150.180.20.191

Bogotá D.C., 6 de septiembre de 2017

Escuela Superior de Administracion publica - ESAP
Radicado: I-2017-003640 2017-10-06T16:32:10
Envìa: 150 - OFICINA DE CONTROL INTER
Destinatario: 100 - DIRECCION NACIONAL
Asunto: POR INCONVENIENTES DEL APLICAT
Paginas:39 Anexos: 38

Doctora
CLAUDIA MARCELA FRANCO DOMINGUEZ
Directora Nacional (E)
Escuela Superior de la Administración Pública.
Ciudad

Asunto: Informe Final de Auditoría Interna de Evaluación y Seguimiento al proceso de Gestión Tecnológica en su primera fase.

Respetados Ingeniera:

La Oficina de Control Interno dando cumplimiento integral a las funciones encomendadas por la Ley 87 de 1993 y las normas que la desarrollan, remite para su conocimiento y análisis el "informe Final de Auditoria Interna de Evaluación y Seguimiento realizada al proceso de Gestión Tecnológica en su primera fase", cuyo objetivo fue hacerle una evaluación y seguimiento a los procesos que realiza este grupo.

Me permito aclarar que el informe definitivo fue entregado el día 16 de mayo de 2017 del presente año a la Jefe de Oficina de Sistemas e Informática para el diligenciamiento formato RE-E-GE-19 Plan de Mejoramiento Auditoria Control Interno, el cual fue aprobado el día 5 de septiembre de 2017 y forma parte integral del informe final.

Cordialmente,

MARIA MAYERLY PEDREROS PINZON
Jefe Oficina Control Interno

Anexo: Informe Final de Auditoria Interna de Evaluación y Seguimiento y plan de mejoramiento aprobado, 38 folios útiles.

Escuela Superior de Administración Pública	**INFORME DE AUDITORIA INTERNA DE EVALUACION Y SEGUIMIENTO**
	DOCUMENTOS DE REFERENCIA: DC-E-GE-02

N° INFORME: 2 Definitivo	
PROCESO/ ACTIVIDAD: PROCESO DE GESTIÓN TECNOLÓGICA	**RESPONSABLE DEL PROCESO:** JEFE OFICNA DE SISTEMAS E INFORMATICA
LUGAR Y FECHA DE REALIZACION AUDITORIA: Bogotá, Escuela Superior de Administración Publica ESAP - Sede Central – Abril 27 de 2017	**PERIODO A AUDITAR:** 1 de enero de 2016 y lo realizado a la fecha.
EQUIPO AUDITOR: ALEXANDRA TRIVIÑO MARTINEZ	

OBJETIVO(S):

- Evaluar la existencia de Políticas, normas y procedimientos informáticos TI.
- Validar las políticas, manuales, procedimientos para el acceso y administración a los cuartos de comunicación.
- Evaluar los controles de acceso físico a los cuartos de comunicación por medio de inspección en sitio.
- Evaluar las características físicas y de seguridad industrial de los cuartos de comunicación por medio de inspección en sitio.
- Validar los equipos de protección física y de seguridad industrial en cuartos de comunicación
- Establecer un conocimiento general sobre las herramientas implementadas por la Oficina de Sistemas e Informática para el monitoreo de la infraestructura tecnológica.
- Evaluar las políticas y procedimientos involucrados en el monitoreo de la infraestructura, teniendo en cuenta como se ejecuta actualmente.
- Evaluación a las actividades de monitoreo y control efectuadas por la Oficina de Sistemas e Informática a la infraestructura de TI.
- Evaluar la aplicación de pruebas de vulnerabilidad y ética Hacking.a la infraestructura tecnológica, sitio web y a los sistemas de información de la Escuela.
- Establecer si la Escuela ha realizado al menos dos veces al año, pruebas de vulnerabilidad a su infraestructura tecnológica.
- Evaluar la gestión y estado de implementación de Gobierno en Línea.
- Evaluar la existencia de un plan de seguridad de TI.
- Evaluar la Gestión de la seguridad de la información.
- Evaluar la disposición y actualización de las políticas de seguridad informática.
- Evaluar la administración del proyecto de implementación del sistema de Información SINU.
- Evaluar la metodología y el plan de trabajo para para el desarrollo y entrega de los productos informáticos que componen el Sistema de Información de Información SINU.
- Evaluar el desarrollo del contrato de actualización, servicio de mantenimiento y soporte del software SINU - última versión WEB con sus módulos para la ESAP.
- Evaluar los Sistemas de información que intervienen en los procesos estratégicos, misionales y de apoyo de la Entidad.

ALCANCE:

El desarrollo de la auditoria consideró la ejecución de objetivos anteriormente descritos, teniendo en cuenta la evaluación a la efectividad de los siguientes controles generales de TI:

- Políticas, Normas y Procedimientos de TI.
- Cuartos de Comunicación.
- Monitoreo de la Infraestructura TI.
- Pruebas de vulnerabilidad y ética Hacking.
- Gobierno en Línea.
- Sistema de Gestión de seguridad de la Información SGSI.
- Verificación Metodología implementación del Sistema SINU.
- Sistemas de información que intervienen en los procesos estratégicos, misionales y de apoyo de la Entidad.

DECLARACIÓN:

La auditoría se realiza con base en el análisis de diferentes muestras aleatorias seleccionadas por los auditores, y se fundamenta en el siguiente soporte documental: expedientes fuente, procesos y procedimientos del Sistema de Gestión, reportes de los sistemas de información, cruces y validaciones, página web, intranet y normas internas y externas.

En aplicación al Decreto 648 de 2017 Artículo 2.2.21.4.8, la Oficina de Control Interno aplica los siguientes **Instrumentos para la Actividad de la Auditoría Interna**:

1. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de éste.
2. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

COMPROMISO DEL AUDITADO:

Carta de representación en la que se establezca la veracidad, calidad y oportunidad de la entrega de la información presentada a las Oficinas de Control Interno.

MARCO NORMATIVO:

NORMAS GENERALES: Constitución Política. Ley 80 de 1993. Ley 1150 de 2007 y sus Decretos Reglamentarios. Ley 190 de 1995. Ley 489 de 1998. Ley 87 de 1993. Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Ley 1474 de 2011, Decreto 219 de 2004. Ley 21 de 22 enero1982 y Decretos Reglamentarios, Decreto 019 de 2012 por medio del cual se suprimen trámites, Ley 962 DE 2005, Ley 1753 de 2015, Decreto 019 de 2012, Ley 1437 DE 2011, Decreto 1078 de 2015, Decreto 415 de 2016, Decreto 2482 de 2012, Decreto 2618 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Ley 23 DE 1982, Decreto 2573 de 2014, así como todos los lineamientos que actualmente son generados y regulados por el Ministerio de las Tecnologías de la Información y las Comunicaciones para las Entidades del Estado.

NORMAS ESPECÍFICAS:

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nación.
- ISO/IEC 27001:2013.
- Cobit 5.

FORTALEZAS:

Se identificó:

- Data Center: Las instalaciones del Data Center se encuentran adecuadas con las siguientes medidas de seguridad:
  - Seguridad física: Acceso controlado mediante puertas con lectores biométricos que garantizan el acceso al personal no autorizado, eespacio físico adaptado para la operación de equipos, piso falso, sistema de aire acondicionado, UP y control de visitantes mediante el registro en una bitácora.
  - Seguridad industrial: Sistema de detención/extinción de incendio, extintores manuales y señalización.
  - Seguridad lógica: Se tiene acceso restringido mediante el sistema biométrico "*Bio Star*".

- Controles en la Red de Cómputo (incluye servidores): Diariamente se realizan actividades de monitoreo y revisión de la disponibilidad del servicio, mediante la herramienta "*Open Mánager*", a los siguientes elementos de la red:
  - Canal de datos: En cada una de las territoriales, en caso de presentarse una alarma, se reportan al proveedor – Ifxnetworks quien es el encardo del soporte y mantenimiento.
  - Controladores de Dominio (AD-DNS,DHCP)
  - Switche –core (recibe el tráfico de las red WAN, y hacia los servicios de Datacenter).
  - Servidor donde se encuentran las bases de datos de los aplicativos suite-academusoft, Olib, Humano Web, Active Document y Seven.

- Servidor donde se encuentra el aplicativo de Academusoft.

- Sistemas de Información: La ESAP con el fin de garantizar el funcionamiento de los procesos misionales y de apoyo que intervienen en el negocio, cuenta con los siguientes sistemas de información: La Suit Academusoft (Academico y Gestasoft), Humano Web, Active Document, PQRS, OLIB, Moodle, Sirecec, Isolucion, Seven.

HALLAZGOS

HALLAZGO No. 1 – Falta de una metodología en la actualización del Proceso de Gestión Tecnológica

CONTEXTO:

El modelo estándar MECI establece lineamientos de control para hacer eficiente la operación de una Entidad a través de los procesos y procedimientos. En lo que respecta a las tecnologías de la información, Gobierno en Línea así como los estándares y marcos de referencia internacionales y buenas prácticas como COSO ERM, COBIT 5, ITIL, ISO 27000, ISO27005, buscan que las Entidades consideren un esquema de gobierno de TI que establezca la implementación de políticas y procedimientos con el fin de garantizar la adecuada gestión y control de la infraestructura de Tecnología de Información y Comunicaciones "TICs".

La Oficina de Sistemas e Informática –OSI, conjuntamente con la Oficina de Planeación y la asesoría del Ministerio de las Tecnologías, se encuentran adelantando una nueva revisión de los procedimientos del proceso de Gestión Tecnológica con el propósito de mejorarlos y establecer cuales hay que crear, actualizar o eliminar, para seguidamente, elaborar y/o actualizar las políticas, manuales, instructivos y/o formatos que se ajusten a las necesidades actuales de la ESAP, plataforma física y tecnológica existente en la Escuela, actividades que se vienen desarrollando desde febrero de 2017.

DESCRIPCION DEL HALLAZGO:

En el ejercicio de actualización documental del proceso del Gestión Tecnológica de la ESAP, se observa la falta de una metodología que incluya un plan de trabajo y un cronograma, que permitan realizar el seguimiento a las actividades ejecutadas.

DESCRIPCIÓN DEL RIESGO:

✓ Inadecuada planeación en la actualización documental.

RECOMENDACIÓN(ES):

Implementar una metodología que incluya un plan de trabajo y un cronograma con las actividades a realizar, responsables y fechas de ejecución, con el fin de establecer el estado de actualización del Proceso de Gestión Tecnológica y la fecha de finalización.

HALLAZGO No. 2 – Documentos desactualizados en el Sistema de Gestión de la Calidad.

CONTEXTO:

La Oficina de sistemas e Informática – OSI, en el año 2016, efectuó una revisión a la documentación que soporta el proceso de Gestión Tecnológica de la ESAP (procedimientos, políticas, manuales, instructivos y/o formatos) con el propósito de cumplir con el compromiso establecido en el plan de acción (actualización documental del 40% para la vigencia 2016), a la fecha de la auditoria no encontró la trazabilidad de la gestión realizada y no se cumplió con la actualización documental en el Sistema de Gestión de Calidad, así como con lo respectivo del plan de acción.

Si bien es cierto la OSI solicitó a la Oficina Asesora de Planeación, el 30 de septiembre de 2016 en el formato RE-S-GC-06 la eliminación de 21 documentos (ver anexo 1), no se realizó dicha eliminación debido a que la OSI no entrego los documentos respectivos en el mismo momento para que se surtiera su sustitución tal como se observa en la justificación dada en el formato diligenciado:

JUSTIFICACIÓN / MODIFICACIONES
Eliminación del SGE, ya que se realizara actualización de los procedimientos y documentación en el proceso Gestión Tecnológica. Los nuevos procedimientos quedarán así: ESTRATEGIA Y GOBIERNO T.I, SISTEMAS DE INFORMACION, INFRAESTRUCTURA DE SERVICIOS TECNOLOGICOS(infraestructura, comunicaciones, mesa de ayuda y virtual), SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

DESCRIPCION DEL HALLAZGO:

En la revisión documental al Sistema de Gestión de Calidad que soporta el Proceso de Gestión Tecnológica, se observa que la documentación allí publicada no está actualizada en concordancia con lo establecido en el plan de acción de la vigencia 2016.

DESCRIPCIÓN DEL RIESGO

✓ Desactualización documental.

RECOMENDACIÓN(ES):

Actualizar los procedimientos y documentos como políticas, normas, manuales, instructivos y/o formatos que soportaran el Proceso de Gestión Tecnología en el sistema de Gestión de la Calidad y solicitar el retiro de la documentación no incluida en el proceso.

HALLAZGO No. 3 – Falta de políticas informáticas

CONTEXTO:

Los lineamientos de Gobierno en Línea así como los estándares, marcos de referencia internacionales y buenas prácticas como COSO ERM, COBIT 5, ITIL, ISO 27000, ISO27005, buscan que las Entidades consideren un esquema de gobierno de TI que establezca la implementación de políticas,

procedimientos con el fin de favorecer, la adecuada gestión y control de la infraestructura de Tecnología de Información y Comunicaciones "TICs".

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

En la evaluación de las políticas, normas, procedimientos, manuales, instructivos y/o formatos que soportan el Proceso de Gestión Tecnológica, se observó que la OSI no ha considerado las políticas y los documentos que desarrollan los siguientes aspectos, los cuales a juicio de esta Auditoria son necesarios para el fortalecimiento del sistema de control interno de las TICs:

- ✓ Gestión de Proyectos de TI
- ✓ Estándares y metodologías para el desarrollo de proyectos y actividades
- ✓ Administración de la infraestructura tecnológica (Hardware, Software y Comunicaciones)
- ✓ Administración de inventarios (hardware, software y licencias)
- ✓ Administración de log (pistas de auditoria) en (S.O., BD, red y aplicativos)
- ✓ Administración del plan de continuidad
- ✓ Licenciamiento de Software
- ✓ Monitoreo a la infraestructura
- ✓ Manejo de Internet y correo Electrónico
- ✓ Políticas y directrices de Gestión de seguridad de la Información SGSI

DESCRIPCIÓN DEL RIESGO

✓ Insuficiente definición de políticas y documentos de TICs.

RECOMENDACIÓN(ES):

Incorporar dentro del Sistema de Gestión de Calidad, las políticas y documentos mencionados y los demás que la OSI considere necesarios para dar respuesta a los lineamientos de Gobierno en Línea.

HALLAZGO No. 4 – Publicación de documentos no institucionales en SGC

CONTEXTO:

La ESAP tiene publicado en su Sistema de Gestión de Calidad, la documentación (procedimientos, planes, políticas, manuales, guías, formatos e instructivos) que soportan el proceso de Gestión Tecnológica, para garantizar la prestación de servicios de TI.

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

En la revisión documental al Sistema de Gestión de Calidad que soporta el Proceso de Gestión Tecnológica, se observaron los siguientes documentos externos que corresponden al "*Ministerio de Tecnologías de la Información y las Comunicaciones*" los cuales por no ser institucionales no deben estar incluidos en el sistema de Gestión de la Calidad. Ver imagen 1.

- ✓ MANUAL GOBIERNO EN LINEA 2010
- ✓ SEGURIDAD DE LA INFORMACION

✓ SEGURIDAD INFORMATICA

Imagen 1. Documentos de MINTIC

DESCRIPCIÓN DEL RIESGO

✓ Publicación no autorizada de documentación no institucional.

RECOMENDACIÓN(ES):

Retirar del sistema de Gestión de Calidad los documentos externos a la Entidad.

HALLAZGO No. 5 – Falta de políticas informáticas para la administración de Cuartos de Comunicación

CONTEXTO:

Los lineamientos de Gobierno en Línea así como los estándares, marcos de referencia internacionales y buenas prácticas como COBIT 5, ITIL, ISO 27000, ISO27005, establecen que toda organización debe definir los procedimientos y responsabilidades operacionales con el objetivo de garantizar la seguridad física y ambiental para proteger la información (accesos no autorizados, daños e interferencias) mientras es procesada, almacenada o transmitida.

DESCRIPCION DEL HALLAZGO:

La Escuela no cuenta con normas, políticas y procedimientos definidos y documentados para la administración y seguridad física e industrial de los cuartos de comunicación y de los elementos tecnológicos allí residentes.

DESCRIPCIÓN DEL RIESGO

✓ Imposibilidad de medir la gestión de la administración, control y seguridad física e industrial de los cuartos de comunicación por falta de procedimientos debidamente documentados.

RECOMENDACIÓN(ES):

Implementar normas, políticas y procedimientos orientados a garantizar la administración, control y seguridad física e industrial de los cuartos de comunicación y de los elementos tecnológicos allí residentes.

HALLAZGO No. 6 – Inadecuada seguridad física e industrial en los Cuartos de Comunicación

CONTEXTO:

El cuarto de comunicación (Cuarto de Telecomunicaciones y/o Centro de Cableado), es el espacio utilizado exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño y operación de los cuartos de comunicación deben aplicar las normas internacionales ANSI/TIA/EIA-569/ISO/NFPA de cableado estructurado y adecuación de cuartos de equipos.

La sede principal de la ESAP en la ciudad de Bogotá D.C. cuenta con: seis (6) cuartos de comunicación en la sede administrativa del CAN, uno (1) en la sede de Teusaquillo y uno (1) en la sede Rosales, en los cuales se encuentran alojados los equipos de conectividad y centro de datos de la red LAN.

DESCRIPCION DEL HALLAZGO:

- ✓ Se observó al interior de los cuartos de comunicaciones, la presencia de cajas de cartón, carpeta de papel, bolsas plásticas, muebles en madera, sacos, tapetes, etc, elementos que no favorecen las condiciones de seguridad industrial, particularmente frente al riesgo de incendio, el cual en caso de materializarse afectaría en forma severa; la comunicación con el Data Center, donde se encuentran los sistemas de información y dificultades para disponer en forma oportuna de la información afectando de manera directa las funciones y los procesos claves de su operación.

- ✓ Al interior de los cuartos de comunicaciones se observa: almacenamiento de archivo, equipos, repuestos en desuso, manuales, cables, cajas con carpetas, rollos de cableado estructurado, etc, elementos que no favorece la seguridad industrial.

- ✓ Algunos racks no cuentan con puertas ni espacio de trabajo libre alrededor (al frente y detrás) de acuerdo a las normas técnicas.

- ✓ Se encuentran cables de conexión y comunicación regados sobre el piso y por las paredes, no se encuentran en canaletas siguiendo los protocolos de seguridad para su protección.

- ✓ Se evidencio al momento de nuestra visita que la puerta de acceso al cuarto de comunicación de la sede Rosales, se encontraba abierta, según lo informado por el celador quien administra la llave, esta se mantiene abierta para permitir aireación y evitar sobre calentamiento en los equipos allí instalados (el cuarto no es refrigerado).

- ✓ Los cuartos de comunicación no se mantienen limpios y ordenados.

- ✓ Se evidencio extintores contra incendios al exterior de los cuartos de comunicación, los cuales se encuentran rodeados de canecas, implementos de aseo (exprimidor de traperos, baldes) elementos que dificultan su uso en caso de presentarse un evento.

- ✓ El sistema de cableado de datos (peinado de los cables) de los rack, no se encuentra organizados técnicamente en los gabinetes conforme lo indica las buenas prácticas para la administración de este tipo de elementos.

- ✓ El día de la visita 28/03/2017 de auditoria, se evidencio que la temperatura ambiente de los cuartos de comunicación de las sedes Rosales y Teusaquillo estaba muy alta debido a daño del equipo de aire acondicionado (Teusaquillo) y a la falta de un sistema de aireación y/o aire acondicionado (Rosales). Un inadecuado nivel de temperatura (sostenido en el tiempo) puede llegar a impactar negativamente el buen funcionamiento y la vida útil de los equipos que estos albergan.

A continuación se relaciona las evidencias encontradas en cada uno de los cuartos de comunicación:

CUARTO DE CABLEADO	OBSERVACION
Sede Central - CAN	
a. Cuarto de cableado A Dirección Piso 2	▪ Puerta de acceso, techo y división en el piso, elaborados en madera. ▪ Se encuentra un rollo de cableado estructurado. ▪ No se tiene acceso libre en la parte posterior del rack, se encuentra cableado sobre el piso. ▪ Se encuentran cables de conexión y comunicación regados sobre el piso y por las paredes, no se encuentran ubicados en canaletas para su protección. ▪ El sistema de cableado de datos, no se encuentra organizado técnicamente. ▪ Los gabinetes del circuito eléctrico se encuentran sin tapa. ver fotografías anexo 2
b. Cuarto de cableado B – Oficina de Sistemas Piso 3	▪ Elementos inflamables como: ✓ Cajas de cartón y bolsas plásticas que contienen elementos varios. ✓ Muebles elaborados en madera y/o aglomerado (archivadores, mesas, escritorios, perchero). ✓ Carpetas de archivo, libros, manuales ✓ Cajas de cartón apiladas cerca del rack del circuito eléctrico. ✓ Bolsas y ganchos plásticos ✓ Un saco ▪ Equipos en desuso como: CPU, teclados, teléfonos, repuestos, elementos de oficina, carteles y otros elementos dispersos sobre escritorios, mesas, archivadores y en el piso. ▪ Se encuentran cables de conexión que no se encuentran ubicados en canaletas para su protección. Ver fotografía anexo 3
c. Cuarto de cableado C - Aulas 302 - Piso 3	▪ Elementos inflamables como: ✓ Puerta de acceso elaborada en madera ✓ Cajas de cartón con elementos ✓ Lamina de icopor ✓ Bolsa plástica en el piso. ▪ Cuenta con una ventana hacia el exterior y por tanto los equipos de comunicación, se encentra expuestos a la polución. ▪ No se tiene acceso libre en la parte de atrás del rack, se encuentra cableado sobre el piso. ▪ Se encuentran cables de conexión y comunicación regados sobre el piso y no se encuentran ubicados en canaletas para su protección.

	▪ El sistema de cableado de datos, no se encuentra organizado técnicamente. (algunos cables de la parte delantera del rack están sobre el piso) Ver fotografía anexo 4
d. Cuarto de cableado D - Baño - Piso 2	▪ Elementos inflamables como: ✓ Puerta de acceso elaborada en madera ✓ Cajas de cartón que contienen papelería, repuestos, cables y otros elementos ✓ Bolsas plásticas ✓ Un tapete ✓ Cerca de la puerta de acceso se encuentran canecas plásticas. ▪ Equipos en desuso como: ventiladores, monitores, un rollo de cableado estructurado. ▪ El acceso al cuarto de comunicaciones, se encuentra ubicado dentro del baño de hombres y detrás de la puerta del mismo dificultando su acceso en caso de presentarse una contingencia. ▪ No se tiene espacio de trabajo libre alrededor (al frente y detrás) del rack, se encuentra cableado sobre el piso en la parte de atrás y al frente cajas de cartón y elementos en desuso (ventiladores) ▪ Se encuentran cables de conexión y comunicación regados sobre el piso y no se encuentran ubicados en canaletas para su protección. ▪ El sistema de cableado de datos del rack, no se encuentra organizado técnicamente. ▪ El acceso al extintor se encuentra obstaculizado por una caneca de basura. Ver fotografía anexo 5
e. Cuarto de cableado E - Biblioteca - Mezanine	▪ Elementos inflamables como: ✓ Cajas de cartón que contienen elementos ✓ Cartelera en madera ✓ Una silla tapizada en paño ▪ A pesar de que la puerta tiene llave se evidencio la apertura de un hueco en la pared que permite abrirla. Ver fotografía anexo 6
f. Cuarto de cableado F - Posgrados - Primer piso	▪ Elementos inflamables como: ✓ Cajas de cartón que contienen archivo, repuestos, cables y otros elementos. ✓ Bolsas plásticas ▪ Equipos en desuso como: CPU, teclados Ver fotografía anexo 7
Otras Sedes	
g. Cuarto de cableado - Sede Teusaquillo	▪ Elementos inflamables como: ✓ Cajas de cartón que contienen elementos. ✓ Escritorios y mesa en madera ✓ A la entrada del cuarto de comunicaciones se evidencio implementos de aseo (baldes, lava trapero), canastas y galones elaborados en plástico ▪ No se tiene espacio de trabajo libre alrededor (al frente y detrás) del rack, en la parte de atrás, se encuentra cableado sobre el piso y al frente un escritorio con computadores. ▪ Se encuentran cables de conexión regados sobre el piso y no se encuentran ubicados en canaletas para su protección. ▪ El sistema de cableado de datos del rack, no se encuentra organizado técnicamente.

	▪ En la fecha de nuestra visita (28/03/2017), el equipo de aire acondicionado se encontraba dañado y se pudo evidenciar que se presentaba niveles de temperatura elevados. ▪ El acceso al extintor se encuentra obstaculizado por una brilladora. Ver fotografía anexo 8
h. Cuarto de cableado - Sede Rosales.	▪ No se tiene espacio de trabajo libre a atrás, el acceso es por el lado izquierdo del rack, lo obstaculiza la UPS y el banco de baterías que dificultan la circulación del personal en caso de una emergencia y para el mantenimiento del mismo. ▪ Se encuentran cables de conexión regados sobre el piso y no se encuentran ubicados en canaletas para su protección. ▪ El sistema de cableado de datos del rack, no se encuentra organizado técnicamente. ▪ La instalación no tiene un sistema de aireación y/o aire acondicionado que mantenga la temperatura ambiente a niveles técnicamente permitidos por los fabricantes de los equipos existentes. ▪ El cuarto de comunicaciones, se encontraba abierto, según lo informado por el celador, al mantenerse cerrado el cuarto de comunicaciones, se eleva la temperatura y puede afectar los equipos que se encuentran en su interior. ▪ Se evidencia que existe una fuga e infiltración de agua por posible rotura de tubo interno localizado en el patio exterior de la casa al lado derecho del ingreso a la misma, la filtración a llegado al sótano desplazándose por el corredor hacia al fondo por el pasillo de acceso al cuarto de comunicaciones, se corre el riesgo que entre agua al cuarto de comunicaciones lo cual ocasionaría daños eléctricos en los equipos que se encuentran ubicados en esta instalación. Ver fotografía anexo 9

DESCRIPCIÓN DEL RIESGO

- ✓ Fallas o interrupción en los servicios de TICs.
- ✓ Accesos no autorizados a los cuartos de comunicaciones.
- ✓ Daño o destrucción en las instalaciones físicas y sistema de comunicaciones.
- ✓ Pérdida o daño en los equipos TICs.
- ✓ Inundación.
- ✓ Humedad.
- ✓ **Fallas físicas en los equipos de cómputo.**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

- ✓ Programar el peinado de los cables de los racks de los cuartos de comunicación.
- ✓ Instalar las puertas de los racks ubicados en los cuartos de comunicación.
- ✓ Retirar en forma permanente (así como prohibir) los muebles, cajas de cartón y demás elementos inflamables mencionados en las observaciones y establecer esta práctica como prohibitiva.
- ✓ Retirar de los cuartos de comunicación los elementos y equipos en desuso, implementos que no se encuentren activos y cables no utilizados.

- ✓ Mantener bajo llave las puertas de accesos a los cuartos de comunicaciones y mantener esta práctica como obligatoria.

- ✓ Llevar a cabo acciones tendientes a acondicionar técnicamente los cuartos de comunicación, garantizando el cumplimiento de estándares técnicos y de seguridad propios de este tipo de instalaciones, en los cuales se asegure como mínimo la atención de las observaciones señaladas, garantizando que sean lugares más seguros, ordenados, accesibles y fáciles de administrar.

- ✓ Realizar el mantenimiento del sistema de aire acondicionado de la sede Teusaquillo; definir, programas para llevar a cabo mantenimientos periódicos (preventivos) a este sistema.

- ✓ Adecuar el cuarto de comunicaciones de la sede rosales, asegurando que la temperatura y humedad, se regule a los niveles técnicos que exigen los diferentes fabricantes de los equipos que residen en él.

- ✓ Asignar un área para el almacenamiento de bienes y archivo de la Oficina de Sistema e Informática.

- ✓ Realizar arreglos locativos tendientes a localizar y evitar la fuga y filtración de agua que se presenta en el sótano de la sede Rosales.

***HALLAZGO No. 7 – Falta de* Lineamientos de Monitoreo y Control a la Infraestructura de TICs**

CONTEXTO:

Los lineamientos de Gobierno en Línea así como los estándares, marcos de referencia internacionales y buenas prácticas como COBIT 5, ITIL, ISO 27000, ISO27005, establecen como objetivo que se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño, disponibilidad y capacidad de la infraestructura de TI, de manera que permita minimizar el riegos de fallas en los sistemas y garantizar la continuidad del servicio.

El proceso de monitoreo a la infraestructura realizado durante el año 2016 por la OSI, no cuenta con una metodología y documentación que permitan visualizar el seguimiento a las actividades ejecutadas.

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

- ✓ No se evidenció la existencia de políticas, manuales e instructivos para el monitoreo, administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.

- ✓ La Oficina de Sistemas e informática no cuenta con una metodología que describa las actividades que se ejecutan frente al monitoreo de la infraestructura de TICs, notificación de eventos críticos y emisión de informes.

- ✓ No se evidencio la existencia de registros en formatos (electrónicos o físicos) de las actividades realizadas, las acciones tomadas, y además que se lleven estadísticas de seguimiento en la optimización, disponibilidad y tratamiento de incidentes presentados en los recursos tecnológicos.

- ✓ No se genera un informe periódico que refleje el análisis de los reportes e indique el comportamiento y acciones respectivas de disponibilidad de servicio prestado con el fin de garantizar su calidad.

DESCRIPCIÓN DEL RIESGO:

- ✓ Pérdida de trazabilidad en la administración de los recursos, infraestructura tecnológica y sistemas de información.
- ✓ Fallas o interrupción de los servicios de TIC que afectan la continuidad de los procesos críticos de la entidad.
- ✓ Pérdida de trazabilidad en la administración de los recursos, infraestructura tecnológica y sistemas de información.
- ✓ Inadecuado o inoportuno monitoreo a la infraestructura de TIC
- ✓ **Fallas físicas en los equipos de computo**
- ✓ **Poca disponibilidad de los servicios TI**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

- ✓ Implementar normas, políticas, manuales, formatos y/o instructivos con el propósito de llevar controles, seguimiento a las actividades realizadas de monitoreo a la infraestructura de TICs.

- ✓ Diseñar un manual y/o instructivo que defina la metodología y las actividades específicas de las tareas que de forma continua, se deben ejecutar para el monitoreo a la infraestructura de TICs, de tal forma que se cuente con un soporte físico o electrónico de las mismas.

- ✓ Presentar informes periódicos de las actividades, análisis, y/o acciones realizadas de monitoreo sobre la infraestructura TICs en documentos físicos o electrónicos.

- ✓ Se recomienda consultar los marcos de referencia internacionales tales como COBIT, ITIL, ISO270001 e ISO 20000.

HALLAZGO No. 8 – No se ejecutan pruebas de vulnerabilidad y ética Hacking a la infraestructura tecnológica

CONTEXTO:

El estándar ISO 27001-2005 y el marco de referencia COBIT 5, establecen que se debe; obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización ante esas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado con el fin de minimizar el impacto en el negocio causado por vulnerabilidades e incidentes operativos de seguridad, a fin de asegurar la continuidad del servicio de TI.

Durante el año 2016, la Entidad no realizo pruebas de vulnerabilidad y ética Hacking a la infraestructura tecnológica.

Dentro de las tareas a desarrollar por la Oficina de Sistemas e Informática para el período 2017, se contempló la ejecución de las pruebas de vulnerabilidad y ética Hacking, actividad a desarrollar en el plan de Gestión del proyecto Telebucaramanga S.A. contrato 183 de 2017, cuyo objeto es: "*ofrecer una solución integral de TI que incluye los servicios de mantenimiento, administración, soporte y operación de la infraestructura tecnológica de redes, telefonía IP, seguridad perimetral, custodia de archivo y gestión documental; alquiler de contenedores, la implementación de una estrategia integral orientada al desarrollo de los 4 componentes establecidos en la estrategia de Gobierno en Línea: Tic para la Gestión, Tic para Gobierno Abierto, Tic para servicio y seguridad y privacidad de la información así como la implementación de SGSI de la Escuela Superior de Administración Pública ESAP*", y se encuentra definida en el numeral 1.4.9 "*Sistema de gestión de Seguridad de la información SGSI*".

Se identificó durante el proceso de auditoría que las pruebas de Vulnerabilidades (internas y externas) y de Ethical Hacking, se iniciaron el día 5 de abril de 2017 y terminaran el día 10 de mayo de 2017, de acuerdo al plan de trabajo y cronograma presentado por Telebucaramanga.

DESCRIPCION DEL HALLAZGO:

No se tienen pruebas de vulnerabilidad y ética Hacking a la infraestructura tecnológica y plan de acción para subsanar las vulnerabilidades identificadas.

DESCRIPCIÓN DEL RIESGO

- ✓ Fallas o interrupción de los servicios de TIC.
- ✓ Accesos no autorizados a la plataforma tecnológica.
- ✓ Perdida de información.
- ✓ **Ataques informáticos a los aplicativos y página web Institucional.**
- ✓ **Pérdida, fuga, borrado intencional y/o accidental de datos de los servidores o unidades de almacenamiento.**
- ✓ **Alteración de la Información de los sistemas de información.**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

- ✓ La Oficina de Sistemas e Informática debe implementar un plan de acción, para subsanar de manera inmediata las vulnerabilidades identificadas, con prioridad crítica, sobre aquellas clasificadas como altas y medias.

- ✓ Diseñar, documentar, aprobar, implementar y supervisar la ejecución de políticas y procedimientos relacionados con la atención oportuna de las vulnerabilidades identificadas en las diferentes pruebas de hacking ético efectuadas a la Entidad.

HALLAZGO No. 9 – Documentación física y/o electrónica incompleta en la implementación de Gobierno en Línea y Sistema de Gestión de seguridad de la Información SGSI

CONTEXTO:

Los estándares, marcos de referencia internacionales y buenas prácticas como COBIT 5, ISO 27000, ISO27005 y PMBOK (PMI), establecen que el sistema de gestión de la documentación es aquella herramienta, bien un programa informático o simplemente un proceso, que nos permite controlar y mantener ordenada la documentación relacionada con la ejecución de actividades (plan de trabajo, actas de reunión, ejecución de pruebas, comités de proyecto, informes, etc.), de procesos y/o proyectos.

Durante el año 2016, la Oficina de Sistemas e Informática, efectuó actividades tendientes a dar cumplimiento a las directrices establecidas por Gobierno en Línea y la adoptar el Sistema de Gestión de seguridad de la Información - SGSI, realizando tareas como; actualización del inventario de los sistemas de información, generación de documentos para la planificación, elaboración y oficialización de la resolución para crear el SGSI y modificación de los procedimientos del Proceso de Gestión Tecnológica.

DESCRIPCION DEL HALLAZGO:

En la revisión y evaluación a la información entregada, se observa la falta de una metodología que incluya un plan de trabajo y un cronograma, que permitan realizar el seguimiento a las actividades ejecutadas.

DESCRIPCIÓN DEL RIESGO

- ✓ Inadecuada administración de procesos y/o proyectos de TI
- ✓ Pérdida de confidencialidad, integridad, disponibilidad de la información.

RECOMENDACIÓN(ES):

- ✓ Diseñar, documentar e implementar normas, políticas, formatos y/o instructivos para el manejo de procesos y/o proyectos de TICs.
- ✓ Diseñar un manual o guía donde se estructure la metodología que establezca los lineamientos a seguir para la gestión de la documentación física y/o electrónica que se va generando en la ejecución de los procesos y/o proyectos de TICs.

HALLAZGO No. 10 – Falta de documentación proyecto de implementación SINU

CONTEXTO:

El estándar ISO 27001-2005, el marco de referencia COBIT 5 y la guía de estándares internacionales PMBOK (PMI), establecen que el sistema de gestión de la documentación es aquella herramienta, bien un programa informático o simplemente un proceso, que nos permite controlar y mantener

ordenada la documentación (plan de trabajo, actas de reunión, pruebas, comités de proyecto, informes, etc.) relacionada con la ejecución de un proceso y/o proyecto.

La Oficina de Sistemas e Informática registra la documentación del proyecto de implementación SINU en la carpeta "*Documentos contrato 211-2017*", en la unidad compartida *"G:\TABLAS DE RETENCIÓN DOCUMENTAL OSI\140.1360.20 PROGRAMAS DE SISTEMATIZACIÓN-SOFTWARE\SOFTWARE 1360.20*".

DESCRIPCION DEL HALLAZGO:

Como resultado de la revisión efectuada a las actas de levantamiento de información en el repositorio del contrato, se evidencio que faltan formatos del "*Levantamiento de información y definición de procesos*" de acuerdo al compromiso definido en el acta de reunión, así:

Proceso	Reunión		Formato Levantamiento de Información y Definición de Procesos	
	Acta	Fecha	Fecha de envío	Entregado
Planta física	Si	21/03/2017	22/03/2017	No
Oferta académica	Si	22/03/2017	23/03/2017	No
Inscripciones	Si	22/03/2017	24/03/2017	
Admisiones (Pregrado)	Si	23/03/2017	23/03/2017	Si
Certificados	Si	24/03/2017	24/03/2017	No
Planes de Estudio	Si	24/03/2017	27/03/2017	Si
Auditorias	Si	24/03/2017	28/03/2017	No
Estructura de conceptos	Si	24/03/2017	28/03/2017	No
Gestión de personas	Si	24/03/2017	28/03/2017	No

DESCRIPCIÓN DEL RIESGO

- ✓ Falta de documentación soporte
- ✓ Pérdida en la trazabilidad en la implementación de sistemas de información
- ✓ **Posibilidad la pérdida de información**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

Establecer controles para que la entrega de información se realice en las fechas indicadas.

HALLAZGO No. 11– No existe una referenciación adecuada en los documentos del proyecto SINU

CONTEXTO:

El estándar ISO 27001-2005, el marco de referencia COBIT 5 y la guía de estándares internacionales PMBOK (PMI), establecen que el sistema de gestión de la documentación es aquella herramienta, bien un programa informático o simplemente un proceso, que nos permite controlar y mantener adecuadamente la documentación (plan de trabajo, actas de reunión, pruebas, comités de proyecto, informes, etc.) relacionada con la ejecución de un proceso y/o proyecto.

Se observó que el repositorio documental del proyecto SINU, se encuentra en la carpeta *"Documentos contrato 211-2017"* ubicada en la unidad compartida *"G:\TABLAS DE RETENCIÓN DOCUMENTAL OSI\140.1360.20 PROGRAMAS DE SISTEMATIZACIÓN-SOFTWARE\SOFTWARE 1360.20* y es administrada por dos funcionarios Así:

- ✓ Las carpetas ACTAS, DOCUMENTOS CONTRATO 211-2017, INFORMES, LICENCIAS y PAGOS, son maneja por la secretaria de la oficina de sistemas tal como se muestra en la imagen 2.

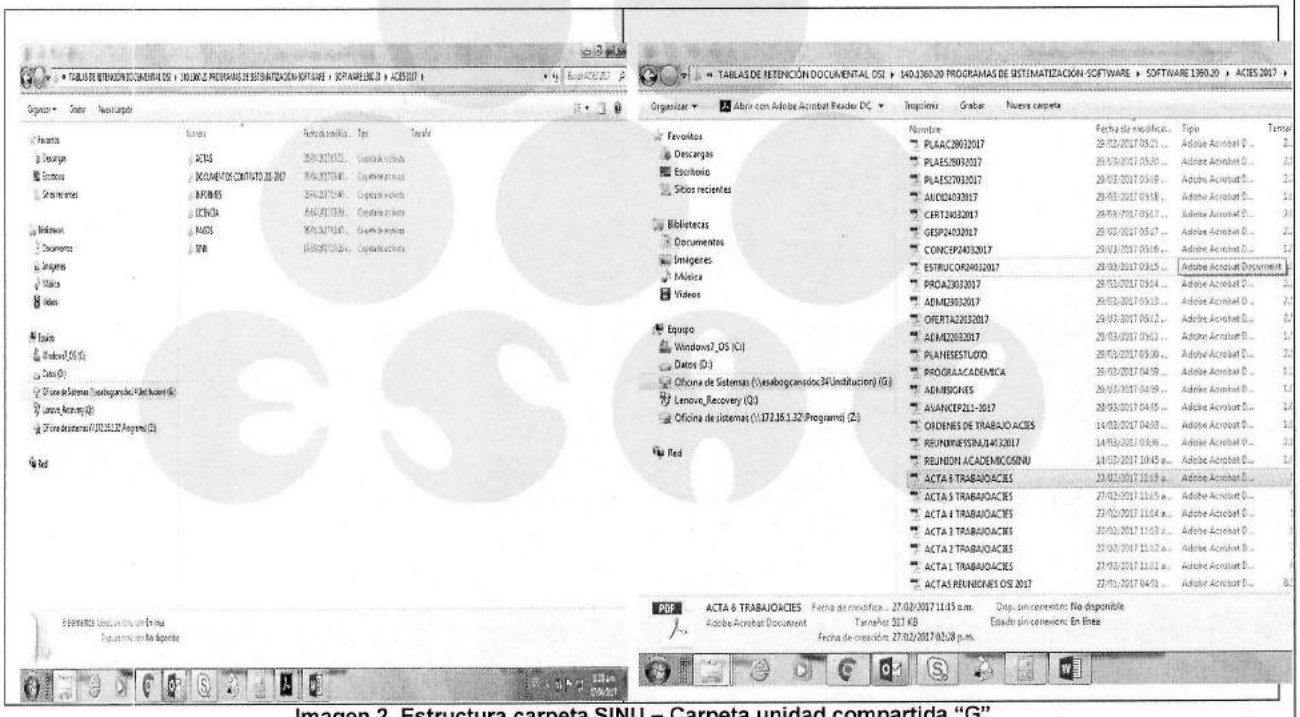


Imagen 2. Estructura carpeta SINU – Carpeta unidad compartida "G"

- ✓ La carpeta SINU, es administrada por el líder del proyecto y maneja la siguiente estructura. Ver imagen 3.

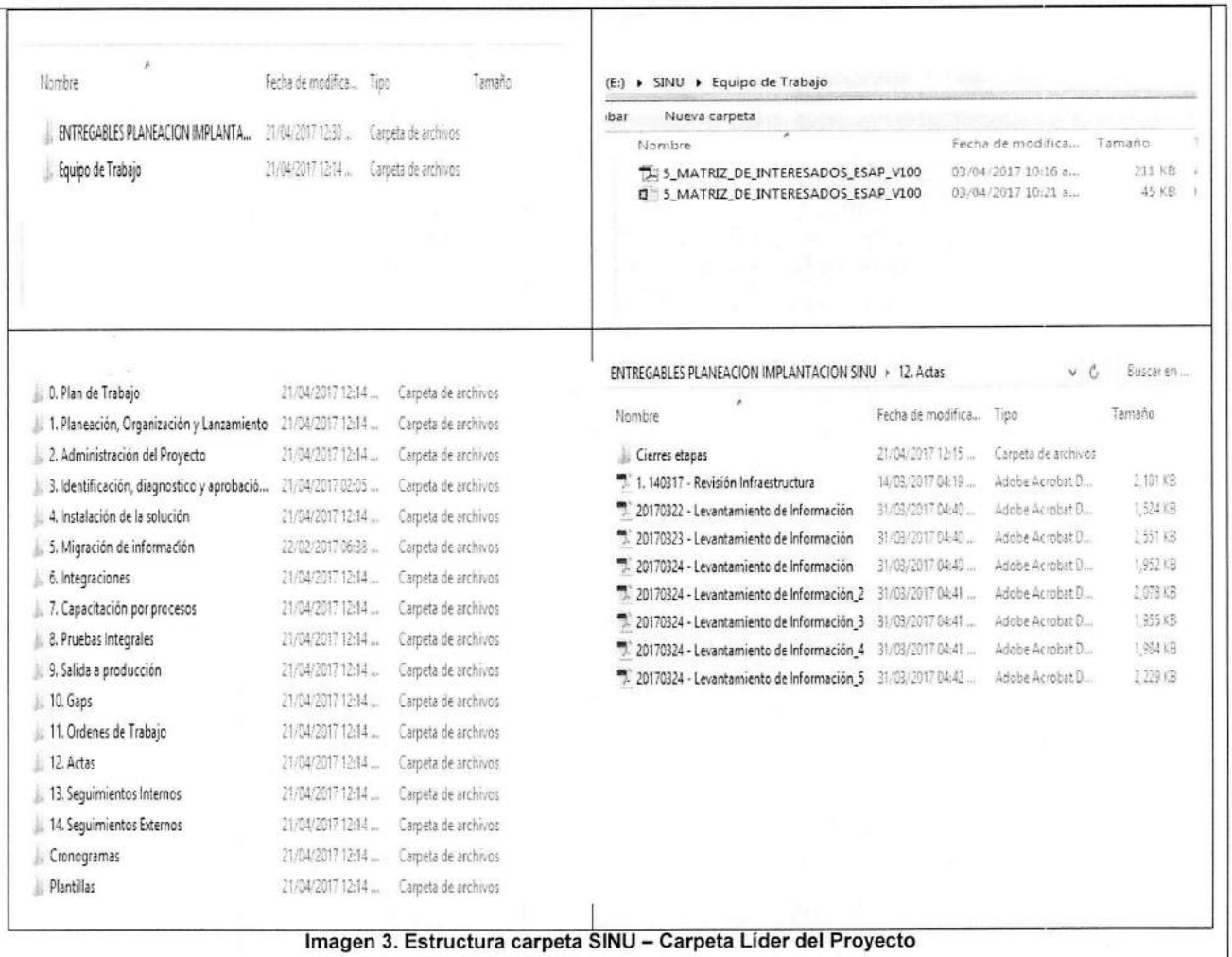


Imagen 3. Estructura carpeta SINU – Carpeta Líder del Proyecto

DESCRIPCION DEL HALLAZGO:

Se observó en el registro documental información duplicada. Igualmente, la descripción de archivos no está estandarizada para facilitar su consulta.

DESCRIPCIÓN DEL RIESGO

- ✓ Pérdida en la trazabilidad de la información del proyecto
- ✓ Ausencia de documentación
- ✓ **Posibilidad de pérdida de información**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

Estandarizar el manejo de registro documental del proyecto bajo una misma estructura precisa y entendible.

HALLAZGO No. 12– Falta de contrato de soporte y mantenimiento de Sistema de información SEVEN

CONTEXTO:

La información de inventarios y activos fijos se procesa en el sistema de información SEVEN. La actualización que debe hacer la ESAP para dar cumplimiento a las Normas Internacional de Información Financiera (NIIF) no la soporta la versión adquirida.

DESCRIPCION DEL HALLAZGO:

La ESAP no dispone de un contrato de soporte y actualización del sistema de información SEVEN.

DESCRIPCIÓN DEL RIESGO

- ✓ Inoperancia de los procesos por obsolescencia del software o desactualización frente a los requerimientos de los usuarios
- ✓ **Posibilidad la pérdida de información.**
- ✓ **Poca disponibilidad de los servicios de TI.**

Nota: Se resalta con negrilla los riesgos incluidos en la matriz de riesgos institucional.

RECOMENDACIÓN(ES):

Realizar la contratación del soporte y actualización del Sistema SEVEN y/o realizar estudios técnicos de mercado para la adquisición de un nuevo sistema, que se ajuste a las necesidades actuales que requiere la ESAP para dar cumplimiento a las NIIF.

HALLAZGO No. 13– No se tiene una interfaz entre el sistema Active Document y PQRs

CONTEXTO:

La Escuela cuenta con los sistemas de información de Gestión Documental "Active Document" y El sistema de atención al ciudadano – Quejas y reclamos "PQRS".

DESCRIPCION DEL HALLAZGO:

El sistema de Peticiones, Quejas y Reclamos – PQRs, no está en interface con el sistema de gestión documental "Active Document", lo que implica que cuando se requiere subir un caso de una PQR en Active Document, sea necesario digitalizar nuevamente los documentos y el cargue de la información del caso.

DESCRIPCIÓN DEL RIESGO

✓ Incumplimiento de la normatividad de atención al ciudadano a través de canales centralizados.

RECOMENDACIÓN(ES):

Llevar a cabo los estudios técnicos correspondientes para la integración de los sistemas de gestión documental y el sistema de peticiones, quejas y reclamos PQRs, con el fin que se aplique el concepto de ventanilla única, para la atención al ciudadano y se optimice el proceso por medio de una base de datos unificada de los dos sistemas de información.

RESPUESTA DEL AUDITADO:

El auditado no emitió observaciones en el término establecido.

Nota: El plan de mejoramiento hará parte integral de este informe definitivo (formato RE-E-GE-19)

RESUMEN DE HALLAZGOS:

N°	Título de hallazgo	Repetitivo	Estado
1	Falta de una metodología en la actualización del Proceso de Gestión Tecnológica		Abierto
2	Documentos desactualizados en el Sistema de Gestión de la Calidad.		Abierto
3	Falta de políticas informáticas		Abierto
4	Publicación de documentos no institucionales en SGC		Abierto
5	Falta de políticas informáticas para la administración de Cuartos de Comunicación		Abierto
6	Inadecuada seguridad física e industrial en los Cuartos de		Abierto

	Comunicación		
7	Falta de Lineamientos de Monitoreo y Control a la Infraestructura de TICs		Abierto
8	No se ejecutan pruebas de vulnerabilidad y ética Hacking a la infraestructura tecnológica.		Abierto
9	Documentación física y/o electrónica incompleta en la implementación de Gobierno en Línea y Sistema de Gestión de seguridad de la Información SGSI		Abierto
10	Falta de documentación proyecto de implementación SINU		
11	No existe una referenciación adecuada en los documentos del proyecto SINU		Abierto
12	Falta de contrato de soporte y mantenimiento de Sistema de información SEVEN		Abierto
13	No se tiene una interfaz entre el sistema Active Document y PQRs		Abierto

ANEXOS: Ver documentos de anexos

Bogotá D.C., 16 del mes de Mayo del 2017

MARIA MAYERLY PEDREROS PINZON
Jefe Oficina de Control Interno

Elaboró: Alexandra Triviño Martínez, Profesional Especializado Oficina de Control Interno.

ANEXO 1

SOLICITUD ELIMINACIÓN DOCUMENTOS SGC

	SOLICITUD DOCUMENTAL AL SISTEMA DE GESTION DE CALIDAD			
ESAP Escuela Superior de Administración Pública	Versión: 03	Fecha: 2015/04/29	Página: 1 de 2	Código: RE-S-GC-06

FECHA DE SOLICITUD			
3 0 SEP 2016			30/09/2016
Año	mes	d.a	3 0 SEP 2016

TIPO DE DOCUMENTO	Interno	X	TIPO DE SOLICITUD	Creación modificación		Eliminación Adquisición	X
	Externo						

Proceso al que aplica	NELSON JOSE OROZCO
Procedimiento al que aplica	GESTION TECNOLOGICA

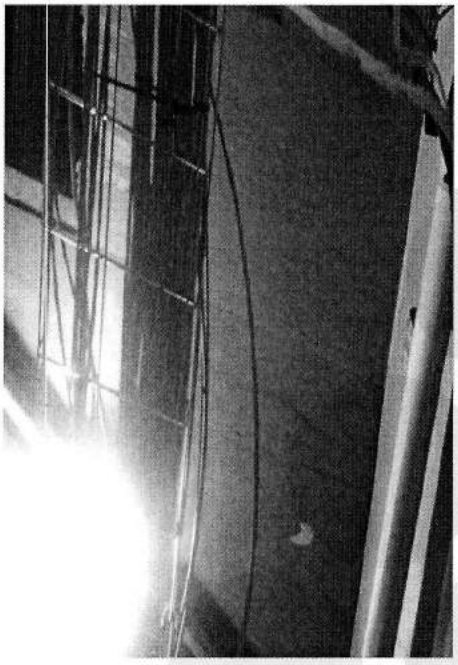
INFORMACIÓN DEL DOCUMENTO / REGISTRO			
NOMBRE:	CÓDIGO:	VERSIÓN ANTERIOR:	VERSIÓN ACTUAL:
Bitácora - Backups	RE-A-GT-01	2	Eliminación
Formato Asignación Salas	RE-A-GT-02	1	Eliminación
Formato Solicitud Usuario de Red	RE-A-GT-03	3	Eliminación
Formato solicitud salas de Sistemas	RE-A-GT-04	1	Eliminación
Formato Solicitud de Videoconferencia	RE-A-GT-05	1	Eliminación
Entrega y Recibo de Bienes Muebles	RE-A-GT-07	1	Eliminación
Acta Levantamiento Hurtos Kit Satelital	RE-A-GT-08	1	Eliminación
Traslado Antena Móvil	RE-A-GT-09	1	Eliminación
Matriz de Seguimiento Conexión Eventos	RE-A-GT-10	1	Eliminación
Ficha Técnica Informe de Visitas y Seguimiento Sistema de Comunicación Satelital	RE-A-GT-11	1	Eliminación
Obsolescencia Tecnológica	RE-A-GT-12	1	Eliminación
Formato Diagnóstico Técnico	RE-A-GT-13	1	Eliminación
Lista Maestra de Registros Gestión Tecnológica	RE-S-GC-01 N.A	3	Eliminación
Lista Maestra Documentos Gestión Tecnológica	RE-S-GC-02 N.A	1	Eliminación
Listado maestro de documentos externos	RE-S-GC-03 N.A	1	Eliminación
Procedimiento gestión de hardware	PT-A-GT-01	3	Eliminación
Procedimiento gestión de software	PT-A-GT-02	3	Eliminación
Procedimiento de soporte	PT-A-GT-03	3	Eliminación
Procedimiento para herramienta satelital	PT-A-GT-05	1	Eliminación
Procedimiento para la publicación de información a través de medios electrónicos	PT-A-GT-06	1	Eliminación
Caracterización Proceso Gestión Tecnológica	PR-A-GT-01	1	Eliminación

JUSTIFICACIÓN / MODIFICACIONES
Eliminación del SGE, ya que se realizara actualización de los procedimientos y documentación en el proceso Gestión Tecnológica. Los nuevos procedimientos quedarán así: ESTRATEGIA Y GOBIERNO T.I, SISTEMAS DE INFORMACION, INFRAESTRUCTURA DE SERVICIOS TECNOLOGICOS(infraestructura, comunicaciones, mesa de ayuda y virtual), SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

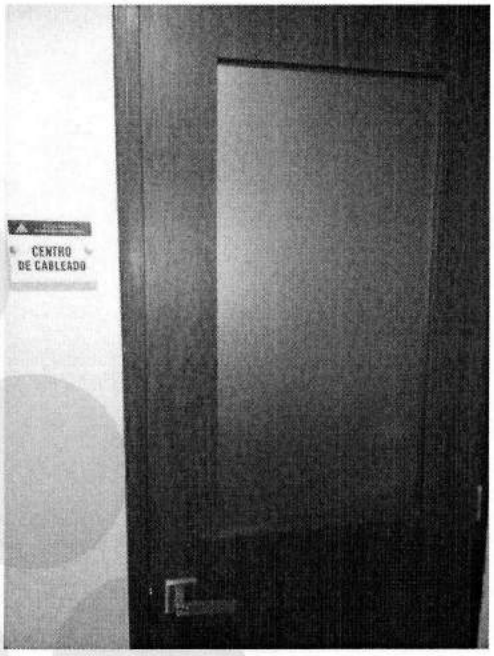
ANEXO 2

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO -A- DIRECCIÓN PISO- 2

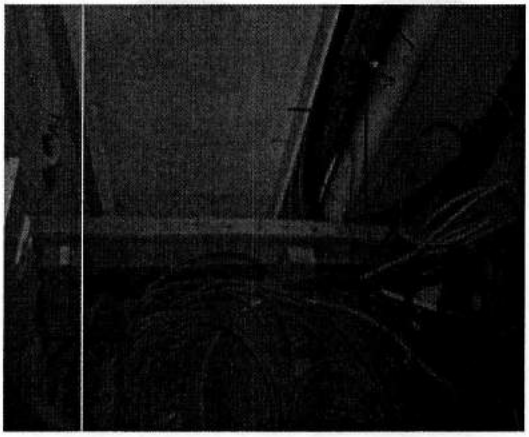
Techo en lamina de madera



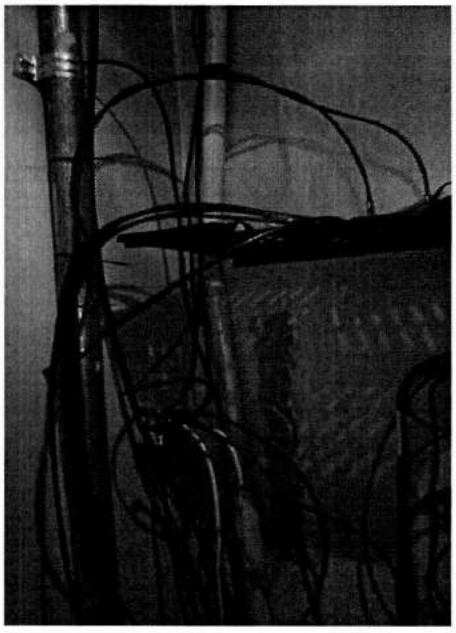
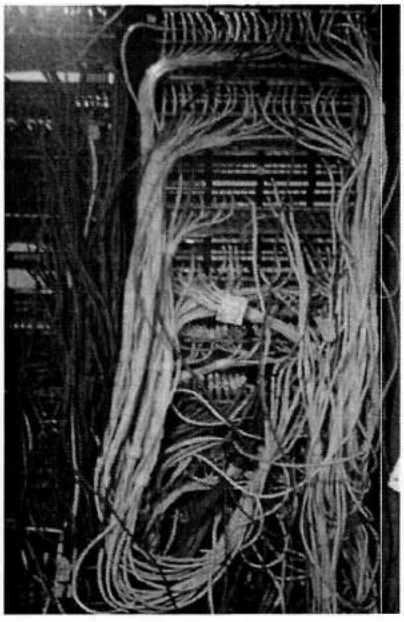
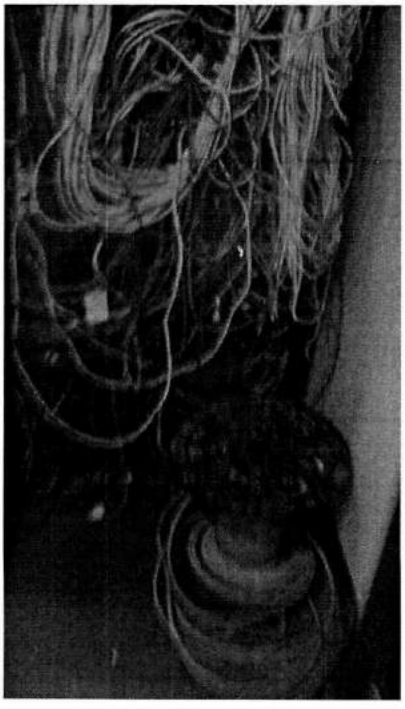
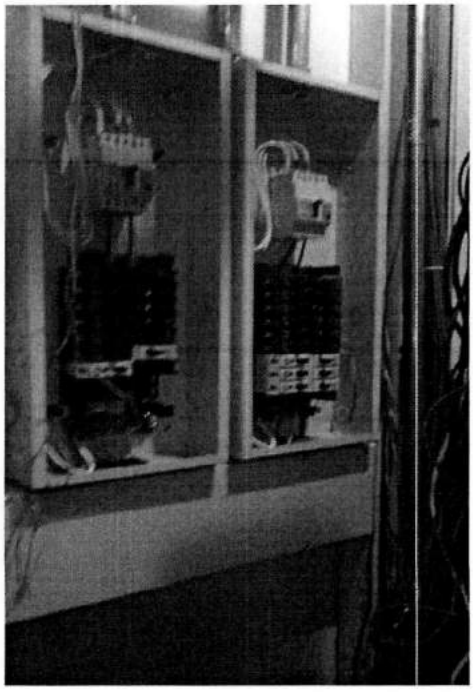
Puerta en madera



Cableado sobre el piso



Continuación Anexo 2

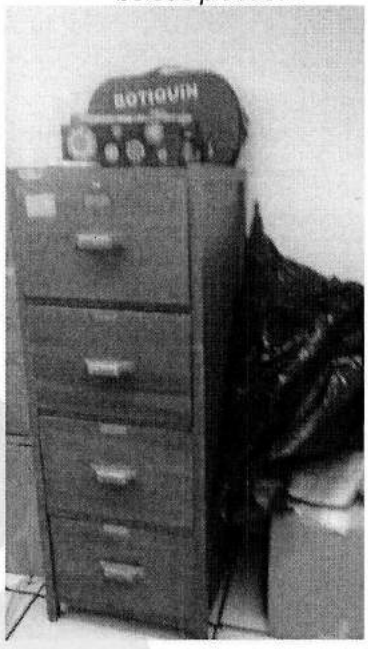
Cableado fuera de canaletas	*Cableado no organizado técnicamente en el rack*
	
Carrete en madera de cableado	*Cajas de circuito eléctrico sin tapas*
	

ANEXO 3

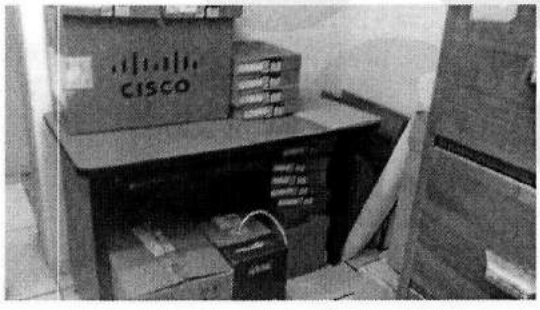
EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO - B - OSI – PISO 3

Cajas de cartón, elementos en desuso

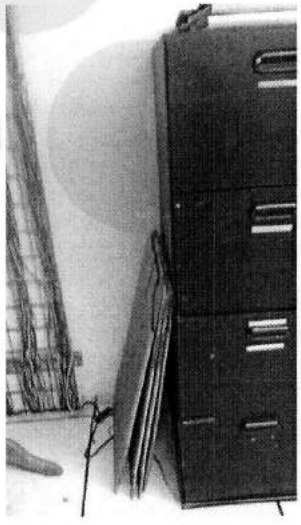
Muebles en madera, cajas de cartón y bolsas plásticas



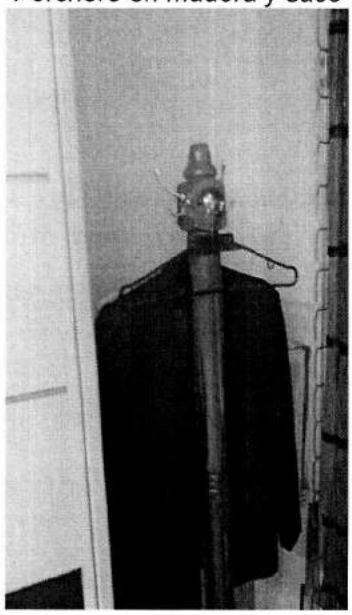
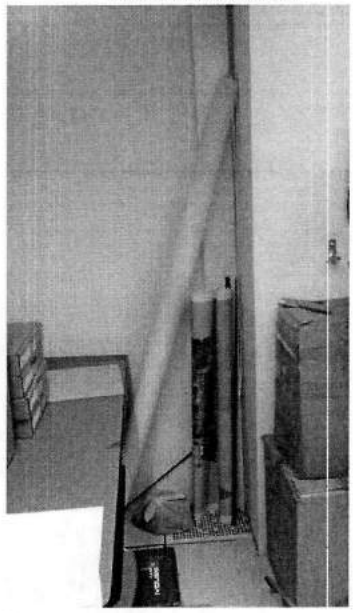
Muebles en madera y cajas de cartón



cajas de cartón



Continuación Anexo 3

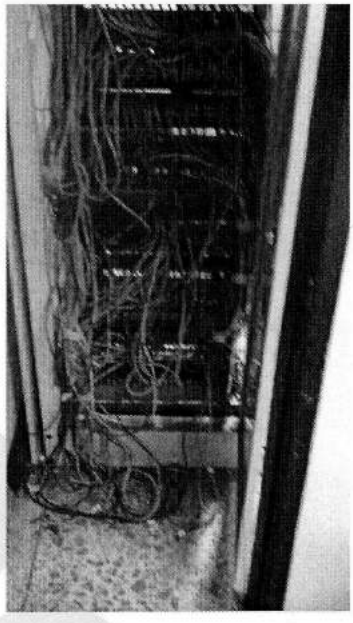
Perchero en madera y saco 	*Muebles en aglomerado, cajas de cartón y otros elementos* 
Cajas de cartón arrumadas cerca de la caja de control del circuito eléctrico 	

ANEXO 4

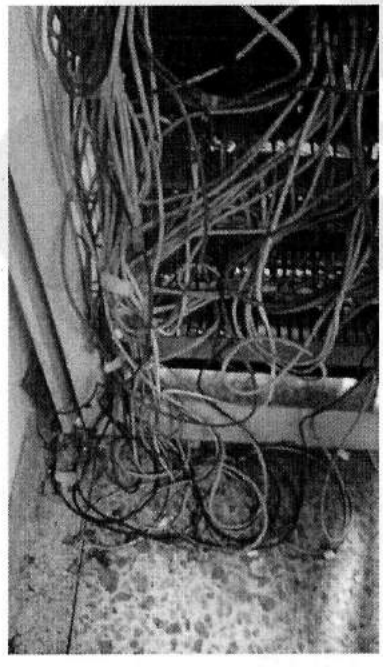
EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – C - AULAS 302

Puerta en madera

Rack de cableado sin tapa

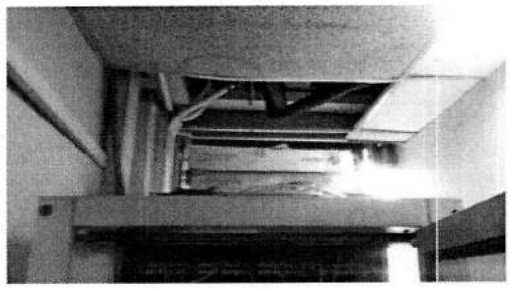
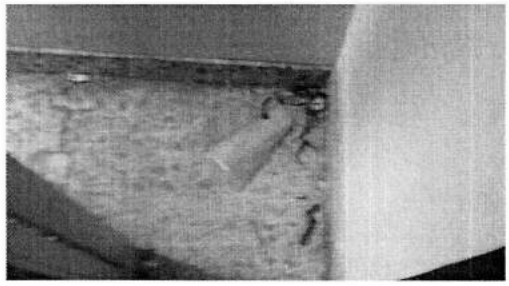
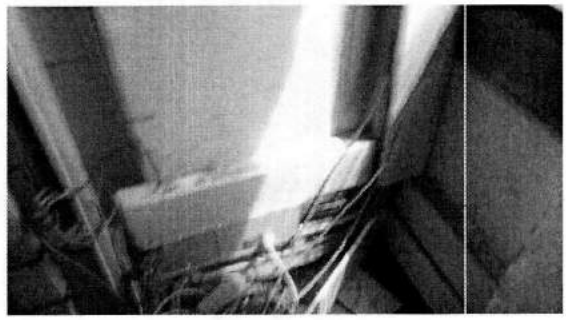


Cableado fuera del rack



Cableado fuera de canaletas y caja de cartón

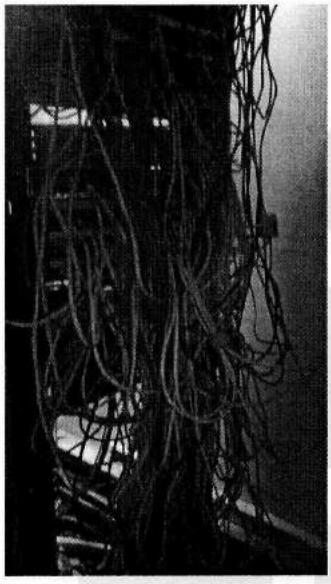
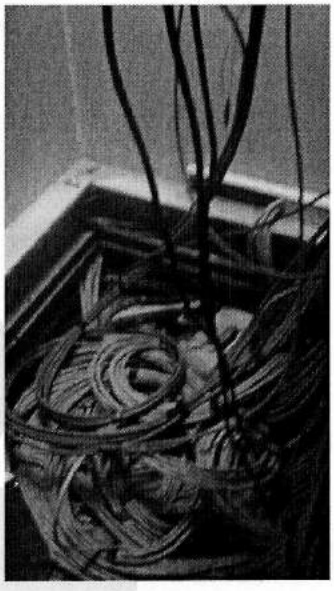
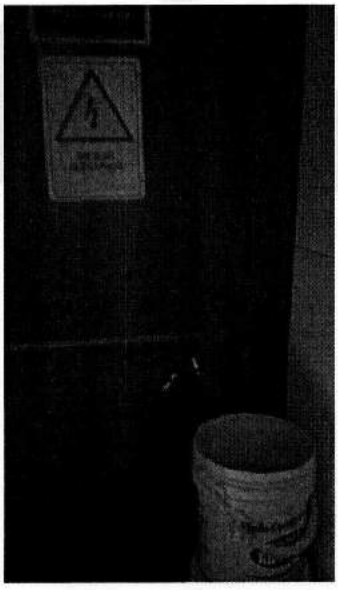
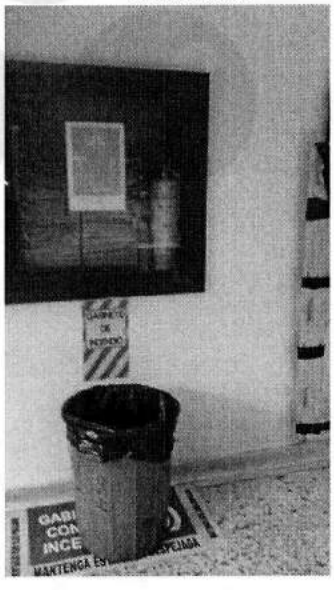
Continuación Anexo 4

Cajas de cartón 	
bolsas plásticas 	*Lamina de icopor* 

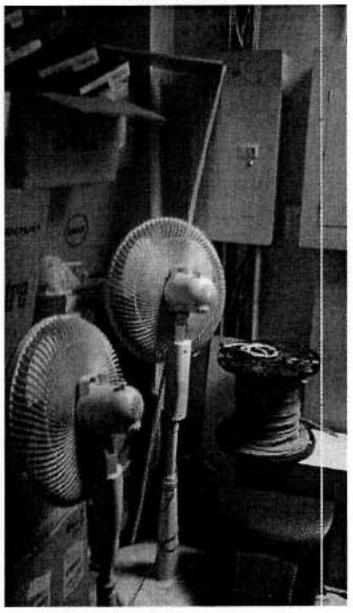
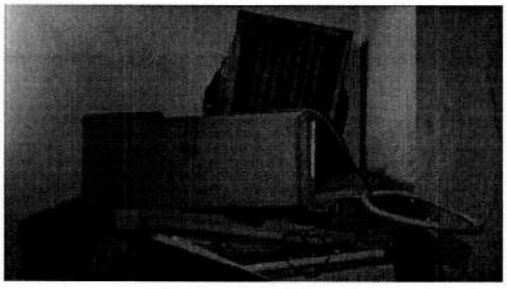
ANEXO 5

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – D - BAÑO HOMBRES PISO 2

Evidencia muebles en madera y cajas de cartón dentro de las instalaciones del Centro de cableado

Cableado no se encuentra organizado en el rack 	*Cableado sobre el piso* 
Puerta en madera y balde plástico 	*Caneca de basura frente al equipo de incendios* 

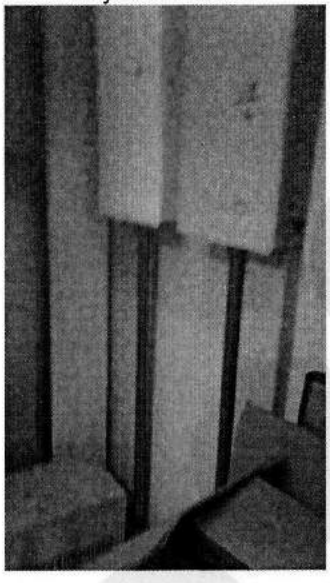
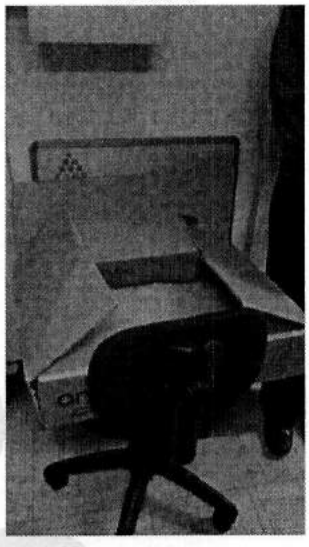
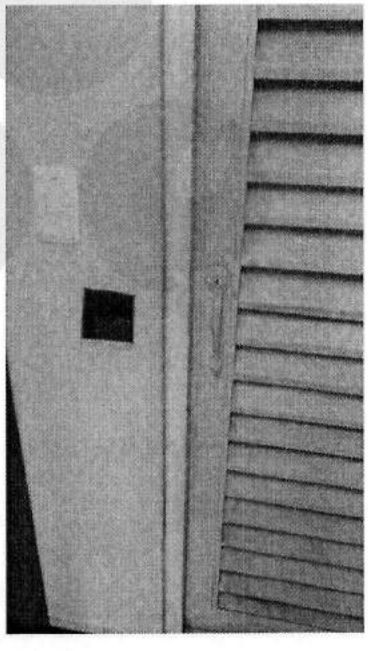
Continuación Anexo 5

Cajas de cartón 	*Cajas de cartón, muebles en desuso, rollo cableado* 
Elementos en desuso 	*Tapete sobre el piso* 

ANEXO 6

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – E - BIBLIOTECA PISO – 2

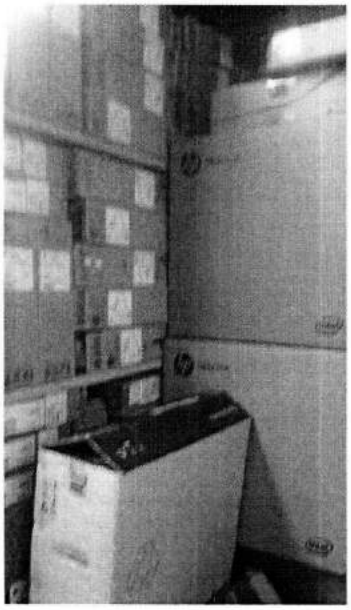
Evidencia muebles en paño, bolsas plásticas y cajas de cartón dentro de las instalaciones del Centro de cableado

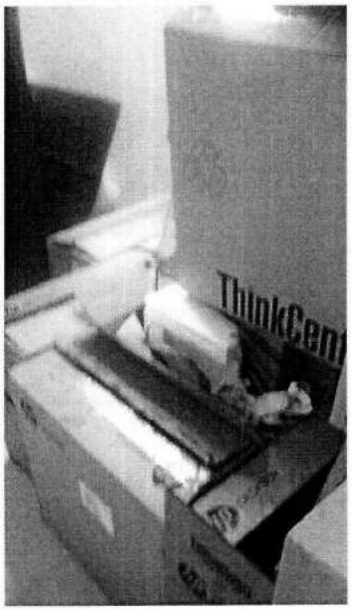
Cajas de cartón 	*Mueble en paño, cajas de cartón y cartera en madera* 
Caja de cartón y bolsa plástica 	*Agujero en la pared de acceso* 

ANEXO 7

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – PREGADO - PISO – 1

Evidencia muebles en desuso y cajas de cartón dentro de las instalaciones del Centro de comunicaciones

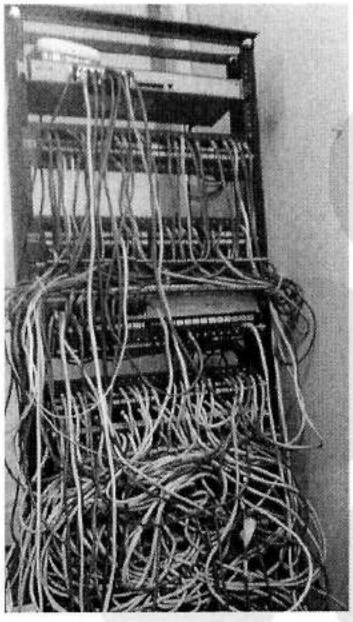
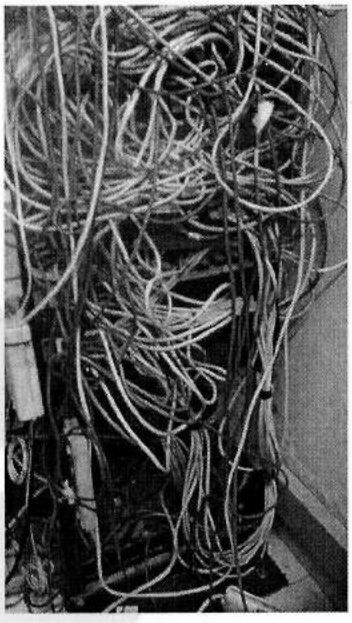
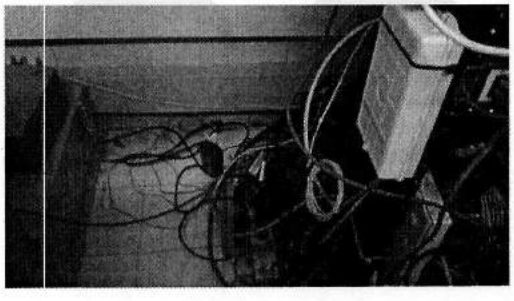




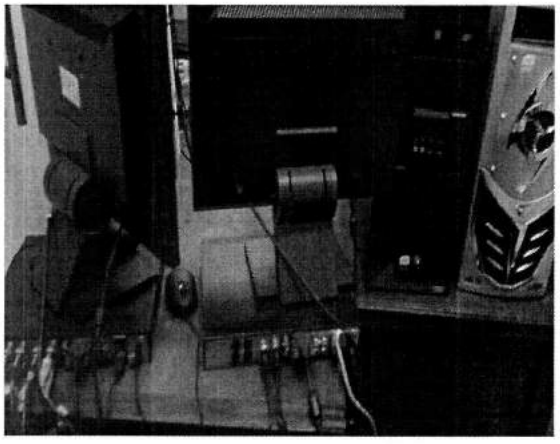
ANEXO 8

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – SEDE TEUSAQUILLO

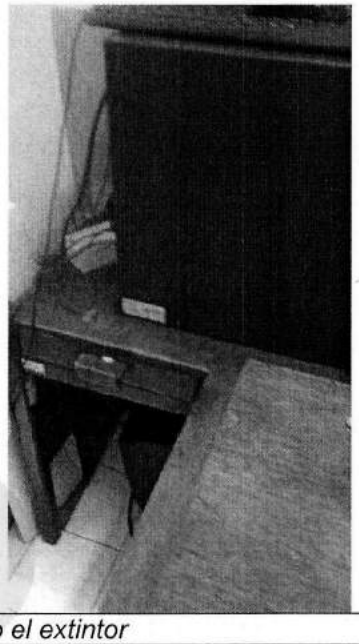
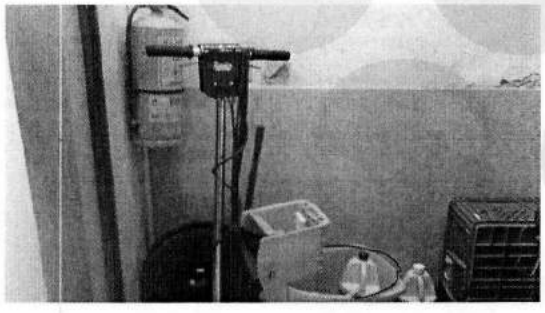
Evidencia Cableado no organizado, muebles en madera y cajas de cartón dentro de las instalaciones del Centro de cableado

Cableado no se encuentra organizado	
	
Cables regados por el piso y fuera de canaletas	*Aire acondicionado dañado*
	

Continuación Anexo 8

Muebles en madera	
	
	

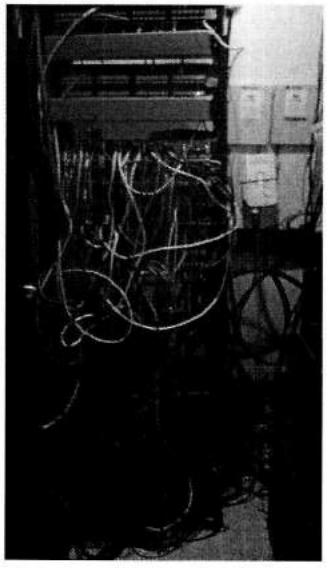
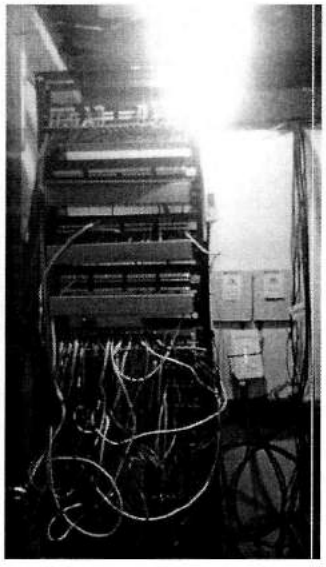
Continuación Anexo 8

Caja de cartón	*Muebles en madera*
	
Mueble de aseo obstaculizando el extintor	
	

ANEXO 9

EVIDENCIAS OBTENIDAS EN VISITA REALIZADA AL CENTRO DE CABLEADO – SEDE ROSALES

Evidencia cables no ordenados adecuadamente en los rack y fuga de agua en el pasillo de entrada al cuarto de comunicaciones

Cableado no peinado 	*Cableado no peinado* 
Cables fuera de canaletas 	*Fuga de agua en el pasillo* 

Proceso o Territorial: Gestión Tecnológica
Responsable: Edilma Herrera Ortiz
Fecha de suscripción: 23-05-2017

Hallazgo 1. Falta de una metodología en la actualización del proceso Gestión Tecnológica	En el ejercicio de actualización documental del proceso Gestión Tecnológica de la ESAP, se observa la falta de una metodología que incluya un plan de trabajo y un cronograma, que permitan realizar el seguimiento a las actividades ejecutadas.	No existe una metodología que incluya un plan de trabajo y cronograma	No hay control en la ejecución y seguimiento de la actualización documental del proceso de Gestión Tecnológica	Elaboración de una metodología que incluya un plan de trabajo, un cronograma y seguimiento al cronograma	Lograr la actualización de todos los documentos que conforman el proceso de Gestión Tecnológica	Documento con la metodología que incluya plan de trabajo, cronograma y seguimiento al cronograma	1	1	01/06/2017	31/07/2017	9			
Hallazgo 2. Documentos desactualizados en el Sistema de Gestión de la Calidad	En la revisión documental al Sistema de Gestión de Calidad que soporta el proceso Gestion Tecnologica se observa que la documentación allí publicada no está actualizada en concordancia con lo establecido en el plan de acción de la vigencia 2016	Documentación desactualizada en el SGC que soporta al Proceso Gestión Tecnológica	Falta de concordancia del proceso de la Oficina de Sistemas e Informática, con lo publicado en la SGC	Actualizar los procedimientos y documentación que soporta al Proceso Gestion Tecnológica en SGC Solicitar el retiro de la documentación que no se vaya a incluir en el SGC del proceso Gestión Tecnológica	Articular el SGC acorde a la documentación y/o actividades que soportan el proceso Gestión Tecnológica	Ficha de caracterización procedimientos, planes, manuales y políticas, documentos, formatos e instructivos del proceso de Gestión Tecnológica actualizados en el SGC.	1	1	01/06/2017	30/11/2017	26			
Hallazgo 3. Falta de políticas informáticas	En la evaluación de las políticas, normas, procedimientos, manuales, instructivos y/o formatos que soportan el Proceso Gestión Tecnológica, se observo que la OSI no ha considerado las políticas y los documentos que desarrollan los siguientes aspectos , los cuales a juicio de esta auditoria son necesarios para el fortalecimiento del sistema de control interno de las TICs. * Gestión de Proyecto TI * Estándares y metodologías para el desarrollo de proyectos y actividades. * Administración de la infraestructura tecnológica (Hardware, software y comunicaciones) * Administración de inventarios (hardware, software y licencias). * Administración de log (pistas de auditoria) en (S.O., BD, red y aplicativos). * Administración del plan de continuidad * Licenciamiento de Software * Monitoreo a la infraestructura * Manejo de internet y correo electrónico. * Políticas y directrices de Gestión de seguridad de la información SGSI.	No existen suficientes definición de políticas, procedimientos, manuales y/o instructivos que soporten el proceso Gestión Tecnológicos.	Insuficiente definición de políticas y documentos de TICs.	Realizar e incorporar dentro del SGC las políticas, manuales y/o instructivos que la OSI considera necesarios como soporte a procedimientos del proceso Gestión Tecnológica	Incorporar dentro del SGC las políticas, manuales y/o instructivos que la OSI considera necesarios como soporte al proceso Gestión Tecnológica	Actualizar los documentos donde se plasmen las políticas e incorporar manuales y/o instructivos en el SGC para el fortalecimiento del proceso de Gestión Tecnológica.	1	10	01/09/2017	01/06/2018	52			
Hallazgo 4. Publicación de documentos no institucionales en SGC.	En la revisión documental al Sistema de Gestión de Calidad que soporta el proceso Gestion Tecnologica, se observaron los siguientes documentos externos que corresponden al "Ministerio de Tecnologías de la Información y las Comunicaciones" los cuales por no ser institucionales no deben estar incluidos en el Sistema de Gestión de Calidad.	Existen documentos que no pertenecen a la ESAP (institucionales) que no deben estar dentro del SGC	Publicación no autorizada de documentación no institucional	Retirar del SGC documentos no institucionales.	Actualizar los documentos que deben hacer parte integral del SGC del proceso de Gestión Tecnológica	Retiro de documentos no institucionales en el SGC			01/06/2017	30/06/2017	4			
Hallazgo 5. Falta de políticas informáticas para la administración de cuartos de Comunicación.	La Escuela no cuenta con normas, políticas y procedimientos definidos y documentados para la administración y seguridad física e industrial de los cuartos de comunicación y de los elementos tecnológicos allí residentes	Imposibilidad de medir la gestión de la administración, control y seguridad física industrial de los cuartos de comunicación	Ingresos no autorizado e inadecuada administración de los centros de cableados.	Definir una política y su protocolo para administración y seguridad física de los centros de cableado.	Garantizar la administración y seguridad física de los centros de cableados	Actualizar el documento donde se plasmen las políticas y protocolo de Administración y seguridad física de los centros de cableado	1	1	05/06/2017	30/11/2017	25			
Hallazgo 6. Inadecuada seguridad física e industrial en los cuartos de comunicación.	Se observó al interior de los cuartos de comunicaciones: presencia de cajas de cartón, carpetas de papel, bolsas plásticas, muebles de madera, etc., elementos que no favorecen las condiciones de seguridad industrial, el sistema de cableado de datos (patinado de cables) de los racks, no se encuentran organizados etc. (Ver informe Definitivo de auditoria).	Condiciones de seguridad industrial inadecuada y no cumplimiento de estandares de seguridad en centros de cableado	Posible incendio	Se retirará de los cuartos técnicos de cableado los elementos inflamables como cajas de cartón, carpetas, bolsas plásticas entre otros	Minimizar los posibles riesgos de daño e interrupción en los equipos de red y servicios de comunicaciones.	Acta de registro de retiro de elementos inflamables para evitar riesgos de incendios y tomas fotográficas.	5	6	01/09/2017	30/09/2017	17			
		Falta de mantenimientos preventivos a los aires acondicionados Falta de aire acondicionado en centros de cableado sede Rosales.	Fallas e interrupción de los servicios Tic Pérdida y/o daños en los equipos TICs.	Realizar solicitud mediante oficio al área de infraestructura y mantenimiento para la adquisición y/o adecuación del aire acondicionado de los cuartos técnicos de sede CAN, rosales y lamaquito y su debido mantenimiento		Solicitud de adquisición y/o adecuación de aire acondicionado, mediante oficio formalizado por Active Document a Infraestructura y Mantenimiento con copia a la Subdirección Administrativa y Financiera.	1	2	01/06/2017	31/12/2017	30			
		Mal diseño en adecuaciones físicas iniciales de los centros de cableado.	Accesos no autorizados a los centros de comunicación Pérdida de equipos y elementos de comunicaciones. Inundación, humedad	Trasmitir ante los responsables los recursos para las adecuaciones físicas y organización de los centros de cableado en el presupuesto de la vigencia del 2018, resaltando la importancia que se requiere para dar cumplimiento a los estándares de seguridad física y lógica que requieren esta instalaciones		Solicitar la inclusión en el presupuesto del año 2018 a la subdirección administrativa y financiera, para realizar el mantenimiento preventivo y organización de centros de cableado	2	1	15/07/2017	31/12/2017	24			

Hallazgo 7. Falta de Lineamientos de Monitoreo y Control a la Infraestructura de TICs	No se evidenció la existencia de políticas, manuales e instructivos para el monitoreo, administracion, desempeño, capacidad y disponibilidad de la infraestructura tecnológica. La OSI no cuenta con una metodologia que describa las actividades que se ejecutan frente al monitoreo de la infraestructura de TICs, notificación de eventos criticos y emisión de informes. (Ver informe Definitivo de auditoria).	no existe procedimiento de monitoreo de la infraestructura tecnologica Falta de capacitación al personal OSI sobre herramientas de monitoreo de infraestructura tecnológica	Perdida de la trazabilidad en la administración de los recursos infraestructura tecnologica y sistemas de información Reaccion proactiva a eventos criticos	Incluir dentro del manual de la política de SGSI los controles, seguimientos de las, del monitoreo de la infraestructura de la TICs.	Mantener una adecuada trazabilidad de la administración de la infraestructura tecnologica y de los servicios TI	Documentar en el manual de la Politica de SGSI los controles seguimien tos de las actividades del monitoreo de la infraestructura TICs.	1	1	01/06/2017	31/12/2017	30			
				General reportes de seguimiento de la infraestructura tecnologica del almacenamiento competent, herramienta opem manage y caja de herradores		Informes tecnicos y ejecutivos sobre el funcionamiento de la infraestructura de TICs.	3	3	01/06/2017	31/12/2017	30			
Hallazgo 8. No se ejecutan pruebas de vulnerabilidad y ética Hackin a la infraestructura tecnológica	No se tienen pruebas de vulnerabilidad y Ética Hacking a la infraestructura tecnológica y plan de acción para subsanar las vulnerabilidades identificadas	No se han realizado pruebas de vulnerabilidad y ética Hacking a infraestructura tecnológica	Ataques informaticos a la plataforma tecnologica	Realizar las pruebas Pruebas de Vulnerabilidades y de Ethical Hacking	Ejecutar pruebas de Vulnerabilidad y Ethica Hacking sobre la plataforma tecnologica TICs	Informe Pruebas de Vulnerabilidad y Ethical Hacking Informe de retest	1	2	05/04/2017	30/11/2017	34			
Hallazgo 9. Documentacion física y/o electrónica incompleta en la implementación de Gobierno en Línea y Sistema de Gestión de Seguridad de la Información SGSI	En la revisión y evaluación a la información entregada, se observa la falta de una metodología que incluya un plan de trabajo y un cronograma, que permita realizar el seguimiento a las actividades ejecutadas	No existe una metodología que permita realizar seguimiento a las actividades ejecutadas de GEL y SGSI	Inadecuada administración de procesos y/o proyectos de TI Pérdida de confidencialidad, integridad y disponibilidad de la información	Organizar la información y soportes de los proyectos GEL según TRD establecidas para el proceso Gestión Tecnológica	Establecer una metodología que permita realizar seguimiento a las actividades ejecutadas de Proyecto GEL	Elaboración del plan de gestión del proyecto que incluye cronograma para la vigencia 2017	1	1	01/06/2017	15/12/2017	28			
				Organizar la información y soportes del proyecto SGSI según TRD establecidas para el proceso Gestión Tecnológica.	Establecer una metodología que permita realizar seguimiento a las actividades ejecutadas de Proyecto SGSI	Elaboración del plan de gestión del proyecto que incluye cronograma para la vigencia 2017	1	1	01/06/2017	15/12/2017	28			
Hallazgo 10. Falta de documentacion proyecto de implementación SINU	Como resultado de la revision efectuada a las actas de levantamiento de información en el repositorio del contrato, se evidenció que faltan formatos del "Levantamiento de información y definición de procesos" de acuerdo al compromiso definido en el acta de reunión (Ver tabla Informe Definitivo de auditoria).	Es un proceso que no depende de la Oficina de Sistemas e Informática y los usuarios se retrasan en el envio de la informacion	Falta de documentación soporte	Legalizar el acta con todos sus anexos en los terminos establecidos	Completar los formatos de levantamiento de información de todos los procesos de gestión académicos	Actas de levantamiento de información con sus respectivos anexos.	1	1	01/06/2017	31/07/2017	9			
Hallazgo 11. No existe una referenciación adecuada en los documentos del proyecto SINU	Se observó en el registro documental información duplicada, igualmente, la descripción de archivos no está estandarizada para facilitar la consulta	No estandarización de la información	Pérdida en la trazabilidad de la información, posibilidad de pérdida de la información	Organización de la información del proyecto SINU, de acuerdo con las TRD definidas para el proceso de gestión tecnológica	Disponer de información organizada para consulta del proyecto	Almacenamiento digital y físico de acuerdo a las TRD	1	1	01/06/2017	15/12/2017	26			
Hallazgo 12. Falta de contrato de soporte y mantenimiento de Sistema de Información SEVEN	La ESAP no dispone de un contrato de soporte y actualización del sistema de información SEVEN	La versión del sistema de información Seven que tiene la ESAP, no soporta los estandares tecnicos del manejo de la información de inventarios y activos fijos para soportar la aplicación de las NHF.	Inoperancia de los procesos por la obsolescencia de software Posibilidad de perdida de la información Incumplimiento en el registro de las operaciones contables de la información financiera de inventarios y activos fijos de acuerdo a las NIIF.	Tramitar ante los responsables los recursos en el presupuesto de la vigencia del 2017 que cubra el soporte y actualización del Sistema SEVEN y/o un nuevo sistema de información, resaltando la importancia que se requiere para dar cumplimiento a la aplicación de las NIIF	Contar con un software para el manejo de inventarios y activos fijos que soporten las NIIF	Solicitar la inclusión en el presupuesto del año 2017 a la subdirección administrativa y financiera, la aquisición y/o actualización de software para el manejo de inventarios y activos fijos que soporte el manejo de las NIIF,	1	1	01/06/2017	31/06/2017	4			
						Contrato ejecutado para el soporte y actualizacion del SEVEN y/o Sistema de información para el manejo de inventarios y activos fijos que soporten el manejo de las NIIF	1	1	01/06/2017	31/12/2017	17			
Hallazgo 13. No tiene una interfaz entre el sistema Active Document y PQRs	El sistema de Peticiones Quejas y Reclamos-PQRs, no está en interfaces con el sistema de gestion documental "Active Document", lo que implica que cuando se requiere subir un caso de una PQR en Active Document, sea necesario digitalizar nuevamente los documentos y el cargue de la información del caso.	No existe una interfaz entre el sistema de información PQRS y el sistema de gestión documental Active Document	Incumplimiento de la normatividad de atención al ciudadano a través de canales centralizados	Detallar el requerimiento de información para lograr integración de PQRS con Active Document	Especificar el requerimiento para integrar los sistemas.	Documento de especificación del requerimiento para la integración de los sistemas	1	1	01/07/2017	31/12/2017	26			
				Analizar la viabilidad del proceso de integración de los dos sistemas, teniendo en cuenta que active Document y PQRS es software no propietario de la ESAP.	Realizar un estudio de viabilidad para la integración del software y elaborar el plan de trabajo en caso de ser viable.	Estudio de viabilidad y plan de trabajo	1	1	01/11/2017	31/12/2017	9			
Nombre de Auditor	Alexandra Triviño Medina													
Cargo	Contratista Profesional Especializado Oficina de Control Interno													
Firma														