 2016 expedida por el Superintendente quedó en firme a partir de su publicación (13 de Mayo de 2016), se debe dar cumplimiento a lo allí resuelto.

1.4 Revisión al documento que contiene la medición del SGSI, realizada en la vigencia 2015 por MINTIC, a la Entidad - mediante la firma Digiware:

Se observó que el objetivo para fue el de presentar las brechas y el estado real de seguridad de la información presente en la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO, contribuyendo al mejoramiento de la estrategia y del programa de seguridad de la información, enfocándose en el Anexo A de la norma ISO 27001:2013; en la evaluación del cumplimiento del ciclo PHVA del Modelo de Seguridad; en el nivel de la madurez de acuerdo al Modelo de Seguridad y en las mejores prácticas de la industria. Así mismo, puntualizar en la línea base2 de la seguridad de la entidad y definir la primera medición frente a los controles, mejores prácticas e indicadores contemplados en el diseño del instrumento de evaluación.

El alcance definido fue en el marco de 3 procesos misionales de la Entidad como son: el VUR.- Ventanilla única de registro, el SIR – Sistema de información Registral y el Sistema EXADATA - EXALOGIC.

Al respecto se observó que la SNR obtuvo una Calificación en la Evaluación de los Controles, de conformidad con el Anexo A de la ISO 27001:2013, de 60 Puntos; lo que ubica a los controles generales evaluados, como "Efectivos" de acuerdo al siguiente criterio: *"Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada."*

- Así mismo, se observó que fueron expuestas diferentes oportunidades de mejora en la implementación de los controles establecidos a través del SGSI y aunque algunas de las acciones fueron programadas en el Plan Anual de Gestión 2016, se **recomienda** que se retomen los resultados de la evaluación y se analicen las recomendaciones de MINTIC y DIGIWARE sobre la adopción de controles, mejores prácticas para la implementación del modelo de seguridad y privacidad de la información, con el fin de plantear las acciones de mejora a que haya lugar para subsanar las vulnerabilidades detectadas, dejando registro de lo actuado al respecto en cada una de ellas.

2. Verificación a los procesos y procedimientos establecidos por la OTI

2.1 Proceso: Gestión Incorporación de Tecnología

2.1.2 Procedimiento: Supervisión y/o Interventoría de Contratos

La OTI tiene contemplado dentro de su proceso de Gestión Incorporación de Tecnología el procedimiento Supervisión y/o Interventoría de Contratos, motivo por el cual durante la auditoría se verificó el uso de los formatos establecidos en dicho procedimiento, tomando como muestra el contrato No.431 de 2016.

Al respecto se encontró que aunque se está llevando de manera oportuna e integral el seguimiento a la ejecución técnica del contrato, ejecución presupuestal y se ha determinado la

viabilidad en los pagos, se encontró que no se están utilizando los formatos establecidos en el Sistema de Gestión Institucional, como son el "Acta de Inicio Contrato- GT-IT-PR-03-FR-01", "Acta de Seguimiento Contrato-GT-IT-PR-03-FR-02", entre otros. Evidenciados en el Acta de Inicio firmada el 11 de Mayo de 2016 e informe de supervisión contrato del 9 de Diciembre de 2016, de la cual no tiene la codificación del Sistema de Gestión Institucional, de acuerdo con lo señalado en el Listado Maestro de Documentos y en el Procedimiento "*SUPERVISIÓN E INTERVENTORÍA DE CONTRATOS*".

Por lo anterior, se hace necesario que la Oficina de Tecnologías de la Información revise su procedimiento con el fin de establecer la viabilidad de unificar los formatos de supervisión de contratos existentes en el Proceso - *Control y Seguimiento Contractual*, del Macroproceso Gestión Administrativa (contratos), o requerir el uso de los formatos existentes para la supervisión de todos los contratos que lleva la Oficina de Tecnologías de la Información.

2.2. Proceso: Gestión Recursos de Tecnología

2.2.1 Procedimiento: Administración del Hardware

Para realizar la verificación al procedimiento de Administración del Hardware se realizaron las siguientes actividades:

➢ Se requirió a la OTI el inventario general de equipos de Cómputo y Comunicaciones existentes en la SNR a Nivel Nacional.

La Coordinación de Tecnologías entregó copia del Inventario General de Equipos, con las siguientes características:

STATUS	TOTAL EQUIPOS
ACTIVOS	211
BUENOS	1
CONTINGENCIA	1
DAÑADO	2
DE BAJA	15
FUNCIONAL	26
INACTIVO	7
INACTIVO (NO USADO)	1
N/T	38
N/V	14
N/A	15
NO ACTIVO	1
NO HAY MOUSE	3
NO OPERATIVOS	11
OBSOLETO	5
OK	23
OPERARIO	18
OPERATIVO	1711
OPERATIVA	70
OPERATIVO EN BODEGA	1
OPTIMO	2
PRESENTA FALLAS	1
SERVIDOR	1
SN	4
SIN INFORMACIÓN (VACIAS)	328
EQUIPOS EN GARANTÍA	423
PORTATILES	52
EQUIPOS PARA DAR DE BAJA	325
TOTAL	3.310

Tabla No.2 – Inventario Equipos OTI, Fuente: OTI

Como se puede observar en la Tabla No.2 el total de equipos de cómputo reportado por la OTI es de 3.310 equipos a Nivel Nacional (Oficinas de Registro y Nivel Central), existiendo diferentes clasificaciones dadas al estado de cada uno y se encontraron clasificados con los siguientes estados: "*Para dar de Baja*", "*Presentan Fallas*", *"Dañados*", "*Obsoleto*", *"De Baja"*, entre otros.

Por lo anterior, y teniendo en cuenta que la OTI cuenta con un inventario que presenta diferentes clasificaciones al estado actual de los equipos, se **recomienda** unificar los criterios de clasificación y en los casos que sea necesario, solicitar a cada ORIP, que se realice el trámite de bajas donde sea necesario, con el fin de contar con el dato exacto de equipos existentes, tanto en las Oficinas de Registro como en Nivel Central.

- Con base en la anterior información y con el ánimo de corroborar el inventario de equipos existente en la SNR se solicitó al área Administrativa la relación General de inventarios, vigentes en cada una de las ORIPs y Nivel Central – (formato F5- de la Herramienta Holística), encontrando que fueron reportados un total de 3.735 equipos, situación que denota una diferencia de 425 equipos de cómputo a nivel nacional.

Con esta situación se genera el riesgo de que la Supernotariado presente partidas no reales en las cuentas de "*Propiedad Planta y Equipo" (Equipos de cómputo),* y en la cuenta "*Depreciación*" de los estados financieros. También podría generar la materialización del riesgo de pérdida de equipos de cómputo por la insuficiencia de controles para la administración de éstos y puede conllevar a que no se dé cumplimiento al Objetivo del procedimiento denominado "Administración del Hardware" que indica "*Planear, administrar y controlar los elementos técnicos a nivel de Hardware, para garantizar su disponibilidad en la Superintendencia de Notariado y Registro y Oficinas de Registro de Instrumentos Públicos, Entidades y Puntos de Servicio Externos."*

De otra parte, genera inobservancia a lo establecido en la NTC-ISO/IEC 27001 - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) requisitos del Anexo A.7.1 – Responsabilidad por los Activos, que establece como control A.7.1.1: "*Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.".*

Por lo anterior, se hace necesario que los responsables de estas actividades implementen las medidas de control necesarias para evitar que estas diferencias continúen presentándose.

- **Revisión al Mantenimiento Preventivo del Hardware**

Para efectuar la revisión al Mantenimiento Preventivo de los respectivos equipos de cómputo, dentro de los cuales se contemplan: computadores de escritorio, impresoras, escáner y armarios del centro de cómputo, se solicitó el cronograma del Plan de Mantenimiento Preventivo establecido para la SNR (Nivel Central y ORIPs) desarrollado en la vigencia 2016 y donde se contemple para los equipos de cómputo la realización de los dos procedimientos: limpieza de Hardware y verificación de configuración de Software.
Al respecto se encontró que la Oficina de Tecnologías de la Información no presentó evidencias del cronograma del Plan de Mantenimiento Preventivo establecido para la vigencia 2016. Sin embargo, presentó los indicadores que contienen las cifras de los equipos a los cuales se les realizó el mantenimiento preventivo en la vigencia 2016, encontrando que solo se logró dar mantenimiento al 1.96% (65 equipos de cómputo), del total de equipos existentes a Nivel

Nacional (3.310 equipos con base en el inventario de la OTI), es así como para los meses de Junio, Julio, Agosto, Septiembre, Octubre y Noviembre de 2016, no hay evidencias del mantenimiento preventivo efectuado a los equipos de cómputo de la SNR a nivel nacional.

Esta situación podría conllevar al riesgo de no dar cumplimiento a lo establecido en la ISO 27001, Seguridad de los equipos, Anexo A.9.2 –Mantenimiento de los Equipos, que establece como control A.9.2.1: *"Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad."* Así como a lo establecido en el Procedimiento de "Administración del Hardware", Actividad No.2- "*Mantenimiento Preventivo del Hardware*", que señala que se deben realizar inspecciones físicas y funcionales del Hardware, de acuerdo con la lista de chequeo establecida y que se deben realizar pruebas de funcionalidad de los diferentes equipos existentes en la SNR.

- **Revisión al Mantenimiento Correctivo del Hardware**

En este ítem se solicitaron evidencias del mantenimiento correctivo del hardware existente en la SNR, y que fue realizado a las diferentes Oficinas de Registro y Nivel Central, tomando como muestra los meses de Julio y Octubre de 2016, encontrando que efectivamente se realizaron mantenimientos y que se cuenta con las evidencias de la "Hoja del Servicio" donde se relaciona la identificación del equipo, el tipo de servicio prestado, entre otros.

2.2.2 Procedimiento: Administración de Usuarios

Se realizó la verificación a los controles establecidos para la creación de los usuarios en la SNR, respecto a los derechos de acceso y de procesamiento de la información.

De acuerdo con la verificación efectuada a través del Directorio Activo del Nivel Central se encontró que los usuarios "Gallón Arias Luz Edith" y "García de Valencia Gloría Inés", continúan en estado "Activo" estando ya retiradas de SNR, situación que genera incumplimiento a lo establecido en la Circular No.1041 de 2015, referente a la "Activación e inactivación de usuarios" y a lo establecido en el Procedimiento "ADMINISTRACIÓN DE USUARIOS", Actividad No.2, Item2 -DESACTIVAR USUARIOS.

Así mismo, una vez verificados los formatos de solicitud para la creación de usuarios de cuentas de acceso a los sistemas de información de las ORIPs, a través de los los tikets: No.286866, 287005, 287559, 289080, 294212, se encontró que se cuenta con las evidencias de las solicitudes efectuadas; sin embargo, se observa que aunque en los correos electrónicos solicitan el servicio que se requiere, en algunos de estos formatos no se están diligenciando completamente; esta situación genera el riesgo de no que no se cuente con la evidencia suficiente para realizar la activación de los servicios requeridos.

2.2.3 Procedimiento: Back-Up y Protección de la Información

Revisado el procedimiento de Back-up y Protección, cuyo objetivo redunda en proteger y garantizar los recursos del sistema de información (Aplicaciones y Bases de Datos) de la

Superintendencia de Notariado y Registro, por medio de la generación de copias de seguridad y conservación de la información en un sitio externo, se encontró lo siguiente:

Se cuenta con el inventario de Medios Magnéticos enviados a custodia externa, cuyo servicio lo ofrece la empresa – TANDEM, entregas controladas a través de la "*Relación de medios magnéticos enviados a custodia a la empresa TANDEM*" y "*Consecutivo entrega de medios*", que son diligenciados y firmados por quien entrega y quien recibe, formatos que no han sido estandarizados a través del Sistema Integrado de Gestión.

Observadas las características de la información contenida en los backups enviados a custodia se encontró que las copias de seguridad pertenecientes al aplicativo de FOLIO Magnético, no están siendo enviadas a custodia externa a través del contratista de la empresa TANDEM, contratada para ello; sin embargo, se informó que estas copias de backup están siendo almacenadas en los diferentes servidores existentes en las ORIPS (con aplicativo FOLIO), por medio de la Red de la SNR.

Al solicitar evidencias del Backup del mes de septiembre de 2016 que se hubiese realizado al aplicativo FOLIO para las ORIPS Yopal y Dosquebradas, se encontró que no se está utilizando el formato de control denominado "*Bitacora Backup*". Así mismo, se presentó como evidencias del último backup realizado a la ORIP Yopal, el del día 19 de Mayo de 2016 (evidencia presentada al momento de la auditoría en sitio), y que estaba alojado en el Servidor 168.10.3 perteneciente a la ORIP Buga; posteriormente y mediante correo del 27 de Diciembre de 2016, se entregaron evidencias de la actualización del backup al 15 de Diciembre de 2016 con la nota: "*Adjunto evidencia del Colba (Backup) ORIP El Yopal y demás ORIPs de Folio Magnetico, el cual se encontraba en el servidor de prueba de la dirección 192.168.200.11, de acuerdo a lo informado por el ing. Tomas Castillo*".

Al respecto se hace necesario implementar mecanismos de control que permitan identificar de manera inmediata, el servidor donde se almacena cada uno de los backups realizados a las ORIPS que cuentan con el aplicativo FOLIO para su misionalidad, de lo contrario, se puede llegar a generar el riesgo de pérdida de la información y/o la no disponibilidad de la misma.

2.2.4 Procedimiento: Administración de Software

Se revisaron los controles establecidos para garantizar la disponibilidad del Software Office en sus diferentes versiones y su licenciamiento, de acuerdo con la existencia en la Superintendencia de Notariado y Registro, con el fin de verificar la ubicación e instalación en los equipos de cómputo y Servidores.

Al respecto se encontró que la OTI no cuenta con un consolidado o inventario general de la totalidad del Office existente en sus diferentes versiones, y no se conoce la distribución y ubicación a Nivel Nacional. Igual situación ocurre con las licencias, dado que al momento de la auditoría solo se presentó la relación de licencias que existen en la plataforma de la línea del Centro de servicios de Licencias por Volumen de Microsoft, encontrando el resumen general de licencias, donde para el Office Professional y Standard - versiones 2003, 2007, 2010, y 2013 existe un total de 3.080 Licencias; sin embargo, y teniendo en cuenta que la SNR aún cuenta con licenciamiento Office de tipo OEM o físicas y que no se lleva el inventario de estas licencias (es decir aquellas que tienen un sticker con hologramas que está pegado a la CPU o en los portátiles), no se logró determinar la totalidad de licencias Office de la SNR, ni el equipo donde

actualmente se encuentran ubicadas. Igualmente, se hace necesario tener presente que en caso de hacer modificaciones al software instalado en los equipos de cómputo cuya licencia sea del tipo OEM, esta carecerá de valor legal, y si el equipo se da de baja, se deberá controlar el licenciamiento existente, así como los CD´S de instalación.

Esta situación conlleva al incumplimiento de lo establecido en las Políticas de Seguridad de la Información de la SNR, numeral 14.1 – Cumplimiento de las Obligaciones Legales "*La Oficina de Informática será la responsable por mantener el control de todas las licencias de software, hardware y aplicaciones utilizadas en la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO*". Así mismo, genera inobservancia a lo establecido en la NTC-ISO/IEC 27001, Anexo A.9: SEGURIDAD FÍSICA Y DEL ENTORNO: A.9.2.6 – Seguridad en la reutilización o eliminación de los equipos. -Control: *"Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación."*

- **Revisión a la Actualización de la Versión del Software - FOLIO Magnético**

En la verificación que se realizó a los controles establecidos para la gestión de cambios o configuración que se realiza sobre el FOLIO Magnético, se tomó como muestra el trigger desarrollado y ejecutado sobre la Tabla Linderos, cuya finalidad fue la de mejorar la administración y trazabilidad de los registros de linderos del aplicativo. Al respecto se encontró que no se cuenta con evidencias del control que se lleva en la trazabilidad y ejecución del trigger, en cuanto al estado de implementación del mismo en las diferentes ORIPS que tienen el aplicativo FOLIO. Así mismo, no se cuenta con una política a nivel del sistema de almacenamiento y versionamiento del código fuente que permita controlar los usuarios con acceso y registrar las acciones de modificación o eliminación, ni se cuenta con la justificación documentada de los cambios o modificaciones realizados al FOLIO.

Esta situación conlleva a generar inobservancia a lo señalado en la NTC-ISO/IEC 27001, Anexo A.10.3 - Planificación y aceptación del sistema – Control: *"Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación."* así como lo establecido en el procedimiento *"ADMINISTRACIÓN DE SOFTWARE"- ACTUALIZAR VERSIÓN DEL SOFTWARE.*

3. Revisión al Avance de la Estrategia de Gobierno en Línea:

En este ítem se solicitaron las evidencias que permitieran identificar el porcentaje de avance actual obtenido en la implementación del componente de "*Seguridad y Privacidad de la Información*". Así mismo, se solicitaron los soportes que determinaron las respuestas efectuadas a través del Formulario Único de Reportes de Avance de la Gestión – FURAG 2015, en cuanto al numeral 4.2 – Gestión de Tecnologías de la Información, encontrando lo siguiente:

Al verificar los porcentajes de avance aplicado a los sujetos obligados del Orden Nacional, de acuerdo con las actividades desarrolladas por la SNR y de conformidad con lo establecido en el Manual de Gobierno en Línea, en lo relacionado con el componente "*Seguridad y privacidad de la Información*", se encontró que no se cuenta con la disponibilidad de los registros que evidencien y permitan identificar los porcentajes de avances alcanzados, registrados para este

componente, que al mes de diciembre de 2016 debía estar implementado en un 60%, de conformidad con el Art.10 –Plazos, del Decreto No.2573 de 2014.

Con respecto a los Componentes: TIC para servicios, TIC para el Gobierno abierto y TIC para la Gestión, durante el desarrollo de la auditoría no se logró identificar los responsables designados para su implementación y/o seguimiento.

Esta situación podría llegar a generar inobservancia a la NTCP1000:2009, numeral 4,2.4 - Control de los Registros, de tal forma que no se logró su identificación y recuperación. Así mismo, esta situación podría conllevar a que no se permita proveer los registros necesarios para realizar el seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en línea, de que trata el Art.7, del Decreto 2573 de 2014 y ante la solicitud de algún ente de control.

Al respecto la Oficina de Tecnologías de la Información remitió mediante correo electrónico del 8 de Febrero de 2016 en donde manifestaron lo siguiente: *"De acuerdo a los hallazgos identificados en el documento se adjuntan las evidencias de la primera fase que permiten verificar lo necesario para corroborar que se han realizado las actividades descritas: Se anexa archivo "Supernotariado - presentación de informe ejecutivo línea base" en el cuál se verifica el porcentaje de cumplimiento de la Entidad de acuerdo al análisis realizado por la firma Digiware contratado por MINTIC bajo el proyecto "servicios técnicos y administrativos, para la ejecución de pruebas de vulnerabilidad, test de intrusión y la identificación de la brecha en la implementación del Modelo de Seguridad de la Información emitido por MINTIC para entidades del Estado".*

De conformidad con el documento presentado se encuentra que si bien es cierto en éste se determina el porcentaje de avance alcanzado en el componente "seguridad y privacidad de la información", de acuerdo con lo señalado en el "*Informe ejecutivo línea base administrativa y técnica – MSPI",* es importante tener presente que la observación se enfoca en que durante la auditoría no fueron presentados los registros o evidencias que permitan determinar el porcentaje del avance alcanzado, por lo que se hace necesario dar cumplimiento a lo establecido en la ISO 27001:2013, numeral 4.3.3-Control de Registros, que señala: "*Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros deben estar protegidos y controlados. El SGSI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros se deben documentar e implementar.*

4. Verificación a los indicadores del proceso Gestión de Recursos de Tecnología

Se revisó el indicador del proceso Gestión de Recursos de Tecnología denominado *"Porcentaje de Equipos (Pcs y Servidores) con protección de antivirus para la vigencia 2016",* y el de "*Porcentaje de mantenimientos preventivos realizados*" donde se observó que los indicadores establecidos para el proceso Gestión de Recursos de Tecnología, cuyas variables son:

Número de equipos con instalación de proteccion (antivirus) / Número total de equipos programados y Número de Mantenimientos realizados /Número de Mantenimientos programados

No permiten realizar un seguimiento y medición a los resultados planificados (eficacia), ni al impacto de la gestión (Efectividad), de tal forma que permita al líder del proceso tener alertas tempranas del cumplimiento dado y si es del caso, se puedan tomar las acciones preventivas o correctivas, según se considere pertinente.

MACROPROCESO: CONTROL INTERNO DE GESTIÓN

8. PROCESO: CONTROL INTERNO DE GESTIÓN

8.1 Procedimiento: Fomento de la cultura del autocontrol

El auditor de la Oficina de Control Interno realizó la sensibilización respecto al Sistema de Control Interno, presentó un video motivacional de autocontrol y aplicó la encuesta "*Cultura del Autocontrol*".

En la sensibilización se contó con la participación de 7 personas de las 3 Coordinaciones de la OTI, quienes al finalizar la sensibilización presentaron la encuesta de cultura de autocontrol, cuyas respuestas nos permitieron determinar lo siguiente:

FUNCIONARIOS PARTICIPANTES	PERCEPCIÓN
El 100% de los funcionarios	Consideran que en sus actividades diarias aportan a la Misión de la Entidad y que existe coherencia entre sus actividades y la visión institucional.
87.5%	Conocen los valores de la entidad.
62.5%	Desarrollan en sus labores diarias, acciones encaminadas a generar la cultura del Autocontrol y El autocontrol que ejerce en sus actividades diarias, permite mejoría en el desarrollo de su labor.
0%	Se evidencia el compromiso, sentido de pertenencia y la motivación de los servidores de la institución.
12.5%	Hay certeza en la calidad de la información y Considera que todos los funcionarios piensan y se involucran en asuntos de la organización en un diálogo maduro y respetuoso.
El 75%	Manifiestan que en su proceso de generan espacios de dialogo de manera respetuosa.
El 37.5%	Expresaron que evitan los diálogos soportados en el rumor o especulación.
Dos de los encuestados informaron que las actividades de autocontrol que ejecutan en sus labores diarias son: Guiando al funcionario que necesita ayuda y dando información a los usuarios. En cuanto a cómo mejoran sus labores a través de la aplicación de actividades de autocontrol, informaron: que siendo responsables de los asuntos que están a cargo de cada uno y tramitando de manera inmediata las solicitudes allegadas.	

RESULTADOS DE LA AUDITORÍA INTERNA DE GESTIÓN – Oportunidades de Mejora

ITEM	HALLAZGO	TIPO DE HALLAZGO	RESPONSABLE
1	1.Respecto a la revisión de la Resolución No.4905 de 2016, sobre la adopción del S.G.S.I., se encontró lo siguiente: 1.1- No se presentaron evidencias de las reuniones trimestrales que se deben realizar por parte del Comité de Seguridad de la Información, actas consecutivas, donde se registren los compromisos y firmada por quien presida la reunión y el Oficial de Seguridad de la Información y/o profesional asignado. Incumplimiento a lo establecido en la Resolución No.4905 de 2016, Art.12-Reuniones, Paragrafo2. 1.2- No existen evidencias de las reuniones bimestrales que se deben realizar por parte del Comité de Seguridad de la Información, incumpliendo lo establecido en el Manual del Sistema Gestión de Seguridad Información, numeral 8.3.1. 1.3- No se presentaron evidencias de la asignación efectuada al Oficial de Seguridad y/o Profesional, incumpliendo lo establecido en el Art.10 de la Resolución No.4905 de 2016.	NC	Oficina de Tecnología de la Información
2	En la revisión efectuada a la supervisión del contrato No.431 de 2016, seleccionado en la muestra, se encontró que no se están utilizando los formatos "*Acta de Inicio Contrato- GT-*IT-PR-03-FR-01", "*Acta de Seguimiento Contrato-GT-*IT-PR-03-FR-02", lo anterior evidenciado en el Acta de Inicio firmada el 11 de Mayo de 2016 que no cuenta con la codificación del Sistema de Gestión Institucional y en el informe de seguimiento al contrato, inobservando lo señalado en el Listado Maestro de Documentos y el Procedimiento "*SUPERVISIÓN E INTERVENTORÍA DE CONTRATOS*", respecto al uso de los formatos establecidos.	NC	Coordinación Asistencia Técnica
3	Verificado el control de inventarios de los equipos de cómputo se encontró que existen diferencias en la cantidad de equipos registrados en el consolidado de la OTI, versus el consolidado reportado por Administrativa (Formato F5-Holistica). Con esta situación se genera el riesgo de que la Supernotariado presente partidas no reales en las cuentas de "*Propiedad Planta y Equipo" (Equipos de cómputo),* y en la cuenta "*Depreciación*" de los estados financieros. También podría generar la materialización del riesgo de pérdida de equipos de cómputo por la insuficiencia de controles para la administración de éstos y puede conllevar a que no se dé cumplimiento al Objetivo del procedimiento denominado "Administración del Hardware" que indica "*Planear, administrar y controlar los elementos técnicos a nivel de Hardware, para garantizar su disponibilidad en la Superintendencia de Notariado y Registro y Oficinas de Registro de Instrumentos Públicos, Entidades y Puntos de Servicio Externos."*	NC	Coordinación Asistencia Técnica y Coordinación Administrativa

	Igualmente genera inobservancia a lo establecido en la NTC-ISO/IEC 27001 - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) requisitos del Anexo A.7.1 –Responsabilidad por los Activos, que establece como control A.7.1.1: "*Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.*". De otra parte, y al verificar el control en el licenciamiento de software en la muestra seleccionada (Office), se encontró que la OTI no cuenta con un consolidado o inventario general de la totalidad del Office existente en sus diferentes versiones, y no se conoce la distribución y ubicación a Nivel Nacional. Igual situación ocurre con las licencias, donde no se lleva el inventario de licencias tipo OEM, conllevando al incumplimiento de lo establecido en las Políticas de Seguridad de la Información de la SNR, numeral 14.1 – Cumplimiento de las Obligaciones Legales "*...La Oficina de Informática será la responsable por mantener el control de todas las licencias de software, hardware y aplicaciones utilizadas en la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.*" y al numeral del Anexo A.9.2.6 señalados en la NTC-ISO/IEC 27001, Anexo A.9: SEGURIDAD FÍSICA Y DEL ENTORNO: A.9.2.6 – Seguridad en la reutilización o eliminación de los equipos. -Control: *"Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación."*		
4	Se encontró que la Oficina de Tecnologías de la Información no presentó evidencias del Plan de Mantenimiento Preventivo establecido para la vigencia 2016. Así mismo se observó que solo se logró dar mantenimiento al 1.96% (65 equipos de cómputo), del total de equipos existentes a Nivel Nacional (3.310 equipos con base en el inventario de la OTI), es así como para los meses de Junio, Julio, Agosto, Septiembre, Octubre y Noviembre de 2016, no hay evidencias del mantenimiento preventivo efectuado a los equipos de cómputo de la SNR a nivel nacional. Esta situación podría conllevar al riesgo de no dar cumplimiento a lo establecido en la ISO 27001, Seguridad de los equipos, Anexo A.9.2 –Mantenimiento de los Equipos, que establece como control A.9.2.1: "*Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.*" Así mismo, podría generar inobservancia a lo establecido en el Procedimiento de "Administración del Hardware", Actividad No.2- "*Mantenimiento Preventivo del Hardware*", que señala que se deben realizar inspecciones físicas y funcionales del Hardware, de	OBS	Coordinación Asistencia Técnica

	acuerdo con la lista de chequeo establecida y que se deben realizar pruebas de funcionalidad de los diferentes equipos existentes en la SNR.		
5	En la revisión efectuada al consolidado de usuarios Activos e inactivos, se encontró que existen usuarios retirados de la entidad (Gallón Arias Luz Edith y Garcia de Valencia Gloria Ines) que aún permanecen en estado "Activo" en el "Directorio Activo" de la entidad. Esta situación genera incumplimiento a lo establecido en el Procedimiento "ADMINISTRACIÓN DE USUARIOS", Actividad No.2, Item2 -DESACTIVAR USUARIOS, Así como a lo establecido en la Circular No.1041 de 2015 - Activación e Inactivación de Usuarios.	NC	Coordinación Centro de Cómputo
6	Se observó que el formato de control utilizado para registrar las cintas de backup enviadas al contratista externo para proteger y garantizar la custodia de los sistemas de información (Aplicaciones y Bases de Datos) de la SNR, no ha sido incluido en el Sistema de Gestión Institucional, situación que puede llegar a generar inobservancia a lo establecido en la NTC-ISO/IEC 27001, numeral 4.3.3 - Control de Registros.	OBS	Coordinación Centro de Cómputo
7	En la revisión efectuada al backup que se realiza al aplicativo FOLIO se encontró que no se utiliza el formato de control denominado "Bitacora Backup". Así mismo, revisado el Backup FOLIO de la ORIP Yopal se presentó como evidencias del último backup realizado, el del día 19 de Mayo de 2016 (evidencia presentada al momento de la auditoría), y que éste fue alojado en el Servidor 168.10.3 - perteneciente a la ORIP Buga; este backup fue actualizado posteriormente al 15 de diciembre de 2016. Por lo anterior, se hace necesario establecer mecanismos de control que garanticen la no materialización del riesgo de pérdida de la información y la no disponibilidad de la misma.	NC	Coordinación Asistencia Técnica
8	No se cuenta con evidencias del control que se lleva en la trazabilidad y ejecución del trigger, en cuanto al estado de implementación del mismo en las diferentes ORIPS que tienen el aplicativo FOLIO. Así mismo, no se cuenta con una política a nivel del sistema de almacenamiento y versionamiento del código fuente que permita controlar a los usuarios con acceso y registrar las acciones de modificación o eliminación, ni se cuenta con la justificación documentada de los cambios o modificaciones realizados al FOLIO. Esta situación conlleva a generar inobservancia a lo señalado en la NTC-ISO/IEC 27001, Anexo A.10.3 - Planificación y aceptación del sistema, así como lo establecido en el procedimiento *"ADMINISTRACIÓN DE SOFTWARE"- ACTUALIZAR VERSIÓN DEL SOFTWARE.*	NC	Coordinación Asistencia Técnica
9	Durante la auditoría no fueron presentados los registros o evidencias que permitan determinar los avances alcanzados en el componente "*seguridad y privacidad de la información*" y con respecto a los Componentes: TIC para servicios, TIC para el Gobierno abierto y TIC para la Gestión, durante el desarrollo de la auditoría no se logró identificar los responsables designados para su implementación y/o seguimiento, situación que genera inobservancia a lo establecido en el numeral 4.3.3-Control de Registros de la NTC-ISO/IEC 27001.	NC	Oficina de Tecnología de la Información Y Oficina Asesora de Planeación

10	Se observó que los indicadores establecidos para el proceso "Gestión de Recursos de Tecnología: *"Número de equipos con instalación de protección (antivirus) / Número total de equipos programados."* y *"Número de Mantenimientos realizados /Número de Mantenimientos programados"* no permiten realizar un seguimiento y medición a los resultados planificados (eficacia), ni al impacto de la gestión (Efectividad). Esta situación genera el riesgo de no permitirle al líder del proceso, tener alertas tempranas del cumplimiento dado y si es del caso, que se establezcan las acciones preventivas o correctivas que se requieran.	OBS	Oficina de Tecnología de la Información

No Conformidad Real (NC): Incumplimiento de una norma o requisito.
Observación (OBS): Situación identificada, que puede dar lugar al incumplimiento de una norma o a la materialización de un riesgo.

RECOMENDACIONES Y/O SUGERENCIAS

1- **Recomendaciones** a la OTI para las observaciones del numeral 1:

1.1 Se recomienda dejar los soportes de cada una de las reuniones trimestrales programadas, de conformidad con lo señalado en la NTC-ISO/IEC 27001, NUMERAL 4.3.3 – Control de Registros, así como a lo establecido en el Paragrafo 2 del Art.12 de la Resolución 4905 de 2016.

1.2 Teniendo en cuenta que en el Manual del Sistema Gestión de Seguridad de la Información, numeral 8.3.1, se establecieron reuniones bimestrales para ser realizadas por parte del Comité de Seguridad de la Información y que en la Resolución 4905/2016, establece una periodicidad de reuniones trimestral, se recomienda unificar los criterios y dejar evidencias de las reuniones que se realicen.

1.3 Se recomienda dar cumplimiento al Art.10 de la Resolución No.4905 de 2016, realizando la asignación del Oficial de Seguridad y/o Profesional, quien liderará al grupo de seguridad de la información.

1.4 Se sugiere retomar los resultados de la evaluación presentados por MINTIC y DIGIWARE, analizando las recomendaciones sobre la adopción de controles, mejores prácticas para la implementación del modelo de seguridad y privacidad de la información, con el fin de plantear las acciones de mejora a que haya lugar para subsanar las vulnerabilidades detectadas, dejando registro de lo actuado al respecto en cada una de ellas.

2- Se **recomienda** a la OTI revisar su procedimiento con el fin de establecer la viabilidad de unificar los formatos de supervisión de contratos existentes en el Proceso - Control y Seguimiento Contractual, del Macroproceso Gestión Administrativa (contratos). Así mismo, que a través del facilitador de la OTI, se socialicen los procedimientos existentes, con los formatos existentes para la supervisión de todos los contratos que lleva la Oficina de Tecnologías de la Información.

3- Teniendo en cuenta que se presentaron diferencias en los inventarios de equipos de cómputo, se **recomienda** que la OTI, unifique criterios para la clasificación de los equipos relacionados en el inventario, como es: "*Para dar de Baja*", "*Presentan Fallas*", *"Dañados*", "*Obsoleto*", *"De Baja",* entre otros; y en los casos que sea necesario, solicitar a cada ORIP, que realice el trámite de baja donde sea necesario, con el fin de contar con el dato exacto de equipos existentes, tanto en las Oficinas de Registro como en Nivel Central.
Así mismo, se recomienda realizar la conciliación entre las dos áreas: Oficina de Sistemas y Administrativa, con el fin de establecer el inventario general tanto en la herramienta Holística como en el registro llevado por la OTI.

Con respecto al inventario del software y licencias existentes se **recomienda** solicitar a los enlaces (ingeniero de sistemas y/o responsables del centro de cómputo) de las ORIPS, enviar el inventario de software existente (versiones, ubicación, etc,), así como realizar el inventario de las licencias tipo OEM con que se cuenta en cada una de ellas, con el fin de lograr establecer su ubicación y lograr establecer el control en el licenciamiento del software con que cuenta la SNR.

4- Dado que el mantenimiento preventivo está contemplado como uno de los requisitos de la Norma ISO 27001, Anexo No.A9.2.1 -*"Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad."* Y teniendo en cuenta que la SNR mediante Resolución No.4905 de 2016 adopto el Sistema de Gestión de Seguridad de la Información se **recomienda** dar cumplimiento a lo allí especificado, dejando los registros de lo actuado al respecto.

5- Se **recomienda** solicitar la actualización de usuarios a Nivel Nacional para todos los aplicativos y establecer mecanismos de control con el Macroproceso de Talento Humano, con el fin de mantener actualizados, tanto el Directorio Activo de la entidad, como los demás aplicativos con que se cuenta.

6- Se **recomienda** estandarizar a través del Sistema de Gestión Institucional, los formatos utilizados en desarrollo de las actividades de control llevadas por el Macroproceso de la OTI.

7- Se **recomienda** como mecanismo de control para el backup que se realiza al aplicativo FOLIO, el uso del formato denominado "Bitacora Backup", y en caso de requerirse, realizar las modificaciones que sean necesarias para su implementación, de tal forma que permitan identificar de manera inmediata, el servidor donde se almacena cada uno de los backups realizados a las ORIPS que cuentan con el aplicativo FOLIO.

8- Se **recomienda** establecer una política a nivel del sistema de almacenamiento y versionamiento del código fuente, que permita controlar los usuarios que tienen acceso y registrar las acciones de modificación o eliminación implementadas, con la debida justificación documentada de los cambios o modificaciones realizados al aplicativo FOLIO.

9- Se **recomienda** dar cumplimiento a lo establecido en la ISO 27001:2013, numeral 4.3.3- Control de Registros, que señala: "*Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros deben estar protegidos y controlados. El SGSI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros se deben documentar e implementar.*

10- Se **recomienda** realizar un análisis y valoración a los indicadores establecidos para el Macroproceso, de tal forma que éstos permitan realizar un seguimiento y medición a los resultados planificados (eficacia), y al impacto de la gestión (Efectividad), permitiendo al líder del proceso obtener alertas tempranas del cumplimiento dado y si es del caso, tomar las acciones preventivas o correctivas, según se considere pertinente.

Se **recomienda** de manera general revisar las presentes observaciones con el fin de establecer si se hace necesario replicar e implementar mecanismos de control por parte de la OTI, a nivel de los diferentes aplicativos con que cuenta la entidad, no solo los aquí tomados como muestra durante el desarrollo de la auditoría y con base en las recomendaciones efectuadas por la Oficina de Control Interno.

Así mismo, se **recomienda** realizar la suscripción del Plan de Mejoramiento con los hallazgos identificados en el presente informe y efectuar el seguimiento a las acciones que sean planteadas en el plan de mejoramiento, de tal forma que se identifique la eficacia de las acciones implementadas.

Equipo Auditor:	Aprobado Por:
Luisa Nayibe Barreto López	Dra. Rita Cecilia Cotes Cotes Jefe Oficina de Control Interno de Gestión

Nota: Este Informe será remitido vía electrónica y publicado en la Página Web de la SNR para su consulta.