1. OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "**Política General de Seguridad de la Información de la Entidad**" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos del Ideam.

2. ALCANCE DEL MANUAL

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes del Ideam por alguna razón tengan cualquier tipo de interacción con los activos de información.

3. DEFINICIONES

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Como parte integral de la implementación del Sistema de Gestión de Seguridad de la Información, el Instituto de Hidrología, Meteorología y Estudios Ambientales - Ideam recibe, genera y transforma información de gran importancia para el país. Por esta razón, la entidad está comprometida con la gestión de esta, de tal manera que tenga la protección necesaria y se evite cualquier falta a la confidencialidad, integridad o disponibilidad, pilares en la seguridad de la información.

El Instituto de Hidrología, Meteorología y Estudios Ambientales - Ideam, para asegurar su dirección estratégica, establece la política de seguridad y privacidad de la información bajo las siguientes premisas:

- Implementar mecanismos y procedimientos para mitigar los riesgos asociados a la gestión de la información en los procesos que soportan la operación del negocio.
- Proteger la información generada, almacenada, procesada, transmitida y/o resguardada por los procesos y procedimientos en el cumplimiento de sus funciones, y de los activos de información que hacen parte de estos. con el fin de minimizar impactos negativos a el Instituto; para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad y/o en custodia
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- protegerá su información de las amenazas internas y/o externas por parte del personal custodio, responsable, usuario de esta y/o personal ajeno a la información de la entidad.

- Implementa un programa de ciberseguridad alineado con mejores prácticas y la Política Nacional de Ciberseguridad. Dicho programa busca el mejoramiento continuo de su postura de seguridad y aumentar su resiliencia.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, contratistas, practicantes y clientes del IDEAM.

5. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACION

El Ideam, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

5.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACION EN GESTION DE PROYECTOS

- Todas las áreas del IDEAM deberán Identificar y gestionar riesgos de seguridad a lo largo del ciclo de vida del proyecto.
- Realizar una evaluación de riesgos de seguridad de la información en la fase de planificación de cada proyecto.
- Establecer controles técnicos y administrativos adecuados para mitigar los riesgos identificados
- Realizar auditorías periódicas de los proyectos para evaluar el cumplimiento de esta política.

5.2 POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.

- Realizar la verificación del personal durante los procesos de vinculación, contratación y/o aspiración de alguna función dentro de la entidad, mediante la definición de mecanismos que permitan verificar aspectos legales, judiciales, fiscales, laborales y disciplinarios de acuerdo con la normativa legal vigente y ética pertinente, dicha documentación deberá anexarse en las historias laborales o expedientes contractuales según sea el caso.
- La entidad deberá incluir dentro de los programas de inducción y/o reinducción, sesiones de capacitación y sensibilización del sistema de gestión de Seguridad de la Información para los funcionarios y contratistas.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

5.3 POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad del IDEAM.
- Los activos dispuestos por el IDEAM**.** para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral del IDEAM.
- La Oficina de Informatica identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

- Los activos de información serán tratados de acuerdo con su nivel de clasificación indicado por los propietarios de los activos de información.
- Cuando sea requerido y con la debida autorización y aprobación del responsable del activo Se debe generar un requerimiento de borrado seguro de información, a través de los canales autorizados por la entidad.
- En el momento de un cambio funcional o de empleo, retiro y/o terminación de otros tipos de vinculación, deben realizar la entrega de su puesto de trabajo al lideres inmediato o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados durante su permanencia en la entidad.
- Los activos de información contenido en el inventario son propiedad de cada líder de proceso por lo cual deben protegerlos aplicando los controles necesarios para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información
- La Oficina de Informatica clasifica los activos de información de acuerdo con su probabilidad e impacto de perdida, modificación o daño en su confidencialidad, integridad y disponibilidad.

5.4 POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- El acceso a la Información, sistemas de información y/o aplicaciones de la entidad, por parte de los funcionarios, contratistas o terceras partes

vinculadas al IDEAM debe darse bajo el principio del mínimo privilegio; quiere decir que cada usuario solo debe tener acceso a lo que necesita conocer de acuerdo con sus actividades y rol dentro de la entidad.

- Todas las solicitudes de acceso (creación, modificación, bloqueo, inactivación y/o eliminación) a los servicios de red, aplicaciones, información; deben ser solicitadas por el Director, Subdirector, Jefe de Oficina, Coordinador y Supervisor de acuerdo con las funciones u obligaciones de los funcionarios por medio del canal dispuesto por la Oficina de Informatica
- Se debe contar con autenticación (preferiblemente doble o triple factor) para acceso a los servicios tecnológicos, sistemas de información e infraestructura de la entidad.
- Los accesos lógicos asignados a los funcionarios serán desactivados una vez terminada su vinculación contractual o laboral con la entidad por lo que el lideres inmediato es el responsable de reportar oportunamente cualquier novedad.
- Se debe suspender el acceso lógico a los sistemas de información, infraestructura y servicios tecnológicos a los funcionarios que no se encuentren en servicio activo por diferentes causas y por un periodo superior a tres (3) días hábiles, esta novedad debe ser reportada oportunamente por el lideres inmediato.
- Todas las partes interesadas deberán conocer los lineamientos y aplicar los controles establecidos con el fin de evitar accesos no autorizados, pérdidas y/o utilización indebida de los activos de información.
- La asignación de privilegios especiales debe ser revisado y autorizado por el lideres directo del funcionario, contratista o tercera parte vinculada y deberá quedar registrado todo el proceso de solicitud y autorización en la herramienta de gestión.
- Todos los usuarios privilegiados deberán tener habilitado el log de acceso y transacciones en todos los sistemas de información, dispositivos de red,

comunicaciones, dispositivos de seguridad y/o cualquier recurso o servicio tecnológico que sea accedido.

- Garantizar que todas las contraseñas de los usuarios y/o sistemas de información conocidas por el usuario privilegiado sean actualizadas inmediatamente después del retiro y/o movimiento de área del funcionarios, contratistas o terceras partes vinculadas al IDEAM, proveedores y terceros.

5.5 POLITICA DE CRIPTOGRAFÍA

- **El IDEAM** implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, la Oficina de Informatica determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.
- Los métodos de cifrado de información serán aplicables para los siguientes casos:
  - Protección de contraseñas de acceso a servicios de información, administración de plataforma de TI entre otros.
  - Transferencia de información digital de carácter clasificada o reservada.
  - Procesos de generación y transporte de copias de seguridad.
  - Conexión y disposición de canales de comunicación con otras entidades públicas y/o privadas.
- La entidad deberá usar e implementar controles criptográficos para proteger la confidencialidad, autenticidad o integridad de la información clasificada de la entidad, al momento de almacenarse o transmitirse.
- Proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información clasificada de forma interna o externa se realice de forma segura.
- La información confidencial y sensible debe almacenarse en repositorios cifrados de acuerdo con sus niveles de confidencialidad e integridad.

- Se debe disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red de la entidad, o recursos de la entidad.
- Todas las llaves criptográficas de la entidad deben estar resguardadas por los responsables y custodios protegiendo su confidencialidad, integridad y disponibilidad.
- Las llaves criptográficas serán deshabilitadas por el área de Tecnología o quien haga sus veces, cuando estas se encuentren en riesgo de divulgación o cuando los Colaboradores de la entidad, autorizados culminen la relación laboral o contractual con la entidad.

5.6 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- El IDEAM adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- El IDEAM definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones del IDEAM deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

5.7 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. El Ideam planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

- Supervisar continuamente el consumo, demanda y comportamiento de los recursos tecnológicos asignados, con el fin de realizar gestionar oportunamente los cambios y/o ajustes que se requieran y proyectar las futuras necesidades de capacidad.
- Se deben designar los responsables encargados de realizar la gestión de capacidad de los componentes tecnológicos.
- Implementar controles para la detección, prevención y recuperación contra códigos maliciosos.
- Instalar, controlar y mantener actualizada en todos los equipos de cómputo y servidores de la entidad, una herramienta de antivirus, que permita la gestión centralizada de las amenazas, eventos, estados de los equipos, entre otros.

5.8 POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Ideam definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.
- La Oficina de Informatica, establecerá los controles para acceso lógico y protección de las redes del IDEAM, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red.

5.9 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- La Oficina de Informatica, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.

- Todos los procesos de la entidad deberán informar a la Oficina de Informatica sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.
- La solicitud de nuevos desarrollos de software o modificaciones al software existente se realizará por los dueños de procesos o lideres de oficina de manera formal y de acuerdo con lo establecido en los procedimientos del IDEAM.
- El software adquirido y desarrollado tanto al interior de la entidad, como por terceras partes, debe cumplir con los requisitos de seguridad y calidad establecidos por la entidad.
- La Oficina de Informatica establecerá un ambiente de desarrollo seguro durante la ejecución de los proyectos, arquitecturas, software o sistemas, estableciendo metodologías que incluyan requisitos de seguridad en cada una de las fases de los proyectos, acuerdos de soporte, niveles de servicio a terceros, y separación física y virtual de todos los ambientes (producción, preproducción, pruebas, desarrollo, entre otros), a través de técnicas de desarrollo seguras.
- La Oficina de Informatica Apoyará en la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
- Los responsables (propietarios y custodios) de los sistemas de información deben gestionar la inclusión de los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo.
- Toda aplicación desarrollada deberá contar con un módulo de seguridad RECAPTCHA en el formulario de autenticación de usuarios, para evitar que un robot ejecute peticiones de manera automática; y/o ataques de fuerza bruta.

- Deben utilizarse mecanismos de transferencia de datos de forma segura bajo protocolos HTTPS, SFTP, FTPS, SSL/TLS, entre otros, con el fin que no se transmita información en texto plano, y que a su vez utilicen algoritmos de cifrado fuertes o reconocidos como seguros.
- El software adquirido y desarrollado tanto al interior de la entidad, como por terceras partes deberá tener un control de versiones del código fuente y documentación, ello con el objeto de verificar el funcionamiento del software y el respectivo control de su ciclo de vida, en el repositorio especializado para este tipo de información definido por la Oficina de Informatica.

5.10 POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- El Ideam establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.
- Guardar la confidencialidad respecto del tratamiento de los datos personales privados y sensibles contenidos en el intercambio de información de acuerdo con lo exigido por la ley 1581 de 2012, su decreto reglamentario y las políticas de protección de datos personales.
- No deben utilizar y/o emplear la información que reciban de la contraparte, para fines distintos a los señalados.
- Utilizar la información que reciba o conozca de la entidad, únicamente para los fines señalados en la relación contractual.

5.11 POLÍTICAS DE TRANSFERENCIA DE INFORMACION

- La entidad o quien haga sus veces, debe definir los modelos de Convenios o Contratos de Transferencia o Transmisión de datos, Acuerdos de

Confidencialidad, así como las cláusulas de Confidencialidad de información entre la entidad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir:

- ✓ La prohibición de divulgar la información entregada por parte de la entidad, a los terceros con quienes no se establecen estos acuerdos.
- ✓ La destrucción de dicha información una vez cumpla su cometido.
- ✓ El periodo del acuerdo.
- ✓ Los medios a través de los cuales se compartirá la información.
- ✓ Los responsables de la custodia de la información.

- Los acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación contractual.
- Los acuerdos, convenios o contratos que requiera la suscripción de un anexo técnico asociado al intercambio, deben establecer un protocolo de intercambio de la información y se fijarán las condiciones técnicas y controles de seguridad que se utilizarán para proteger la información.
- Los propietarios y custodios de los activos de información deben proteger la confidencialidad e integridad de la información durante los procesos o actividades de transferencia de la información, estableciendo los riesgos y los canales de transferencia seguros que eviten la divulgación o modificación no autoriza de la información, los cuales permitan brindar los niveles de seguridad apropiados.
- Los propietarios de los activos de información son los responsables de definir los controles de seguridad, niveles y perfiles de autorización para el acceso, modificación y/o eliminación de estos, garantizando siempre la privacidad e integridad, asegurando así, que se establezcan los acuerdos de confidencialidad entre la entidad, proveedores y/o aliados y los cuales deben ser revisados y aprobados por la entidad, o quien haga sus veces,

en los cuales reposarán las responsabilidades y se garantice la reserva de la información y el alcance frente al tratamiento de esta.

- En el caso de presentarse un incidente de seguridad, el responsable del proceso de la transferencia de la información deberá seguir lo indicado en los procedimientos de gestión de Incidentes de la entidad.
- Queda prohibido que el personal de la entidad, y terceros revelen o intercambien información confidencial de la entidad, por cualquier medio, sin contar con la debida autorización y documento jurídico que la garantice y del titular de la información cuando haya lugar a ello.

5.12 POLITICA DE ALMACENAMIENTO EN NUBE

- La entidad, o quien haga sus veces no será responsables por la pérdida o daño de la información que se encuentra almacenada en el equipo de cómputo de los funcionarios y contratistas, dado que la información debe ser almacenada y sincronizada en las herramientas organizacional en la nube.
- El uso del servicio de almacenamiento de archivos en la nube deberá ser solo para fines organizacionales y nunca debe usarse para fines personales.
- Está prohibido almacenar archivos de la entidad, en nubes públicas como Dropbox, Mega, entre otros.
- Es responsabilidad del funcionario y contratista realizar la copia de su información local en el Drive o SharePoint institucional.

5.13 POLITICA DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- El Ideam establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.

- La Oficina de Informatica generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

5.14 POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar a la Oficina de Informatica por cualquiera de los medios dispuestos para tal fin.
- Sera responsabilidad de la Oficina de Informatica seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

5.15 POLÍTICAS DE CUMPLIMIENTO

- El Ideam velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

5.16 POLITICA DE ESCRITORIO LIMPIO:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Conservar su escritorio libre de información propia del Ideam (papeles o unidades de almacenamiento externo) y conservar la pantalla del equipo de cómputo despejada de archivos office, pdf, entre otros, los cuales podrían ser copiados, utilizados o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

  Nota: Los archivos que se trabajen en los equipos de cómputo deben ser almacenados en el OneDrive o SharePoint institucional.

- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Toda la información (documentos impresos, medios de almacenamiento removibles, cd´s) declarada no pública utilizada para el desarrollo de las actividades laborales, debe permanecer en lugares seguros o bajo llave en el escritorio mientras el puesto de trabajo esté desatendido o en horas no laborales con el fin de evitar pérdidas, alteraciones o accesos no autorizados. Adicionalmente, toda la información no pública que se envía a las impresoras debe ser recogida de manera inmediata.
- Después de imprimir documentos de carácter CONFIDENCIAL, evitar reutilizar y antes de reciclar destruir papel que contenga información CONFIDENCIAL
- Salir de todas las aplicaciones y apagar los equipos de cómputo y otros equipos de hardware que se encuentren en su puesto de trabajo al finalizar sus actividades diarias

5.17 POLITICA DE USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

- La Oficina de Informatica podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.
- No deben utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la entidad, o para actividades que no corresponden con el desempeño de las funciones asignadas.
- No deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
- No deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la entidad.
- Deben asegurarse de que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.

5.18 POLITICA DE USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen al IDEAM, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina de Informatica podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.
- Las cuentas de correo de la entidad son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar

la contraseña, cambiarla periódicamente, y no prestarla en ninguna circunstancia.

- De acuerdo con la política de seguridad y privacidad de la información de la entidad, y las diferentes políticas complementarias del Modelo de seguridad y privacidad de la información, el correo electrónico es una herramienta Tecnológica proporcionada por la entidad, con el propósito de apoyar el desarrollo de las actividades de los funcionarios en sus actividades de comunicación. Por tal motivo la información manejada en el correo electrónico es un activo de la entidad y no de los funcionarios, contratistas o terceras partes vinculadas al IDEAM.
- Está prohibido utilizar la plataforma de correo electrónico de la entidad, o las herramientas colaborativas para realizar proselitismo político o religioso, actividades de negocios privados, distribución de cadenas de mensajes, propagación de falsas alarmas por correo electrónico, diversión, entretenimiento personal y demás condiciones que degraden la condición humana y resulten ofensivas para los miembros de la entidad.
- Esta prohibido utilizar la cuenta de correo electrónico del Ideam para la suscripción en páginas de entretenimiento, noticias, música y en el registro a suscripciones de sistemas de periodos de prueba, software de uso personal o en practicas como crackeo de aplicaciones o apps.
- Una vez terminada la relación contractual con el Ideam se retirará el acceso a cuentas de la entidad.
- La retención de la información de las cuentas de correo electrónico del Ideam se realizará desde la desvinculación del funcionario y/o contratista y hasta tres (3) meses después.
- Sera responsabilidad del jefe Inmediato antes de finalizar la relación contractual del funcionario o contratista solicitarle la entrega del Backup de correo electrónico e información de apoyo que considere importante para la continuidad del servicio y almacenar esta

información en los medios que la misma oficina tenga dispuestos para tal fin.

5.19 POLITICA DE USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

6.1.1 SENSIBILIZACIÓN Y COMUNICACIÓN

La Oficina de Informatica a través del "Plan de comunicación y sensibilización de TI" planificará anualmente la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad.

La creación de los contenidos se hará con apoyo de la Oficina de Comunicaciones y el grupo de Arquitectura Empresarial y Seguridad de la Información

6.1.2 CAPACITACIONES EN SEGURIDAD

El Ideam a través del Grupo de Administración y Desarrollo del Talento Humano, incluirá dentro de su plan institucional de capacitaciones y demás planes estratégicos las capacitaciones e inducciones en temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se

vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información y se mantengan actualizados mediante capacitaciones permanentes en temas de seguridad de la Información. La oficina de Informatica y el Oficial de Seguridad de la Información apoyará en dichas inducciones.

7. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del Ideam.

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal del IDEAM de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. La Oficina de Informatica será el encargado de recopilar y entregar a la Oficina de Control Interno Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

Control de cambios

VERSIÓN	FECHA	DESCRIPCIÓN
1	01/12/2020	Creación del Documento
2	18/05/2021	Segunda versión. Modificación de acuerdo con directiva presidencial 03 del 15 de marzo de 2021, recomendaciones consejería de transformación digital y recomendaciones de auditoría Externa
3	11/12/2024	Actualización, Manual de Políticas Complementarias de Seguridad y Privacidad de la Información de acuerdo con la actualización de la Política General de Seguridad y Privacidad de la Información

Documento aprobado en la IV sesión Comité Institucional de Gestión y Desempeño llevada a cabo el 29 de noviembre del 2024.