INSTITUTO DE HIDROLOGÍA METEOROLOGÍA Y ESTUDIOS AMBIENTALES - IDEAM

RESOLUCIÓN N.° 0371 **de** 30 de abril 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"

LA DIRECTORA GENERAL DEL INSTITUTO DE HIDROLOGÍA, METEOROLOGÍA Y ESTUDIOS AMBIENTALES - IDEAM

En ejercicio de sus facultades legales y en especial las conferidas por el artículo 4 de la Ley 87 de 1993, el artículo 5 del Decreto 291 de 2004, el artículo 2.2.2.2.1 del Decreto 1083 de 2015, y

CONSIDERANDO QUE:

La Constitución Política de Colombia en su artículo 15, estipula que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución Política. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Los artículos 209 y 269 de la Constitución Política establecen que la Administración Pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley. Por ello las autoridades de las entidades públicas están en la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control Interno.

El artículo 17 de la Ley Estatutaria 1581 de 2012 *"Régimen General de Protección de Datos personales",* consagra la necesidad de garantizar de forma integral la protección y el ejercicio del Derecho Fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

La Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

El artículo 2.2.9.1.1.3. del Decreto 1078 de 2015, subrogado por el artículo 1 del Decreto 1008 de 2018, determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través de este se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

El artículo 2.2.9.1.2.1. del Decreto 1078 de 2015, también subrogado por el artículo 1 del Decreto 1008 de 2018, estableció que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la

Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Igualmente, el artículo 1 del Decreto 1499 de 2017 sustituyo el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015. El nuevo artículo 2.2.22.1.1 del Decreto 1083 de 2015, señala que el Sistema de Gestión, que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad.

El artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital". En el 2.2.22.3.2. del Decreto 1499 de 2017 se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

El Documento CONPES 3995 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo 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 y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El IDEAM adoptó su política de seguridad y privacidad de la información mediante Resolución No. 0390 del 15 de marzo del 2016, sin embargo es necesaria su actuazliacion debido a los nuevos hitos de seguridad que se han detectado y que deben soportar la política del SGSI de la entidad.

De acuerdo con el acta del Comité del Comité de Gestión y Desempeño Institucional # 36 realizado el 26 de marzo del 2021, se aprobó la actualización de la "*Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM",* ajustada a los cambios estipulados en la política de Gobierno Digital y Seguridad Digital.

En virtud de lo anterior, es necesario actualizar mediante acto administrativo, 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.

En merito de lo expuesto,

RESUELVE:

CAPITULO I

DISPOSICIONES GENERALES

ARTÍCULO 1. Objeto: La presente Resolución tiene como objeto adoptar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM, así como definir los lineamientos frente al uso y manejo de la información

ARTÍCULO 2. Ámbito de Aplicación: La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, aplica a todos los niveles funcionales y organizacionales del IDEAM, a todos sus funcionarlos, contratistas, proveedores, operadores, así como aquellas personas o terceros que en cumplimiento de sus funciones y las del Instituto, utilicen, generen, procesen, recolecten, consulten, compartan e intercambien su información, así como a las entidades de control, y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el IDEAM en el marco de la operación por procesos y en cumplimiento a sus objetivos institucionales, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

ARTÍCULO 3. Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la Operación de los Servicios del IDEAM. El IDEAM, con la adopción e implementación de la Política Nacional de confianza y seguridad digital enmarcado en el Modelo de Seguridad y Privacidad de la información enmarcado en el Sistema de Gestión de Seguridad de la Información, tiene como propósito asegurar la confidencialidad, integridad, disponibilidad, no repudio y autenticidad de la información, con el desarrollo de buenas prácticas que permitan a la entidad gestionar de forma integral riesgos de seguridad y privacidad de la información y seguridad digital, para la prevención de incidentes que puedan comprometer o generar perjuicios severos al IDEAM, es así que también se debe dar un enfoque a la mejora continua y propender por el alto desempeño del Sistema de Gestión de Seguridad de la Información.

La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM es la declaración general que representa la disposición de la administración del IDEAM, con respecto a la protección de los activos de información (Procesos, Personas y tecnologías de Información incluido el hardware y software), que soportan los procesos de la entidad y apalancan la implementación del sistema de gestión de seguridad de la información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

ARTÍCULO 4. Objetivo general. La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM tendrá los siguientes objetivos:

1. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información, de seguridad digital y continuidad de la operación de los servicios.

2. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.

3. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del IDEAM.

4. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.

5. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital

6. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

7. Definir, operar y mantener el Plan de Continuidad de la Operación de los servicios del IDEAM

8. Proteger los activos de información

9. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información

CAPITULO II

POLÍTICAS ESPECÍFICAS DE MANEJO DE INFORMACIÓN

ARTÍCULO 5. Objetivos específicos. Las políticas definidas tienen como objetivo establecer, estandarizar y normalizar la seguridad de las personas, las tecnologías y los procesos, a partir de un conjunto de directrices, normas, procedimientos e instrucciones que guíen las actuaciones de trabajo y definan los criterios de seguridad que deben ser adoptados a nivel institucional en el IDEAM. Con su divulgación se busca que todos los funcionarios, contratistas, practicantes y terceros que ofrezcan servicios al IDEAM, conozcan el presente plan y de forma individual y colectiva brinden su apoyo para el cumplimiento del mismo, con niveles adecuados de

seguridad, así mismo aplican a todos los funcionarios, contratistas, pasantes y terceros que utilicen recursos del IDEAM. Estas políticas deben ser revisadas y en caso de necesitarse, actualizarlas periódicamente para garantizar que siguen siendo adecuadas, suficientes y eficaces para el sistema de gestión de seguridad de la información.

ARTÍCULO 6. Políticas de seguridad. La protección de los activos de información del IDEAM, han sido y continuarán siendo una de las mayores preocupaciones del Instituto. Las tecnologías cambiantes, hacen que los sistemas sean mayormente optimizados y requieran más recursos y compromiso de la alta gerencia, auspiciando a los procesos del Instituto y evitando que existan brechas de seguridad de la información. Esto tendrá un impacto sobre nuestros programas de seguridad existentes y afectará las medidas de procedimiento de seguridad, que den a lugar a implementar tanto existentes como futuras políticas de seguridad.

Para responder a este ambiente de cambio, el Oficial de Seguridad de la Información o quien haga sus veces desarrollará las políticas necesarias, para la aprobación, con el fin de proteger a todos los activos de información y recursos institucionales. (Por ejemplo: software o información sin importar en qué medio se encuentre).

El Oficial de Seguridad de la Información o quien haga sus veces con el apoyo del Grupo de Seguridad Informática o quien haga sus veces, serán los encargados del desarrollo y mantenimiento de las políticas de seguridad, para administrar y proteger los recursos y para coordinar el desarrollo de los procedimientos necesarios para ejecutar las políticas aprobadas.

El Oficial de Seguridad de la Información, coordinará el desarrollo de un Plan de Continuidad del Negocio y el Plan de Recuperación de Desastres para la sede central y velará por la realización de un plan de sensibilización para todos los funcionarios y será el encargado de reportar al comité institucional de gestión y desempeño los abusos reales y/o sospechados de las Políticas de Seguridad aprobadas.

El Oficial de Seguridad de la Información y el Jefe de la Oficina de Informática, de ser necesario en el comité institucionales de gestión y desempeño proveerán un reporte escrito el cual incluirá la evaluación de las políticas, procedimientos y medidas de seguridad que están siendo adoptadas; de darse el caso un resumen de violaciones sospechosas de seguridad y las medidas adoptadas para mitigarlas.

Cualquier funcionario, contratista o tercero que brinde servicios al Instituto, de no cumplir con políticas de seguridad de información aprobadas, puede dar lugar a acción disciplinaria. La acción disciplinaria será la que designe la oficina de control interno disciplinario, así como de requerirse se entregará el caso al órgano competente.

PARÁGRAFO. Acceso a los servicios de información: Todos los funcionarios públicos, contratistas, pasantes y terceros que brinden sus servicios al Instituto, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de requerirse acceso a recursos de información, por ejemplo, por un proyecto nuevo, solo las personas responsables deben autorizar el acceso a los recursos indispensables de acuerdo con el trabajo a realizar, previa justificación.

Los funcionarios, contratistas, aspirantes/candidatos, proveedores y ciudadanos deberán autorizar al IDEAM, el tratamiento de datos personales, de acuerdo con la normativa legal vigente, de conformidad con el Reglamento (UE) 2016/679 ("GDPR") y la 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.

Todos los privilegios de acceso para el uso de los sistemas de información deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios al Instituto.

El grupo de Administración y Desarrollo de Talento Humano debe notificar a la Oficina de Informática cuando un funcionario es transferido o deja el instituto o la Oficina Asesora Jurídica en caso de tratarse de un contratista. La falta de notificación de dichas transferencias o salidas, será incluida en el reporte y enviada al Grupo de Arquitectura Empresarial TI y Seguridad de la Información. También deben notificar a la Oficina de Informática cuando un funcionario o contratista es reemplazado por licencia médica, o es asignado a un proyecto especial que no requiera que el funcionario deba acceder al sistema por un periodo superior a un mes, u otras circunstancias similares.

Para dar acceso a la información, se tendrá en cuenta la clasificación de la misma al interior de la Instituto, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Instituto.

Las solicitudes para permisos de acceso a las diferentes aplicaciones, deben ser radicadas en la plataforma con que se cuente en su respectivo momento mediante el formato formalizado para la creación de usuarios respectivamente.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica, se efectuará un seguimiento a los accesos realizados por los usuarios a la información del Instituto, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

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.

Administración de usuarios (*Kronos*): El Administrador de Dominio debe asignar una identificación o nombre de acceso único a cada rol, funcionario o contratista dentro del IDEAM, para tener una única clave de acceso a la red, aplicaciones y servicios del instituto excepto para los dispositivos que operan en un modo independiente. Los nombres de acceso asignados por el Administrador de Dominio serán uniformes a través de todas las plataformas dentro del Instituto y la clave inicial asignada, también deberá ser la misma a través de todas las plataformas en que el individuo tenga un acceso autorizado.

La contraseña de acceso debe tener una longitud no menos de 8 caracteres alfabéticos y numéricos con caracteres especiales, la frecuencia con la que los usuarios deben cambiar su contraseña y los periodos de vigencia de las mismas debe ser cada 60 días o cuando se sospeche que la clave haya sido comprometida. La clave no podrá ser reutilizada antes de seis meses.

Los sistemas están programados para que la contraseña del funcionario que sea requerido, entre separadamente de la identificación de acceso y de tal forma que la contraseña no sea mostrada en la pantalla cuando se ingrese.

Las rutinas de seguridad de los sistemas de computadores, estarán programadas para que se bloquee automáticamente cuando el usuario cuyo nombre de identificación, haya tenido cinco intentos de acceso sin éxito.

Las suspensiones implementadas deberán ser levantadas por el Administrador de Dominio cuando se determine que el propietario del nombre de identificación, era el usuario que causó la suspensión al olvidar su clave o por otro error humano como errores de digitación y se debe consignar el detalle en la bitácora designada para tal fin.

El Administrador de Dominio podrá suspender identificaciones de acceso de las cuales se sospeche, hayan sido pasadas a través de otra persona diferente al funcionario al cual fue asignada o en cualquier evento que se vulnere la confidencialidad del sistema. El Administrador de Dominio reportará dichas suspensiones al Oficial de Seguridad.

El control de acceso lógico a todos los sistemas informáticos del instituto debe realizarse por medio de códigos de identificación y contraseña únicos para cada usuario o rol.

Se debe realizar el acceso a la red mediante (Identificación, Autenticación, Acceso) por ello las claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas, terceros, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona por ningún medio, en caso tal que se detecte que esta se ha expuesto se tomara la medida correctiva por parte de las áreas involucradas. Se permite la creación de roles basados en cargo a una única persona más se prohíbe tener identificaciones de usuario genéricos. Las identificaciones de usuario deben únicamente identificar individuos o roles específicos.

Los sistemas de información deben tener definidos y documentados los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de cifrado para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los Subdirectores y demás Jefes de Oficina, en conjunto con la persona que para tal efecto defina el Jefe de la Oficina de Informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño del sistema hasta su conversión a un sistema de producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

La implementación de esta política estará coordinada por la Oficina de Informática, con el apoyo de los servicios externos que para tal efecto se requieran y su plazo corresponderá al del plan de trabajo que se establezca conforme a las acciones que deban programarse.

ARTÍCULO 7. Politica de gestión de activos: La Oficina de Informática, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta los siguientes literales, que serán consolidados y publicados según el procedimiento publicado en el SGI.

a. **Inventario de Activos**: Los activos del IDEAM deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres Por tal motivo, la Oficina de Informática, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.

b. Protección: Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Oficina de Informática.

c. Archivos de Gestión: La Secretaria General deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física del IDEAM

d. Clasificación de la Información: La Secretaria General deberá establecer una metodología para la clasificación y rotulado de la información del IDEAM, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Titulo 1 de la Parle 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la Oficina de informática implementará una herramienta informática que permita rotular la información digital y la Secretaria general mecanismos para rotular la información física, de acuerdo con la metodología establecida.

e. Firma de documentos: Las firmas de documentos que produzca el IDEAM será válida en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información de los documentos expedidos por los servidores públicos y contratistas en el marco de sus funciones y competencias:

I. En físico con firma autógrafa mecánica.

II. Con firma digital de persona natural asignadas por la Oficina de Informática según lo dispuesto por la Ley 527 de 1999.

III. Con firma electrónica, de acuerdo con lo dispuesto en el Decreto 2364 de 2012 y el Decreto 1287 de 2020, para lo cual la Oficina de Informática deberá adquirir o implementar un aplicativo integrado con el sistema de gestión documental que contenga como mínimo lo siguiente:

1. Control seguro de acceso y uso al aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado pueda hacer uso del mecanismo de firma electrónica,

2. Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser.

3. El sistema debe solicitar la firma digitalizada o escaneada y quedar estampada en el documento junto con el nombre completo, cargo, correo electrónico institucional del servidor o contratista que firma.

4. Identificador único provisto por el sistema que permita la verificación de la veracidad del documento

5. Fecha de creación y finalización de la firma provisto por el servidor y sincronizado con la hora legal colombiana de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto 4175 de 2011

6. Estado del trámite de firma

7. Firma digital de persona jurídica del IDEAM según sea el caso

8. En ningún caso se debe utilizar firmas facsimil, salvo en aquellos que se autorice por Resolución expedida por la Directora del IDEAM, indicando para que fin y porqué medios podrá ser utilizada.

ARTÍCULO 8. Soporte de subsistemas de información: Todo cambio (creación modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el líder del área funcional del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Bajo ninguna circunstancia, un cambio puede ser aprobado, realizado e implantado por la misma persona responsable o área.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por el IDEAM, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que afecte de la menor manera posible su disponibilidad, deberá darse previo aviso a los potenciales usuarios del sistema o establecer un mecanismo de divulgación de la información.

Anunciar las modificaciones es requerido por el usuario, el Líder Técnico para la planificación de su capacidad, siguiendo la realización de pruebas de aplicaciones, que han pasado por cambios de diseño o nuevas aplicaciones, se deben ajustar antes de puesta en producción, asimismo informar al Administrador de Base de Datos – DBA para la puesta producción o las pruebas de los datos de producción. Adicionalmente el DBA, solicitara esta información, para nuevas aplicaciones y/o acceso de datos adicionales que permita cargar o descargar datos no previamente aprobados para tal fin.

El Líder Técnico deberá autorizar el acceso de cada funcionario o contratista para introducirse a su sistema de aplicación.

Una excepción a esta política, son los cambios de emergencia que sean requeridos por el sistema de producción para completar el ciclo de producción. Estos cambios serán realizados cuando sea requerido. Todos estos cambios serán reportados al siguiente día o al Administrador del Sistema, según aplique.

Este reporte indicará el sistema de aplicación al cual fue hecho el cambio, la razón del cambio, el (Analista o Programador) que lo solicitó, y la persona que hizo el cambio al sistema de producción y todo deberá quedar debidamente reportado en una bitácora asignada para tal fin.

En las aplicaciones cada responsable debe cambiar su propia clave continuamente y esta quedará escrita en un contenedor cifrado que estará a cargo del Oficial de Seguridad. Cada responsable será encargado de asignación de claves para pruebas.

Si un usuario diferente al responsable requiere ingresar como usuario root al sistema operativo, se debe solicitar autorización al jefe de la oficina informática para que se revele la clave de acceso la cual debe ser cambiada e informada al oficial de seguridad por parte del responsable tan pronto retome el control del aplicativo y/o producto asignado.

El Oficial de Seguridad de la Información con apoyo del administrador de aplicaciones auditará periódicamente los sistemas de información en búsqueda de vulnerabilidades, las cuales serán reportadas al administrador de cada sistema para su acción preventiva o correctiva según el caso y correspondiente seguimiento.

ARTÍCULO 9. Gestión de la seguridad de la información: Los funcionarios, contratistas, pasantes y terceros que prestan servicios al IDEAM son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Instituto, así como los derivados de la ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y/o utilización indebida de la misma.

Los funcionarios públicos, contratistas y pasantes no deben suministrar ningún tipo de información del instituto a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los activos de información del IDEAM, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los funcionarios, contratistas, pasantes y terceros que le presten servicios al IDEAM, deben firmar al momento de firma de contrato, un acuerdo de uso de los activos de la información, en el cual se establecen condiciones sobre la confidencialidad y demás requerimientos de seguridad que garanticen el buen manejo de la misma.

Una vez el funcionario, contratista, pasante o tercero que preste servicios al IDEAM, deje de prestar sus servicios al Instituto, se compromete a entregar los activos de información a su cargo. Así mismo el personal que detecte el mal uso de la información, estará en la obligación de reportar el hecho a la dependencia de Control Interno Disciplinario del Instituto.

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción, se debe ejecutar al menos una vez cada cuatro años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según sea el caso.

La Oficina de Informática divulgará las políticas, estándares y procedimientos en materia de seguridad de la información. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la Dirección General, los casos de incumplimiento con copia a la Oficina de Control Interno y Secretaría General para las acciones pertinentes.

ARTÍCULO 10. Almacenamiento y respaldo: La información que es soportada por la infraestructura de tecnología informática del IDEAM deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad.

La estrategia formal de generación, retención y rotación de las copias de respaldo se encuentra establecida en el procedimiento de almacenamiento y respaldo para tal fin y los instructivos anexos.

Dentro de la estrategia la Oficina de Informática tiene definidos los formatos de retención de backups, ubicaciones, tipos de backups y nombres de los archivos que componen los diferentes backups.

Las copias de almacenamiento, serán guardadas en cintas magnéticas o en nuevos sistemas de almacenamiento, requeridos para cualquier ciclo de producción (ej. Diario, Semanal y Mensual), se deben realizar copias de seguridad y dichas copias deben ser almacenadas de la siguiente manera: una copia internamente (on-site realizada por el Data Protector) para evitar problemas de acceso a los sistemas, esta copia se envía a custodia externamente (off-site) como mecanismo de recuperación de la información.

Las áreas misionales y de apoyo del instituto deberán evaluar conjuntamente con la Oficina de Informática, la estrategia a seguir para el respaldo de la información.

Cada usuario es responsable del respaldo de la información a su cargo. Para tal efecto, podrán efectuar copias de respaldo en ubicaciones de red o servidores de archivos siguiendo las indicaciones técnicas que dicte la Oficina de Informática.

Teniendo en cuenta que el Instituto cuenta con información de años anteriores, para archivos con un periodo de retención que excede tres (3) años, los procedimientos serán establecidos para verificar periódicamente la habilidad de leer los datos contenidos en los medios magnéticos y cuando sea necesario, crear nuevas copias para retención leyendo los errores encontrados. Dichas copias de respaldo off-site deberán ser revisadas periódicamente por el Oficial de Seguridad.

Los responsables de cada dependencia deberán velar por la disponibilidad e integridad de la información y determinarán la frecuencia con que se requiera hacer una copia de seguridad de la información institucional almacenada en el servidor dispuesto para tal fin.

ARTÍCULO 11. Registro de activos informáticos institucionales: Se hace necesario ejercer un control sobre los elementos que generan, procesen y almacenan información en el Instituto de hidrología, Meteorología y Estudios Ambientales IDEAM, mediante el registro de la información básica de elementos físicos y lógicos que faciliten su asignación, redistribución y mantenimiento, además de establecer las necesidades en herramientas tecnológicas que se tienen en las diferentes áreas del Instituto.

Mediante el inventario base del almacén o por medio de la herramienta de mesa de servicio, se mantendrá un inventario de los recursos dentro del instituto.

ARTÍCULO 12. Soporte y mantenimiento a hardware, software, bases de datos, redes y comunicaciones: Cualquier brecha de seguridad o sospecha en la mala utilización de Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Jefe de la Oficina de Informática o quien él delegue para tal efecto.

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo del Instituto, deberán ser consideradas y tratadas como información confidencial.

La red de amplia cobertura geográfica a nivel nacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Instituto, debe someterse a los sistemas de defensa electrónica adquiridos por el Instituto a través de la Oficina de Informática. Estos incluyen servicios de inscripción y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, antivirus, control de correo no deseado, administración de permisos de circulación y autenticación de usuarios, entre otros.

Todo intercambio electrónico de información o interacción entre sistemas de información externas deberá estar soportado con un acuerdo o documento de forma que permita establecer competencias y responsabilidades de cada una de las partes.

Los computadores del IDEAM se conectarán de manera directa con computadores de entidades externas mediante conexiones seguras, previa autorización de la Oficina de Informática.

Los usuarios terceros tendrán acceso a los recursos informáticos del IDEAM que sean estrictamente necesarios para el cumplimiento de su función, estos servicios deben ser solicitados por quien ejerza la condición de Jefe inmediato, supervisor o interventor.

En todo caso el usuario tercero deberá firmar el acuerdo de confidencialidad y deberá acatar todas las condiciones y obligaciones que del mismo se deriven, así como las directrices y/o recomendaciones que para el efecto establezca la Oficina de Informática.

La conexión entre sistemas internos del instituto y otros de terceros debe ser aprobada y certificada por la Oficina de Informática con el fin de no comprometer la seguridad de la información interna del instituto.
Los equipos de usuarios, terceros que deban estar conectados a la Red, deben cumplir con todas las disposiciones y normas de seguridad informática que se encuentren vigentes en el Instituto.

Como requisito para interconectar las redes del instituto con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por el Instituto. El instituto se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. El instituto se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por el IDEAM.

ARTÍCULO 13. Soporte a la contratación e interventoria de bienes y servicios: Para adelantar la contratación y supervisión de bienes y servicios informáticos y cubrir los requerimientos identificados por las diferentes dependencias del IDEAM, se hace necesario realizar todo lo estipulado en el procedimiento inscrito en el SGI para tal fin.

Todos los funcionarios de las dependencias del instituto que requieran de bienes o servicios informáticos, deberán ceñirse estrictamente al proceso inscrito en el SGI para tal fin.

Cualquier contrato con terceros no debe vulnerar en forma alguna el contenido de las políticas de seguridad informática definidas.

ARTÍCULO 14. Control de uso de licencias de software: Todo software que utilice el IDEAM será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos adoptados por el Instituto, tales como el de Contratación de Bienes y/o Servicios Informáticos. La compra de cualquier tipo de software deberá efectuarse a través de la Oficina de Informática del IDEAM, con el objeto de que se garantice su compatibilidad con la arquitectura informática del IDEAM y se disponga lo necesario para facilitar su correcto funcionamiento.

Todo el software de manejo de datos que utilice el IDEAM dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria con el propósito de disfrutar todos los beneficios de las nuevas tecnologías y propender así por la disponibilidad e integridad de los datos.

El software empleado por los funcionarios, contratistas, pasantes y terceros que presten servicios al IDEAM, deberá ser utilizado en estricto acatamiento de las disposiciones legales sobre la materia y será responsabilidad de cada usuario, el software que se encuentre instalado en su equipo de cómputo, así como su adecuado uso. El usuario tiene la obligación de reportar a la Oficina de Informática cualquier duda o inquietud que tenga al respecto al origen de cualquier software que encuentre en el equipo asignado.

Software pirata es la duplicación de software sin autorización y/o uso del software por más de un usuario de los que tienen licencia. Dicha piratería es una violación a las leyes de derecho de autor.

Cualquier incumplimiento sobre lo aquí estipulado que sea conocido por la Oficina de Informática, deberá ser puesto en conocimiento de las instancias pertinentes a efecto de determinar responsabilidades disciplinarias, e incluso penales según corresponda.

Se propenderá por la consolidación de una cultura informática al interior del Instituto que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores del IDEAM.

Además del control de inventarios a cargo del Grupo de Almacén e Inventarios, el grupo de tecnologías y comunicaciones de la Oficina de Informática contará con un inventario de las licencias de software del IDEAM que facilite su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

Los responsables de recursos informáticos que no hagan parte del inventario del Instituto, pero que por condiciones del servicio deban ser ubicados en las instalaciones del IDEAM, deben disponer de todas las condiciones de legalidad del respectivo recurso para su funcionamiento, esto se refiere específicamente a aspectos tales como licencias de software ofimático, herramientas especializadas de desarrollo o bases de datos, entre otros.

Estos elementos deberán igualmente registrarse en bitácora de la compañía de vigilancia a cargo de las instalaciones del IDEAM y su retiro deberá ser autorizado por la Jefatura de la Oficina de Informática.

Adicionalmente es necesario mantener un inventario exacto de los recursos informáticos dentro del instituto. Debe existir un documento en el que se oficialice el inventario de elementos en el sistema de gestión de inventario institucional y su ubicación en el instituto, con el detalle de sus componentes de hardware y software.

Toda instalación de software en calidad de demostración en los computadores del IDEAM, deberá ser coordinada con la Oficina de Informática.

ARTÍCULO 15. Reubicación traslado de hardware: Cualquier cambio que se requiera realizar en los equipos de cómputo del Instituto (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y la autorización respectiva por parte de la Oficina de Informática.

La reparación técnica de los equipos, así como cualquier tipo de intervención sobre los mismos, únicamente puede ser ejecutada por el personal autorizado por el grupo de tecnología y comunicaciones de la Oficina de Informática.

Los equipos tales como computadores, servidores, impresoras y equipos de comunicaciones, entre otros, no deben moverse o reubicarse sin la aprobación previa del Director General, Secretario General, Subdirector, Jefe o coordinador del área respectiva y el visto bueno de la Oficina de Informática, como responsable del inventario de la plataforma tecnológica del instituto.

En el caso de que además del movimiento se requiera cambiar el responsable del equipo o elemento, deberá efectuarse el trámite de traslado respectivo ante la Coordinación del Grupo de Almacén e Inventarios, el cual deberá disponer de visto bueno de la Oficina de Informática.

ARTÍCULO 16. Seguridad física y del entorno: El centro de cómputo, oficinas de tesorería y demás áreas que el instituto considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar en una bitácora el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

El centro de cómputo, Tesorería, Informática y demás áreas que el instituto considere críticas, deberán existir elementos de control de incendio, inundación y alarmas. Igualmente, deberán estar demarcados con zonas de circulación y zonas restringidas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso. Estas áreas no deben de ser utilizadas para almacenar elementos diferentes a equipos de cómputo y comunicación

Todos los computadores portátiles y equipos de comunicación se deben registrar su ingreso y salida en las bitácoras de seguridad.

Los funcionarios públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que pueda generar indisponibilidad de la operación por caídas de energía.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos o contratistas no están autorizados para utilizar los recursos informáticos del instituto, ni a conectar equipos personales que puedan introducir vulnerabilidades a la red del Instituto.

ARTÍCULO 17. Áreas seguras: El Instituto debe garantizar el acceso físico autorizado, evitando daño e interferencia a la infraestructura y la información del Instituto. El acceso a las áreas seguras debe ser supervisado, así como también deben registrarse en las bitácoras con la fecha y hora de entrada y salida del personal.

ARTÍCULO 18. Escritorios limpios: Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD´s, Memorias USB, Discos Extraíbles entre otros con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Adicionalmente el Grupo de Recursos Físicos debe adoptar la adquisición de gavetas con llave para cada puesto de trabajo de manera que los funcionarios puedan guardar bajo llave todo tipo de documentación del Instituto y así mantener los escritorios despejados; por otro lado se deben tener las pantallas limpias de iconos o accesos directos que generen acceso más fácil a la información.

ARTÍCULO 19. Estructura de contingencia: La administración del Instituto se debe preparar, actualizar periódicamente y probar en forma regular mediante un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación, etc.

Para la implementación de esta política, la Oficina de Informática podrá apoyarse en servicios de una empresa especializada, que además de las indicaciones de carácter técnico, deberá proponer el plan de acción y los costos asociados para su ejecución.

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.

Todos los archivos de registro de los diferentes sistemas, deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso. Este aspecto podrá evaluarse conforme a los requisitos establecidos por las tablas de retención documental que puedan asociarse a la gestión de datos.

Todos los archivos de soporte a auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos a la Oficina de Informática.

Todos los computadores del Instituto deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoría sea correcto. La Oficina de Informática deberá evaluar e implementar el mejor mecanismo disponible para cumplir este propósito

ARTÍCULO 21. Continuidad de negocio: El objetivo en general de la continuidad de negocio del Instituto de Meteorología, Hidrología y Estudios Ambientales- IDEAM, es realizar los preparativos adecuados y planificar un conjunto suficiente de objetivos, controles, procesos y procedimientos para responder de forma adecuada ante un incidente, desde el momento en que se active el plan, hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

La Política de Continuidad establece un marco apropiado a las características del IDEAM como parte de la gestión general, para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y

mejora de la continuidad de negocio, donde se tendrán cuenta algunos criterios como naturaleza, complejidad, criticidad de las actividades etc, que repercute directamente en el entorno nacional, operativo central, así como la entrega de información oportuna, mitigando el riesgo en cuanto a pérdidas humanas, imagen organizacional, medio ambiente e impacto financiero.

Es por ello que el instituto debe asegurar un escenario para la continuidad de la operación donde se identificará, desarrollará, implantará, operará, mantendrá, revisará y probará las medidas necesarias para garantizar el correcto funcionamiento de estos planes ante la materialización de un incidente.

La Política de Continuidad se sustenta en un conjunto de principios que han sido formulados basándose en las necesidades del negocio y el entendimiento de los riesgos asociados.

Dichos principios son:

1. La primera premisa y el objetivo prioritario es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.

2. El IDEAM revisara continuamente la gestión de los riesgos clave para la continuidad operativa de los procesos considerados críticos para la Organización.

3. El IDEAM garantizará que el Plan de Continuidad de Negocio se desarrolla e implanta de forma adecuada, teniendo en cuenta las aplicaciones críticas del negocio.

4. IDEAM garantizará que el Plan de Continuidad de Negocio se mantiene actualizado, se revisa, se prueba y, en caso de requerirse, se mejora de forma periódica o ante cambios significativos en aplicaciones, personas, procesos, mercados, tecnología o estructura organizativa; para lo cual participarán activamente en dicha revisión las distintas Áreas de Negocio y de Soporte del Instituto con los procesos identificados como críticos.

5. Las distintas dependencias del IDEAM nombrarán representantes con la debida experiencia para que formen parte de los grupos de trabajo y Equipos de Continuidad de Negocio y participen en los Planes de Continuidad de Negocio.

6. El IDEAM garantizará que todo el personal que formen parte de los grupos de trabajo y Equipos de Continuidad de Negocio estén informados de las responsabilidades que le competen en el marco de la Continuidad de Negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad de Negocio.

7. El IDEAM garantizará que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad de Negocio.

8. Se deberá realizar la promoción y divulgación de la capacidad de Continuidad de Negocio dentro de la cultura de empresa, al igual que el impacto en el Plan de Continuidad de Negocio de nuevos proyectos informáticos.

9. El IDEAM garantizará la elaboración de planes de comunicación apropiados, tanto internos como externos, que serán revisados y actualizados de forma periódica.

ARTÍCULO 22. Excepciones a políticas y procedimientos aprobados: Las Políticas de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM y los procedimientos desarrollados para aprobarlas e implementarlas, deben ser aplicables en la mayoría de las circunstancias. Se reconoce, de todas formas, que algunas circunstancias puedan requerir una desviación de las políticas y procedimientos normales. Esta política identifica cómo el funcionario puede obtener una excepción dentro de una política regular o procedimiento aprobado.

Las excepciones de emergencia de las políticas de seguridad de la información pueden solicitarse por la mesa de servicio al Oficial de Seguridad de la Información y al Jefe de la Oficina informática quienes decidirán sobre la pertinencia de la excepción y el tiempo de duración de la misma.

CAPITULO III

DISPOSICIONES FINALES

ARTÍCULO 23. Revision: La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del IDEAM, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el oficial de seguridad de la entidad.

ARTÍCULO 24. Vigencia y derogatorias. La presente resolución rige a partir de la fecha de su publicación y deroga la Resolución No. 0390 del 15 de marzo del 2016.

Dada en Bogotá, D. C. a los 30 de abril 2021

PUBLIQUESE Y CÚMPLASE

GONZALEZ HERNANDEZ YOLANDA

Firmado digitalmente por GONZALEZ HERNANDEZ YOLANDA
Fecha: 2021.05.03 05:47:05 -05'00'

YOLANDA GONZÁLEZ HERNÁNDEZ
Directora General

	Nombre	***Cargo***	***Firma***
Proyectó:	Harbey Arnulfo Martinez Guerrero	Oficial de seguridad	
Proyectó:	Nancy Patricia Bravo	Abogada Oficina Asesora Jurídica	**NPBI**
Revisó aspecto jurídico:	Gilberto Ramos Suárez	Jefe Oficina Asesora Jurídica	
Vo. Bo.	Alicia BarónLeguizamón	Jefe de Oficina de Informatica	
Vo. Bo.	Eduardo Emilio Ramirez	Coordinador Grupo Arquitectura Empresarial y seguridad de la infromación	
Rad. Orfeo	20211020001391		
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes, por lo tanto bajo nuestra responsabilidad lo presentamos para la firma de la Directora General.			