IDEAM

Instituto de Hidrología, Meteorología y Estudios Ambientales

INFORME AUDITORIA INTERNA INFOMÁTICA- PROCESO GESTIÓN DE RECURSOS INFORMATICOS Y TECNOLOGICOS

03/11/2016

TABLA DE CONTENIDO

Auditoría N° IAIOINF-2016-23		
Fecha		
Día	Mes	Año
17	11	2016

1. DATOS GENERALES

PROCESO AUDITADO	Proceso Gestión de recursos informáticos y tecnológicos		
TEMA:	Oficina Informática		
LIDER DE PROCESO	Leonardo Cárdenas Ch.	CARGO	Jefe Oficina Informática
AUDITOR RESPONSABLE DEL SEGUIMIENTO	Carlos Guevara	CARGO	Contratista

2. OBJETIVO.

Realizar auditoría integral al proceso de gestión de recursos informáticos y tecnológicos, evaluar normas, controles, técnicas y procedimientos que se tiene establecidos para conocer la situación actual de la entidad en cuanto a la infraestructura tecnológica y sus componentes.

3. ALCANCE.

La revisión consta de 4 Fases:
Fase 1. ESTRUCTURA ORGANIZACIONAL OFICINA INFORMÁTICA (Misión, Visión, políticas, procesos, procedimientos, niveles de servicio, contratos).
Fase 2. SOFTWARE Y HARWARE(O&M, sistemas de información, BD, derechos de autor, Inventarios, pruebas técnicas).
Fase 3. INFRAESTRUCTURA TECNOLÓGICA(O&M, Redes, Data center, pruebas técnicas).

Fase 4. SEGURIDAD (Lógica y Física, redes, software, BD, hardware, manejo información, backups, pruebas técnicas). Sep. 2015-Sep 2016.

4. CRITERIOS.

Atendiendo lo establecido en la Ley 87 de 1993, en la cual se define que en el proceso del control interno, se deben considerar: El esquema de la organización, el conjunto de los planes, métodos, principios, normas, procedimientos y los mecanismos de verificación y evaluación; los cuales se verifican a través de la auditoría Interna que realiza la Oficina de Control Interno a cada proceso; es así, que se constituye en la herramienta estratégica para el seguimiento y evaluación de los controles establecidos para el cumplimiento de los objetivos y compromisos de la Entidad.

En virtud de lo enunciado, la Oficina de Control Interno, planificó la auditoria a los procedimientos del Proceso gestión de recursos informáticos y tecnológicos, considerando entre otras las siguientes normas:
Constitución Política: Artículos 269, 209 NTC GP-1000: Norma Técnica de Calidad de la Gestión Pública Numeral 4.2, 6.1, 6.3, 7.4, 8.3, 8.4, Ley 87 de 1993,
Directiva Presidencial 01 del 25 de febrero de 1999(Derechos de autor)
Ley 1403 de 2010-La Ley 603 de 2000 (Derechos de autor)
Norma Iso 9001(capítulo 6.3 Infraestructura)
Decreto 2573 del 12 Dic 2014 (Gobierno en línea)
Ley 1712 de 2014(Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)
Decreto 415 de marzo 2016 (Plan estratégico de tecnologías de información y las comunicaciones
Norma ISO 27001(Seguridad de la información)
Iso 27033 (seguridad redes)
Norma ISO27002 (antes ISO 17799)(Norma internacional seguridad de la información)
Norma ANsi/Tia/Eia 568-B, ANsi/Tia/Eia 568-A (normas cableados estructurado)
Estándar IEEE 802.11(redes inalámbricas Wi-Fi)
Norma ANsi/Tia/Eia 606 (Estándar para la administración de telecomunicaciones de edificios comerciales)
Norma ANsi/Tia/Eia 607 (Estándar para instalaciones de puesta en tierra de telecomunicaciones a edificios comerciales)
Norma TIA 942(Data Center)
RETIE NORMA NTC 2050(Norma instalaciones eléctricas)
Circular 0006 11 de Febrero de 2016 Sobre liquidación de contratos de IDEAM.
Resolución 0390 15 Marzo de 2016
Ley 1581 de 2012
Plan de seguridad y privacidad de la información A-GI-M002

5. METODOLOGÍA Y DESARROLLO DE LA AUDITORIA.

Para el desarrollo de la presente auditoria se realizó la evaluación de los siguientes temas:

5.1 Acceso a los servicios de información

5.2 Soporte de subsistemas de información

5.3 Gestión de la seguridad de la información

5.4 Almacenamiento y respaldo

5.5 Registro de activos informáticos

5.6 Soporte mantenimiento de Hardware, software, bases de datos, redes.

5.7 Soporte e interventoría de bienes y servicios

5.8 Control de uso de licencias de software

5.9 Reubicación traslado de software

5.10 Seguridad física y del entorno

5.10.1 Aéreas seguras

5.11 Escritorios Limpios

5.12 Estructura de contingencia

5.13 Auditoria

5.14 Continuidad del negocio DCP

5.16 Contratos(233 de 2015 y 287/2015)

5.18 Pruebas técnicas

5.19 Infraestructura- Datacenter

5.20 Seguridad de la información

6. FORTALEZAS

6.1 El IDEAM cuenta con un Data center de última tecnología y cumple con standard TIA-942 (Telecomunicación Infrastructure Standard for Data Centers) además la entidad puede certificar este datacenter en un Nivel de Tier (es una certificación o "clasificación" de un Data Center en cuanto a su diseño, estructura, desempeño, fiabilidad, inversión y retorno de inversión). El datacenter cuenta con redundancia en infraestructuras mínimas como refrigeración, UPS o fuente alternativa de electricidad en caso de emergencia, cuenta con una disponibilidad de servicio del 99,671 %.

6.2 La oficina de Informática cuenta con un sistema de monitoreo el cual permite detectar las fallas en tiempo real presentadas en el Datacenter y poder dar solución oportuna a los inconvenientes presentados.

6.3 La oficina de informática está trabajando en la transición de IPV4 a IPV6 cuenta con los recursos para realizar esta labor.

6.4 La oficina informática adelanta trabajos con la consultoría GPPG ITACA arquitectura empresarial de TI para cumplir con el componente de gobierno en línea TIC para gestión - Arquitectura empresarial.

6.5 Buena disposición del equipo auditado para la atención de la auditoría y disposición de la información para consulta.

6.6 Actualización permanente de la infraestructura tecnológica.

7. OBSERVACIONES

7.1 Las entidades del estado, la oficina de tecnologías de información y comunicaciones debe ser una dependencia estratégica, las entidades tendrán que adecuar sus estructuras organizacionales de acuerdo con sus disponibilidades presupuestales (sin incrementar los gastos de personal) a fin de garantizar el posicionamiento de los líderes de las áreas de TI, en un cargo que dependa del máximo jefe de la respectiva entidad y garantizando su participación en el comité directivo de la misma, a efecto de que generen valor al desarrollo misional y estratégico de las entidades, y de los sectores del Estado. Es así, como las entidades estatales tendrán un Director de Tecnologías y Sistemas de Información responsable, entre otras asignaciones, de la planeación y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información y que deberá acogerse a los lineamientos que en la materia defina el MinTIC. Teniendo en cuenta que los decretos son nuevos, se deja como una observación que no hay incumplimiento, pero se genera la obligatoriedad de proceder a su implementación. Decreto 415 2016.

Observación: el Jefe de la oficina informática nos informa que tiene adelantos los estudios y presentados en su oportunidad a la Secretaria General, relacionados con el manual de funciones para el Jefe de la Oficina, basado en Decreto 415 de 2016.

7.2 Es importante se busque un mecanismo para disponer de forma oportuna los bancos de datos hidrológicos y meteorológicos del IDEAM y así lograr minimizar los tiempos de respuesta.

Observación: La oficina de informática se encuentra trabajando en función de disponer de los Datos de forma oportuna a través de procesos de reingeniería en el sistema de gestión de datos hidrológicos y meteorológicos y los mecanismos de interoperabilidad para el SIAC.

7.3 Se requiere fortalecimiento Humano para la oficina informática ya que la oficina maneja procesos de gran complejidad por tal razón se recomienda ampliar personal especializado en la oficina.

7.4 Se sugiere adelantar por parte de la oficina de informática pruebas de penetración ingeniería social, las cuales además de ser consideradas buenas prácticas permiten mitigar los riesgos y vulnerabilidades de hackeo a los cuales se ve abocada la entidad. Lo anterior evidenciado que dichas pruebas

se realizaron durante la vigencia 2011, lo cual se hace necesario se realicen estas pruebas. Iso 27001

7.5 De acuerdo al contrato No. 287/2015 se recomienda adelantar trámites pertinentes para la liquidación ante la oficina asesora Jurídica en el menor tiempo posible. Circular 0006 11 de Febrero de 2016.

7.6 De acuerdo al seguimiento a los sistemas de información misionales se realizó evaluación de flujo de información, procedimientos, desarrollo, compatibilidad y copias de respaldo, de los siguientes aplicativos:

- SISAIRE – SISTEMA DE INFORMACION DE LA CALIDAD DEL AIRE
- SNIF - SISTEMA NACIONAL DE INFORMACION FORESTAL
- SIUR – SISTEMA DEL USO DEL RECURSO “SUBDIRECCIÓN ESTUDIOS AMBIENTALES”
    - o RUA MANUFACTURERO
    - o RUA RESPEL
    - o RUA PCB
    - o RUA MERCURIO
- SIRH SISTEMA DE INFORMACION DEL REGISTRO HIDRICO

De acuerdo a la evaluación realizada los sistemas misionales cumple su grado de madurez con los protocolos de datos exigidos, cuenta con sus manuales técnicos, además existe en sistema de copias de respaldo y una empresa externa (TANDEM) que almacena la información brindando seguridad y tranquilidad para la entidad.

Se recomienda adelantar acciones e implementar mecanismos, los cuales permitan fortalecer el Sistema de información ambiental y lograr brindar apoyo y acompañamiento para sintonizar a las autoridades ambientales con el manejo y destreza del SIAC y de sus subsistemas.
La Resolución 1600 de 1994 por la cual se reglamenta parcialmente el Sistema Nacional Ambiental – SINA, *ARTICULO 2o. Dirección y coordinación del Sistema de Información Ambiental.*

De acuerdo a la evaluación de los aplicativos que se describen a continuación,

- SIORH SISTEMA DE INFORMACION PARA LA OPERACIÓN DE LA RED HIDROMETEOROLOGICA
- FQA – FISICO QUIMICA AMBIENTAL
- SISDHIM – SISTEMA DE INFORMACION HIDROMETEOROLOGICO BAJO UNIX.

Se observa debilidad en el manejo de la información ya que son aplicativos que requieren una reingeniería (Recupera información sobre el diseño de un programa existente y utiliza esta información para reestructurar o reconstruir el programa existente, con vistas a adaptarlo aun cambio, a ampliarlo o a mejorar su calidad general, con el objeto de conseguir una mayor facilidad de mantenimiento en el futuro) en el sistema de gestión de datos hidrológicos y meteorológicos esto con el fin de brindar a la entidad datos eficientes en tiempo real y mejorar las necesidades del negocio de la entidad.(Concordante con la observación 7.2)

8 OPORTUNIDADES DE MEJORA

8.1 HALLAZGO: De acuerdo a la información suministrada por la oficina informática, se evidencia que no se cuenta con un Plan estratégico de tecnologías de información y comunicaciones PETIC con vigencia 2016. El que se encuentra publicado, corresponde a la vigencia 2015. ANEXO PETIC V2 PERFILES PROYECTOS.
DECRETO 2573 Gobierno en línea.

De acuerdo a las buenas prácticas y las recomendaciones de Gobierno en línea en su componente TIC para la gestión se recomienda actualizar el plan estratégico TI (PETIC) que satisface el requerimiento del negocio de TI para sostener o extender los requerimientos de la entidad y la estrategia del negocio, al mismo tiempo que se mantienen los beneficios, costos y riegos el cual debe estar alineado con el plan estratégico de la entidad. Además de la actualización debe ser expuesto a aprobación por la alta dirección.

8.2 HALLAZGO: Dentro del Plan de seguridad y privacidad de la información del IDEAM A-GI-M002 V2, no se evidencian políticas de seguridad de la información del sitio web y protección datos personales de acuerdo a las disposiciones de la Ley 1581 de 2012.
Se recomienda generar una política de seguridad de la información del sitio web y protección datos personales, de acuerdo a lo dispuesto por la ley 1581 de 2012 y llevara a cabo la respectiva aplicación y socialización dentro de la entidad.

Observación: El jefe de la oficina informática nos informa que las políticas de Protección de datos personales es trasversal a varias dependencias de la entidad con las que se debe establecer los lineamientos de protección de datos personales.

8.3 HALLAZGO: Se evidencio niveles de seguridad bajos en la intranet, la cual permite acceder desde redes externa públicas generando vulnerabilidades al sistema. Resolución 0390 15 Marzo de 2016

Se recomienda ingresar políticas de seguridad a la intranet y minimizar los riegos y vulnerabilidades.

8.4 HALLAZGO: Se evidencio que el aplicativo PROACTIVANET no cuenta con todo el inventario de licencias de software y Hardware activo en la institución, no se evidencia un acta donde describa esta acción. Inventario de Software y Hardware desactualizado.

Se recomienda actualizar inventario de software y hardware en coordinación con el Grupo de servicios administrativos (Inventario y Almacén), tanto en el área central como en las áreas operativas.

8.5 HALLAZGO: La Oficina de Informática y el Grupo de servicios administrativos (Inventario y Almacén), no cuentan con un inventario de hardware y software debidamente conciliado que garantice cifras unificadas entre las dos dependencias. (Situación y hallazgo elevado en la Auditoria de Derechos de Autor, con plan de mejoramiento en ejecución)

Se recomienda realizar conciliación entre las dos áreas responsables, teniendo en cuenta que existe un plan de mejoramiento sobre el mismo hallazgo que se está ejecutando actualmente.

8.6 HALLAZGO: Área Operativa 11. De acuerdo a las Normas ANsi/Tia/Eia 568-B, ANsi/Tia/Eia 568-A, EIA / ECA 310E y ISO/IEC 14763-2 El Rack no cuenta con medidas de seguridad, no existe etiquetación en los patch cord ni en los dispositivos de red, el cableado se encuentra desorganizado.

Se recomienda cumplir la norma de estandarización ISO/IEC 14763-2 Buenas Prácticas de Planificación e Instalación.

Observación: La oficina informática adentro el levantamiento de la planimetría del cableado estructurado, para la construcción de laboratorio en donde se incluye esta intervención; Con ocasión al aplazamiento de la construcción del laboratorio de igual manera se postergo el tendido de cableado para el área operativa 11.

8.7 HALLAZGO: De acuerdo a las Normas ANsi/Tia/Eia 568-B, ANsi/Tia/Eia 568-A y ISO/IEC 14763-2 el cableado de los equipos terminales del edificio central no cuentan con la instalación correcta a la exigida por la normas de estandarización de instalaciones de cableado estructurado, además está violando la norma OHSAS *18001 en donde se* establece los requisitos mínimos de las mejores prácticas en gestión de Seguridad y Salud en el Trabajo.

Se recomienda cumplir la norma de estandarización ISO/IEC 14763-2 Buenas Prácticas de Planificación e Instalación.

8.8 HALLAZGO: Con el objeto de verificar el cumplimiento de la liquidación de los contratos suscritos por el Ideam y bajo la supervisión de la oficina informática, se tomó como muestra el contrato Número 233 de 2015, el cual, una vez revisado en el sistema de gestión documental Orfeo, se evidenció que el mismo fue liquidado por el supervisor del área de informática y remitidos a la oficina asesora Jurídica para su respectiva revisión y archivo; sin embargo, a la fecha dicha actividad no se ha llevado a cabo.
Se recomienda que la oficina asesora Jurídica se pronuncie respecto a estos contratos con el objeto de establecer si la liquidación cumple con los

requisitos legales o deben ser ajustados- Circular 0006 11 de Febrero de 2016.

Se recomienda a la oficina asesora Jurídica que para la revisión y liquidación de los contratos remitidos por los supervisores, con las actas de liquidación, se defina un término para resolver sobre la viabilidad de la liquidación o se devuelvan para los ajustes por parte de los supervisores.

9. SEGUIMIENTO A LOS PLANES DE MEJORAMIENTO SUSCRITOS.

Revisados los compromisos suscritos en los Planes de Mejoramiento, se evidenció que el Proceso Gestión de recursos informáticos y tecnológicos que continúan abiertos los siguientes Hallazgos:

PLAN DE MEJORAMINTO CONTRALORIA

9.1 H7A2.1 Cont. negocio: La falta de un Plan de Continuidad del Negocio y Recuperación ante Desastres que incluya la implementación de un Centro de Cómputo Alterno – CCA, se constituye en un riesgo para la continuidad de las operaciones de la entidad ante un eventual desastre.

Avance: 50%
Observación: Anexan memorando número 20161040002103 Se encuentra estudios previos en la oficina Jurídica. Queda pendiente a la implementación CCA. Ya que actualmente la Entidad cuenta con un riego para la continuidad de las operaciones.

9.2 H7A3.1 El plan de Recuperación ante Desastres fue elaborado en el 2012 por consultoría NewNet S.A. y realizando la evaluación no se evidencia actualización posterior ya que entre otros aspectos aún se tiene como sede principal de operaciones la Cra 10 # 20-30 Piso 9, en Bogotá. Este cambio de sede involucra una serie de ajustes tecnológicos que no están contemplados dentro del plan.
Avance: 50%
Observación: Anexan memorando número 20161040002103 Se encuentra

estudios previos en la oficina Jurídica. Queda pendiente a la implementación DRP.

9.3 H8A2 Riesgos tic: Además, examinando el Mapa de Riesgos del Plan Estratégico de las TIC, no se evidencia un tema asociado a las "Políticas de Seguridad de la Información" que formule la prevención de eventos que pongan en riesgo la seguridad de la información, y se pueda cruzar contra las acciones de Valoración, Prevención y Mitigación adoptadas por la entidad.
Avance:70%
Observación: Anexa Mapa de riesgos y acta de reunión. De acuerdo al Plan estratégico de tecnologías de información se requiere actualizarlo y relacionar "Políticas de Seguridad de la Información"

PLAN DE MEJORAMIENTO INTERNO

9.4 H1 El software desarrollado por el Instituto, no se encuentra incluido en los aplicativos de Propiedad, planta y equipo del Instituto.
Avance:10%
Observación: La coordinadora de Contabilidad envió oficio No. 20162040000841 de sep. 23 de 2016 solicitando concepto. No se ha recibido respuesta.

9.5 H2 Debilidades en la presentación y revelación de los Estados Financieros del Instituto al no incluirse los softwares desarrollados por la Entidad para el uso de su cometido estatal por lo que se podría manifestarse el riesgo de inexactitud en la Información presupuestal y financiera.
Avance:10%
Observación: La coordinadora de Contabilidad envió oficio No. 20162040000841 de sep. 23 de 2016 solicitando concepto. No se ha recibido respuesta.

9.6 H3. La Oficina de Informática no cuenta con un debido inventario de licencias de software utilizado en el Instituto; asimismo, no se tiene información debidamente conciliada con los registros del Grupo de Almacén e Inventarios que garanticen información y cifras unificadas en las dos dependencias.

Avance:0%

Observación: Actualmente la Oficina de Informática junto con la coordinación de recursos físicos está recopilando la información necesaria para la conciliación del inventario de software de la entidad. Luego de ello se procederá a redactar el procedimiento que dé continuidad a la conciliación de los inventarios. Como información adicional el funcionario asignado renunció al cargo a partir de 30-10-2016. Las evidencias aportadas no corresponden a la acción de mejoramiento y la descripción de las metas propuestas por la oficina informática.

9.7 H4. Se mantiene en custodia licencias y software que es susceptible de ser dado de baja.

Avance:0%

Observación: Se adelanta el proceso de conciliación, para: verificar los registros de software que figuran en el Almacén y determinar el software que debe ser dado de baja. Las evidencias aportadas no corresponden a la acción de mejoramiento y la descripción de las metas propuestas por la oficina informática.

9.8 H5. Continúan las diferencias entre los aplicativos SICAPITAL y PROACTIVANET respecto de la unificación de la información de los equipos de cómputo de la entidad.

Avance:0%

Observación: Se está realizando el levantamiento del inventario de equipos activos, aprovechando el proceso de mantenimiento preventivo de equipos de cómputo que finaliza el 31-10-2016. En el mes de noviembre 2016 se iniciará la conciliación con el Almacén. Las evidencias aportadas no corresponden a la acción de mejoramiento y la descripción de las metas propuestas por la oficina informática.

10. CONCLUSIONES

En términos generales el Proceso Gestión de recursos informáticos y tecnológicos cumple con el manejo de sus procesos. Producto de la auditoría realizada, se identificaron seis (6) Fortalezas, seis (6) Observaciones y ocho (8) oportunidades de mejora.

1. La Oficina de Informática presenta debilidades en el inventario de software y hardware.
2. La Oficina de Informática presenta fortalezas en la infraestructura tecnológica.
3. Detallar en el Plan de acción del PETIC las actividades puntuales que se van a ejecutar durante la vigencia y establecer las acciones a ejecutar con los objetivos específicos y estrategias del Plan estratégico de la oficina informática.

11. EVIDENCIAS

Todas las evidencias de la auditoria y del seguimiento se encuentran en la carpeta “AUDITORIA Y SEGUIMIENTO OFICINA INFORMATICA”

Nombre completo	Responsabilidad	Firma
Nombre: Carlos Guevara Cargo: Contratista	Auditor Líder	
Nombre: María Eugenia Patiño J. Cargo: Jefe Oficina OCI	Líder del Proceso	