Introducción

En el marco de la evolución tecnológica y la creciente importancia de la gestión eficiente de la información, la Oficina de Informática del IDEAM, en conjunto con el Grupo de Arquitectura Empresarial y Seguridad de la Información (GAESI), ha desarrollado este manual con el propósito de establecer directrices claras y efectivas para la planeación, operación, control y mejoramiento continuo de la gestión de Tecnologías de la Información y las Comunicaciones (TIC) dentro de la entidad.

Objetivo

Establecer directrices para la planeación, operación, control y mejoramiento de la gestión de Tecnologías de la información y las Comunicaciones al interior de la entidad y que sirvan de base para apalancar los procesos tecnológicos en todo su ciclo de vida generando valor público y optimización de recursos.

Alcance

El manual de políticas de Tecnologías de la Información involucra todas las subdirecciones, oficinas, áreas técnicas y procesos que desde la competencia técnica requieran el uso, compra de tecnología, desarrollo de proyectos de software, adquisición de licenciamiento en el marco de la innovación y transformación digital de sus respectivos procesos.

Definiciones

Se adopta para este manual de políticas de tecnologías de Información, el glosario del Marco de Referencia de Arquitectura Empresarial para la gestión TI, el cual hace parte de la política de gobierno digital según el decreto 1008 de 2018, publicado en el portal oficial https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html y la norma ISO/IEC 27000.

Siglas

(MSPI): Modelo de Seguridad y Privacidad de la Información

Marco Normativo

Para la construcción de este manual se tiene como base, el lineamiento G.ES.03 Guía del dominio de Estrategia: Definición y diseño de una política de TI, la directriz de Gobierno Digital en su Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma internacional ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información; siendo esta última una norma emitida por la Organización Internacional de Normalización, que describe cómo gestionar la seguridad de la información en una organización.

DESCRIPCIÓN METODOLÓGICA DEL TEMA A DESARROLLAR

Este manual constituye un marco de referencia esencial para garantizar la eficiencia, seguridad y conformidad de las operaciones tecnológicas en el IDEAM, promoviendo así la excelencia en la gestión de las Tecnologías de la Información y las Comunicaciones.

Cada política se complementará con procedimientos específicos, como el software, la gestión de proyectos de desarrollo de software, y la administración de credenciales de acceso, asegurando así la implementación efectiva de las políticas establecidas.

1. POLÍTICA GENERAL DE TECNOLOGIAS DE LA INFORMACION IDEAM

La Oficina de Informática del IDEAM tiene por política administrar la habilitación tecnológica de todos los procesos institucionales, buscando mejorar las

interacciones de las áreas internas y sus grupos de interés, prestando servicios oportunos, efectivos y eficientes.

En el proceso de Gestión de Tecnologías de Información y Comunicaciones y según los dominios fundamentales del Marco de referencia de Arquitectura Empresarial y las buenas prácticas para la gestión de Tecnologías y proyectos se definieron las siguientes políticas:

1.1. POLITICA DE ADQUISICION DE INFRAESTRUCTURA TECNOLOGICA, SOFTWARE Y LICENCIAMIENTO

- Todo proceso de adquisición de recursos informáticos, licencias de software, hardware y otros dispositivos tecnológicos deberá ser incluido en las necesidades anuales del Plan Estratégico de Tecnologías – PETI.

- Toda necesidad de adquisición de Tecnología de las áreas del IDEAM deben ser gestionadas en coordinación con la Oficina de Informática, previa validación de la infraestructura actual para identificar la disponibilidad de esta, el plan de gestión de la infraestructura tecnológica y no generar gastos a la entidad.

- Las áreas del IDEAM deberán hacer uso del procedimiento E-GI-P004 Procedimiento Adquisición Bienes Y Servicios Informáticos toda vez que se requiera realizar una adquisición de tecnología.

- Para la adquisición de dispositivos tecnológicos es necesario que se tengan en cuenta marcas reconocidas, con representación en Colombia para la garantía y repuestos y con certificaciones de eficiencia energética.

- Toda adquisición de dispositivos tecnológicos debe llevar consigo la cláusula de disposición final de desechos tecnológicos y que cumpla con la normatividad vigente de protección al medio ambiente.

- La adquisición de licenciamiento de software deberá iniciar con el procedimiento E-GI-P007 - procedimiento control uso licencias software.

- Cuando se realice adquisición de licenciamiento de software este deberá ser entregado a la Oficina de Informática para la instalación, gestión, control y administración de las mismas para no incurrir en sobredimensionamiento o violación de derechos de autor.

- Para la adquisición de software, la Oficina de Informática será quien determine los criterios de adopción de tecnologías estableciendo la línea base de Arquitectura, bases de datos, ambientes de producción y pruebas, versionamientos y documentación de acuerdo con la Arquitectura Empresarial de referencia del IDEAM.

- Toda Adquisición de Software debe ser valorado y aprobado por la Oficina de Informática. previa validación del software actual, la arquitectura de sistemas de información y la capacidad instalada, para identificar la disponibilidad de esta y no generar gastos a la entidad

- La adquisición de nuevo software, debe contar con una etapa de verificación (estudio previo) por parte de la Oficina Informática, para determinar que no existan en la entidad soluciones que cubran la necesidad.

- Los usuarios de los sistemas informáticos en producción serán responsables de la calidad y veracidad de los datos que se ingresen u obtenga.

1.2. POLITICA DE DESARROLLO DE SOFTWARE INHOUSE Y TERCERO

- Todo proyecto de desarrollo de software in House o por tercero deberá ser incluido en las necesidades anuales del Plan Estratégico de Tecnologías – PETI.

- Todo desarrollo de software In House y mediante tercero así como el mantenimiento evolutivo de los componentes de software de los sistemas de información se deberá aplicar el procedimiento E-GI-P012 - procedimiento construcción o mantenimiento evolutivo software misional y apoyo y el E-GI-P009 - procedimiento gestión proyectos sistemas información.

- Los sistemas de información que se desarrollen por terceros, deberán realizarse previa contratación acorde a los lineamientos del área jurídica (contratación) y con el pleno aval de la Oficina de Informática.

- Todo desarrollo de software In House y Tercero de aplicaciones debe contar con un análisis de requerimientos enmarcado en la misión, las responsabilidades y los servicios de la entidad y estar acorde con la visión de arquitectura de referencia de la Oficina de Informática del IDEAM y contar con todos los involucrados para lograr el cumplimiento de objetivos y beneficios esperados.

  Para ello se deben considerar los siguientes aspectos como mínimo:

- La capacidad de la infraestructura tecnológica del IDEAM.
- La capacidad del recurso humano necesario y con experiencia para desarrollar el proyecto.
- El cronograma de actividades definiendo fases e hitos de ejecución del proyecto.
- Análisis de viabilidad financiera del proyecto.
- Alineación con los planes institucionales del IDEAM.

- Los proyectos relacionados con la tecnología de información generalmente involucran distintas fases durante su "ciclo vital". Por ejemplo, el ciclo vital de un sistema computadorizado comienza con el análisis de las necesidades y termina cuando se remplaza por un nuevo sistema o se determina que deja de ser necesario. En términos generales, el ciclo vital de un proyecto de informática consta de las siguientes fases:
  - Análisis
  - Diseño
  - Desarrollo
  - Pruebas
  - Implementación
  - Mejora continua.

- Todo desarrollo de software In House y mediante tercero deberá contar con separación de ambientes de TI - ambientes de desarrollo, prueba y producción del IDEAM, siempre que sea posible se separan de forma física, en caso contrario se segmentan como máquinas virtuales.

- El software o aplicación desarrollada deberá tener la integración con los sistemas de información existente (Si lo requiere) y orientado a la integración con el marco de interoperabilidad del estado colombiano.

- Todo desarrollo, mejora o actualización de un sistema de información que afecte un servicio tecnológico, debe incluir una estrategia de gestión del cambio organizacional que permita la gestión del impacto y los intereses de los usuarios del servicio y que garanticen el uso y apropiación de este.

- Se debe definir e implementar un plan de transferencia de conocimiento por cada proyecto de implementación de los servicios tecnológicos, que fortalezca las competencias de los usuarios (funcionarios, contratistas y terceros), y garantice el uso y apropiación de la solución tecnológica.

- Todos los desarrollos de las bases de datos elaborados por terceros serán producidos por los estándares definidos por la oficina de Informática y según la guía - E-GI-G014 Guía base de datos.

- Al crearse una Base de Datos se deberá generar la documentación propia que permita comprender su estructura física y lógica y su contenido.

- La migración de la información obtenida en las bases de datos será elaborada por personal capacitado (interno o externo) y deberá ser supervisado por la Oficina de Informática
- Previo al proceso de migración se requiere realizar las copias de respaldo respectivos, de igual forma se requiere hacer pruebas de migración en un servidor o máquina virtual..

1.3. POLITICA DE GESTION DE TI

- Toda solicitud de servicio contemplada en el catálogo de servicios, será recibida únicamente por los canales dispuestos para tal fin.

- Las credenciales de acceso a cada uno de los servicios tecnológicos será responsabilidad única y exclusivamente del usuario asignado.

- Es responsabilidad del usuario (Funcionario y contratista) hacer buen uso de la cuenta de correo electrónico para la gestión administrativa y no con fines personales en suscripciones y violación de derechos de autor para aplicaciones no autorizadas por el IDEAM.

- Todo acceso no autorizado por el usuario (Funcionario y contratista) a sistemas de información, bases de datos, aplicaciones o carpetas compartidas será reportado a la Oficina de control Interno del IDEAM.

- El uso, almacenaje, copiado y reproducción de software en los servicios tecnológicos del IDEAM, requieren del consentimiento del propietario de los derechos de autor.

- Toda sustracción de información sensible y propia del IDEAM por medios físicos o electrónicos para fines comerciales o de vulneración de la seguridad será reportado a la Oficina de control Interno del IDEAM.

- Toda instalación o manipulación de software no propietario del IDEAM en las estaciones de trabajo propias de la entidad y sin previa autorización será reportado a la Oficina de control Interno del IDEAM.

- La Oficina de Informática podrá remover cualquier tipo de Software ilegal que se encuentre instalado en cualquier máquina, sin informar

al usuario responsable de esta remoción y sin ningún tipo de responsabilidad que dicha eliminación de software pueda acarrear directa o indirectamente.

- Es responsabilidad del usuario (Funcionario y contratista) realizar el reporte por la mesa de servicios de cualquier acto sospechoso, evento o incidente de seguridad.

- La Oficina de Informática es el encargado de la administración de los servicios tecnológicos entre otros el control y filtrado de los servicios de internet y podrá realizar el bloqueo de páginas web cuando las mismas sean reportadas como sospechosas.

- Para todo sistema de información que se encuentren en el ambiente de producción se deberá definir un líder por parte del área funcional (Líder funcional).

1.4. POLITICA DE CONTINUIDAD

- La Oficina de Informática es la encargada de velar por la confidencialidad, integridad y disponibilidad de la información contenida en las bases de datos y servidores del Data Center para lo cual realizaría los backups y pruebas de restauración que sean necesarias.

- La Oficina de Informática establece los parámetros de retención para efectuar las copias de respaldo con base en los tiempos determinados en las tablas de retención documental (TRD) y teniendo en cuenta la criticidad de la información de acuerdo con el procedimiento de Gestión del control de activos de información.

- Es responsabilidad del usuario (Funcionario y contratista) realizar la respectiva copia de sus archivos de gestión y demás actuaciones administrativas en los sitios dispuestos para tal fin.

- Toda la documentación, archivos ejecutables, códigos fuente, librerías de software, script de bases de datos, así como la documentación de paquetes de software adquiridos, así como la gestión de versiona miento de cada desarrollo siguen la arquitectura de referencia definida por la Oficina de Informática.

1.5. POLITICA DE SEGURIDAD

- Todo usuario con acceso a un sistema de información dispondrá de una autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y contraseña.

- Las contraseñas tendrán plazo de vigencia, que en ningún caso podrá ser superior a los 2 meses.

- Cada sistema informático del IDEAM deberá tener segmentados por roles a sus usuarios que permitan los cambios o modificaciones necesarias autorizadas.

- Si los usuarios sospechan que su acceso autorizado (identificador de usuario y/o contraseña) está siendo utilizado por otra persona, deberá informar a la Oficina Informática y solicitar una nueva contraseña.

- Los usuarios no deben intentar obtener otros derechos de acceso al cual no están autorizados, ni utilizar ningún otro acceso autorizado que

corresponda a otro usuario, aunque disponga de la autorización de éste. Salvo a la autorización dada por la autoridad competente.

- En caso el caso de terminación de contrato o vacaciones de un colaborador, el jefe del área funcional deberá informar a la Oficina Informática para realizar la baja a las credenciales asignadas.

1.6. POLITICA DE GESTION DE CREDENCIALES DE ACCESO

- La custodia del inventario de credenciales de acceso de superadministrador y administrador para sistemas de información, bases de datos, infraestructura tecnológica física y virtual, redes y comunicaciones, suscripciones y licenciamiento estará exclusivamente a cargo del Jefe de la Oficina de Informática o quien haga sus veces.

- La delegación de credenciales de acceso a sistemas de información, bases de datos, infraestructura tecnológica física y virtual, redes y comunicaciones, suscripciones y licenciamiento a funcionarios y contratistas que necesiten acceso en el curso de sus funciones será exclusivamente realizada por el Jefe de la Oficina de Informática.

- El Jefe de la Oficina de Informática podrá requerir en cualquier momento que los funcionarios y contratistas proporcionen un inventario actualizado de las credenciales de acceso que tengan bajo su responsabilidad.

- El Jefe de la Oficina de Informática tiene la facultad de revocar los privilegios de administración sobre cualquier sistema de información, bases de datos, infraestructura tecnológica física y virtual, redes y

comunicaciones, suscripciones y licenciamiento según lo considere necesario.

- Las credenciales de acceso suministradas a funcionarios y contratistas de la Oficina de Informática no podrán cambiarse sin la autorización escrita del Jefe de la Oficina de Informatica o quien haga sus veces, so pena de una sanción.

1.7. POLITICAS MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS INFORMÁTICOS

- La Oficina Informática comunicará el programa de mantenimiento preventivo a las diferentes Áreas u Oficinas del IDEAM, informado a cada una de ellas la fecha de mantenimiento.

- Con el objetivo de evitar pérdidas de datos o información relevante, antes de llevarse a cabo la actividad de mantenimiento, los usuarios deberán respaldar la información almacenada en la computadora.

- Las Áreas u Oficinas deberán programar sus actividades de tal manera que el equipo esté disponible en la fecha indicada para ejecutarle el mantenimiento preventivo.

2. EXCEPCIONES AL ALCANCE DEL MANUAL DE POLÍTICAS

Toda solicitud de excepción de alguna política debe ser solicitada a la Dirección General y Oficina de Informática con la debida justificación y documentación conforme la naturaleza de su cargo o dado por eventos no contemplados en este documento; y debe evaluar el alcance y las implicaciones de la solicitud.

3. RESTRICCIONES

Queda prohibido, a otras áreas distintas a la Oficina Informática:

- La manipulación o extracción de piezas internas de los equipos de cómputo o informáticos.
- La instalación de Software.
- Acceso al área de Servidores sin previa autorización.

El presente documento es un marco de referencia para los usuarios del IDEAM y en virtud de la imposibilidad de enumerar todos los elementos existentes en referencia a las Tecnologías de Información (TI), dejamos aquí constancia de que todo aquello que no se encuentra expresamente permitido se encuentra restringido.

4. SANCIONES

El inadecuado uso o incumplimiento de las políticas de Tecnologías de Información y/o la política de seguridad y privacidad de la información, será sancionado por la entidad en los términos que establecen la normativa vigente y los procedimientos administrativos existentes En el IDEAM.

5. ROLES Y RESPONSABILIDADES

OFICINA DE INFORMÁTICA.

- Es responsable del uso de la política de TI como herramienta de gestión y definir los estándares para que la entidad de cumplimiento a la misma.

- Poner a disposición los recursos humanos y técnicos necesarios para el cumplimiento de las políticas de TI.

- Realizar la actualización de las políticas cuando se requiera por cambios de normatividad y mejora continua.

- **FUNCIONARIOS CONTRATISTAS Y TERCEROS.**

- Son responsables del cumplimiento de las políticas de TI.

- **OFICIAL DE SEGURIDAD**

- Realizar la investigación y seguimiento a los eventos e incidentes de seguridad.

- Ejecutar planes de divulgación de uso y apropiación de la política de TI.

- **OFICINA DE CONTROL INTERNO / CONTROL INTERNO DISCIPLINARIO.**

- Apoyar en las auditorias y seguimientos de los incidentes de seguridad.

- **ALTA DIRECCION**

- Realizar la aprobación de exclusiones a la política de TI.

- Realizar aprobaciones de mejoras de la Política de TI.

6. VIGENCIA DE LA POLÍTICA

Las Políticas de Tecnologías de la Información – TI, entra en vigencia con acta de aprobación del Comité Institucional de Gestión y Desempeño firmada por el Director General del Instituto de Hidrología, Meteorología y Estudios Ambientales; y pueden ser actualizadas cuando exista cambio en normatividad o mejora en los procesos por parte de la Oficina de Informática.

Documentos relacionados en el SGI

Control de cambios

Versión	Fecha	Descripción
1.0	27/07/2024	Creación del Manual de Políticas de Tecnologías de la Información.

Documento aprobado en la III sesión Comité Institucional de Gestión y Desempeño llevada a cabo el 27 de junio del 2024