IDEAM Instituto de Hidrología Meteorología y Estudios Ambientales	**RESUMEN INFORME DEFINITIVO AUDITORÍA**	**CÓDIGO:** C-EM-F019
		VERSIÓN: 03
		FECHA: 21/11/2022
		PÁGINA: 1 de 3

Auditor Líder	Martha Angélica Salinas Arenas
Jefe Oficina de Control Interno	María Eugenia Patiño Jurado
Fecha de Ejecución de la Auditoría	21/02/2024
Fecha de Reunión de Apertura	21/02/2024
Fecha de Reunión de Cierre	09/04/2024
Fecha de Emisión del Informe	03/04/2024

Aspecto Evaluable (Unidad Auditable):	GESTIÓN DE CONTROL DISCIPLINARIO INTERNO GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES GESTIÓN DEL DESARROLLO DEL TALENTO HUMANO
Líder de Proceso / Jefe(s) Dependencia(s):	JAMIL ALBERTO BELTRÁN CALDERÓN WILMER ESPITIA MUÑOZ ANGELA MARÍA BETÍN
Objetivo de la Auditoría:	Verificar la efectividad de los controles en materia de seguridad de la información, en atención a peticiones allegadas a la Oficina de Control Interno.
Alcance de la Auditoría:	La auditoría se llevará a cabo en la sede del Instituto ubicado en la Calle 25 D No. 96 B - 70 Bogotá D.C. a la Oficina de Informática y a los grupos de Instrucción de Control Disciplinario Interno y Administración y Desarrollo del Talento Humano y comprende peticiones relacionadas con presuntas debilidades en la seguridad de la información allegadas a esta Jefatura.
Criterios de la Auditoría:	**EXTERNOS:** ▪ LEY 87 de 1993. *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"* ▪ Ley 1712 de 2014. "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."* ▪ LEY 1755 DE 2015. *"Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo".* ▪ LEY 1952 DE 2019. *"Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el*

	derecho disciplinario." ▪ LEY 2094 DE 2020. "*Por medio de la cual se reforma la ley 1952 de 2019 y se dictan otras disposiciones*" ▪ Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5. ▪ Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Noviembre 2022. ▪ RESOLUCIÓN N° 001519 DE 24 DE AGOSTO DE 2020 *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*. ▪ Estándares de gestión de tecnología: Cobit 5, ISO 27001:2013, ISO 20000. **INTERNOS:** ▪ Instructivo de Gestión de Incidentes de Seguridad E-SGI-SI-I004 v7 del 10/12/2021. ▪ Manual de políticas de seguridad de la Información E-GI-M002 V2 del 18/05/2021. ▪ Resolución Nro. 0371 de 30/04/2021 emitida por la Dirección General del IDEAM, que comprende la *"Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios, así como definir los lineamientos frente al uso y manejo de la información".*

RESUMEN EJECUTIVO

HALLAZGO No 1. INOBSERVANCIA A LO DISPUESTO EN EL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEFINIDAS EN EL MANUAL DE POLÍTICAS DE SEGURIDAD E-GIM005 V2 DEL18/05/2021, ELIMINANDO LA CUENTA NOTIFICACIONDISCIPLINARIO@IDEAM.GOV.CO Y CAMBIO EN LA PROPIEDAD DE LOS ARCHIVOS DEL GRUPO DE INSTRUCCIÓN DE CONTROL DISCIPLINARIO INTERNO CON INFORMACIÓN DE CARÁCTER RESERVADA DE LOS PROCESOS DISCIPLINARIOS, INCIDENTE QUE VULNERA SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD (D) (A).

RESPONSABLE: OFICINA DE INFORMÁTICA

CRITERIO

El artículo 115 de la ley 1952 de 2019 establece la reserva de la actuación disciplinaria en los siguientes términos:

"En el procedimiento disciplinario las actuaciones disciplinarias serán reservadas hasta cuando se cite a audiencia y se formule pliego de cargos o se emita la providencia que ordene el archivo definitivo, sin perjuicio de los derechos de los sujetos procesales.

El disciplinado estará obligado a guardar la reserva de las pruebas que por disposición de la Constitución o la ley tengan dicha condición."

Resolución Nro. 0371 del 30 de abril de 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"*

El Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5 establece frente al Gobierno Digital y la seguridad de la información lo siguiente:

3.2.1.4 Política de Seguridad Digital

"(…) el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital: Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia."

En ese sentido, el Documento CONPES 3854 de 2016 LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA indica lo siguiente:

"(…) las entidades involucradas tendrán la responsabilidad de desarrollar bases de datos y generar mecanismos que permitan garantizar la seguridad de la información a nivel nacional. Para lo anterior, se tendrán en cuenta las normas técnicas y los estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad."

Manual de políticas de seguridad de la Información E-GI-M002 V2 del 18/05/2021 (IDEAM).

5.13. REGISTRO (LOGGING) Y SEGUIMIENTO

"Objetivo: Definir lineamientos que permitan asegurar el registro de eventos y generación de evidencias en las operaciones de los servicios tecnológicos.

Lineamientos:

● *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.*

o La información contenida en los logs se debe proteger contra intentos de alteración y acceso no autorizado conservando integridad.

● *La generación de registros de auditoría debe contribuir con la protección contra cambios no autorizados y errores operacionales.*

● *Los registros de auditoría deben ser custodiados y retenidos por el tiempo que el IDEAM lo determine. Según sea el caso, se debe hacer copia de respaldo de información de los registros de auditoría, ya que en caso de un incidente de seguridad de la información estos deberán estar disponibles.*

● *La oficina de informática debe implementar y documentar controles que permitan monitorear la operación, disponibilidad y capacidad de la infraestructura tecnológica*

● *La oficina de informática debe sincronizar los relojes de los servidores y demás componentes de la plataforma tecnológica, con una fuente única de referencia de tiempo con la hora legal colombiana http://horalegal.inm.gov.co/.*

Esta sincronización permitirá evidenciar con exactitud los registros de auditoría.

Esta sincronización se debe presentar mediante informe con evidencias al jefe de la oficina de informática, a los coordinadores de los grupos y al oficial de Seguridad de dicha dependencia. Además, se debe monitorear los relojes de todos los servidores con una periodicidad semanal y ajustarlos en caso de ser necesario y presentar dicho informe y sus evidencias cada vez que se realicen ajustes de sincronización.

El protocolo de tiempo de red (NTP) se recomienda su uso en todos los dispositivos de red para mantener la hora sincronizada entre la infraestructura corporativa. También es recomendable activar mecanismos de seguridad para NTP para evitar ataques contra este protocolo."

Se identificó incidente de seguridad de la información el 14 de septiembre de 2023 al suprimirse por error humano el correo de notificaciondisciplinario@ideam.gov.co donde reposaba toda la información de los procesos disciplinarios que se adelantaban por parte del Grupo de Instrucción de Control Disciplinario Interno del instituto, al revisar la consola de la administración de Google, tomada desde la sección de auditoría e investigación, se determinó que al recuperarse la información se cambió la propiedad de los

archivos, vulnerándose la reserva legal de la información que hacía parte de los procesos disciplinarios de la entidad, de acuerdo a lo establecido en la ley 1952 de 2019.

HALLAGO No. 2. NO SE REALIZÓ LA DOCUMENTACIÓN PERTINENTE A LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. NO SE REGISTRÓ UN REPORTE, DE GESTIÓN Y DOCUMENTACIÓN RESPECTIVA, DÓNDE INCLUYA EVIDENCIA DEL INCIDENTE DE SEGURIDAD. (A).

RESPONSABLE: OFICINA DE INFORMÁTICA

CRITERIO:

El Manual de Políticas de Seguridad de la Información, Código: E-GI-M005. Versión: 2.0 de fecha: 18/05/2021, establece:

"5.20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Gestionar oportunamente los incidentes de seguridad de la información, mediante un enfoque coherente y eficaz.

Lineamientos:

● La oficina de informática a través del grupo de arquitectura empresarial y seguridad de la información, deberá definir un procedimiento para la gestión de incidentes de seguridad de la información, así mismo la disposición de los medios y canales de comunicaciones para la atención de los mismos.

● Definir lineamientos para el cumplimiento frente a los tiempos de respuesta a incidentes.

Para este fin se deberá registrar el reporte, gestión / atención y documentación respectiva y evidencia de los incidentes de seguridad.

● Llevar el asunto a una instancia superior (escalar) el incidente de seguridad en caso de requerirlo.

● El oficial de seguridad de la información del IDEAM deberá mantener el contacto apropiados con autoridades, grupos de interés en materia a la gestión de incidentes de seguridad de la información.

● La oficina de informática será la encargada de realizar la recolección de evidencias de los incidentes de seguridad de la información.

● Para la recolección de evidencias y el transporte de elementos, se debe realizar teniendo en cuenta el

proceso de la cadena de custodia." (Negrilla y subrayado fuera de texto)

HALLAZGO No. 3. OMISIÓN EN EL REPORTE DE LA MATERIALIZACIÓN DEL RIESGO DENOMINADO: *"Posibilidad de pérdida Económica y Reputacional por afectación de la confidencialidad, integridad y disponibilidad de los servicios institucionales brindados al ciudadano debido a posible daño, fuga o pérdida de información física o digital, Inadecuada custodia de la información, ataques cibernéticos, descuido por parte de los colaboradores y acciones de personal mal intencionado."* (A)

RESPONSABLE: OFICINA DE INFORMÁTICA

CRITERIO:

El Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5 establece frente al Gobierno Digital y la seguridad de la información lo siguiente:

3.2.1.3 Política Gobierno Digital

"(…) la política de Gobierno Digital cuenta con cinco grandes propósitos que se pretenden alcanzar a través del uso y aprovechamiento de las TIC, por parte del Estado y de los actores de la Sociedad que se relacionan con éste:

– Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

– Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

– Tomar decisiones basadas en datos, a partir del aumento del uso y aprovechamiento de la información.

– Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.

– Impulsar el desarrollo de territorios y ciudades inteligentes, para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC. "

3.2.1.4 Política de Seguridad Digital

"(…) el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital: Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un

marco de cooperación, colaboración y asistencia."

El Manual de Políticas de Seguridad de la Información, Código: E-GI-M005. Versión: 2.0 de fecha: 18/05/2021, establece:

"5.20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Gestionar oportunamente los incidentes de seguridad de la información, mediante un enfoque coherente y eficaz.

Lineamientos:

● *La oficina de informática a través del grupo de arquitectura empresarial y seguridad de la información, deberá definir un procedimiento para la gestión de incidentes de seguridad de la información, así mismo la disposición de los medios y canales de comunicaciones para la atención de los mismos."*

HALLAZGO No. 4. OMISIÓN EN IDENTIFICACIÓN Y EN EL TRATAMIENTO A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, ESTABLECIDOS EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS VERSIÓN 6 (A)

RESPONSABLE: OFICINA DE INFORMÁTICA

CRITERIO

La Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 define el Riesgo de Seguridad de la Información como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)."*

La política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) 12, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales, la caracterización de esta matriz debe observar como mínimo:

"6.1. Identificación de los activos de seguridad de la información: como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

6.2. Identificación del riesgo: se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información: 1) Pérdida de la confidencialidad; 2) Pérdida de la integridad; 3) Pérdida de la disponibilidad.
6.3. Valoración del riesgo.

6.4 Controles asociados a la seguridad de la información."

El Modelo Nacional de Gestión del Riesgo de Seguridad de la Información de las Entidades Públicas establece que las entidades públicas deben implementar la Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.

CONCLUSIONES

1. El Instituto a la fecha no cuenta con una identificación de riesgos de seguridad de la información, situación que dificulta su gestión para mitigar su materialización.

2. El Instituto, a través del liderazgo de la Oficina de Informática debe fortalecer la función institucional mediante la implementación, difusión y mejoramiento continuo del modelo de seguridad y privacidad de la información para mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información de la entidad.

3. A pesar de que todos los servidores públicos, contratistas y terceros que conforman las diferentes áreas del IDEAM deben clasificar la información que tengan bajo su custodia en alguna de las categorías que previamente hayan sido establecidas en aras de mitigar la materialización de riesgos de seguridad de la información, en la presente auditoría se determinó que existen terceros que pueden vulnerar la custodia y/o reserva de estos activos de la información del Instituto, lo cual debe quedar documentado en una matriz de riesgos de seguridad de la información a fin de establecer controles efectivos y el monitoreo de los mismos para mitigar la ocurrencia de incidentes informáticos.

4. Se encuentra debilidades en la gestión de logs de auditorías de Google, pues se evidencia que la Oficina de Informática no los tiene en cuenta para detectar desviaciones y/o afectaciones a la seguridad de la información. Los logs son herramientas que permiten ayudar a detectar y analizar los errores y problemas relativos a eventos de red, sistemas de información y aplicaciones, por ejemplo, incidentes de seguridad, actividades irregulares o problemas operacionales, situaciones que se evidenciaron en el presente ejercicio auditor.

5. Los riesgos asociados a la seguridad de la información deben observar cómo parámetros mínimos el acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos. Se considera que hay uso indebido de la información y de los recursos, cuando se incurre en cualquiera de las siguientes conductas:

"a. Suministrar información confidencial o que tenga carácter reservado a quien no tenga derecho a conocerla.
b. Usar la información con el fin de obtener beneficio propio o de terceros.

c. Ocultar la información maliciosamente causando cualquier perjuicio.
d. Hacer pública la información sin la debida autorización.
e. Hurtar software del Instituto (copia o reproducción entre usuarios finales).
f. Realizar copias no autorizadas de software del Instituto, dentro y fuera de sus instalaciones.
g. Falsificar y duplicar un producto informático de Instituto.
h. Descargar software, a través de Internet sin la debida autorización.
i. Intentar modificar, reubicar o sustraer equipos de cómputo, software, Información o periféricos sin la debida autorización.
j. Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
k. Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
l. Utilizar la infraestructura del Instituto (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.
m. Enviar cualquier comunicación electrónica fraudulenta.
n. Apropiarse los aplicativos, desarrollos o información del Instituto y publicarla como propio.
o. Adueñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
o. Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
p. Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
q. Descargar o publicar material ilegal, o implique la vulneración de derechos de terceros, material nocivo usando un recurso del Instituto.
r. Uso personal de cualquier recurso informático del Instituto para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material prohibido.
s. Acceder sin autorización a información o documentos públicos que tengan carácter reservado por disposición constitucional o legal.
t. Violar cualquier Ley o Regulación Nacional respecto al uso de sistemas de información." (Política general de TIC MinTIC`S)
Las situaciones resaltadas se presentaron en el incidente del 14 de septiembre de 2023.

6. De acuerdo con los resultados enunciados en el presente informe, se debe remitir a la Procuraduría General de la Nación por cuanto existe un hallazgo con una posible connotación disciplinaria.

7. Así mismo se remitirá a la Oficina Asesora de Planeación para tener en cuenta el tema de la materialización del riesgo y la necesidad de definir riesgos de seguridad de la información.

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 darán a conocer los resultados de las auditorías a los miembros de esta instancia.

Para constancia se firma en Bogotá D.C., a los 03 días del mes de abril del año 2024.

APROBACIÓN DEL INFORME DE AUDITORÍA*		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
MARÍA EUGENIA PATIÑO JURADO	Jefe de la Oficina de Control Interno	PATIÑO JURADO MARIA EUGENIA Firmado digitalmente por PATIÑO JURADO MARIA EUGENIA Fecha: 2024.04.03 15:32:18 -05'00'
MARTHA ANGÉLICA SALINAS ARENAS	Auditor Líder	

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	8/10/2021	Creación del documento.
02	7/10/2022	Revisión y ajustes identificados en el desarrollo de autoevaluación del proceso.
03	21/11/2022	Se ajusta el orden de los cuadros de información.

ELABORÓ:	REVISÓ Y APROBÓ:
JUAN SEBASTIÁN LEAL CÁRDENAS CONTRATISTA OFICINA DE CONTROL INTERNO MARIANELLA MENDOZA RODRÍGUEZ PASANTE OFICINA DE CONTROL INTERNO	MARÍA EUGENIA PATIÑO JURADO JEFE OFICINA CONTROL INTERNO