



**IDEAM**

Instituto de Hidrología,  
Meteorología y  
Estudios Ambientales

**INFORME DE AUDITORÍA  
INTERNA A LA GESTION DE  
BASES DE DATOS**

**08/10/2021**

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 2 de 31

## TABLA DE CONTENIDO

1.	DATOS GENERALES .....	3
2.	OBJETIVO DE LA AUDITORIA .....	3
3.	ALCANCE DE LA AUDITORIA .....	3
4.	DECLARATORIA .....	4
5.	CRITERIOS DE AUDITORÍA .....	4
6.	METODOLOGÍA Y DESARROLLO DE LA AUDITORIA INTERNA .....	5
7.	FORTALEZAS .....	22
8.	HALLAZGO Y OBSERVACIONES DETECTADAS.....	22
9.	CONCLUSION .....	27
10.	EVIDENCIAS FOTOGRÁFICAS .....	27
11.	CONTROL DE APROBACIÓN INFORME DE AUDITORÍA INTERNA .....	27
12.	CONTROL DE CAMBIOS .....	28

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 3 de 31

<b>Auditoría N° IAIGBDD-2021-42</b>		
<b>Fecha entrega informe</b>		
<b>Día</b>	<b>Mes</b>	<b>Año</b>
08	10	2021

### 1. DATOS GENERALES

<b>PROCESO(S) /ACTIVIDAD (ES) AUDITADO (S)</b>	GESTIÓN DE TECNOLOGIAS DE IIFORMACION Y COMUNICACIONES		
<b>LIDER(ES) DE PROCESO</b>	ALICIA BARON LEGUIZAMÓN.	<b>CARGO</b>	Jefe de la Oficina de Informática.
<b>AUDITOR LÍDER</b>	EIDA RUTH MALDONADO OMEN	<b>CARGO</b>	Contratista Oficina de Control Interno

<b>OBSERVADORES Y/O ACOMPAÑANTES.</b>	


<b>FECHA DE APERTURA AUDITORIA</b>	30/08/2021
<b>FECHA DE CIERRE DE LA AUDITORIA</b>	10/09/2021

### 2. OBJETIVO DE LA AUDITORIA

Verificar aspectos relacionados con la administración de usuarios de bases de datos del ambiente productivo del Instituto.
--

### 3. ALCANCE DE LA AUDITORIA

La auditoría comprende el periodo de junio a julio de 2021, y se enfoca en:
1. Verificación de la efectividad de los controles asociados a la administración de usuarios de bases de

 <p><b>IDEAM</b> Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 4 de 31

datos.

2. Revisión de los usuarios que tienen privilegios de DBA en las bases de datos de los sistemas críticos.

#### 4. DECLARATORIA

- Esta auditoría fue realizada con base en la consecución y análisis de información relacionada con la Administración de las bases de datos.
- 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.

- ✓ Contrato 464 de 2020 suscrito entre el IDEAM e IMPRETICS.
- ✓ Procedimiento gestión de acceso a servicios de TI, E-GI-P001 del 11/09/2020.
- ✓ Formato matriz de riesgos E-SGI-F006 v7 del 24/03/2021.
- ✓ Modelo Integrado de Planeación y Gestión - MIPG.
- ✓ 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"
- ✓ Formato solicitud de base de datos E-GI-F023, versión 02 del 05/04/2018.
- ✓ Y las demás normas que sean concordantes, coincidentes y complementarias.

## **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 Sistema de Información, el Administrador de bases de datos, el Gerente de Proyecto, el Oficial de seguridad, entre otros.
3. Se remitió mediante correo electrónico del 29/08/21, la solicitud de la información requerida para la auditoría.
4. Se hizo un análisis de la información asociada al contrato y 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 la Líder de Proceso, al Coordinador de Sistema de Información, al Administrador de bases de datos, al Gerente de Proyecto, al Oficial de seguridad, entre otros Ingenieros que participan en el proceso. 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. 20211030002473 del 27 de agosto del 2021, se anunció el inicio de la auditoría y se entregó el programa de auditoría y el formato de “Carta de Representación” a la Líder del proceso auditado.

✓ **Reunión de Apertura**

Se realizó reunión virtual de apertura el 30 de agosto del 2021, con la presencia de la Jefatura de Oficina de Informática, el Coordinador de Sistema de Información, el Administrador de bases de datos, el Gerente de Proyectos, y el Oficial de seguridad.

Se presentó al auditor Líder, se dio a conocer el objetivo y el alcance de la auditoría, así como el correspondiente programa y metodología a seguir. Se estableció la fecha de entrega de la información y en general se explicó la dinámica del ejercicio de la auditoría.

✓ **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 a través de correo corporativo. 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, Procedimiento gestión de acceso a servicios de TI, E-GI-P001 del 11/09/2020, y el Formato de solicitud de base de datos E-GI-F023, versión 02 del 05/04/2018.

✓ **Reunión de Pre Cierre**

Con el fin de socializar el resultado de la auditoría, se realizaron reuniones virtuales el 2 y el 7 de septiembre de 2021 con la Líder del proceso, y algunos de los Ingenieros de la Oficina de Informática e IMPRETICS. Se dio oportunidad de controvertir los hallazgos y observaciones, para respetar el debido proceso y derecho de réplica, con la finalidad de llegar a la reunión de cierre con los hallazgos decantados y conciliados.

✓ **Reunión de Cierre**

Con el fin de socializar el resultado de la auditoría, se realizó una reunión virtual el día 10 de septiembre de 2021 con la Líder del proceso y algunos de los Ingenieros de la Oficina de Informática e IMPRETICS. 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 reputacional por accesos no autorizados a las bases de datos del Instituto debido a que no se dispone de manuales y/o procedimientos que apoyen la implementación de las políticas de seguridad asociadas a la administración de usuarios de bases de datos.
2. Posibilidad de afectación reputacional por no contar con el Manual de políticas de seguridad de la información actualizado en el Sistema de Gestión Integrado SGI debido a debilidades de control asociadas a su publicación.
3. Posibilidad de afectación económica y reputacional debido a la carencia de información que permita establecer la trazabilidad de las operaciones realizadas por los usuarios de bases de datos.
4. Posibilidad de afectación económica y reputacional por consultas o modificaciones no autorizadas en las bases de datos, debido a que el Instituto posee debilidades de control en lo referente a la administración de los usuarios de bases de datos.
5. Posibilidad de afectación reputacional por debilidades de control asociados a la identificación de los sistemas críticos del Instituto.

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. MANUALES, PROCEDIMIENTOS Y FORMATOS QUE RIGEN LA ADMINISTRACION DE USUARIOS DE BASES DE DATOS**

#### **CONDICIÓN**

1. El Instituto no tiene establecido un procedimiento que contemple la administración de usuarios de bases de datos.

El numeral 5.7.1.2 del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0

del 18/05/2021, cita: “La oficina de informática definirá un procedimiento formal para el acceso a los servicios de TI institucionales, así mismo los lineamientos para la creación de cuentas de usuario del dominio ideam.gov.co.” (Subrayado fuera de texto). Es de anotar que el Instituto dispone del procedimiento gestión de acceso a servicios de TI, E-GI-P001 del 11/09/2020, pero éste únicamente aplica para la administración de usuarios de los sistemas de información y de los procesos básicos, tales como directorio activo, correo electrónico servicio de impresión.

2. El Instituto tiene institucionalizado en el SGI, el Formato solicitud de base de datos E-GI-F023 Versión 02 del 05/04/2018, sobre el cual se identificaron las siguientes debilidades de control:

- El formato está delimitado, por cuanto refiere que es para “Solicitar creación y/o asignación de roles en aplicación”, y además, está concebido para que lo diligencien únicamente los Líderes Técnicos. Sin embargo, las bases de datos del ambiente productivo no necesariamente están asociadas a sistemas de información.

Además, se debe tener en cuenta que el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, cita: “La inactivación, modificación y retiro de los privilegios de acceso deberán formalizarse mediante una solicitud a través de la mesa de servicios y ser remitida por los jefes de oficina, subdirectores o coordinadores de grupo de las dependencias...”

- Con base en el seguimiento efectuado a las solicitudes asociadas a administración de usuarios de bases de datos, para el período evaluado, se evidenció que los Líderes Técnicos no anexan el citado formato a través de la mesa de servicio, a pesar de que éste refiere: “Una vez este diligenciado el formato debe anexarse y enviarse a través de la mesa de ayuda (Sistema GLPI), diligenciándola y seleccionando:”. Si bien, el texto antes citado refiere el sistema de mesa de ayuda GLPI, en lugar de ProactivaNet, que es el que usa actualmente, se debe hacer uso del formato toda vez que éste se encuentra vigente en el SGI.
- El formato en mención es referenciado en el Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, versión 05 del 05/04/2018, el cual en la actividad 5 refiere lo siguiente:

ACTIVIDAD	RESPONSABLE	REGISTRO
Gestión para obtención de la cuenta de usuario de dominio, base de datos, correo institucional, servidor de versiones, geodatabase, metadatos, geoservicios, acceso VPN en ambiente de pruebas y/o desarrollo.	Funcionario y/o contratista responsable por las actividades de liderazgo técnico y/o Administración del sistema.	Correos electrónicos remitiendo datos de conexión, usuarios y claves. Formato de solicitudes de base de datos.



Fuente: Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018

Según se observa en la última columna, los “datos de conexión, usuarios y claves” son remitidos vía correo electrónico, por lo que existe un grado de vulnerabilidad, máxime porque el Instituto no tiene implementado un control automático para que se obligue a los usuarios a hacer el cambio de la contraseña cuando se loguea por primera vez a la base de datos, según prueba realizada con la bases de datos Dhime e Idema11pr.

Al respecto, 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.”

Para mayor claridad, se sugiere ver Anexo 1 del presente informe.

Respecto a los dos puntos descritos anteriormente, se resalta que la Cláusula novena, obligaciones específicas del contrato interadministrativo 464 suscrito con Impretics, en el numeral Seguridad de la Información y Continuidad, 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 1**

1. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.7.1.2.
2. Procedimiento gestión de acceso a servicios de TI, E-GI-P001 del 11/09/2020.
3. Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018.
4. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena, ítem g.
5. Formato solicitud de base de datos E-GI-F023, versión 02 del 05/04/2018.

### **HALLAZGO 1**

No se cuenta con manuales y/o procedimientos que apoyen la implementación de las políticas asociadas a la administración de usuarios de bases de datos. De otra parte, no se utiliza el Formato solicitud de base de datos E-GI-F023 Versión 02 del 05/04/2018, el cual se encuentra institucionalizado a través del Sistema de Gestión Integrado SGI.

### **Retroalimentación del Formato de reporte de hallazgo**

Mediante correo electrónico del 21/09/2021, 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. Así mismo, el Plan de mejoramiento propuesto, fue aceptado.

#### 6.4.2. OBSERVACION 1. DEBILIDADES DE CONTROL EN LA PUBLICACION DEL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

##### CONDICIÓN

1. La Oficina de Informática mediante correo del 20/05/21 solicitó a la OAP la publicación del Manual de políticas de seguridad de la Información, versión 2.0 del 20/05/21, según se observa en el anexo 1 del presente informe.

Al respecto, no fue posible evidenciar en qué fecha la OAP informó a la OI que la publicación del manual fue atendida, en razón de que el soporte que facilitó la OAP no corresponde, dado que el correo tiene fecha anterior a la solicitud de publicación, 18/05/21, y adicionalmente, ese soporte refiere que “El documento fue publicado...”, y no menciona de manera explícita el Manual de políticas de seguridad de la Información. Para mayor claridad, ver anexo 2 del presente informe.

De acuerdo con el Listado maestro de documentos, la fecha a partir de la cual empieza la vigencia del documento es el 18/05/2021, la cual coincide con la fecha que aparece en la parte superior del manual, y con el historial de cambios del documento:

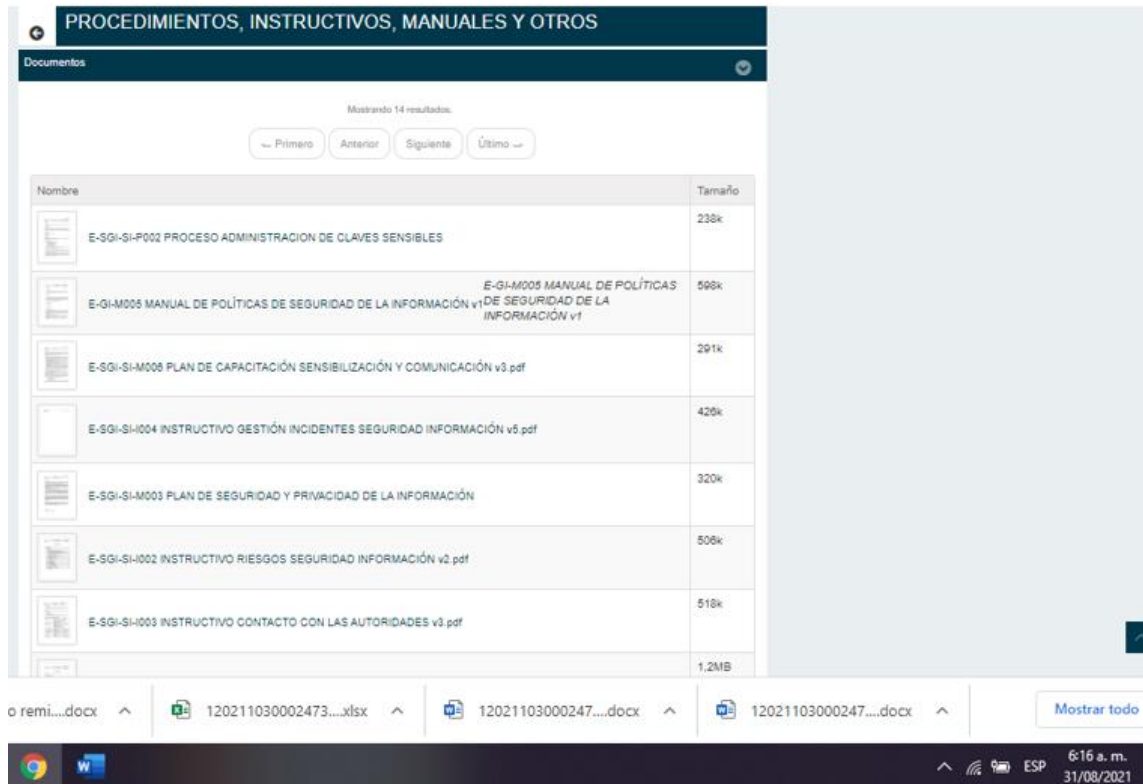
<p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<p><b>MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION</b></p>	Código: E-GI-M005
		Versión: 2.0
		Fecha: 18/05/2021
		Página: 1 de 72

Fuente: Print screen tomado al Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.

**6. HISTORIAL DE CAMBIOS**

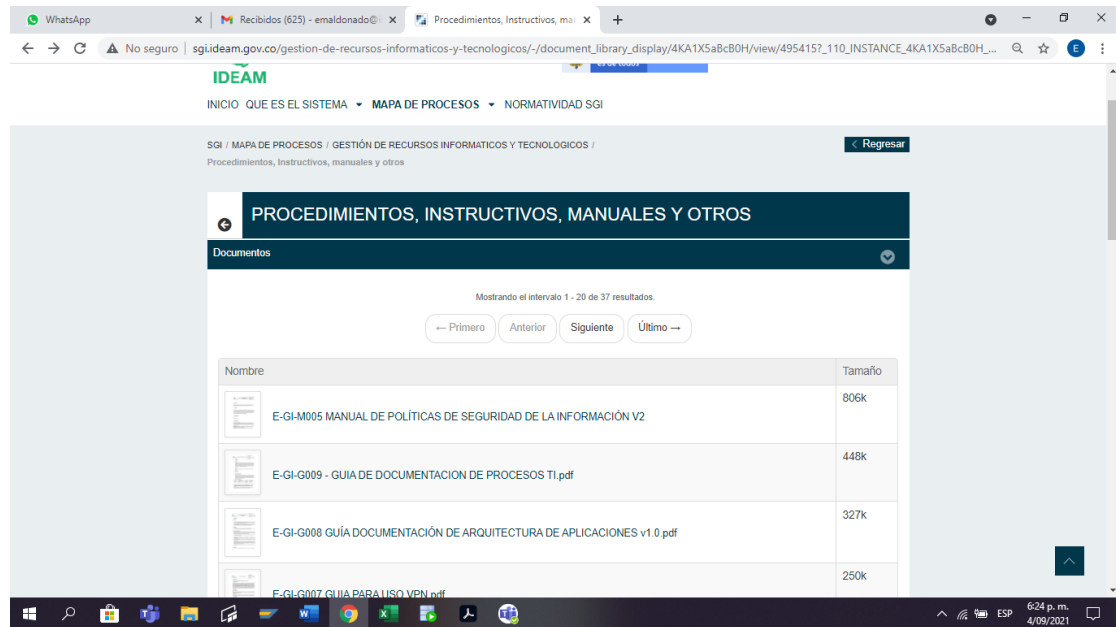
VERSIÓN	FECHA	DESCRIPCIÓN
1.0	01/12/ 2020	Primera versión Manual de políticas de seguridad de la Información.
2.0	18/05/2021	Segunda versión. Modificación de acuerdo a directiva presidencial 03 del 15 de marzo de 2021, recomendaciones consejería de transformación digital y recomendaciones de auditoria Externa

2. Según lo anterior, a partir del 18/05/21 se encontraba vigente la versión 2.0 del manual de políticas de seguridad, sin embargo, se encuentra una inconsistencia dado que al 31/08/21, el Instituto tenía dispuesto en el Sistema Integrado de Gestión el Manual de políticas de seguridad de la Información E-GI-M005 versión 1, según se evidencia en la siguiente imagen:



Fuente: Print screen tomado a la consulta efectuada al SGI, el 31/08/2021

Posteriormente, el 04/09/21, la auditoría volvió a consultar el SGI, y evidenció que en esa fecha se encontraba dispuesta la versión 2.0 del citado Manual de políticas de seguridad de la información E-GI-M005 del 18/05/2021, según se observa:



Fuente: Print screen tomado 04/09/2021, al listado de algunos de los documentos publicados en el SGI.

Además de la diferencia en la versión del documento publicado en esas dos fechas, las dos imágenes también permiten evidenciar diferencias en el tamaño de los archivos:

- ✓ El Manual de políticas de seguridad de la información E-GI-M005, versión 1.0 dispuesto en el SGI el 31/08/2021 a las 6:16 a.m. pesaba 598k.
- ✓ El Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 dispuesto en el SGI el 04/09/2021 a las 6:24 p.m. pesaba 806k.

### **CRITERIOS OBSERVACION 1**

1. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.
2. Listado maestro de documentos.
3. Correo electrónico del 20/05/21 mediante el cual la OI solicitó a la OAP la publicación del Manual de políticas de seguridad de la Información.

### **OBSERVACION 1**

Existen debilidades de control en la publicación del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, toda vez que se evidenció que estando vigente la versión 2.0, al 31/08/2021 aparecía publicado en el SGI la versión 1.0 del citado documento.

### **Retroalimentación del Formato de reporte de hallazgo**

Mediante correo electrónico del 21/09/2021, la Oficina Asesora de Planeación informó que acepta el hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004 Versión 1.0 del 02/04/2019. Así mismo, el Plan de mejoramiento propuesto, fue aceptado.

## **6.4.3. OBSERVACION 2. INVENTARIO DE BASES DE DATOS DEL AMBIENTE PRODUCTIVO**

### **CONDICIÓN**

Según la información entregada y según reunión sostenida el 07/09/21, la Oficina de Informática no dispone de un inventario de base de datos por cada dependencia; el inventario de bases de datos contempla únicamente las instancias de bases de datos que operan sobre motores de bases de datos, tales como Oracle, Postgres y MySQL.

Identificar las bases de datos que utilizan cada una de las dependencias, ayudará a que el Ideam tenga un control centralizado de la información, y se brinde apoyo a los Líderes de procesos, por ejemplo, en el fortalecimiento de la seguridad de la información en temas como los que se relacionan enseguida:

- Identificación de prioridades según el tipo de información que se manejen en las bases de datos, por ejemplo, si estas manejan información confidencial, y/o información que es usada en procesos de transferencia de información, tanto interna como externa.
- Definición e implementación de las políticas de seguridad de la información.
- Diseño e implementación de manuales, procedimientos, formatos e instructivos (si aplica).
- Verificación del cumplimiento de las políticas de seguridad de la información, y de los demás instrumentos de control que se tengan institucionalizados.
- Administración de las bases de datos.
- Controles de acceso a la información.

### **CRITERIOS OBSERVACION 2**

Inventario de bases de datos del Instituto.

### **OBSERVACION 2**

El inventario de bases de datos del ambiente productivo del Instituto contempla únicamente con las bases de datos que operan sobre motores de bases de datos, tales como Oracle, Postgres y MySQL; no contempla las bases de datos que manejan las dependencias para el desarrollo de sus funciones.

### **Retroalimentación del Formato de reporte de hallazgo**

Mediante correo electrónico del 21/09/2021, la Oficina de Informática informó que acepta parcialmente el hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004 Versión 1.0 del 02/04/2019, y expuso las siguientes justificaciones:

*“Respecto a este aspecto se indica que la Oficina de informática cuenta con el inventario de base de datos de ambiente de producción que están alojadas en los servidores dispuestos para tal fin en los diferentes motores que administra y hace la respectiva gestión sobre las mismas. De igual manera, cuenta con los procedimientos inscritos en el SGI para la creación, administración y mantenimiento de sistemas de información y por ende las bases de datos.*

*La Oficina de Informática no puede responder, conocer, ni es responsable por los sistemas de información / bases de datos que se maneje al interior de las dependencias y que no hayan sido entregados en custodia, administración u operación sobre la plataforma tecnológica que administra en el Data center.*

*La Oficina de informática no cuenta con los mecanismos para obligar a las áreas externas a lo solicitado en el presente hallazgo, por lo tanto, de manera respetuosa solicitamos que esta recomendación sea atendida de manera conjunta con la participación de la Dirección General.”*

Al respecto, la OCI dio a conocer a la Oficina de Informática la siguiente observación relacionada con el plan de mejoramiento: *“Se sugiere evaluar la conveniencia de incluir una acción orientada a verificar el cumplimiento de los procedimientos establecidos en el SGI relacionados con el tema en mención, dado que estos son instrumentos que deben ser atendidos por las diferentes áreas del instituto, según apliquen.”*

### **6.4.4. OBSERVACION 3. IDENTIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN CRÍTICOS**

#### **CONDICIÓN**

Según lo informado por la Oficina de Informática en la reunión sostenida el 30/08/21, los sistemas que se consideran críticos para el Instituto fueron identificados por la citada Oficina, y no se ha surtido la actividad de aprobación de parte de los Líderes de procesos, respecto a este tema. Es importante

contar con la aprobación de los Líderes de procesos dado que son ellos los responsables de los procesos, y cualquier decisión que se tome respecto a los sistemas podría tener impacto a nivel de la operación.

La OI indicó que los sistemas de información críticos son los que se encuentran referidos en el Acta de reunión E-SGI-F002, versión 03 del 02/05/2017, suscrita el 13/08/2021, la cual refiere lo siguiente: "Sistemas de misión crítica que van a ser objeto de la prueba de operación en el CDA, y que corresponden a las herramientas de información que operan sobre los servidores contemplados en el contrato 443/2020:

- Portales institucionales (www, pronósticos y alertas, meteorología aeronáutica, cambio climático, intranet, SGI).
- APP mi pronóstico
- Polaris
- Orfeo
- DHIME
- SmartMET
- DNS"

### CRITERIOS OBSERVACION 3

Acta de reunión E-SGI-F002, versión 03 del 02/05/2017, suscrita el 13/08/2021.

### OBSERVACION 3

Debilidades de control respecto a la identificación de cuáles son los sistemas de información críticos del Instituto, toda vez que únicamente se tienen identificados los "Sistemas de misión crítica que van a ser objeto de la prueba de operación en el CDA, y que corresponden a las herramientas de información que operan sobre los servidores contemplados en el contrato 443/2020", y de otra parte, porque no se ha formalizado su aprobación por parte de los Líderes de procesos.

### **Retroalimentación del Formato de reporte de hallazgo**

Mediante correo electrónico del 21/09/2021, 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. Así mismo, el Plan de mejoramiento propuesto, fue aceptado.

### **6.4.5. HALLAZGO 2. LOGS DE AUDITORÍA DE LAS BASES DE DATOS**

## CONDICIÓN

1. En relación con los logs de auditoría de las bases de datos, se pudo evidenciar que el Instituto únicamente cuenta con logs de auditoría básicos para nueve (9) bases de datos:

- AQTS: Almacena la información del producto Aquarius Time Series de DHIME.
- AQWP: Almacena la información del producto Aquarius Web Portal de DHIME.
- BDIDEAM: Almacena la información de los sistemas de información de apoyo a la gestión.
- DHIME: Almacena la información del módulo personalizado del sistema DHIME.
- GEODATA: Almacena la información geográfica oficializada (GEODATABASE Institucional).
- IDEAM9PR: Almacena la información del sistema de información FEWS.
- IDEAM11PR: Almacena la información de los sub sistemas ambientales (PCB, RESPEL, SNIF, SMBYC: RENARE, SIRH y RUA MANUFACTURERO), y Portales Web.
- PANET: Almacena la información del sistema PROACTIVANET (mesa de servicio)
- ORFEODB: Almacena la información del sistema de gestión documental ORFEO.

Dado que la información que registran los logs de auditoría es la básica (tales como eventos de ingreso o salida del usuario de base de datos), no es viable conocer en detalle la trazabilidad de los cambios efectuados en las bases de datos, 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.

2. Adicionalmente, se carece de logs de auditoría de las siguientes bases de datos:

- ✓ GDBIDEAM: Almacena la información geográfica que soporta el sistema DHIME.
- ✓ POLARIS: Soporta el sistema de información que permite la administración y control de las estaciones hidrometeorológicas automáticas del IDEAM.
- ✓ MANTIS: Sirve para controlar los errores aparecidos en el software y que permite a desarrolladores, testers o clientes reportar fallos y realizar el seguimiento de los mismos hasta su resolución para su posterior paso a producción.
- ✓ KOHA: El Sistema integrado de Gestión del Centro de Documentación KOHA, permite procesar técnicamente las publicaciones producidas por el Instituto y su acceso en línea, ingresar usuarios nuevos, consultar usuarios, hacer préstamo de libros, hacer devolución de libros, reservar libros, hacer consulta en línea.

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, obligaciones específicas del contrato interadministrativo 464 suscrito con Impretics refiere lo siguiente:

- ✓ Numeral Administración de bases de datos “q) Garantizar el cumplimiento de los procedimientos y políticas formulados por el IDEAM en relación con los productos que hace parte de su administración.”
- ✓ Numeral Seguridad de la Información y Continuidad. “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**

Debilidades de control relacionadas con los logs de auditoría de las bases de datos, dado que 9 bases de datos tienen logs de auditoría que registran información básica (tales como eventos de ingreso o salida del usuario de base de datos) y de otra parte, 4 bases de datos no cuentan con logs de auditoría.

## **Retroalimentación del Formato de reporte de hallazgo**

Mediante correo electrónico del 21/09/2021, la Oficina de Informática informó que acepta parcialmente el hallazgo socializado mediante Formato de reporte de hallazgos C-EM-F004, versión 1.0 del

02/04/2019, y expuso las siguientes justificaciones:

*“Se está haciendo auditoria a nueve bases de datos, aunque es básico se está cumpliendo con lo establecido en el artículo 20 de la Resolución 371 del 30/04/2021.*

*En relación con las bases de datos que no tienen habilitado el log de auditoría:*

- *Gdbideam y Polaris son base de datos PostgreSQL que requieren habilitar el módulo adicional Pgaudit*
- *Mantis y Koha, son productos con el motor embebido.”*

Al respecto, la OCI dio a conocer a la Oficina de Informática que no acepta el Plan de mejoramiento, y expuso las siguientes observaciones:

1. *“La OCI no comparte la justificación manifestada por la Oficina de Informática en cuanto a “Se está haciendo auditoria a nueve bases de datos, aunque es básico se está cumpliendo con lo establecido en el artículo 20 de la Resolución 371 del 30/04/2021.”, por las siguientes razones:*

- ✓ *A nivel de las bases de datos, los logs de auditoría básicos no contienen la suficiente información que facilite las labores de monitoreo y control, tal como lo refiere la Resolución 371 del 30/04/2021, la cual 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.” (subrayado fuera de texto).*

*Con logs de auditoría básicos no es viable conocer en detalle la trazabilidad de los cambios efectuados en las bases de datos, 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.*

- ✓ *Si bien la citada Resolución, en el Artículo 20, habla de logs de auditoría para “...los sistemas automáticos que operen y administren información sensible, valiosa o crítica para el Instituto”, es importante tener en cuenta que el numeral 5.13 del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, no hace ninguna delimitación en relación con los logs de auditoría, dado que 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.” (subrayado fuera de texto).*

2. *En relación con el plan de mejoramiento, se identificaron las siguientes observaciones:*

- ✓ *Falta complementar las acciones de manera que se cuente con logs de auditoría en las bases de datos, alineados con lo que refieren la Resolución 371 del 30/04/2021, y el numeral 5.13 del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.*
- ✓ *La acción “Hoja de ruta para los sistemas de información sin registros de auditoría implementados y susceptibles de ser intervenidos mediante mantenimiento evolutivo, siempre que se disponga del presupuesto correspondiente.”, y la meta “Hoja de Ruta para la implementación de registros de auditoría en sistemas de información con viabilidad presupuestal.” refieren sistemas de información, y no las bases de datos que soportan dichos sistemas.”*

#### **6.4.6. HALLAZGO 3. USUARIOS DE BASES DE DATOS Y SUS CONTRASEÑAS DE ACCESO**

Se identificaron las siguientes debilidades de control en relación con los usuarios de bases de datos:

1. En las bases de datos Polaris, Dhime y Ideam11pr, existen usuarios no nombrados, también llamadas cuentas genéricas. A manera de ejemplo, se cita el usuario DHIME\_R y CUSTOMHM.

Para la administración de las base de datos se utilizan usuarios no nombrados, los cuales en su mayoría vienen creados por default con el motor de la base de datos, así:

- Para la administración de las base de datos AQTS, AQWP, DHIME y IDEAM11PR se utilizan los usuarios SYSTEM.
- Para la administración de las base de datos ORFEO, POLARIS y BDBIDEAM, se utilizan los usuarios POSTGRES.

Al respecto, la Resolución 371 del 30/04/2021 cita: “Los accesos a la información, se deberán ofrecer mediante mecanismos que permita identificar de manera única a la persona responsable de la cuenta, siendo esta la única responsable en el evento que, mediante registro informático, se determine el uso inadecuado de la información. El instituto con base en estos registros podrá acudir a los mecanismos legales que considere pertinentes para los fines que correspondan según sea el caso.”

2. En las siguientes bases de datos hay más de un usuario con privilegios de DBA que los faculta a ejecutar todas las operaciones, tales como: modificación, eliminación e inserción, tanto a nivel de la información como a nivel de los objetos que conforman la base de datos; por lo tanto, son usuarios que tienen asociado un mayor nivel de riesgo. Teniendo en cuenta que en reunión sostenida el 06/09/21 la Oficina de Informática manifestó la necesidad de que esos usuarios tengan ese nivel de privilegios para efectos de la operación, la auditoría recomienda evaluar la conveniencia de

implementar un control orientado a dejar documentada y formalizada la justificación del porqué es indispensable tener habilitados esos usuarios con privilegios de Administrador de bases de datos:

<b>NOMBRE</b>	<b>DESCRIPCION</b>	<b>USUARIOS CON PRIVILEGIOS DBA</b>
IDEAM11PR	Almacena la información de los sub sistemas ambientales del IDEAM y Portales Web.	SYS SYSTEM
DHIME	Almacena la información del módulo personalizado del sistema DHIME.	SYS SYSTEM
AQTS	Almacena la información del producto Aquarius Time Series de DHIME	SYS SYSTEM
AQWP	Almacena la información del producto Aquarius Web Portal de DHIME	AQWEBPORTAL SYS SYSTEM
ORFEODB	Almacena la información del sistema de gestión documental ORFEO	ORFEO POSTGRES
GDBIDEAM	Almacena la información geográfica que soporta el sistema DHIME	SDE POSTGRES

Fuente: Elaboración propia.

Al respecto, el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021 señala que “La oficina de informática a través de sus grupos de Tecnología y Comunicaciones y Sistemas de Información, con el apoyo del oficial de Seguridad del grupo de Arquitectura Empresarial y Seguridad de Información, será la encargada de liderar y coordinar la inspección y revisión de los controles de acceso a los sistemas de información y recursos otorgados a los diferentes usuarios y terceras partes de IDEAM, con el fin de verificar que únicamente tengan los accesos y privilegios autorizados a los diferentes servicios de Información.

3. Se evidenció que la funcionalidad para el cambio de contraseña de acceso a las bases de datos, no valida la longitud, ni exige que estén compuestas por caracteres alfanuméricos, uso de mayúsculas, y de caracteres especiales tales como: (@+\*/&%\$#”.

El Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.7.1.3. cita:

“La generación de contraseñas de acceso deberá cumplir con las características mínimas, bien sea cuentas de usuario estándar, administradores, entre otros..”

“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.

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

4. Según prueba realizada con las bases de datos DHIME e Ideam11pr, no se tienen implementado un control automático para que el motor de base de datos 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."

5. En la base de datos DHIME, después de que transcurren 15 minutos desde que se bloquea la cuenta de acceso por intentos fallidos, no se genera su desbloqueo de manera automática.

El Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.7.1.3. cita: "Una vez realizado el bloqueo el usuario deberá esperar un tiempo prologando de 15 minutos para volver a intentar el inicio de sesión, en dado caso de presentar dificultad para restablecer el acceso podrá acudir por medio de una solicitud a la mesa de servicios de IDEAM."

### CRITERIOS HALLAZGO 3

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.
3. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena, ítems g y q.

### HALLAZGO 3

Existen debilidades de control asociados a las cuentas de usuario y a las contraseñas de acceso a las bases de datos del ambiente productivo del Instituto, dado que se existen cuentas genéricas, 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.

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 22 de 31

## 7. FORTALEZAS

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

Disposición del personal del área auditada.
---

## 8. HALLAZGO Y OBSERVACIONES DETECTADAS

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
X		<p><b>HALLAZGO Nro. 1. MANUALES, PROCEDIMIENTOS Y FORMATOS QUE RIGEN LA ADMINISTRACION DE USUARIOS DE BASES DE DATOS.</b></p> <p>No se cuenta con manuales y/o procedimientos que apoyen la implementación de las políticas asociadas a la administración de usuarios de bases de datos. De otra parte, no se utiliza el Formato solicitud de base de datos E-GI-F023, versión 02 del 05/04/2018, el cual se encuentra institucionalizado a través del Sistema de Gestión Integrado SGI.</p> <p><b>CRITERIOS</b></p> <ol style="list-style-type: none"> <li>Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.7.1.2.</li> <li>Procedimiento gestión de acceso a servicios de TI, E-GI-P001 del 11/09/2020.</li> <li>Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012, v 05 del 05/04/2018.</li> </ol>	<p>Dar cumplimiento a lo dispuesto en el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, al Procedimiento construcción o mantenimiento evolutivo de software misional y de apoyo E-GI-P012 (en lo referente al uso del Formato solicitud de base de datos E-GI-F023 Versión 02 del 05/04/2018), y al ítem g de la Cláusula novena del contrato 464 de 2020 suscrito con Impretics.</p>

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		<p>4. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.</p> <p>5. Formato solicitud de base de datos E-GI-F023 Versión 02 del 05/04/2018.</p>	
	X	<p><b>OBSERVACION Nro. 1. DEBILIDADES DE CONTROL EN LA PUBLICACION DEL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b></p> <p>Existen debilidades de control en la publicación del Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, toda vez que se evidenció que estando vigente la versión 2.0, al 31/08/2021 aparecía publicado en el SGI la versión 1.0 del citado documento.</p> <p>CRITERIOS</p> <ol style="list-style-type: none"> <li>Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.</li> <li>Listado maestro de documentos.</li> <li>Correo electrónico del 20/05/21 mediante el cual la OI solicitó a la OAP la publicación del Manual de políticas de seguridad de la Información.</li> </ol>	<p>Fortalecer los controles asociados a la publicación de los documentos que hacen parte del Sistema de Gestión Integrado SGI.</p>
	X	<p><b>OBSERVACION Nro. 2. INVENTARIO DE BASES DE DATOS DEL AMBIENTE PRODUCTIVO</b></p> <p>El inventario de bases de datos del</p>	<p>Complementar el inventario de bases de datos del ambiente productivo del Instituto.</p>

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		<p>ambiente productivo del Instituto contempla únicamente con las bases de datos que operan sobre motores de bases de datos, tales como Oracle, Postgres y MySql; no contempla las bases de datos que manejan las dependencias para el desarrollo de sus funciones.</p> <p>CRITERIOS</p> <p>Inventario de bases de datos del ambiente productivo del Instituto suministrado por la OI para la presente evaluación.</p>	
	X	<p><b>OBSERVACION Nro. 3. IDENTIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN CRÍTICOS</b></p> <p>Debilidades de control respecto a la identificación de cuáles son los sistemas de información críticos del Instituto, toda vez que únicamente se tienen identificados los “Sistemas de misión crítica que van a ser objeto de la prueba de operación en el CDA, y que corresponden a las herramientas de información que operan sobre los servidores contemplados en el contrato 443/2020”, y de otra parte, porque no se ha formalizado su aprobación por parte de los Líderes de procesos.</p> <p>CRITERIOS</p>	<p>Socializar, complementar (si aplica) y gestionar la aprobación de parte de los Líderes de Proceso, del listado de sistemas críticos del Instituto.</p>




H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		Acta de reunión E-SGI-F002, versión 03 del 02/05/2017, suscrita el 13/08/2021.	
X		<p><b>HALLAZGO Nro. 2. LOGS DE AUDITORÍA DE LAS BASES DE DATOS</b></p> <p>Debilidades de control relacionadas con los logs de auditoría de las bases de datos, dado que 9 bases de datos tienen logs de auditoría que registran información básica (tales como eventos de ingreso o salida del usuario de base de datos) y de otra parte, 4 bases de datos no cuentan con logs de auditoría.</p> <p><b>CRITERIOS</b></p> <ol style="list-style-type: none"> <li>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"</li> <li>Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, numeral 5.13.</li> <li>Contrato interadministrativo 464 suscrito con Impretics, cláusula novena.</li> </ol>	<p>Dar cumplimiento a lo establecido en la Resolución 371 del 30/04/2021, Artículo 20, en el Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021, y en el contrato interadministrativo 464 suscrito con Impretics, cláusula novena, ítems g y q.</p>
X		<p><b>HALLAZGO Nro. 3. USUARIOS DE BASES DE DATOS Y SUS CONTRASEÑAS DE ACCESO</b></p>	<ol style="list-style-type: none"> <li>Dar cumplimiento a lo establecido en la Resolución 371 del 30/04/2021, en el Manual de políticas de seguridad de la</li> </ol>

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES
		<p>Existen debilidades de control asociados a las cuentas de usuario y a las contraseñas de acceso a las bases de datos del ambiente productivo del Instituto, dado que se existen cuentas genéricas, 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.</p> <p>CRITERIOS</p> <ol style="list-style-type: none"> <li>4. 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".</li> <li>5. Manual de políticas de seguridad de la información E-GI-M005, versión 2.0 del 18/05/2021.</li> <li>6. Contrato interadministrativo 464 suscrito con Impretics, cláusula novena, ítems g y q.</li> </ol>	<p>información E-GI-M005, versión 2.0 del 18/05/2021, y en el contrato interadministrativo 464 suscrito con Impretics, cláusula novena, ítems g y q.</p> <ol style="list-style-type: none"> <li>2. Evaluar la conveniencia de elaborar y formalizar un documento con la justificación del porqué los usuarios que actualmente son DBA, requieren tener acceso privilegiado, y la función que cumplen cada uno de ellos en las bases de datos. Además, en caso que se identifique que es susceptible restringir el nivel de privilegios, se recomienda hacer los ajustes a que haya lugar, y dejar documentada esa actividad.</li> </ol>

**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.

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 27 de 31

## 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 al diseño, implementación de manuales y procedimientos asociados a la administración de usuarios de bases de datos. Así como el seguimiento para verificar el cumplimiento de estos instrumentos, y de las políticas de seguridad establecidas por el Instituto.

### AUTORIZACIÓN PARA COMUNICAR ESTE INFORME:

En cumplimiento del párrafo 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 BARON Líder del proceso	Jefe Oficina de Informática	

## 10. EVIDENCIAS FOTOGRÁFICAS

No aplica.

## 11. CONTROL DE APROBACIÓN INFORME DE AUDITORÍA INTERNA

CONTROL INFORME DE AUDITORÍA INTERNA		
<b>ELABORÓ:</b> <b>Eida Ruth Maldonado Omen</b>  Cargo: Contratista OCI	<b>REVISÓ:</b> <b>María Eugenia Patiño Jurado</b>  <b>PATIÑO JURADO</b> <b>MARIA EUGENIA</b> Jefe Oficina Control Interno	<b>APROBÓ:</b> <b>María Eugenia Patiño Jurado</b>   <small>Firmado digitalmente por PATIÑO JURADO MARIA EUGENIA Fecha: 2021.10.13 08:40:17 -05'00'</small> Jefe Oficina Control Interno

 <p><b>IDEAM</b> Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 28 de 31

## 12. CONTROL DE CAMBIOS

<b>VERSIÓN</b>	<b>FECHA</b>	<b>DESCRIPCIÓN</b>
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-13-10-2021

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

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 29 de 31

**ANEXO 1. FORMATO SOLICITUD DE BASE DE DATOS E-GI-F023 VERSIÓN 02 DEL 05/04/2018**

	<b>SOLICITUD DE BASE DE DATOS</b>	<b>Código:</b> E-GI-F023
		<b>Versión:</b> 02
		<b>Fecha:</b> 05/04/2018
		<b>Página</b> 1 de 1

**INSTRUCCIONES DE DILIGENCIAMIENTO**

1. Una vez este diligenciado el formato debe anexarse y enviarse a través de la mesa de ayuda (Sistema GLPI), diligenciándolo y seleccionando:  
**CATEGORÍA:** 24. SISTEMAS DE INFORMACION.  
**SUBCATEGORÍA:** 24. SISTEMAS DE INFORMACION —> Solicitudes de BASES DE DATOS

Una vez envíe la solicitud, el sistema de forma automática la envía a quien debe atender y/o coordinar su atención en la Oficina de Informática.

4. La persona autorizada para enviar el mensaje de ayuda es el Jefe Inmediato o Supervisor del Contrato, o por la persona a quien ellos designen.

DILIGENCIAR POR EL LIDER TÉCNICO		
<b>TRÁMITE</b>	<b>BASE DE DATOS</b>	<b>AMBIENTE</b>
CREACIÓN <input type="checkbox"/> ACTIVACIÓN <input type="checkbox"/> MODIFICACIÓN <input type="checkbox"/> BLOQUEO <input type="checkbox"/> OTRA SOLICITUD <input type="checkbox"/>		Producción <input type="checkbox"/> Desarrollo <input type="checkbox"/> Pruebas <input type="checkbox"/>
<b>Solicitar creación y/o asignación de roles en aplicación</b> Nombre de la aplicación <input type="text"/> Login de la cuenta <input type="text"/> Nombres y Apellidos del Usuario <input type="text"/> Número de Identificación <input type="text"/> Correo Electrónico <input type="text"/> Fecha de vencimiento dd/mm/yyyy <input type="text"/> Descripción de la solicitud <input style="height: 40px;" type="text"/>  Indicar: Privilegios de Sistema, de objetos, roles, sinónimos o adjuntar script. <input style="height: 40px;" type="text"/>  Nombre Jefe Inmediato o Supervisor <input style="width: 150px;" type="text"/> <b>FECHA</b> <input style="width: 50px;" type="text"/>		

**CONTROL DE ATENCION** ID GLPI

HISTORIAL DE CAMBIOS		
VERSION	FECHA	DESCRIPCION
01	31/05/2015	Creación del documento.
02	5/04/2018	Actualización del documento.

ELABORÓ:	REVISÓ:	APROBÓ:
Naney Maldonado Profesional Oficina de Informática.	Leonardo Cárdenas Chitiva Jefe Oficina de Informática	Leonardo Cárdenas Chitiva Jefe Oficina de Informática

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 30 de 31

**ANEXO 2. CORREO REMITIDO POR LA OFICINA DE INFORMATICA A LA OAP EL 20/05/21, A TRAVES DEL CUAL SE SOLICITA LA PUBLICACION DEL MANUAL POLITICAS DE SEGURIDAD DE LA INFORMACION E-GI-M005 DEL 18/05/21**

----- Forwarded message -----

De: Eduardo Emilio Ramirez Acosta <eramirez@ideam.gov.co>

Date: jue, 20 may 2021 a las 18:18

Subject: Publicación en el SGSI del SGI de E-GI-M005 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

To: German Ignacio Ahumada Valbuena <gahumada@ideam.gov.co>

Cc: Telly De Jesus Month Parra <tmonth@ideam.gov.co>, Harbey Amulfo Martinez Guerrero <hamartinez@ideam.gov.co>, Alicia Baron Leguizamon <abaron@ideam.gov.co>

Apreciado German.

Ingeniero buenas tardes.

Por favor publicar en el SGSI del SGI;

1. Documento actualizado "E-GI-M005 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN", el cual ha quedado como Versión 2.

2. Adjunto formato "E-SGI-F010 FORMATO GESTIÓN DEL CAMBIO\_20052021" exigido por la OAP del IDEAM para la publicación inmediata de la nueva versión del documento anterior.

Agradezco atender a la brevedad la presente solicitud.

Gracias por su valiosa colaboración.

Cordialmente,

<https://mail.google.com/mail/u/0?ik=ca81cacfc5&view=pt&search=all&permmsgid=msg-f%3A1710544422031938143&simpl=msg-f%3A17105444220...> 1/2

13/0/21 06:07

Correo de IDEAM - INSTITUTO DE HIDROLOGIA, METEOROLOGIA Y ESTUDIOS AMBIENTALES - Fwd: Publicación en el SGSI d...



Instituto de Hidrología,  
Meteorología y  
Estudios Ambientales

Eduardo Emilio Ramirez Acosta

Profesional Especializado


Oficina de Informática

Tel: (571) 352 7160 Ext. 1346 - 1343

Línea nacional 018000 110 012

Calle 25D No. 96B - 70 Bogotá D.C

[www.ideam.gov.co](http://www.ideam.gov.co)

	<b>FORMATO INFORME DE AUDITORÍA INTERNA</b>	<b>CÓDIGO:</b> C-EM-F003
		<b>VERSIÓN:</b> 7
		<b>FECHA:</b> 27/04/2020
		<b>PÁGINA</b> 31 de 31

### ANEXO 3

## RESPUESTA REMITIDA POR LA OAP A LA OFICINA DE INFORMATICA EL 18/05/21, INFORMANDO QUE SE PUBLICÓ EL DOCUMENTO

El mar, 18 may 2021 a las 12:51, German Ignacio Ahumada Valbuena (<[gahumada@ideam.gov.co](mailto:gahumada@ideam.gov.co)>) escribió:  
Cordial saludo Dr. Eduardo,

El documento fue publicado en el link adjunto para los fines pertinentes.

Politica

--

Cordialmente,



**Germán I Ahumada V**

Contratista  
Oficina Asesora de Planeación  
Tel: (571) 352 7160  
Linea nacional 018000 110 012  
Calle 25D No. 96B - 70 Bogotá D.C  
[www.ideam.gov.co](http://www.ideam.gov.co)