IDEAM

Instituto de Hidrología,
Meteorología y
Estudios Ambientales

INFORME DE SEGUIMIENTO A LA LEY 1581 DE 2012 PROTECCIÓN DE DATOS PERSONALES

08/06/2021

TABLA DE CONTENIDO

Auditoría N° INPDAT-2021-23		
Fecha entrega informe		
Día	**Mes**	**Año**
31	05	2021

1. DATOS GENERALES

PROCESO(S) /ACTIVIDAD (ES) AUDITADO (S)	Oficina Asesora Jurídica, Oficina de Informática		
LIDER(ES) DE PROCESO	Gilberto Antonio Ramos Suarez. Alicia Barón Leguizamón.	**CARGO**	Jefe Oficina Asesora Jurídica. Jefe Oficina de Informática.
AUDITOR LÍDER	Carlos Hernán Rodríguez Rodríguez	**CARGO**	Abogado Contratista - OCI

OBSERVADORES Y/O ACOMPAÑANTES.	
NOMBRE: N/A	**CARGO: N/A**
NOMBRE:	**CARGO:**
NOMBRE:	**CARGO:**

FECHA DE APERTURA AUDITORIA	25 / 03 / 2021
FECHA DE CIERRE DE LA AUDITORIA	28 / 05 / 2021

2. OBJETIVO DE LA AUDITORIA

Evaluar el adecuado diseño, implementación y ejecución establecidos dentro de la gestión realizada por las oficinas Asesora Jurídica e Informática en la gestión de los controles aplicables al interior del IDEAM para garantizar el adecuado tratamiento con la seguridad de la información de conformidad con lo establecido en la Ley 1581 de 2012.

3. ALCANCE DE LA AUDITORIA

El proceso de verificación se realizó a partir de la información suministrada por las Oficinas Asesora Jurídica e Informática, de una muestra selectiva, para el período comprendido entre el 1º de enero de 2020 a lo corrido de la presente vigencia, dentro del marco de la Resolución 2821 de diciembre 14 de 2016 *"Por la cual se adopta la política de protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM"*. No obstante, se podrán incorporar hechos adicionales que se evidencien durante el seguimiento y se tomarán muestras de soportes

posteriores.

4. DECLARATORIA

- Este seguimiento fue realizado con base en la consecución y análisis de la información aleatoria, seleccionada por el auditor encargado de llevar a cabo el trabajo de aseguramiento.

  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 de cada 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

Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales".*
Circular Presidencial No. 01 de 2019.
Circular Externa No. 0001 de 2015 expedida por la Superintendencia de Industria y Comercio.
Circular Externa No. 003 de 2018 expedida por la Superintendencia de Industria y Comercio.
Resolución 2821 de diciembre 14 de 2016 expedida por el IDEAM
Manual de Políticas de Seguridad de la Información E-GI-M002 v1,
Las demás normas que sean concordantes, coincidentes y complementarias.

6. METODOLOGÍA Y DESARROLLO DE LA AUDITORIA INTERNA

Con el fin de dar cumplimiento a los objetivos propuestos en el presente seguimiento, la Oficina de Control Interno, atendiendo lo dispuesto por la Ley 1581 de octubre 17 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", mediante memorando con radicado No. 20211030000783 de fecha 25 de marzo del presente año, solicito a las Oficinas Asesora Jurídica e Informática, la siguiente información.

1. Cuál es el procedimiento de inscripción en el Registro Nacional de Bases de Datos — RNBD, utilizado por parte del Instituto.
2. Existe un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos por parte de los titulares.
3. Mediante que mecanismo, conserva el IDEAM la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
4. Como se actualiza la información de los reclamos presentados por los titulares.
5. Que procedimiento se sigue con el fin de Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
6. Señalar el mecanismo utilizado por la entidad para permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
7. Indique la forma en que se realiza oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
8. Cuál es el mecanismo utilizado para informar a la Superintendencia de Industria y Comercio cuando se presentan violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Mediante memorando radicado 20211020001483 de fecha 7 de abril de 2021, la Oficina Asesora Jurídica, envió respuesta en los siguientes términos:

"1. Cuál es el procedimiento de inscripción en el Registro Nacional de Base de Datos – RNBD, utilizado por parte del Instituto"

Respuesta: El procedimiento aplicado es el establecido por la Circular Externa No. 0001 de 2015 expedida por la SIC y la Circular Presidencial No. 01 de 2019.

2. Existe un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos por parte de los titulares.

Respuesta: Sí existe en la Resolución 2821 de diciembre 14 de 2016 "Por la cual se adopta la política de protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM", la cual contiene dicha política y el procedimiento para garantizar el adecuado cumplimiento de la ley. Se adjunta el citado documento.

"(…)

Frente a cualquier consulta o reclamo por parte de los titulares, en el numeral 6 del mencionado documento, se señala:

" (…)

A las preguntas 3 y 6: "3. Mediante qué mecanismo, conserva el IDEAM la información bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento." 6. Señalar el mecanismo utilizado por la entidad para permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

Respuesta: Cada área es la encargada de manejar y controlar la base de datos personales y la seguridad de los mismos, según su competencia; los cuales se encuentran bajo la condición de confidencialidad. Así mismo, cada persona tiene acceso a la información autorizada por su superior, bajo claves asignadas por la Oficina de Informática del IDEAM.

Dentro del manual acogido mediante la Resolución 2821 de diciembre 14 de 2016 "Por la cual se adopta la política de protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM", se consagra lo siguiente:

" (…)

A las preguntas 4, 5 y 7: "4. Cómo se actualiza la información de los reclamos presentados por los titulares" "5. Qué procedimiento se sigue con el fin de garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data". "7. Indique la forma en que se realiza oportunamente la actualización, reactivación o supresión de los datos en los términos de la presente ley"

Respuesta: Dentro del manual adoptado mediante la Resolución 2821 de diciembre 14 de 2016 "por la cual se adopta la política de protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM", se consagra lo siguiente:

"(…)

8. Cuál es el mecanismo utilizado para informar a la Superintendencia de Industria y Comercio cuando se presentan violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares".

Respuesta: Se hará a través del enlace previsto en la página web de la Superintendencia de Industria y Comercio, dentro del término legal establecido en el capítulo II del Título V de la Circular única de la SIC.

Internamente se cuenta con un Instructivo de Gestión de Incidentes (E- GI-I005), que tienen por objetivo: "Definir un proceso que permita manejar adecuadamente los incidentes de seguridad de la información a través de un esquema que involucra la preparación para la gestión del Incidente, detección y análisis, contención, erradicación y recuperación y la actividad Post-Incidente". NO RESPONDIÓ NADA

Posteriormente, la Oficina de Informática, mediante memorando radicado 20211040002703 de fecha 26 de abril de 2021, dio respuesta así:

"1. Cuál es el procedimiento de inscripción en el Registro Nacional de Base de Datos – RNBD, utilizado por parte del Instituto.

Respuesta:

El procedimiento de inscripción al RNBD, es como lo establece la SIC, y el cual el IDEAM en su momento realizó al pie de la letra a saber:

a) El IDEAM descarga de la plataforma MUISCA de la DIAN el RUT.

b) La validación de la información del IDEAM se realizará a través de los datos consignados en el RUT, para ello el IDEAM cargó el RUT en el aplicativo RNBD.

c) Lo anterior dando cumplimiento a lo indicado en el "anexo 3 generación del RUT del manual de usuario", publicado en la página de la superintendencia de industria y comercio.

d) La aplicación el sistema RNBD solicita al usuario su registro, para ello se seleccionó la opción "**regístrese**".

e) En el caso del IDEAM como entidad pública que realiza tratamiento de bases de datos personales a la cual le aplica la ley 1581 de 2012, se seleccionó tipo de persona jurídica y de naturaleza jurídica pública.

f) Posteriormente se seleccionó el archivo del RUT en el botón seleccionar archivo.

g) Luego se inició el diligenciamiento del formulario correspondiente a cada una de las opciones según la naturaleza y el tipo de persona del sujeto obligado.

h) El sistema RNBD, realiza la validación de los datos del IDEAM con el RUT en forma automática.

i) Al finalizar el diligenciamiento del formulario en el sistema RNBD, este envió al correo registrado en el RUT del IDEAM, su usuario y contraseña definitivas.

j) Finalmente, la contraseña se modificó por seguridad.

2. Existe un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos por parte de los titulares.

Respuesta:

El cumplimiento de la ley 1581 de 2012 y lo concerniente al habeas data y al RNBD se incluyen en los documentos emitidos por la Oficina de Informática a saber:

1. Nueva Política de Seguridad digital recientemente aprobada en el comité de gestión y desempeño institucional realizado el 23 de marzo de 2021 y cuya publicación definitiva en el SGO del IDEAM se encuentra en curso.

2. El documento denominado E-GI-M002 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN v1, el cual complementa a la política digital mencionada en el punto anterior.

En cuanto a las políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos por parte de los titulares, se debe seguir y cumplir lo estipulado en la resolución del IDEAM número 2821 de 2016, por la cual se adopta la Política de Protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales.

3. Mediante que mecanismo, conserva el IDEAM la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Respuesta:

El IDEAM tiene información en la nube y su acceso se limita mediante autenticación de usuarios de dominio y políticas de lista de accesos. Para la información que reposa en el datacenter se debe ingresar autenticado por usuario de dominio y a esta información se aplican políticas de control de acceso y directiva de grupo local - GPO del controlador del dominio. La mencionada ley 1581 de 2012 se estipula en la Política de Seguridad Digital y los controles se especifican en el manual de políticas de seguridad de información "E-GI-M002 MANUALDE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN v1" de la entidad.

4. Como se actualiza la información de los reclamos presentados por los titulares.

Respuesta:

El mecanismo para actualizar la información de los reclamos presentados por los titulares es el **"Formulario PQRS"** establecido mediante resolución 2628 del 18 de noviembre de 2016 del IDEAM, esta establece el procedimiento interno para peticiones, quejas, reclamos y sugerencias en el Instituto del IDEAM- y se regulan mecanismos para la atención de las peticiones verbales. El propósito de dicha resolución consiste en trazar de forma clara y detallada, la ruta que debe seguirse al interior del IDEAM, para la correcta presentación, radicación y constancia de las peticiones que se presenten al Instituto por cualquiera de los medios dispuestos para la atención al ciudadano. En este formulario puede registrar peticiones, quejas, reclamos, sugerencias o denuncias de actos de corrupción y solicitar servicios de soporte técnico para los aplicativos de IDEAM.
Para más información relacionada con la pregunta de este ítem recomendamos remitirse a la Oficina Asesora

Jurídica, la cual es la responsable de la gestión y control del RNBD para el IDEAM.

5. Que procedimiento se sigue con el fin de Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

Respuesta:

Para la información relacionada con la pregunta de este ítem recomendamos remitirse a la Oficina Asesora Jurídica, la cual es la responsable de la gestión y control del RNBD para el IDEAM.

6. El IDEAM para dar cumplimiento a lo establecido en el Derecho de Habeas Data que permite a los ciudadanos conocer, actualizar y rectificar toda la información que tengan las diferentes entidades y bases de datos del país, emite la Resolución número 2821 de 2016, por la cual se adopta la Política de Protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales. Esta resolución se constituye en el procedimiento que sigue la entidad para Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

Para más información relacionada con la pregunta de este ítem recomendamos remitirse a la Oficina Asesora Jurídica, la cual es la responsable de la gestión y control del RNBD para el IDEAM.

7. Señalar el mecanismo utilizado por la entidad para permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

Respuesta:

El IDEAM tiene información en la nube y su acceso se limita mediante autenticación de usuarios de dominio y políticas de lista de accesos. Para la información que reposa en el datacenter se debe ingresar autenticado por usuario de dominio y a esta información se aplican políticas de control de acceso y directiva de grupo local - GPO del controlador del dominio. La mencionada ley 1581 de 2012 se estipula en la Política de Seguridad Digital y los controles se especifican en el manual de políticas de seguridad de información “E-GI-M002 MANUALDE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN v1” de la entidad.

8. Indique la forma en que se realiza oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

Respuesta:

La respuesta a esta pregunta debe ser respondida por la Oficina Asesora Jurídica, como responsable por la gestión y control del RNBD para el IDEAM.

9. Cuál es el mecanismo utilizado para informar a la Superintendencia de Industria y Comercio cuando se

presentan violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Respuesta:

El mecanismo utilizado para informar a la Superintendencia de Industria y Comercio cuando se presentan violaciones a los códigos es el que establece dicha entidad para ello, a saber:
Ante la violación de los códigos de seguridad, la pérdida robo o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, para que se pueda registrar un incidente, el usuario del IDEAM desde su cesión deberá acceder al módulo RNBD de inscripción de bases de datos. Luego selecciona la opción inscribir bases de datos y posteriormente, en reporte de novedades, ya en este módulo, el usuario selecciona el botón reporte de incidentes de seguridad.

Se debe tener claro que la base de datos a la que se quiere reportar el incidente debe estar finalizada y activo, teniendo conocimiento el sistema abrirá una ventana emergente de aquellas bases de datos a las que se les puede reportar el incidente, se debe seleccionar una base de datos a la que se quiere reportar y por consiguiente se selecciona el botón registrar novedad, posteriormente se selecciona la opción agregar reporte de incidentes, esto despliega la ventana para ingresar la información solicitada para el tipo de incidente y la causal. Allí, se selecciona una de las opciones de la lista que despliega cada ítem, la fecha del incidente será en la cual ocurrió la vulneración de seguridad de la base de datos y la fecha de conocimiento será en la que se detectó dicha vulneración.

En el cuadro de descripción debe ingresar el por qué se va a eliminar la base de datos, si adicionalmente requiere y se desea ampliar la descripción se adjunta un archivo pdf en el botón adjuntar archivo, este no puede superar los 3 megabytes en información comprometida.

Si la opción seleccionada es algunos datos, el RNBD habilitará el campo tipo de información para que seleccione las categorías de datos que conforman la base de datos, agregando cada una de ellas; en caso de ser necesario de manera individual el sistema también pedirá la cantidad de titulares afectados. El mismo procedimiento se debe realizar tantas veces como tipos de información se hayan visto afectada.

Finalmente, según lo exige la SIC, se debe tener en cuenta que la cantidad de titulares afectados no pueden superar la cantidad de titulares que tiene la base de datos. Finalmente, el proceso de denuncia culmina al dar clic en la casilla de verificación para guardar y radicar.

La oficina de Control Interno evidenció que, el IDEAM, mediante Resolución 2821 de diciembre 14 de 2016, adoptó la política de protección de datos, la cual contiene dicha política y el procedimiento para garantizar el adecuado cumplimiento de la citada ley.

Igualmente, cuenta con un Manual de Políticas de Seguridad de la Información E-GI-M002 v1, de fecha 31/12/2020, el cual define los lineamientos que permitan al IDEAM, asegurar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

Así Mismo, el procedimiento de inscripción en el Registro Nacional de Base de Datos – RNBD, utilizado por parte del

Instituto, es el establecido por la Circular Externa No. 0001 de 2015 expedida por la SIC y la Circular Presidencial No. 01 de 2019.

La Oficina de Control Interno, evidenció que, el Instituto se encuentra registrado en el Registro Nacional de Base de Datos – RNBD, dando cumplimiento a lo establecido en la normatividad vigente, de acuerdo con la información reportada y la verificación realizada a la plataforma de la Superintendencia de Industria y Comercio, "Consulta del registro de las Bases de Datos inscritas", En esta sección se encuentran las bases de datos con información personal que el Responsable del Tratamiento ha inscrito en el RNBD, por el IDEAM como entre otros a saber:

- Inventario de Compuestos Bifenilos Policlorados-PCB
- Hojas de vida – Digital.
- Gestión de Datos Geográficas.
- Procesos Judiciales y Administrativos.
- Contratos Oficina Asesora Jurídica.
- Informática.

En cuanto a las políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos por parte de los titulares, se sigue lo estipulado en la resolución del IDEAM número 2821 de 2016, por la cual se adopta la Política de Protección de Datos en el Instituto de Hidrología, Meteorología y Estudios Ambientales.

Por otra parte, de acuerdo con lo informado por la Oficina de Informática, el IDEAM tiene información en la nube y su acceso se limita mediante autenticación de usuarios de dominio y políticas de lista de accesos. Para la información que reposa en el datacenter se debe ingresar autenticado por usuario de dominio y a esta información se aplican políticas de control de acceso bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Para tal efecto la Resolución 2821 de 2016, en sus numerales 9 y 11 dispone:

"(…)

9. SEGURIDAD DE LA INFORMACIÓN

El IDEAM, está comprometido en efectuar un correcto uso y tratamiento de los datos personales contenidos en sus bases de datos, evitando el acceso no autorizado a terceros que puedan conocer o vulnerar, modificar, divulgar y/o destruir la información que allí reposa. Para este fin, cuenta con protocolos de seguridad y acceso a los sistemas de información, almacenamiento y procesamiento, qu incluyen medidas físicas de control de riesgos de seguridad.

Permanentemente se realiza monitoreo al sistema a través de análisis de vulnerabilidades. El acceso a las diferentes bases de datos se encuentra restringido incluso para los empleados y colaboradores. Todos los funcionarios se encuentran comprometidos con la confidencialidad y manipulación adecuada de las bases de datos atendiendo a los lineamientos sobre tratamiento de la información establecida en la Ley.

La información personal suministrada para acceso a los servicios que lo requieren por aplicativos de diferentes a los canales de atención al ciudadano, está asegurada por una clave de acceso a la cual

sólo el usuario puede acceder y que sólo él conoce; el usuario es el único responsable del manejo de dicha clave; en lo referente a los aplicativos, ninguna transmisión por Internet es absolutamente segura ni puede garantizarse dicho extremo, el usuario asume el hipotético riesgo que ello implica, el cual acepta y conoce, en consecuencia es responsabilidad del usuario tener todos los controles de seguridad en sus equipos o redes privadas para su navegación hacia el portal del IDEAM.

El IDEAM ha implementado todos los mecanismos de seguridad de los que dispone acorde con los tramites y servicios del Instituto. Además, ha desplegado una serie de documentos y actividades a nivel interno para garantizar el correcto funcionamiento; en todo caso, el IDEAM no se responsabiliza por cualquier consecuencia derivada del ingreso indebido o fraudulento por parte de terceros a la base de datos y/o por alguna falla técnica en el funcionamiento.[2]

(…)

Cuando los datos personales son suministrados de manera voluntaria, los mismos son almacenados en la base de datos pertinente de acuerdo al servicio o trámite adquirido; en consecuencia, quien tiene acceso a estos datos (funcionario – contratista) está obligado a garantizar la confidencialidad de la información, garantizando la protección de los datos personales de los usuarios

(…)

- ***Principio de seguridad:*** *La información sujeta a tratamiento por el IDEAM, se deberá manejar con las ¿medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

- ***Principio de confidencialidad****: Todas las personas que, en el IDEAM, administren, manejen, actualicen o tengan acceso a informaciones de cualquier tipo que se ncuentre en Bases de Datos, están obligadas a garantizar la reserva de la información personal que en ellas repose.*

(…)

11. DEBER DE SECRETO Y CONFIDENCIALIDAD

El IDEAM garantizará y exigirá a cada persona que intervenga en cualquier etapa del tratamiento de los datos de carácter personal privado, sensible o de niños o adolescentes, el secreto profesional, respecto de los mismos y al deber de guardarlos, obligación que subsistirá aún después de finalizar sus relaciones contractuales con el IDEAM.

El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la normatividad vigente laboral y disciplinaria.

(…)

Cuando los datos personales son suministrados de manera voluntaria, los mismos son almacenados en la base de datos pertinente de acuerdo al servicio o trámite adquirido; en consecuencia, quien tiene acceso a estos datos (funcionario – contratista) está obligado a garantizar la confidencialidad de la información, garantizando la protección de los datos personales de los usuarios".

Así mismo, en el Manual de Políticas de Seguridad de la Información (Código: E-GI-M002), se indica:

9. SEGURIDAD DE LOS RECURSOS HUMANOS (…)

Lineamientos:

- *Los funcionarios, contratistas, aspirantes/candidatos, ciudadanos deberán autorizar al IDEAM, el tratamiento de datos personales, de acuerdo con la normativa legal vigente, Ley 1581 de 2012, para el cual se regula el manejo de la información personal almacenada en las bases de datos, para tal fin la entidad deberá informar al titular sobre la autorización de tratamiento de datos personales.*

(…)

12. 4. TÉRMINOS Y CONDICIONES DE EMPLEO

(…)

- *En los procesos contractuales se deberá incluir cláusulas que permitan dar cumplimiento y contribución a la protección de los Derechos de autor, propiedad intelectual, tratamiento y protección de datos personales, acceso a la información.*

(…)

12.23. CONTROLES DE ACCESO FÍSICOS

(...)

- *La oficina de Informática, deberá controlar el ingreso y salida a los centros de datos y centros de cableado así mismo registrar y verificar el Ingreso y salida de elementos de tecnología de estas áreas, igualmente en caso de requerir acceso por parte de personal ajeno a la entidad, este deberá estar supervisado y acompañado por quien sea autorizado, éste se hará responsable de la estadía durante el tiempo de permanencia en las instalaciones.*

(...)

20. CUMPLIMIENTO

(…)

- *La entidad deberá definir, aprobar y mantener actualizada una política para la regulación, tratamiento de datos personales conforme a la ley 1581 de 2012. (…)".*

La oficina de Control Interno pudo establecer que, de acuerdo con lo señalado en la citada resolución el Instituto se encuentra comprometido en dar un correcto uso a la información de la base de datos que tiene en custodia, con el fin de que estos no puedan ser vulnerados por terceros, de igual manera se indica allí, que se realiza un monitoreo permanente, el cual debe ser realizado por el Oficial de Seguridad quien es funcionario de la Imprenta Departamental Soluciones Integrales y de las Tecnologías de la Información y Comunicaciones – IMPRETIC´S E.I.C.E, de acuerdo con lo establecido en el contrato 464 de 2020, responsable de verificar políticas y procedimientos, y adicionalmente el Instituto tiene formalizado y divulgado en el SIG, los siguiente documentos:

- Manual de Políticas de Seguridad de la Información (Código: E-GI-M002)

- Procedimiento de Incidentes de seguridad
- Formato de Incidentes de Seguridad.
- Procedimientos.

En lo correspondiente al Manual de Políticas de Seguridad de la Información (Código: E-GI-M002) Versión 1.0 de fecha 31/12/2020, cuyo objetivo es: Definir Lineamientos que permitan al IDEAM, asegurar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

La Oficina de Control Interno considera que este se encuentra en etapa de maduración, por lo que se realizará un próximo seguimiento con el fin de verificar su cumplimiento y eficacia, pues de acuerdo con lo anteriormente expuesto el citado manual inicio su aplicación el 31 de diciembre de 2020.

En cuanto, al mecanismo para actualizar la información de los reclamos presentados por los titulares es el "Formulario PQRS" establecido mediante resolución 2628 del 18 de noviembre de 2016 del IDEAM, su propósito consiste en trazar de forma clara y detallada, la ruta que debe seguirse al interior del IDEAM, para la correcta presentación, radicación y constancia de las peticiones que se presenten al Instituto por cualquiera de los medios dispuestos para la atención al ciudadano.

El IDEAM para dar cumplimiento a lo establecido en el Derecho de Habeas Data que permite a los ciudadanos conocer, actualizar y rectificar toda la información que tengan las diferentes entidades y bases de datos del país, mediante la Resolución número 2821 de 2016, constituye el procedimiento que sigue la entidad para Garantizar al titular, el pleno y efectivo ejercicio del derecho de hábeas data.

De otra parte, el Instituto realiza la actualización, rectificación o supresión de los datos en los términos de la presente ley, de acuerdo con los lineamientos establecidos en el numeral 8.1.2 de la Resolución 2821 de 2016, que dispone:

> **8.1.2. Para presentar una solicitud de corrección, actualización o supresión de datos, o para presentar reclamo por presunto incumplimiento de los deberes del IDEAM relacionados con la Protección de Datos:**
>
> 1. La solicitud se puede presentar por cualquiera de los canales dispuestos para atención al ciudadano.
>
> 2. La solicitud o reclamo debe realizarse a través de comunicación dirigida al IDEAM, con el nombre completo del titular, la descripción de los hechos que dan lugar a la solicitud o reclamo, datos para notificación y los documentos que soportan el reclamo; si la solicitud o reclamo resulta incompleto, se le requerirá dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
>
> 3. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de (2) días hábiles, e *informará* de la situación al interesado.
>
> 4. Las solicitudes de actualización, corrección, rectificación o supresión de los datos serán entestadas dentro de los quince (15) días hábiles siguientes, contados a partir del día siguiente la fecha de su recibo. Cuando no fuere posible atender la solicitud dentro del término señalado e informará al interesado antes del vencimiento del referido plazo manifestando de manera expresa los motivos de la demora y la fecha en que se atenderá la solicitud,

la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Igualmente, de acuerdo con la respuesta dada por las Oficinas Asesora Jurídica e Informática mediante memorandos radicados Nos. 20211020001483 y 20211040002703 de fecha 7 y 26 de abril de 2021 respectivamente, dieron respuesta en el sentido que el mecanismo utilizado para informar a la Superintendencia de Industria y Comercio cuando se presentan violaciones a los códigos de seguridad es el que establece dicha entidad, según Circular 003 de 2018, estos incidentes de seguridad se refieren a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, los cuales deberán reportarse al RNBD por parte de los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

Es de aclarar que, la información relacionada con las medidas de seguridad, los reclamos presentados por los Titulares y los incidentes de seguridad reportados por el RNBD no estará disponible para consulta pública, de acuerdo con la citada circular.

De acuerdo con la respuesta dada por los responsables de la información, en caso de presentarse pérdida robo o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, para que se pueda registrar un incidente, el usuario del IDEAM debe seleccionar el botón reporte de incidentes de seguridad.

Se debe tener claro que la base de datos a la que se quiere reportar el incidente debe estar finalizada y activo, teniendo conocimiento el sistema abrirá una ventana de aquellas bases de datos a las que se les puede reportar el incidente.

Respecto a la Seguridad de la Información el Gobierno Nacional ha establecido la estrategia de Gobierno Digital mediante el Decreto 1008 de 2018 en el cual se establecen los componentes, habilitadores transversales, responsables de su implementación y principios de la estrategia de Gobierno Digital.

Determinada su importancia y la necesidad de evaluar, mantener y mejorar la Gestión de Seguridad de la Información, cabe resaltar que la Oficina de Control Interno realizará auditorías internas en materia de Tecnología y Seguridad de la Información, evidenciando (i) la existencia de diferentes elementos que dan cuenta de la implementación de un Sistema de Gestión de Seguridad de la Información, (ii) que dicho sistema se encuentra en fase de mejora continua. Lo cual se verificará durante la Auditoría a realizarse a Tecnología de la Información - Gestión de Tecnología de Información y Comunicaciones, en donde se evaluará la aplicación normativa, procedimental, actividades y riesgos del proceso auditado.

Para la continuación del desarrollo de este seguimiento, se procedió a solicitar mediante correo electrónico de fecha 10 de mayo de 2021, la siguiente información, con el fin de verificar y evaluar los soportes documentales:

a. Informes de avance revisión y/o seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información.

La Oficina de Control Interno, una vez verificado el Plan de implementación modelo de seguridad y Privacidad de la

información, evidenció que, este contempla actividades para los siguientes componentes con fecha máxima de ejecución 31 de diciembre del presente año:

Activos de información

Gestión de Riesgos

Gestión de Incidentes

Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación

Matriz de verificación de Requisitos Legales de Seguridad de la Información

Plan de Continuidad del Negocio

Acciones correctivas y Notas de mejoras SGSI

Planeación

Auditorías Internas y Externas

Revisión de los controles de la norma ISO 27001:2013

Indicadores SGSI

Vulnerabilidades

Se evidenció, Informe de gestión mensual de PSPI, correspondiente al mes de abril de 2021, en el cual se detallan las siguientes actividades entre otras.

- Cumplimiento de actividades contractuales

- Seguimiento a las actividades realizadas durante el periodo de ejecución del objeto contractual

- Estrategia de Gobierno Digital – Ciberseguridad.

- Seguimiento de los controles de seguridad de la información.

Una vez revisada y verificada la información suministrada se concluye que este informe fue elaborado y presentado por la firma Imprenta Departamental Soluciones Integrales y de las Tecnologías de la Información y Comunicaciones – IMPRETICS´S E.I.C.E, que presta el servicio de outsourcing al Instituto, como lo establece el contrato 464 en las obligaciones del contratista.

b. Reportes y otros registros técnicos de los sistemas de información, equipos de cómputo, y plataformas

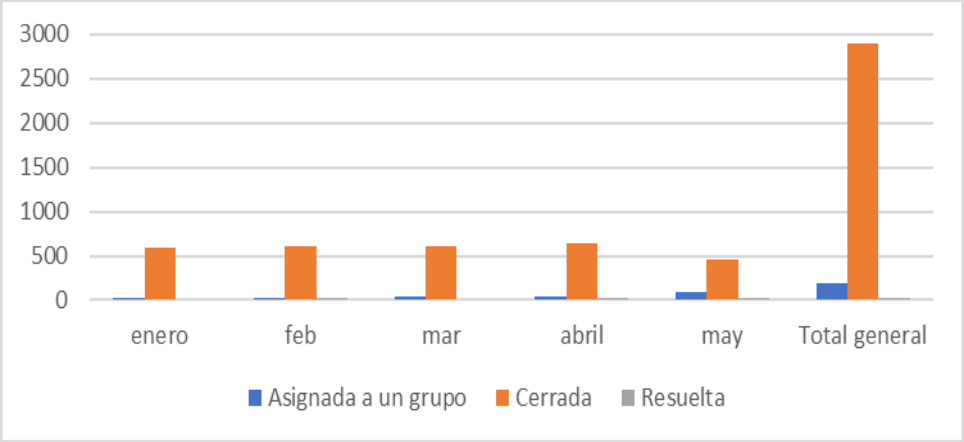
tecnológicas que sean objeto de la revisión de aplicación de políticas de seguridad, la Oficina de informática para este ítem anexo las siguientes evidencias:

- Listado de usuarios correo electrónico: archivo: "Usuarios Correo electrónico 20210518.xlsx"
- Matriz de escalamiento del sistema de Monitoreo de servicios Nagios, archivo: "Nagios matriz de escalamiento.docx".
- Listado de casos atendidos por ProactivaNET en la presente vigencia, archivo: "Casos 2021 ProactivaNET.xlsx"
- Listado de VPN:

Listado de usuarios del directorio activo, archivo: "Usuarios_ldap.xlsx".

- En relación con sistemas de información, se adjuntan listados de usuarios de:
- Listado usuarios sistema de gestión de datos hidrológicos y meteorológicos, archivo: "Usuarios_Grupos_DHIME.xlsx".
- Listado usuarios sistema de gestión documental, archivo: "Usuarios_ORFEO.xlsx".
- Listado usuarios portal institucional; archivo: "Usuarios_Portal_IDEAM.xlsx".
- Listado usuarios sistema nacional de información forestal - SNIF; archivo: "Usuarios_SNIF.xls".
- Listado usuarios sistema Suite visión empresarial; archivo: "Usuarios_SVE.xlsx".

La Oficina de Control Interno, revisó aleatoriamente la información remitida, observando que, para los casos atendidos por ProactivaNET en la presente vigencia, archivo: "Casos 2021 ProactivaNET.xlsx", se han recibido 3119 casos durante el periodo enero – mayo de 2021, (ver gráfica).



De la gráfica anterior la Oficina de Control Interno concluye que, de los 3119 casos presentados durante el periodo comprendido entre enero y mayo de 2021, se tiene que:

- Asignadas a un grupo pendientes de solución de enero a mayo, se evidenciaron 193 que equivalen al 6% del total de los casos.
- Resueltas durante el mismo período 31 y
- Cerradas durante el periodo enero – mayo se observa un total de 2.895

Igualmente, se pudo establecer que, todas las solicitudes tienen registrado el nombre de la persona que notifica el caso, así como todas las solicitudes tienen asignado un responsable del caso.

Por otra parte, se analizó Listado usuarios portal institucional; archivo: “Usuarios_Portal_IDEAM.xlsx”, evidenciando que este se encuentra actualizado.

Una vez revisado el listado usuarios sistema Suite visión empresarial; archivo: “Usuarios_SVE.xlsx”. el cual cuenta a la fecha de este seguimiento con 400 usuarios con su respectivo login, dando cumplimiento con los reportes y otros registros técnicos de los sistemas de información.

c. Reportes, informes de supervisión u otros pertinentes para los contratos de prestación de servicios profesionales u otros enmarcados dentro del Sistema de Gestión de Seguridad de la Información y/o la disposición de plataformas y servicios tecnológicos, la Oficina de informática anexo la carpeta correspondiente adjuntando las siguientes evidencias.

- Contrato prestación de servicios de soporte y administración y operación de la plataforma tecnológica (Outsourcing) Contrato 464/2020.

- Contrato prestación de servicios de centro de datos alterno para el plan de DRP, contrato 443 – 2021.
- Contrato Licencias de software que incluyen el correo electrónico: contrato 443 – 2019,
- Documento de estudios previos que se adelantan para la contratación del servicio: "Renovación de extensión de garantías, actualización y soporte para web Access firewall, firewall y red inalámbrica".
- Contrato de prestación de servicios 125-2021, para mantenimiento evolutivo de sistemas de información misionales, suscrito con SANDRA YANETH MORENO CRUZ.

Para tal efecto la OCI, verificó los contratos: Contrato prestación de servicios de soporte y administración y operación de la plataforma tecnológica (Outsourcing) Contrato 464/2020, del cual se observó:

- Contrato interadministrativo No. 464 de fecha 30 de noviembre de 2020 celebrado entre el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM e Imprenta Departamental Soluciones Integrales y de las Tecnologías de la Información y Comunicaciones – IMPRETIC´S E.I.C.E cuyo objeto fue prestar el servicio de soporte, administración y operación de la plataforma tecnológica del Ideam, incluyendo la herramienta de gestión; todo esto enmarcado en la implementación y ejecución de procesos bajo la metodología itil versión 2011 O. Cabe destacar que el contrato en mención se encuentra en ejecución, pues será hasta por doce (12) meses, sin sobrepasar el 30 de noviembre de 2021, con un valor total de Dos Mil Ciento Cincuenta y Siete Millones Setecientos Cincuenta Mil Pesos ($2.157.750.000) IVA incluido.

  Una Vez revisados los documentos soporte, se encontraron 9 informes tales como; 202104 Informe Gestión MS Abril TI IDEAM, 202104 Informe Gestión Liferay Abril OI TI IDEAM, 202104 Informe Gestión Pruebas Abril OI TI IDEAM y 202104 Informe Gestión Bases de datos Abril OI TI IDEAM, dando cumplimiento a este ítem.

- Contrato de prestación de servicios 125-2021, suscrito con SANDRA YANETH MORENO CRUZ, cuyo objeto es prestar el soporte informático, atención a incidencias y mantenimiento evolutivo a los aplicativos administrados por la SEA: SISAIRE y PCB, este se encuentra en ejecución ya que va hasta el 15 de diciembre de 2021, previo cumplimiento de los requisitos de ejecución del contrato. Por un valor total de SESENTA Y CUATRO MILLONES TRESCIENTOS SESENTA Y OCHO MIL PESOS ($ 64.368.000) sin IVA, incluyendo todos los costos.

Recomendación

Una vez revisadas las evidencias, se observó que, en las consideraciones de la minuta del contrato en su literal *"d) Que el criterio adoptado por EL INSTITUTO para fijar los honorarios del CONTRATISTA, para la vigencia 2021 corresponde a la suma de SEIS MILLONES CUATROSCIENTOS OCHENTA SIETE MIL PESOS ($6.480.000) sin IVA, corresponde a la aplicación de la tabla de honorarios adoptada por el INSTITUTO a través de la Resolución No. 002 de del 05 de enero de 2021".*

La oficina de Control Interno, recomienda ajustar el valor en letras en la minuta del contrato "consideraciones literal d)".

d. Reportes de Actividades y Metas Operativas.

- Plan de acción anual oficina de informática, informe de avance primer trimestre 2021: "Seguimiento PAA primer trimestre 2021.xlsx".

Revisado el PAA 2021, de la Oficina de Informática se evidenció 5 actividades para el presente año y de acuerdo con la verificación realizada a los soportes documentales remitidos por la oficina de Informática a marzo de 2021, se observó que, se viene dando cumplimiento con el porcentaje de avance programado.

e. Incidentes de Seguridad de la Información.

Reporte de ProactivaNet de casos o incidentes escalados relacionados con seguridad de la información. Archivo: "Casos Seguridad Informacion.xlsx. (soporte revisado en el literal b.).

f. Inventario de activos de Información.

El artículo 37 del Decreto 103 de 2015 (2.1.1.5.1.1. del Decreto 1081 de 2015), dispone:

> *"Artículo 2.1.1.5.1.1. Concepto del Registro de Activos de Información. El Registro de Activos de Información es el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal".*

Por otra parte, el Artículo 38 del citado Decreto (2.1.1.5.1.1. del Decreto 1081 de 2015), establece:

> ***"Artículo 38.*** Componentes del Registro de Activos de Información*. El Registro de Activos de Información debe contener, como mínimo, los siguientes componentes:*
>
> *(1) Todas las categorías de información del sujeto obligado.*
>
> *(2) Todo registro publicado.*
>
> *(3) Todo registro disponible para ser solicitado por el público.*

La oficina de Control Interno, evidenció que, el Instituto cuenta con el Formato Inventario de Activos de Información CÓDIGO: E-GI-F001 VERSION: 002 FECHA: 21/07/2020, en el cual se detalla el instructivo de diligenciamiento paso a paso, dando cumplimiento a lo establecido en la normatividad vigente.

En lo concerniente a la actualización de la información contenida en el Registro Nacional de Bases de Datos – RNBD de acuerdo con la Circular 003 de 2018, este se realiza por parte del IDEAM, anualmente, entre el 2 de enero y el 31 de marzo, a partir de 2020, a través del portal web de la Superintendencia de Industria y Comercio, por el encargado

del tratamiento.

7. FORTALEZAS

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

1. En el desarrollo del Seguimiento se observó que el Instituto cuenta con herramientas tecnológicas que le permiten tomar decisiones para mejorar los servicios de la entidad frente al Sistema de Protección.
2. Se evidenció una buena estructura y resultados del programa ProactivaNET, un modelo de vigilancia preventiva con objetivos claros y medibles.

8. HALLAZGO Y OBSERVACIONES DETECTADAS

H/NC	OBS	DESCRIPCIÓN (Debe contener criterio afectado)	RECOMENDACIONES

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. CONCLUSIONES

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

1. El Instituto expidió la Resolución 2821 de diciembre 14 de 2016 en la cual se adopta la política de protección de datos, con el fin de garantizar el adecuado cumplimiento de la normatividad vigente.
2. Verificados los documentos soporte allegados se encontró, en la minuta del contrato 125 de 2021, que este debe ser modificado de acuerdo con la observación realizada.
3. La oficina de Informática cumple con los reportes de ProactivaNet de casos o incidentes relacionados con seguridad de la información.
4. El IDEAM cuenta con un documento denominado E-GI-M002 Manual de Políticas de Seguridad de la Información v1 de fecha 31/12/2020, el cual se encuentra en etapa de maduración.
5. El IDEAM reporta a la Superintendencia de Industria y Comercio, según lo establecido en la Circular 003 de 2018, esto es anualmente entre el 2 de enero y el 31 de marzo, a partir de 2020, en el portal web de la Superintendencia.
6. Limitación en la obtención de la información por parte de los responsables de su entrega, ya que para la segunda solicitud realizada el día 10 de mayo de 2021 con plazo de entrega el 12 del mismo mes, ésta se allegó por parte de

la Oficina de Informática hasta el día 24 de mayo y para el caso de la Oficina Asesora Jurídica a la fecha del cierre de este informe no se recibió.

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
Nombre: Carlos Hernán Rodríguez Rodríguez. Cargo: Contratista -OCI	Auditor Líder	
Nombre: Gilberto Antonio Ramos Suarez. Cargo: Jefe Oficina Asesora Jurídica Alicia Barón Leguizamón. Cargo: Jefe oficina de Informática	Líder del Proceso	

10. EVIDENCIAS FOTOGRÁFICAS

11. CONTROL DE APROBACIÓN INFORME DE AUDITORÍA INTERNA

CONTROL INFORME DE AUDITORÍA INTERNA		
ELABORÓ:  Carlos Hernán Rodríguez Rodríguez Cargo: Contratista Oficina de Control Interno.	**REVISÓ:** PATIÑO JURADO MARÍA EUGENIA Firmante: CN=PATIÑO JURADO MARÍA EUGENIA C=CO O=INSTITUTO DE HIDROLOGIA METEOROLOGIA Y ESTUDIOS AMBIENTALES 2.5.4.97=NITCO-830000602S Llave publica: RSA/2048 bits María Eugenia Patiño Jurado Jefe Oficina de Control Interno	**APROBÓ:** 2021.06.17 13:00: María Eugenia Patiño Jurado Jefe Oficina de 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-CHR-08-06-2021

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**