IDEAM

Instituto de Hidrología,
Meteorología y
Estudios Ambientales

INFORME DE AUDITORÍA INTERNA AL SISTEMA QUE CONSOLIDA EL INVENTARIO NACIONAL DE EQUIPOS CONTAMINADOS CON BIFENILOS POLICLORADOS PCB

05/11/2021

TABLA DE CONTENIDO

Auditoría N° IAISIPCB-2021-48		
Fecha entrega informe		
Día	**Mes**	**Año**
5	11	2021

1. DATOS GENERALES

PROCESO(S) /ACTIVIDAD (ES) AUDITADO (S)	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		
LIDER(ES) DE PROCESO	ALICIA BARON LEGUIZAMÓN. CONSTANTINO HERNANDEZ	**CARGO**	Jefe de la Oficina de Informática. Subdirector de Estudios Ambientales (E).
AUDITOR LÍDER	EIDA RUTH MALDONADO OMEN	**CARGO**	Contratista Oficina de Control Interno

OBSERVADORES Y/O ACOMPAÑANTES.	

FECHA DE APERTURA AUDITORIA	07/10/2021
FECHA DE CIERRE DE LA AUDITORIA	15/10/2021

2. OBJETIVO DE LA AUDITORIA

Verificar los controles asociados al sistema que consolida el inventario nacional de equipos contaminados con bifenilos policlorados PCB.

3. ALCANCE DE LA AUDITORIA

La auditoría comprende el siguiente alcance:

1. Revisión de los controles asociados al proceso interno que lleva a cabo el Instituto a través del sistema PCB.
2. Revisión de los controles asociados al soporte y mantenimiento del sistema de información PCB.

4. DECLARATORIA

- Esta auditoría fue realizada con base en la consecución y análisis de información de un período específico, relacionada con el sistema de información PCB.

  Una consecuencia de lo anterior, es la presencia del riesgo de muestreo; es decir, el riesgo de que la conclusión basada en la muestra analizada, no coincida con la conclusión a que se habría llegado en caso de haber evaluado todos los elementos que componen la población; sin embargo, la muestra genera una alerta frente a los resultados obtenidos.

- Es responsabilidad del Líder de proceso el suministro y contenido de la información base del análisis del proceso de aseguramiento. La responsabilidad de la Oficina de Control Interno se circunscribe a producir un informe contentivo de los resultados de la auditoría ejecutada; las pruebas, procedimientos y análisis de la auditoría se practican de acuerdo con las normas legales vigentes de auditoría y las políticas y procedimientos formulados para el proceso de Evaluación y Mejoramiento Continuo/Oficina de Control Interno que se encuentran incluidos en el Sistema de Gestión Integrado del instituto.

- En caso, de que en el desarrollo de la auditoría se detecten asuntos no contemplados en el alcance y en los criterios de la misma, la Oficina de Control Interno tiene la obligación y el deber de informar a través del presente informe los hechos que puedan perjudicar el funcionamiento de la administración pública, de acuerdo con lo establecido en el numeral 25 del Artículo 34 de la Ley 734 de 2002, el cual determina los deberes de los servidores públicos; de igual forma, el Artículo 231 del Decreto-Ley 019 de 2012, en el que se estipula que el Jefe de la Oficina de Control Interno *"sin perjuicio de las demás obligaciones legales, deberá reportar a los organismos de control los posibles actos de corrupción e irregularidades que haya encontrado en ejercicio de sus funciones".*

  Así mismo, el literal c) del Artículo 2.2.21.4.9 del Decreto 648 de 2017 "informes", señala que "Los jefes de Control Interno o quienes haga sus veces deberán presentar los informes que se relacionan a continuación: … sobre actos de corrupción, directiva presidencial 01 de 2015, o aquella que la modifique, adicione o sustituya…".

  Complementariamente, el Artículo 67 del Código de Procedimiento Penal, señala que el servidor público que conozca de la comisión de un delito que deba investigarse de oficio, iniciará sin tardanza la investigación si tuviere competencia para ello; en caso contrario, pondrá inmediatamente el hecho en conocimiento ante la entidad competente.

5. CRITERIOS DE AUDITORÍA

- ✓ Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.
- ✓ Resolución 371 del 30/04/2021, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016".
- ✓ Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.
- ✓ Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018.
- ✓ Resolución 222 de 2011.
- ✓ Formato matriz de riesgos E-SGI-F006 v7 del 24/03/2021.
- ✓ Modelo Integrado de Planeación y Gestión - MIPG.

6. METODOLOGÍA Y DESARROLLO DE LA AUDITORIA INTERNA

6.1 METODOLOGÍA

Para la auditoría se ejecutaron las siguientes actividades:

1. Se toma como referencia para la ejecución de la auditoría el Procedimiento de Auditoría Interna C-EM-P001 versión 7.

2. Se efectuaron reuniones virtuales con la Ingeniera Alicia Barón, Jefe de Oficina de Informática, el Coordinador de Sistemas de Información, la Coordinadora del Grupo de Seguimiento a la Sostenibilidad del Desarrollo Subdirección de Estudios Ambientales, la Líder Técnico, la Líder funcional, la Ingeniera que tiene a cargo el soporte y mantenimiento del sistema, entre otros.

3. Se remitió mediante correo electrónico la solicitud de la información requerida para la auditoría.

4. Se hizo un análisis de la información recibida, con el fin de documentar las situaciones evidenciadas.

5. De otra parte, a través del desarrollo de la auditoría, se dieron a conocer los hallazgos a los Líderes de Proceso, al Coordinador de Sistemas de Información, la Coordinadora del Grupo de Seguimiento a la Sostenibilidad del Desarrollo Subdirección de Estudios Ambientales, la Líder Técnico, la Líder funcional, la Ingeniera que tiene a cargo el soporte y mantenimiento del sistema, entre otros. De

esta forma se garantizó el debido proceso y el derecho a la réplica.

La auditoría interna de gestión se desarrolló en el siguiente orden:

- ✓ **Anuncio de Auditoría**

Mediante comunicado Orfeo No. 20211030002893 del 7 de octubre del año en curso, se anunció el inicio de la auditoría y se entregó el programa de auditoría y el formato de "Carta de Representación" a los Líderes de proceso.

- ✓ **Reunión de Apertura**

Se realizó reunión virtual de apertura el 7 de octubre del 2021, con la presencia de la Ingeniera Alicia Barón, Jefe de Oficina de Informática, el Coordinador de Sistemas de Información, la Coordinadora del Grupo de Seguimiento a la Sostenibilidad del Desarrollo Subdirección de Estudios Ambientales, la Líder Técnico, la Líder funcional, la Ingeniera que tiene a cargo el soporte y mantenimiento del sistema, entre otros.

Se dio a conocer el objetivo y el alcance de la auditoría, así como el correspondiente programa, metodología a seguir, auditores, tiempos, entre otros aspectos relacionados con la ejecución de la auditoría. Se estableció la fecha de entrega de la información y en general se explicó la dinámica del ejercicio de la auditoria.

- ✓ **Recolección y análisis de Información**

Durante la planeación de la auditoría, se identificó la información a solicitar, con el fin de alcanzar los objetivos del ejercicio, lo cual se hizo correo corporativo del 7 de octubre de 2021.

También se tuvo en cuenta para el análisis, los siguientes documentados que se encontraron en el mapa de procesos de la página web de la entidad: Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, Resolución 371 del 30/04/2021, y Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018.

- ✓ **Reunión de Cierre**

Con el fin de socializar el resultado de la auditoria, se realizó una reunión virtual el día 15 de octubre de los corrientes. De esta manera, se dio oportunidad de controvertir los hallazgos y observaciones, para respetar el debido proceso y derecho de réplica.

- ✓ **Informe Final**

Junto con la entrega del Informe final de Auditoría por parte de la Oficina de Control Interno, se envía la formulación del Plan de Mejoramiento, el cual, se debe diligenciar en las condiciones y plazos de conformidad con el Procedimiento de Planes de Mejoramiento C-EM-P002 versión 08 de fecha 4 de

septiembre de 2020.

6.2 LIMITANTES DE LA AUDITORÍA

Ninguna.

6.3 RIESGOS IDENTIFICADOS

Durante el proceso de la Auditoría, se identificaron los siguientes riesgos:

1. Posibilidad de afectación económica y reputacional por consultas o modificaciones no autorizadas, debido a que el Instituto posee debilidades de control en lo referente a la administración de las contraseñas de acceso al sistema PCB.

2. Posibilidad de afectación económica y reputacional debido a que no se dispone de logs de auditoría que permita establecer la trazabilidad de las operaciones realizadas por los usuarios.

3. Posibilidad de afectación económica y reputacional por consultas o modificaciones no autorizadas, debido a que, en lo transcurrido del año en curso, se vienen realizando modificaciones de la información a través de la base de datos, y no a través del sistema PCB.

Los citados riesgos, no están identificados ni registrados en el Formato matriz de riesgos E-SGI-F006 versión 7 del 24/03/2021, proceso de Gestión TIC.

6.4. DESARROLLO DE LA AUDITORÍA

6.4.1. HALLAZGO 1. ADMINISTRACIÓN DE CONTRASEÑAS DE ACCESO AL SISTEMA

CONDICIÓN

Se identificaron las siguientes debilidades de control en relación con las contraseñas de acceso al sistema PCB:

1. Las contraseñas de acceso al sistema no validan la longitud, ni exige que estén compuestas por caracteres alfanuméricos, uso de mayúsculas, y de caracteres especiales tales como (@+*/&%$#", conforme lo establece el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.7.1.3. el cual cita:

   "La generación de contraseñas debe contener cierto grado de complejidad, por tal razón no se recomienda que contengan palabras comunes, o algún dato referente al titular de la cuenta de

usuario ejemplo, fechas de acontecimientos, nombres familiares, números de identificación entre otros.

- ✓ Tener mínimo 8 caracteres
- ✓ Caracteres en mayúsculas
- ✓ Caracteres en minúsculas
- ✓ Contener dígitos numéricos (0 a 9)
- ✓ Contener caracteres especiales (@+*/&%$#)"

2. Se evidenció que se informa por escrito las claves o contraseñas de acceso al sistema PCB, según se detalla a continuación:

   - ✓ El instituto, una vez le crea a cada una de las autoridades ambientales el usuario de acceso al sistema PCB, le remite mediante correo electrónico el usuario junto con la clave o contraseña de acceso al sistema.

   - ✓ De acuerdo con el "Manual de diligenciamiento cargue individual del inventario nacional de bifenilos policlorados PCB "que está dispuesto en la página Web del Instituto, una vez el propietario tramita en el sistema la solicitud para la creación de la cuenta de acceso, éste genera el usuario, la contraseña de acceso, y el modelo de la carta de inscripción, la cual también contiene el usuario y la contraseña de acceso al sistema.

     Posteriormente, el aplicativo le notifica mediante correo electrónico al representante legal, y al responsable del diligenciamiento, que la inscripción fue satisfactoria, e informa en esa comunicación, el usuario y la contraseña de acceso al sistema.

   - ✓ Para efectos de atención de determinadas solicitudes, el Ideam solicita el usuario y clave de acceso al propietario, a manera de ejemplo se cita el siguiente caso:

8/3/2021 Correo de IDEAM - INSTITUTO DE HIDROLOGÍA, METEOROLOGÍA Y ESTUDIOS AMBIENTALES - Actualización de Representante Le...

IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales

Anyela Andrea Villada Villada <avillada@ideam.gov.co>

Actualización de Representante Legal e Ingreso Transformador

Anyela Andrea Villada Villada <avillada@ideam.gov.co> 8 de marzo de 2021, 11:55
Para: Victor.Cardenas@weatherford.com

Cordial saludo,

Estimado Victor, atendiendo su requerimiento, amablemente me permito informar que es pertinente indicar el nombre de la Autoridad Ambiental a través de la cual realizó inscripción, así mismo el usuario y clave del propietario (Weatherford Colombia Limited) para realizar la respectiva gestión.

Quedo atento para atender su requerimiento.

[El texto citado está oculto]

Cordialmente,

El Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, cita: "Las credenciales de acceso a los sistemas de información y recursos de TI, son de carácter personal e intransferible, por tal razón su uso será responsabilidad del funcionario, contratista y/o proveedores a los que se les ha realizado formalmente la asignación."

3. No se tienen implementado un control automático para que el sistema PCB obligue al usuario a hacer el cambio de la contraseña cuando se loguea por primera vez.

   El Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, cita: "Una vez asignado los accesos a la plataforma tecnológica, en su primer inicio de sesión deberán cambiarse las contraseñas suministradas por la mesa de servicio."

4. No se tiene implementado el uso de algoritmos de encripción para proteger la contraseña de acceso al sistema.

   La resolución 371 del 30/04/2021, por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016, cita: "Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de cifrado para garantizar que no sea inapropiadamente descubierta, modificada."

Adicionalmente, la cláusula novena del contrato 464 suscrito con Impretics, refiere: "Velar por el cumplimiento de las políticas de seguridad con el fin de reducir el impacto de los incidentes de seguridad en la infraestructura tecnológica e información institucional, teniendo en cuenta los niveles de

funcionalidad aceptables para la gestión del IDEAM."

CRITERIOS HALLAZGO 1

1. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.
2. Resolución 371 del 30/04/2021, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016".
3. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.

HALLAZGO 1

Existen debilidades de control asociados a las contraseñas de acceso al sistema PCB, dado que no se valida la estructura de la contraseña de acceso, no se cuenta con un control automático para el cambio de la contraseña cuando el usuario se loguea por primera vez, no se manejan algoritmos de encripción y se comparten las contraseñas de acceso mediante correo electrónico corporativo, y en algunos casos, mediante el sistema de mesa de servicio Proactivanet.

Retroalimentación del Formato de reporte de hallazgo

Mediante correo electrónico del 02/11/2021, los Líderes de proceso dieron a conocer el Plan de mejoramiento respecto del hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004 Versión 1.0 del 02/04/2019, y, de otra parte, manifestaron lo siguiente:

"Con relación al numeral 3 del hallazgo se informa que en el documento E-GI-P001 PROCEDIMIENTO GESTIÓN DE ACCESO A SERVICIOS DE TI capítulo 5 Políticas Operacionales se indica la siguiente política: "Para los aplicativos que no tienen la funcionalidad de cambio de clave luego de su primer login, el envío de las credenciales se realizará vía correo al solicitante cumpliendo con la complejidad de la clave"".

Al respecto, la OCI recomendó evaluar la viabilidad de ajustar el citado procedimiento por cuanto la mencionada política no se encuentra alineada con el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, la cual cita "Una vez asignado los accesos a la plataforma tecnológica, en su primer inicio de sesión deberán cambiarse las contraseñas suministradas por la mesa de servicio."

6.4.2. HALLAZGO 2. LOGS DE AUDITORÍA DEL SISTEMA

CONDICIÓN

Según lo informado por la Oficina de Informática en reunión sostenida el 12/10/21, no se dispone de logs de auditoría del sistema de información PCB.

Al respecto, la Resolución 371 del 30/04/2021 cita: "ARTÍCULO 20. Auditoría: Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para el Instituto, tales como los sistemas de información en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones, deben generar registros electrónicos o bitácoras, que permitan disponer de pistas que faciliten la ejecución de auditorías tanto a los procesos de los sistemas informáticos, como de las afectaciones a sus datos. Todos los archivos de registro deben proporcionar información suficiente para apoyar el monitoreo y control.".

Así mismo, el numeral 5.13 del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, cita "La oficina de informática deberá generar registros de auditoría (logs) que permitan verificar y revisar eventos que puedan comprometer la seguridad de la información en los servicios de tecnología y sistemas de información."

De otra parte, la Cláusula novena del contrato interadministrativo 464 suscrito entre el Instituto e Impretics refiere "…g) Velar por el cumplimiento de las políticas de seguridad con el fin de reducir el impacto de los incidentes de seguridad en la infraestructura tecnológica e información institucional, teniendo en cuenta los niveles de funcionalidad aceptables para la gestión del IDEAM."

CRITERIOS HALLAZGO 2

1. Resolución 371 del 30/04/2021, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016"
2. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.13.
3. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.

HALLAZGO 2

El sistema de información PCB carece de logs de auditoría; es decir, que no es viable conocer, a través del sistema, la trazabilidad de los cambios efectuados en el sistema, como, por ejemplo, qué dato fue modificado o eliminado, cuál dato estaba anteriormente, quién realizó el cambio, desde qué equipo se efectuó, fecha y hora de la operación.

Retroalimentación del Formato de reporte de hallazgo

Mediante correo electrónico del 29/10/2021, la Oficina de Informática informó que acepta el hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004, versión 1.0 del 02/04/2019.

6.4.3. HALLAZGO 3. DEBILIDADES DE CONTROL RELACIONADAS CON LA ATENCIÓN DE LOS REQUERIMIENTOS

CONDICIÓN

Para dar solución a algunas de las solicitudes relacionadas con el sistema PCB, durante lo transcurrido del presente año, se vienen haciendo ajustes directamente sobre la base de datos, en lugar de implementar correctivos o ajustes en el sistema PCB. Si bien, en la reunión sostenida el 12/10/21, y de acuerdo con la documentación asociada a los requerimientos gestionados entre el 15/09/21 y el 14/10/21, se evidenció que los citados cambios se documentan a través de los formatos de Actas de pruebas de aceptación E-GI-F020, versión 03 del 05/04/2018, la realización de este tipo de cambios a través de base de datos conlleva riesgos para el instituto, porque podrían generarse modificaciones no autorizados, bien sea por errores humanos o de manera intencional.

Es por esa razón que, en caso de ser necesario realizar este tipo de cambios, es conveniente que primero se formalice y se institucionalice en el SGI el respectivo marco procedimental.

Para mayor claridad, a continuación, se relacionan algunos de los cambios que han sido gestionados a través de bases de datos:

a. Eliminación de equipos duplicados: Correo remitido a la Corporación Autónoma Regional de Cundinamarca CAR, el 16 de febrero de 2021, y correo remitido a CVC, en relación con Ingenio Mayagüez, el 31 de mayo de 2021.

b. Reapertura de períodos de balance:

   Respuesta Orfeo No. 20219050013812 CAR, del 15/02/21, cita "…me permito informarle que la incidencia que se presentó con el Inventario Nacional de PCB con respecto a la apertura de balance 2017 y la migración de equipos ya fue resuelta, por lo cual le invito a ingresar de nuevo al aplicativo y continuar con la gestión de información de los equipos y desechos de su propiedad…".

   Correo remitido a CARSUCRE, del 11/05/21, cita: "…con relación a su requerimiento de actualizar la información del equipo en estado desechado a estado en uso sobre el PB 2013 conforme los

datos suministrados del propietario HOTELES ARAWAK DE COLOMBIAS.A.S. con NIT 91269464; éstos ya fueron efectuados. En conclusión, quedaron actualizados para dicho propietario los PB 2012 y2013".

Correo remitido a la CAR, del 13/05/21, cita: "... me permito informarle que a partir de la verificación de los datos suministrados de la razón social Flores el Aljibe S.A.S con NIT 800227103, se realizó la actualización del mismo; en donde se elimina periodo de balance PB 2014 y se apertura PB 2013. Por lo cual. se invita a verificar dicha información y comunicar al usuario, para que realice la debida actualización y cierre de formato antes del 30 de junio."

Correo remitido a la CAR, del 13/05/21, cita: "... me permito informarle que a partir de la verificación de los datos suministrados de la razón social ATC SITIOS DE COLOMBIA S.A.S con NIT 900377163, se realizó la actualización del mismo; en donde se elimina periodo de balance PB 2013 y se apertura PB 2012. Por lo cual, se invita a verificar dicha información y comunicar al usuario, para que realice la debida actualización y cierre de formato antes del 30 de junio."

Correo remitido a la CAR, del 25/0521, cita: ".. de acuerdo con tu solicitud relacionada con la empresa Emgesa S.A. E.S.P con NIT 860063875, acerca de aperturar periodo de balance 2019, me permito informar que dicha actualización ya fue realizada. Por lo cual se invita a validar lo anterior e informar al propietario para que continúe con el diligenciamiento."

Correo remitido a alianzateam, del 08/07/21, cita: "…se da apertura al periodo de balance 2019. Por lo cual, le invitamos ingresar al aplicativo para continuar con la actualización y diligenciamiento de la información realizando cierre periodos de balance 2019 y 2020.

De otra parte, en reunión efectuada el 12/10/21, la Oficina de Informática manifestó que en lo transcurrido del año en curso no se han implementado mejoras o ajustes en el sistema de información PCB, dado que desde enero del 2020 se está trabajando en un proceso de reingeniería del sistema, el cual se tiene previsto terminar en el año 2022. El levantamiento de requerimientos fue evidenciado a través de las siguientes historias de usuario:

- Iniciar sesión.
- Activar usuario.
- Revisar - Trasmitir formato.
- Reporte de novedad.
- Consulta general.
- Indicadores.
- Sábana de información.

- Notificaciones.
- Encriptar contraseña.
- Consultar log de auditoría.

Se observó que ninguna de las historias de usuario ha sido firmadas, y algunas de esos documentos están en proceso de construcción.

Para construir sistemas de información, o para hacer ajustes los mismos, el Instituto tiene establecido el Procedimiento de construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018, cuyo objetivo es "Establecer la secuencia de actividades para adelantar las fases de: análisis, diseño, construcción e implementación de herramientas de software misionales (alfanuméricos y SIG) y de apoyo, para nuevos componentes o manteniendo evolutivo de sistemas de información del IDEAM", sobre el cual se identificaron las siguientes debilidades de control:

El citado procedimiento no refiere tiempos para la ejecución de las actividades, no menciona cuál es la metodología de desarrollo de software que se debe seguir, ni indica bajo cuáles condiciones se podrían efectuar cambios a la información mediante acceso directo a la base de datos (o mediante ejecución de scripts), tales como:

- Cómo se documentan esos cambios.
- Quién autoriza esos cambios.
- Criterios de aceptación de los cambios.
- Tiempo máximo de tolerancia.
- Controles que se deben implementar.

CRITERIOS HALLAZGO 3

1. Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, versión 05 del 05/04/2018.
2. Solicitudes relacionadas con el sistema PCB.

HALLAZGO

Debilidades de control relacionadas con la atención de los requerimientos cuya solución involucra modificaciones en la información registrada en el sistema PCB, toda vez que en lo transcurrido del año en curso se vienen realizando ajustes directamente sobre la base de datos.

Retroalimentación del Formato de reporte de hallazgo

Mediante correo electrónico del 02/11/2021, los Líderes de proceso dieron a conocer el Plan de mejoramiento respecto al hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004 Versión 1.0 del 02/04/2019. En relación con el citado Plan, la OCI recomienda evaluar la viabilidad de hacer ajustes al Procedimiento de construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018, teniendo en cuenta lo referido en la sección "Condición".

7. FORTALEZAS

En el proceso de auditoría, fueron detectadas las siguientes fortalezas:

Disposición del personal de las áreas auditadas.

8. HALLAZGO Y OBSERVACIONES DETECTADAS

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
X		**HALLAZGO Nro. 1. ADMINISTRACION DE CONTRASEÑAS DE ACCESO AL SISTEMA** Existen debilidades de control asociados a las contraseñas de acceso al sistema PCB, dado que no se valida la estructura de la contraseña de acceso, no se cuenta con un control automático para el cambio de la contraseña cuando el usuario se loguea por primera vez, no se manejan algoritmos de encripción y se comparten las contraseñas de acceso mediante correo electrónico corporativo, y en algunos casos, mediante el sistema de mesa de servicio Proactivanet. CRITERIOS	1. Dar cumplimiento a lo dispuesto en la Resolución 371 del 30/04/2021, en el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, y a la Cláusula novena del contrato 464 de 2020 suscrito con Impretics. 2. Fortalecer los controles asociados a la administración de contraseñas de acceso del sistema.

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		1. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021. 2. Resolución 371 del 30/04/2021, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016". 3. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.	
X		**HALLAZGO Nro. 2. LOGS DE AUDITORÍA DEL SISTEMA** El sistema de información PCB carece de logs de auditoría, es decir que no es viable conocer, a través del sistema, la trazabilidad de los cambios efectuados en el sistema, como, por ejemplo, qué dato fue modificado o eliminado, cuál dato estaba anteriormente, quién realizó el cambio, desde qué equipo se efectuó, fecha y hora de la operación. CRITERIOS 1. Resolución 371 del 30/04/2021, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, se definen lineamientos frente al uso y manejo	Dar cumplimiento a lo dispuesto en la Resolución 371 del 30/04/2021, en el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, y a la Cláusula novena del contrato 464 de 2020 suscrito con Impretics.

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		de la información y se deroga la Resolución No. 0390 del 15 de marzo del 2016" 2. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.13. 3. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.	
X		**HALLAZGO Nro. 3. DEBILIDADES DE CONTROL RELACIONADAS CON LA ATENCIÓN DE LOS REQUERIMIENTOS** Debilidades de control relacionadas con la atención de los requerimientos cuya solución involucra modificaciones en la información registrada en el sistema PCB, toda vez que en lo transcurrido del año en curso se vienen realizando ajustes directamente sobre la base de datos. CRITERIOS 1. Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, versión 05 del 05/04/2018. 2. Solicitudes relacionadas con el sistema PCB.	1. Evaluar la conveniencia de hacer ajustes al Procedimiento de construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, versión 05 del 05/04/2018. 2. Evaluar la conveniencia de implementar los ajustes al sistema de manera paralela al levantamiento de requerimientos, según la priorización que se establezca de manera conjunta con el área usuaria responsable del proceso.

Notas:

- Para las auditorias de gestión, el Hallazgo (H) corresponde al incumplimiento de un criterio.
- Para las auditorias de calidad el incumplimiento de un criterio se determinará como una No Conformidad (NC).

- Tanto los Hallazgos como las No Conformidades y las Observaciones (OBS) identificadas requieren Plan de Mejoramiento.

9. CONCLUSION

Describir de manera breve los aspectos a rescatar de la auditoría Interna y/o los cambios que afecte a la organización

Es necesario dar prioridad a fortalecer el nivel de seguridad del sistema BCP. Así como el seguimiento para verificar el cumplimiento de las políticas de seguridad establecidas por el Instituto.

AUTORIZACIÓN PARA COMUNICAR ESTE INFORME:

En cumplimiento del parágrafo 1° del Artículo 2.2.21.4.7 del Decreto 648 de 2017 "Relación administrativa y estratégica del Jefe de Control Interno o quien haga sus veces", el presente informe tendrá como destinatario principal al representante legal del Instituto y al líder del proceso auditado. A través del Comité Institucional de Coordinación de Control Interno, se dará a conocer los resultados de las auditorías a los miembros de esta instancia.

Así mismo y en cumplimiento de la Ley 1712 de 2014, este informe se publicará en la página web del Instituto-Ley de Transparencia.

Nombre completo	Responsabilidad	Firma
Eida Ruth Maldonado Omen Cargo: Contratista OCI	Auditor Líder	
Alicia Barón Leguizamón Cargo: Jefe Oficina de Informática	Líder del proceso	
Constantino Hernández Cargo: Subdirector de Estudios Ambientales (E).	Líder del proceso	

10. EVIDENCIAS FOTOGRÁFICAS

No aplica.

11. CONTROL DE APROBACIÓN INFORME DE AUDITORÍA INTERNA

CONTROL INFORME DE AUDITORÍA INTERNA		
ELABORÓ: **Eida Ruth Maldonado Omen** Cargo: Contratista OCI	**REVISÓ:** **María Eugenia Patiño Jurado** PATIÑO JURADO MARIA EUGENIA Jefe Oficina Control Interno	**APROBÓ:** **María Eugenia Patiño Jurado** Firmado digitalmente por PATIÑO JURADO MARIA EUGENIA Fecha: 2021.11.08 11:23:14 -05'00' Jefe Oficina Control Interno

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1	30/10/2012	Creación del documento
2	19/11/2014	Revisión y ajustes identificados en el desarrollo de la autoevaluación del proceso.
3	05/12/2014	Revisión y ajustes identificados en el desarrollo de la autoevaluación del proceso.
4	27/04/2015	Revisión y ajustes identificados en el desarrollo de la autoevaluación del proceso, en donde se suprime el ítem de recomendaciones.
5	29/09/2017	Revisión y ajustes identificados en el desarrollo de la autoevaluación del proceso.
6	11/12/2019	Revisión y ajustes identificados en el desarrollo de la autoevaluación del proceso.
7	27/04/2020	Se incluye el numeral 11 “Control De Aprobación Del Informe De Auditoría Interna”; con el texto "Elaboró-Revisó-Aprobó"

MEPJ-ERMO-08-11-2021

ELABORÓ:	REVISÓ:	APROBÓ:
MÓNICA ROCÍO CASTRO SÁNCHEZ **PROFESIONAL OFICINA DE CONTROL INTERNO** **JAIME HUMBERTO LA ROTTA** **PROFESIONAL OFICINA DE CONTROL INTERNO**	**MARÍA EUGENIA PATIÑO JURADO** **JEFE OFICINA CONTROL INTERNO**	**MARÍA EUGENIA PATIÑO JURADO** **JEFE OFICINA CONTROL INTERNO**