INTRODUCCIÓN

La información es un activo que tiene un alto valor para el Instituto y requiere en consecuencia una protección adecuada. Con base en el análisis de seguridad de la información se identificaron algunas vulnerabilidades, por lo que se emitió recomendaciones que contribuyen a mejorar el nivel de seguridad.

El Plan de Seguridad de la Información que se ha desarrollado se centra en la seguridad de los activos de información, de las personas y de los procesos del Instituto, salvaguardando la confidencialidad, integridad y disponibilidad mediante políticas que apalanquen la protección de la información y sea una guía para establecer las pautas que se deben cumplir al interior del Instituto (Sede Central), así como los integrantes del grupo de Seguridad de la Información.

El plan propone políticas que desarrollarán de acuerdo a los controles que se consideren necesarios, las cuales son la base para la implantación de instructivos y procedimientos.

El cumplimiento de las Políticas de Seguridad de Activos de Información es obligatorio. Ningún funcionario está exento del cumplimiento de estas políticas. Si un individuo del instituto viola las disposiciones en las Políticas de Seguridad de la Información, por negligencia o intencionalmente. El Instituto se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, despido, acciones legales, reclamo de compensación por daños, u otras[1], tal como lo describe la política de seguridad y privacidad de la información.

OBJETIVO

Las políticas definidas en este Plan de Seguridad de la Información 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.

ALCANCE

Las políticas definidas en el presente plan de seguridad de la información 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.

GLOSARIO

[1] Ley 1273 de 2009: Ley de Delitos Informáticos

- **Activo de Información:** La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades del instituto y, en consecuencia, necesita una protección adecuada.
- **Administrador de Dominio:** Persona encargada de administrar un conjunto de ordenadores (servidores + estaciones de trabajo) que comparten características comunes en cuanto a accesos.
- **Administrador de TI:** Profesionales encargados de operar y administrar la infraestructura tecnológica, comunicaciones, seguridad, aplicaciones y bases de datos del instituto.
- **Amenaza:** Causa potencial de un incidente no deseado, que pueda ocasionar daño a un sistema u organización.
- **Análisis de Impacto al Negocio:** Donde se determinan los recursos críticos y el tiempo de recuperación con las respectivas ventanas de criticidad mediante las cuales se debe restaurar los activos evaluados.
- **Análisis del Riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Aplicación:** Es un tipo de programa Informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.
- **Ataque:** intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo.
- **Cifrar:** quiere decir transformar un mensaje en un documento no legible.
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para quienes están autorizados.
- **Contratista:** Persona jurídica o natural externa al Instituto encargada de adelantar actividades por encargo del instituto.
- **Cuenta de acceso***:* Identificación y contraseña a través de la cual un usuario accede a un servicio o aplicación. Las cuentas de acceso son autorizadas por los Jefes de las diferentes dependencias y suministradas por los Administradores de los servicios o aplicaciones y está sujeta a la disponibilidad de licencias adquiridas por el Instituto.
- **Custodio:** Encargado de guardar el activo con cuidado y vigilancia. Es una parte designada del instituto, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información; además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario de la información haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.
- Incidente de Seguridad de la Información: Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.
- **Política:** Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.
- **Propietario:** El término “Dueño” o “Propietario” identifica a un individuo o a un instituto que tiene responsabilidad aprobada por la Dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.
- **Recurso Informático:** Cualquier componente físico (Hardware) o lógico (Software) empleado para almacenar, manipular, procesar o transmitir información del IDEAM.

- **Requerimiento:** es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Se usa en un sentido formal en la ingeniería de sistemas o la ingeniería de software.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- **Rol:** Grupo de usuarios que cumplen un papel determinado, a los cuales se les asigna o niega permisos dentro de un aplicativo.
- **Servidor:** un computador que ofrece servicios a máquinas de cliente distantes o a aplicaciones, como el suministro de contenidos de páginas u otros recursos.
- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas [ISO/IEC 27001:2005].
- **Servicio o Aplicación:** Programa o conjunto de programas diseñados para la realización de una(s) tarea(s) concretas. Los servicios están destinados principalmente para apoyar los diferentes procesos del Instituto. Por ejemplo, correo electrónico, Internet, SISAIRE, SNIF, SIORH, etc.

DESCRIPCIÓN DE 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 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 los comités de seguimiento 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 que se tomará acarreará desde reprimenda verbal, memorando y hasta incluso destitución inmediata del cargo, dependiendo de la severidad de la violación, así como de requerirse se entregará el caso al órgano competente.

DESARROLLO

POLÍTICA 1. 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.
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 Talento Humano debe notificar a la Oficina de Informática cuando un individuo es transferido o deja el instituto. La falta de notificación de dichas transferencias o salidas, será incluida en el reporte y enviada al Grupo de Seguridad de la Información. También debe notificar a la Oficina de Informática cuando un individuo 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 extenso de tiempo, u otras circunstancias similares.
Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

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 aplicación 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 que se brinda, 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 funcionario, contratista o tercero dentro del IDEAM, para tener una única clave de acceso a la red, aplicaciones y servicios del instituto excepto para los laptop 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 las plataformas en que el individuo tenga un acceso autorizado (ej. Correo electrónico, gestor documental).

La contraseña de acceso de los usuarios y administradores de TI (dispositivos de comunicaciones y seguridad, servidores, bases de datos y aplicaciones) debe tener una longitud no menor de 8 caracteres alfabéticos y

numéricos, debe contener mayúsculas/ minúsculas y 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 y para los administradores de TI cada 180 días, o cuando se sospeche que la clave haya sido comprometida o por sustitución de administrador de TI.

Luego del cambio de las contraseñas de los diferentes accesos de la infraestructura tecnológica por parte de los administradores de TI, estas deberán ser entregadas en sobre sellado al Oficial de Seguridad de la Información para realizar la custodia de las mismas en cajilla de seguridad. El acceso y uso de dichas contraseñas en custodia se realizará en caso de ausencia total del administrador de TI con aprobación previa del Jefe de Informática y en presencia del Oficial de Seguridad de la Información.

El grupo de Talento Humano debe notificar a la Oficina de Informática cuando un individuo es reemplazado por licencia médica o cualquier otra novedad, o es asignado a un proyecto especial que no requiera que el funcionario deba acceder al sistema por un periodo extenso de tiempo, u otras circunstancias similares. En estas instancias, el código de acceso será retenido como activo mientras dure la ausencia. De todas formas, la clave de acceso o password expirará.

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

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

Si por múltiples intentos de logueo el usuario bloquea su cuenta, tendrá la posibilidad de intentarlo de nuevo después de 15 minutos; si finalmente no recuerda la clave deberá comunicarse telefónicamente a la mesa de servicio donde el operador le solicitará alguna información de validación y procederá a reactivar el usuario.
La otra forma de reestablecer la contraseña es acercándose a la mesa de servicio ubicada en la oficina de informática piso 2 sede principal, el procedimiento para el restablecimiento de credenciales se encuentra dispuesto en el Sistema de Gestión integrado SGI, llamado E-GI-P001 PROCEDIMIENTO ACCESO SERVICIOS INFORMATICOS BASICOS, el grupo de gestión de recursos informáticos y tecnológicos.

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 palabras claves o contraseñas únicos para cada usuario.

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 prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos 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 ciframiento 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.

Nota: La intención se expresa en los numerales 3 (Administración de identidad) y 4 (Acceso a los datos y la información por parte de los funcionarios, contratistas y colaboradores) del Artículo 9 (Criterios sobre la seguridad de los datos y la información) de la Resolución 2367 del 31 de diciembre de 2009.

POLÍTICA 2. 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 responsable de la administración 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 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 y soporte 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, 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.

POLÍTICA 3. 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.

POLÍTICA 4. 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.

POLÍTICA 5. 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.

POLÍTICA 6. SOPORTE Y MANTENIMIENTO A HARDWARE, SOFTWARE, BASES DE DATOS, DISPOSITIVOS DE SEGURIDAD PERIMETRAL, 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 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.

El servicio de FTP público hacia internet debe contemplar los niveles de complejidad de autenticación definidos por el IDEAM y se debe especificar cuota de almacenamiento de la carpeta, vigencia, tipo de accesibilidad entre otros parámetros establecidos en el formato E-GI-F034 FORMATO SERVICIO FTP que se encuentra disponible en el Sistema de Gestión Integrado – SGI, en el grupo de gestión de recursos informáticos y tecnológicos.

Los accesos a servicios tecnológicos del IDEAM por parte de terceros y/o proveedores por medio de internet a excepción del servicio FTP, deberán realizarlo por conexión segura denominada (Virtual Private Network – VPN) de tipo VPN Client to Site el cual se caracteriza por un acceso de un usuario a un recurso(s) especifico(s) por un puerto o servicio determinado, es importante destacar que se debe definir un tiempo de caducidad para este tipo de VPN y una serie de parámetros específicos, para ello se debe diligenciar el formato E-GI-F031 FORMATO SOLICITUD DE CONEXIÓN VPN CLIENT TO SITE disponible en el Sistema de Gestión Integrado – SGI, en el grupo de gestión de recursos informáticos y tecnológicos. El otro tipo de VPN es el tipo Site to Site, el cual se caracteriza para intercomunicar de manera segura dos entidades a servidores y servicios puntuales para su solicitud se debe diligenciar el formato E-GI-F032 FORMATO SOLICITUD DE CONEXIÓN VPN SITE TO SITE disponible en el Sistema de Gestión Integrado – SGI, en el grupo de gestión de recursos informáticos y tecnológicos. Para la parametrización de las VPNs deberán configurarse con los algoritmos más estables y seguros.

Para toda publicación WEB hacia internet deberá incluirse en las políticas de los dispositivos de seguridad perimetral Firewall y WAF del Instituto, adicionalmente tendrá que ser aprobado por el Oficial de Seguridad de la información, quien realizará las pruebas de seguridad pertinentes dentro de las que se encuentra el escaneo de vulnerabilidades.

Los permisos de acceso a internet de los equipos finales estarán limitados por cada área de acuerdo a sus necesidades; tendrán como regla general los privilegios estrictamente necesarios. Todo privilegio particular deberá ser aprobado por el jefe del área y el jefe de informática, para su solicitud se debe registrar el formato E-GI-F033 FORMATO SOLICITUD ACCESO A INTERNET disponible en el Sistema de Gestión Integrado – SGI, en el grupo de gestión de recursos informáticos y tecnológicos.

En todo caso el usuario tercero deberá firmar el acuerdo de buen uso de los Recursos Informáticos 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 (revisar talento humano y jurídica).

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.

POLÍTICA 7. SOPORTE A LA CONTRATACIÓN E INTERVENTORIA DE BIENES Y SERVICIOS

Para adelantar la contratación e interventoría 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 para tal fin.

Todos los funcionarios de las dependencias del instituto que requieran de bienes o servicios informáticos, deberán ceñirse estrictamente al proceso.

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

POLÍTICA 8. 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 específicos de la Instituto o reglamentos internos, 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 aplicativo 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 de la 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, 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 de la 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 del SICAPITAL 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.

POLÍTICA 9. REUBICACIÓN TRASLADO DE HARWARE

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 utilizada por el personal autorizado de la Oficina de Informática o terceros autorizados por esta dependencia para su ejecución.

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.

POLÍTICA 10. SEGURIDAD FÍSICA Y DEL ENTORNO

El centro de cómputo, Tesorería, Informática y demás áreas que el instituto considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar 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.

Todos los computadores portátiles y equipos de comunicación se deben registrar su ingreso y salida.
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.

POLÍTICA 10.1 ÁREAS SEGURAS

El Instituto debe garantizar el acceso físico no 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 la fecha y hora de entrada y salida del personal.

POLÍTICA 11. 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 debe tener en cuenta que se deben tener las pantallas limpias de iconos o accesos directos que generen acceso más fácil a la información.

POLÍTICA 12. 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.

POLÍTICA 13. 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 de la 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

POLÍTICA 14. CONTINUIDAD DE NEGOCIO

El objetivo en general de la continuidad de negocio del Instituto de Meteorología, Hidrología y estudios ambientales 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 de las distintas dependencias del Negocio esté informado 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.

POLÍTICA 15. EXCEPCIONES A POLÍTICAS Y PROCEDIMIENTOS APROBADOS

Las Políticas de Seguridad de la Información 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.

POLÍTICA 16. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

De acuerdo a la cadena de seguridad el recurso humano puede llegar a ser el eslabón más débil; por tal motivo el IDEAM debe generar periódicamente campañas de sensibilización, entrenamiento y educación en seguridad de la información de acuerdo en lo descrito en el manual E-SGI-SI-M006 PLAN DE CAPACITACIÓN SENSIBILIZACIÓN Y COMUNICACIÓN, el cual busca fortalecer el conocimiento en seguridad a los funcionarios públicos, aprendices, practicantes y usuarios de la entidad, permitiendo mitigar la materialización de incidentes de seguridad propendiendo así por la integridad, disponibilidad y confidencialidad de los activos de información del IDEAM. Lo anterior en cumplimiento de los lineamientos establecidos en el dominio de Uso y Apropiación de la política de Gobierno Digital.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
001	14/02/2013	Creación del documento.
002	25/11/2015	Actualización del documento.
003	29/11/2017	Actualización documento para SGI
004	11/04/2018	Actualización del documento y para dar cumplimiento al decreto 415
005	21/09/2018	Actualización documento. Política 1 y 6
006	11/10/2018	Actualización documento. Política 6
007	29/08/2019	Creación de la Política 16

ELABORÓ:	REVISÓ:	APROBÓ:
Luis Alejandro Pinilla **Oficial de Seguridad de la Información**	Eduardo Ramírez Acosta **Profesional Especializado Oficina Informática**	Leonardo Cárdenas Chitiva **Jefe Oficina Informática**