POLÍTICA: TECNOLOGÍAS DE LA INFORMACIÓN - IDPC

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 2 del 29 de diciembre de 2023

Contenido

1. Propósito

EL instituto Distrital de Patrimonio Cultural a través de Grupo de Gestión de Sistemas de Información y Tecnología , dando cumplimiento a sus funciones de servir a todos los bogotanos y promover una ciudadanía activa y responsable, enuncia esta política conscientes de que no solo la entidad sino también los diferentes actores de la sociedad, son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público; dando cumplimiento a la estrategia de TI del gobierno y el Modelo Integrado de Planeación y Gestión-MIPG, según lo establecido en el Decreto 1078 de 2015, 1008 de 2018 y el Decreto 1499 de 2017 respectivamente.

2. Objetivo

El objetivo del presente documento es guiar el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público en un entorno de confianza digital, mediante la implementación de un modelo de gestión (PETI); y así mejorar la provisión de servicios digitales, el desarrollo de procesos internos eficientes, la toma de decisiones basadas en datos y el empoderamiento de los ciudadanos.

3. Alcance

Establecer un marco de gobierno para la gestión de las tecnologías de la información y las comunicaciones - TIC en el Instituto Distrital de Patrimonio Cultural - IDPC, que permitan satisfacer la necesidades actuales y futuras del negocio, basada en criterios de innovación, calidad, eficiencia, escalabilidad y arquitectura empresarial. Esta política debe ser aplicada por funcionarios, contratistas y terceros que gestionen las tecnologías de la información y las comunicaciones en la entidad.

4. Definiciones

Política de TIC: Es un conjunto de reglas que controlan las características y las funciones de los dispositivos. Puede utilizar las reglas de políticas de TI para controlar las características del dispositivo, el espacio de trabajo en los dispositivos, o ambos.

Modelo de seguridad y privacidad de la información MSPI. Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

NTC ISO 22301:2012: Es la primera norma internacional para la **gestión de la continuidad de negocio** y se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones. Esta norma remplaza a la norma británica BS25999. Especifica los requisitos necesarios para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar de forma continua el Sistema de Gestión para responder y recuperarse pronto de las interrupciones, en el momento en el que sucedan.

NTC ISO/IEC 27001: 2013. Son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). ... Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia.

La norma ISO 9001: Tiene carácter internacional, da respuesta a la implementación de un Sistema de Gestión de Calidad. La norma ISO 9001 demuestra a los clientes que tus productos o servicios cumplen con la ley y con los estándares de calidad que requiere la ISO, que es la Organización Internacional de Normalización.

Ley 734 de 2002: Denominado el Código Disciplinario Único. Es ejercida por la Procuraduría General de la Nación, las Personerías, las Oficinas de Control Interno, los funcionarios con potestad disciplinaria y la jurisdicción disciplinaria.

Procesos: Se define un proceso de negocio como conjunto de actividades que reciben una o más entradas para crear un resultado/producto de valor para el cliente o para la propia compañía/proceso (concepto de Cliente Interno de Calidad). Normalmente, una actividad empresarial cuenta con múltiples procesos que sirven para el desarrollo su objeto de negocio.
Procedimientos: Pasos operacionales que los colaboradores deben realizar para alcanzar ciertos objetivos/resultados.
Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
Servicio de tecnologías de la información: Es un conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos (llámese activos), potenciando el valor de estos y reduciendo el riesgo inherente del sistema.
Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas del IDPC en un momento dado.
Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la entidad.
Acceso lógico: En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.
Aceptación de riesgo: Decisión de asumir un riesgo.
Activo: Cualquier elemento que represente valor para la organización.
Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
Acuerdos de Confidencialidad: Es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
Acuerdos de Intercambio de información: Es un contrato legal entre al menos dos entidades para compartir información o conocimiento para ciertos propósitos, donde se definen las responsabilidades de protección que se le deberá dar a dicha información.
Acuerdos de Niveles de Servicio: Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

Alta Dirección: Se considera Alta Dirección a los directivos con cargo más alto en una organización; el Gerente General y los directores de las distintas áreas. En el caso del IDPC se entiende como Alta Dirección a la integrada por la Gerente de la entidad y el Comité Directivo.
Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).
Adaptabilidad: Define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.
Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Cifrado: Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.
Cifrar: Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.
Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

5. Descripción de la Política

El Instituto Distrital de Patrimonio Cultural, en su Plan estratégico de Tecnologías de la Información y las Comunicaciones establece el uso adecuado de cada una de sus herramientas de TIC para la gestión del día a día en cumplimiento de sus objetivos estratégicos. Por lo anterior, cada uno de los funcionarios, contratistas y terceros de la entidad debe tener en cuenta, que la política:

1. Se encuentra adecuada al propósito de la entidad.
2. Proporcionar el marco para establecer los objetivos del negocio.
3. Incluye un compromiso para satisfacer los requisitos aplicables.
4. Está disponible como información documentada y aprobada, para las partes interesadas, según sea apropiado.
5. Debe ser mediable.
6. Es coherente con las demás políticas Institucionales del IDPC.
7. Debe ser divulgada al interior de la entidad.
8. Debe contar con una periódica adecuación y cuando se produzcan cambios significativos.

5.1 Política de Servicios Tecnológicos

La gestión y uso de los servicios Tecnológicos se rigen por una serie de políticas que apoyan el cuidado y correcto funcionamiento de cada uno de los servicios.

a. Política general de uso

- El grupo de Gestión de Sistemas de Información y Tecnología, es quien asigna, configura, soporta, modifica y brinda asesoría sobre el uso y acceso a los servicios tecnológicos (equipos de cómputo, servidores de la red interna, externa y los datos).
- Los equipos de cómputo deben ser configurados para las necesidades de gestión de cada uno de los funcionaros, contratistas y terceros.
- Los servicios tecnológicos del IDPC, no deben ser gestionados por personas ajenas a la entidad.
- La conexión de red internas y externas, deben ser especificadas claramente, con las características técnicas y de seguridad requeridas, para ser aprobadas por El grupo de Gestión de Sistemas de Información y Tecnología.
- La gestión sobre los servicios tecnológicos del IDPC, son para dar cumplimiento a las funciones establecidas para los funcionaros, contratistas y terceros, y no para actividades personales o de ocio.
- El uso, almacenaje, copiado y reproducción de software en los servicios tecnológicos de la entidad, requieren del consentimiento del propietario de los derechos de autor.
- Se deben establecer Acuerdos de Nivel de Servicio – ANS, para cada uno de los servicios que ofrece El grupo de Gestión de Sistemas de Información y Tecnología.
- Se deben determinar los Acuerdos de Nivel Operativo – ANO, conjuntamente con el proveedor para cada uno de los proyectos.
- Todo 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, 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.

b. Política de Restricciones y Obligaciones de los Usuarios

- Mantener limpios los espacios donde se encuentren ubicados los servicios tecnológicos.
- No se debe fumar, consumir alimentos o líquidos en los espacios donde se encuentre ubicados los equipos de cómputo (computadores, impresoras, escáner, etc.).
- No se permite la implementación de aplicaciones no autorizadas en los equipos de cómputo asignados a los funcionarios, contratistas y terceros o servidores que administren los datos.
- No se permite la realización de modificaciones a las configuraciones de los servicios tecnológicos asignados, sin el conocimiento y la debida autorización del grupo de Gestión de Sistemas de Información y Tecnología.
- No se permite la conexión o desconexión de hardware de los equipos de cómputo, sin autorización del grupo de Gestión de Sistemas de Información y Tecnología.
- Debe ser reportada al Grupo de Gestión de sistemas de información y Tecnología las fallas que presenten los equipos de cómputo, para que ellos sean quienes den solución a la incidencia a través de la mesa de ayuda dispuesta para esto.
- Los equipos de cómputo asignados no son para realizar actividades ociosas en la Internet que puedan generar inconvenientes y saturaciones en el ancho de banda del IDPC.
- No se permite que a través de los servicios tecnológicos a los que se tiene acceso se generen ataques a otros equipos internos o externos.
- Cualquier daño o falla que presenten los equipos tecnológicos del IDPC, debe ser reportado al grupo de Gestión de Sistemas de Información y Tecnología a través de la mesa de ayuda dispuesta para ello.

c. Política de modificaciones al servicio

- El grupo de Gestión de Sistemas de Información y Tecnología, puede modificar o suspender los servicios tecnológicos de manera parcial o total a uno o varios de los funcionarios, contratistas y terceros, cuando se requiera por motivos de seguridad, por mantenimiento de los servicios preventivo o correctivo, o por causas de fuerza mayor.

5.1.1 Política de Adquisiciones Tecnológicas.

Toda la adquisición de infraestructura debe estar contemplada en el Plan Anual de Adquisiciones PAA, el documento de la Arquitectura TI, el PETI y debe estar sujeta a los procedimientos establecidos por el IDPC. No obstante, de acuerdo con las necesidades de la Entidad, será posible la adquisición de hardware que no estuviera inicialmente previsto, para ello se debe actualizar el PAA ya que de no hacerlo no se podrán viabilizar los recursos. Cualquier necesidad de adquisición

de las dependencias deben ser gestionadas en coordinación con el grupo de Gestión de Sistemas de Información y Tecnología, 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 adquisiciones de la infraestructura deben generarse como una solución integral del IDPC, se deben establecer como obligatorio la adquisición de las pólizas necesarias, velar por cubrir las necesidades de la adquisición de repuestos y el mantenimiento de la infraestructura.

La adquisición de la Infraestructura se debe priorizar en los fabricantes con presencia en el país y con capacidad de brindar soporte técnico garantizado. De igual manera, se pueden realizar adquisiciones por empresas distribuidoras nacionales e internacionales, debidamente autorizadas por los fabricantes y así poder garantizar el soporte técnico.

5.1.2 Política de custodia.

El Grupo de Gestión de sistemas de información y Tecnología es al responsable de la custodia de los activos fijos tecnológicos, mediante los procesos establecidos y aprobados por el Sistema de Gestión de Calidad. Los activos físicos tecnológicos deben estar protegidos de los riesgos del entorno físico y lógico, esta protección es necesaria para reducir las posibles pérdidas o averías de los activos y está bajo responsabilidad del grupo de bienes e infraestructura.

El grupo de Gestión de Sistemas de Información y Tecnología emite un concepto técnico de los equipos puede ser dado de baja según las características, el grupo de bienes e infraestructura es quien define los activos físicos tecnológicos que deben ser dados de baja según lo establece los procedimientos aprobados en el sistema de gestión de calidad, por su nivel de obsolescencia, por no encontrarse aptos para su funcionamiento y por no poder realizarle un efectivo mantenimiento, los cuales se pasaran al grupo de bienes e infraestructura para su baja con su debida aprobación.

Los funcionarios, contratistas y terceros que tengan bajo su custodia los equipos de cómputo son responsables de su buen uso y deben atender la normatividad establecida por el IDPC. Los equipos de cómputo pueden ser reasignados según las necesidades para la ejecución de las actividades de cada uno de los funcionarios, contratistas o terceros de la entidad.

Los equipos de cómputo que sean de propiedad de los funcionarios, contratistas o terceros, e ingresados a la entidad son de total responsabilidad de estos.

5.1.3 Control y mantenimiento de Infraestructura Tecnológica.

El grupo de Gestión de Sistemas de Información y Tecnología, debe elaborar, actualizar y mantener el documento de la Arquitectura TI.

Los mantenimientos preventivos o correctivos sobre la infraestructura tecnológica de la Entidad, deben ser planeados, coordinados, comunicados y ejecutados por el grupo de Gestión de Sistemas de Información y Tecnología y el proceso de bienes e infraestructura.

El grupo de Gestión de Sistemas de Información y Tecnología, debe gestionar la configuración sobre cada uno de los componentes de la solución de TIC, como se establece en el procedimiento.

El grupo de Gestión de Sistemas de Información y Tecnología, debe realizar el monitoreo continuo de los servicios tecnológicos y validar el cumplimiento de los ANS de cada uno de ellos.

Es de obligatorio cumplimiento la adquisición de las pólizas de garantía sobre toda la infraestructura tecnológica que se adquiera en el IDPC.

5.1.4 Equipos y servicios de cómputo.

Esta política está orientada a formar a los usuarios en el cuidado y adecuado funcionamiento de los equipos y servicios de cómputo asignados.

La asignación de los equipos de cómputo y el acceso a la red de datos, debe ser realizada por el grupo de Gestión de Sistemas de Información y Tecnología. La asignación debe ser a personal del IDPC (funcionarios, contratistas o terceros), en ninguna circunstancia deben ser operados por personas ajenas al Instituto Distrital de Patrimonio Cultural.

Los usuarios, que requieran apoyo u orientación en el manejo y gestión de los equipos de cómputo asignados y la información que contengan, deben solicitar el mismo al grupo o El grupo de Gestión de Sistemas de Información y Tecnología a través de la mesa de ayuda dispuesta para ello.

Los equipos de cómputo y el acceso a la red de datos, no pueden ser utilizados para fines personales o de ocio. Las actividades a realizarse sobre estos equipos y la red deben relacionarse a los programas y proyectos administrativos y misionales del IDPC.

La instalación de licenciamiento en cada uno de los equipos de cómputo debe ser realizado o autorizado por el Grupo de Gestión de sistemas de información y Tecnología del IDPC.

Es prohibido el uso, almacenamiento y reproducción de software sin el consentimiento del propietario de los derechos de autor.

5.1.4.1 Usos aceptables.

Los siguientes son los usos aceptables de los recursos de cómputo y el acceso a la red de datos, que permitan lograr un correcto desempeño a los usuarios en sus funciones y optimización de los recursos de cómputo:

- Las actividades en desarrollo de las funciones propias del IDPC (misionales, administrativas y de apoyo)

- Presentaciones, talleres y cursos virtuales organizados por el IDPC.

- Actividades propias del IDPC, que requieran el uso de medios electrónicos y redes de datos.

5.1.4.2 Obligaciones de los usuarios.

Se requiere que los usuarios respeten la integridad de los equipos tecnológicos, el acceso a la red de datos y las instalaciones asignadas.

- No se debe fumar, consumir alimentos y/o bebidas en los espacios donde se encuentren los equipos de cómputo.

- Los usuarios deben mantener limpias las áreas donde se encuentren

- Cualquier incidencia sobre los equipos de cómputo y acceso a la red de datos, debe ser reportado a través de la mesa de ayuda dispuesta para ello al grupo de Gestión de Sistemas de Información y Tecnología, para apliquen la solución pertinente.

- No se debe conectar o desconectar hardware externos al equipo de cómputo sin autorización de Oficina de Gestión de Sistemas de Información y Tecnología.

- No puede realizar instalaciones de software sin contar con la aprobación de Oficina de Gestión de Sistemas de Información y Tecnología.

- El software de comunicación instantánea a instalar y utilizar debe ser aprobado por Oficina de Gestión de Sistemas de Información y Tecnología

- Los equipos de cómputo no pueden ser utilizados para actividades ociosas o juegos; de igual manera, no puede ser utilizado para descargar archivos o software que saturen el ancho de banda del IDPC.

- Los usuarios no pueden utilizar sus equipos de cómputo asignados para lanzar ataques a otros equipos conectados en red.

- Los usuarios no cuentan con autorización para realizar modificaciones a la configuración del equipo de cómputo asignado.

5.1.5 Código Malicioso.
Se encuentra en la política de Seguridad y Privacidad de la Información.

5.1.6 Gestión de Medíos Magnéticos.
El IDPC, debe generar un inventario de todos los medios magnéticos que gestionan la información de la Entidad, este inventario debe contener las condiciones y restricciones de cada uno de los medios, indicadas por los fabricantes para determinar su tiempo de conservación. Cada medio debe ser debidamente marcado para la correcta gestión de la información que contenga.

Los medios magnéticos que no sean requeridos y ya cumplieron con su función debe ser destruido y se debe garantizar porque su información no pueda ser recuperada.

Los medios magnéticos que requieran ser almacenados y salvaguardados, deben ser protegidos contra el acceso no autorizado, el mal uso de este o corrupción del medio, dentro o fuera de la IDPC.

5.1.7 Políticas de soporte de TIC a los usuarios.
El IDPC, por medio Oficina de Gestión de Sistemas de Información y Tecnología, debe garantizar una única mesa de ayuda como canal oficial para atender los incidentes y requerimientos sobre los servicios de TIC de acuerdo con el catálogo de servicios de la entidad y los Acuerdos de Nivel de Servicio – ANS establecidos para cada uno de ellos.

5.1.7.1 Gestión de requerimientos.
La mesa de ayuda, debe mantener informado a los usuarios solicitantes de la evolución de sus requerimientos. Si el requerimiento no puede ser implementado en los tiempos establecidos en los ANS, el usuario debe ser informado.

5.1.7.2 Gestión de incidentes.
La mesa de ayuda, debe aplicar el procedimiento para gestión del registro, asignación de prioridad, valoración del impacto, clasificación, actualización, escalado, resolución y cierre formal del incidente reportado.
Si la incidencia requiere restauración de servicios, este debe ser atendido de manera inmediata mediante la aplicación de una solución temporal o definitiva. Debe informarse al usuario de la solución aplicada.
Si la incidencia no requiere una restauración de servicios inmediata, durante su gestión, se debe mantener informado a los usuarios solicitantes de la evolución del incidente. Si el requerimiento no puede ser implementado en los tiempos establecidos en los ANS, el usuario debe ser informado.

5.1.8 Políticas sobre el Servicio de Internet.

Esta política se encuentra inmersa en el Manual de Políticas de Seguridad y Privacidad de la Información del 28 de abril de 2023.

5.1.9 Políticas sobre el Correo Electrónico.

Esta política se encuentra inmersa en el Manual de Políticas de Seguridad y Privacidad de la Información del 28 de abril de 2023.

5.1.10 Políticas Antivirus y Gestión de la Información.

Lineamientos que cada uno de los funcionarios, contratistas o terceros deben tener en cuenta para brindar la protección adecuada a los equipos de cómputo ante un posible ataque de virus informático.

5.1.10.1 Políticas Generales.

- No se debe abrir archivos cuya extensión no sea conocida o que se esté absolutamente seguro de que el mail proviene de una persona conocida y confiable o que haya informado previamente del envío de este.
- El Grupo de Gestión de sistemas de información y Tecnología debe implementar firewall a nivel físico y lógico, para minimizar el riesgo de ataques sobre la infraestructura tecnológica del IDPC, filtrar los contenidos y la gestión de las políticas para el Internet.
- Los archivos deben ser trabajados en el equipo de cómputo asignado por la Entidad y luego copiados a un medio magnético externo, no deben trabajarse directamente sobre el medio magnético externo debido a que si es dañado por un virus su recuperación puede no ser realizada.
- Se debe realizar la copia de seguridad de la información de los equipos de cómputo asignados a los funcionarios, contratistas y terceros, como lo establece en el procedimiento aprobado por el sistema de gestión de calidad de la Entidad.
- El grupo de Gestión de Sistemas de Información y Tecnología, lanzará periódicas actualizaciones a los sistemas operativos o aplicaciones para minimizar las posibilidades de acceso de virus y aumentar la protección contra los ataques informáticos.

5.1.10.2 Política sobre la Aplicación de Antivirus

- Los funcionarios, contratistas y terceros, deben generar una cultura de ejecución periódica de vacunación de las unidades internas del equipo de cómputo asignado como funcionario, contratista o tercero.
- Los funcionarios, contratistas y terceros, deben realizar la aplicación y revisión del antivirus a las unidades externas que requiera conectar al equipo de cómputo, antes de ser utilizadas.

- El grupo de Gestión de Sistemas de Información y Tecnología, debe velar por que todos los funcionarios, contratistas y terceros, tengan el conocimiento operativo para la aplicación del antivirus en las unidades internas y externas del equipo de cómputo.

5.2 Políticas de software.

El Grupo de Gestión de sistemas de información y Tecnología es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo, actualizaciones e instalaciones del software del IDPC. De igual manera, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de colocar en producción.

5.2.1 Políticas de Adquisición Software.

Esta política se encuentra inmersa en el Manual de Políticas de Seguridad y Privacidad de la Información del 28 de abril de 2023.

5.2.2 Políticas de Software Libre

Según la Free Software Foundation, el software libre se refiere a la Libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el Software; de modo más preciso, se refiere a cuatro libertades de los usuarios del software: la libertad de usar el programa, con cualquier propósito; de estudiar el funcionamiento del programa, y adaptarlo a las necesidades; de distribuir copias, con lo cual se puede ayudar a otros y de mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie (para la segunda y última libertad mencionadas, el acceso al Código fuente es un requisito previo).
La política de software libre del MINTIC que dicta “La iniciativa de software libre de la Dirección de Gobierno Digital es una iniciativa que promueve el uso de software libre para la solución a necesidades y/o problemáticas de la administración pública por parte de funcionarios y/o contratistas del estado.

- La política de software libre debe contribuir en la creación e innovación de servicios eficientes, evitando duplicaciones de herramientas tecnológicas dentro de la entidad.
- Evitar la doble contratación de soluciones por parte de la entidad, promoviendo el eficiente uso de los recursos públicos.
- Ahorrar presupuestos en la entidad con el uso de software libre.
- Incentivar la innovación en la entidad en todos sus niveles, disminuyendo los riesgos inherentes a la innovación, para consolidar casos de éxito que sean referente local e internacional.
- Promover el uso de software libre en la entidad.

- Incentivar el aumento de la masa de desarrolladores e implantadores de software libre en la entidad, para crear nuevos modelos de negocio, permitiendo la adopción y reutilización de soluciones e intercambio de experiencias entre entidades y funcionarios.

5.2.3 Políticas de Desarrollo de software.
Esta política se encuentra inmersa en el Manual de Políticas de Seguridad y Privacidad de la Información del 28 de abril de 2023.

5.2.4 Custodia.
El Grupo de Gestión de sistemas de información y Tecnología es la responsable de la administración del software (sistemas operativos, aplicativos, utilitarios, administradores de bases de datos, lenguajes de programación, a la medida) de uso del IDPC. De igual manera, debe mantener actualizado el inventario del software y su licenciamiento.
Los desarrolladores del IDPC y terceros, no deberán tener acceso a información de producción que contenga datos sensibles.
Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.
Los accesos al código fuente y los archivos del sistema, se debe encontrar restringido.
Las actualizaciones del software deben ser realizadas por los administradores de estos al interior del IDPC, siguiendo las indicaciones establecidas en los controles de cambio debidamente documentados.

5.2.5 Política para la gestión de Vulnerabilidades
Se deberá establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.
Se deberá establecer un plan de actualización para el software que es desarrollado o se utiliza en la Entidad, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada.

5.2.6 Uso.
Solo se encuentra permitido el software legalmente adquirido por parte del IDPC. En caso de tratarse de equipos personales, (teléfonos celulares, agendas

electrónicas, dispositivos de almacenamiento de música y archivos, cámaras digitales, etc.) que sean utilizados con propósitos institucionales, cada usuario debe garantizar y tener las licencias que acrediten la legalidad del software que se está utilizando.
Cada usuario es responsable por la instalación del software no licenciado que se encuentre en los equipos de cómputo a su cargo.
El sistema operativo de los equipos de cómputo que se encuentran bajo la modalidad de arriendo debe estar licenciado por el proveedor de la empresa que presta el servicio.
La instalación de cualquier software ya sea institucional, personal o de libre distribución debe contar con la autorización previa del grupo de Gestión de Sistemas de Información y Tecnología.
El software utilizado por los proveedores de servicio y no suministrado por el IDPC, debe ser de su autoría o tener las licencias de uso correspondientes.
El software desarrollado a la medida es de propiedad del IDPC y es responsabilidad del Grupo de Gestión de sistemas de información y Tecnología adelantar, si es necesario, el debido registro del producto.
Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.
Todo despliegue de software, debe incluir una estrategia de gestión del cambio organizacional que permita la gestión del impacto y los intereses de los usuarios de este, que garanticen el uso y apropiación del software.
Se debe definir e implementar un plan de transferencia de conocimiento por cada proyecto de software, que fortalezca las competencias de los usuarios (funcionarios, contratistas y terceros), y garantice el uso y apropiación de la solución tecnológica.

5.2.7 Manejo de versiones de Cambio.

Los cambios de versiones del software deben ser planeados, analizados, evaluados y acordados conjuntamente entre el área responsable o solicitante del cambio y El grupo Gestión de Sistemas de Información y Tecnología.
La actualización y configuración de un nuevo sistema operativo deberá realizarse únicamente por personal autorizado.
Los controles de cambio deben estar debidamente documentados y deben ser ejecutados bajo los lineamientos de seguridad para no comprometer los sistemas.

5.3 Políticas de Seguridad de la Información.

Las políticas de Seguridad de la Información del IDPC, propende por el aseguramiento de la confidencialidad, integridad y disponibilidad de la información

de la Entidad; así como sus activos de información, la gestión de riesgos, la identificación de requerimientos legales y regulatorios acorde a la misión de la Entidad. Las políticas específicas de la seguridad de la información definidas para la Entidad, se encuentran en el Manual de Políticas de Seguridad de la Información que hace parte del MSPI, a continuación:

- Políticas para dispositivos móviles
- Políticas de teletrabajo
- Políticas de seguridad de los recursos humanos Políticas gestión de activos Políticas control de acceso
- Políticas seguridad física y del entorno
- Políticas transferencia de información
- Políticas de copias de respaldo
- Políticas seguridad en las operaciones
- Políticas seguridad de las comunicaciones
- Políticas adquisición, desarrollo y mantenimiento de sistemas
- Políticas relaciones con los proveedores
- Políticas gestión de incidente
- Políticas cumplimiento

6. Responsables

- **Grupo de Gestión de Sistemas de Información y Tecnología:** Es responsable del uso de la política de TIC como herramienta de gestión y definir los estándares para que la entidad de cumplimiento a la misma.
  - Poner a disposición los recursos necesarios para que las políticas de TIC de la Entidad se lleven a cabo de acuerdo con lo establecido en la presente política.
  - Designar el personal idóneo para apoyar la implementación de la presente política. - Cualquier requerimiento de modificación de las políticas debe ser dirigido al grupo Gestión de Sistemas de Información y Tecnología, quien será el encargado de mantener actualizado la política de TIC del IDPC.
- **Los funcionarios, Contratistas y terceros:** Son responsables de dar cumplimiento a las políticas de TIC.
- **Alta Dirección:** Dará aprobación de las modificaciones a las políticas de TIC, previa validación de la Oficina de Planeación a través del comité institucional de gestión y desempeño.
- **Equipo de Seguridad de la Información:** Velar que el cumplimiento de la presente política se lleve a cabo de acuerdo con los lineamientos de seguridad establecidos por el IDPC.

- **Coordinador Talento Humano:** Deberán informar al Grupo de Gestión de sistemas de información y Tecnología cuando finalice el contrato de cualquier miembro del personal de planta de la Entidad.
- **Jefe de la Oficina Jurídica o Supervisores de Contrato**: Deberán informar al Grupo de Gestión de sistemas de información y Tecnología cuando finalice el contrato de contratistas de la Entidad, además definir e implementar los controles de acceso físico
- **Oficina de Planeación:** Dará aprobación a los procesos, procedimientos y a las modificaciones a las políticas de TIC, previa validación del grupo de Gestión de Sistemas de Información y Tecnología.

7. Indicadores

7.1 Capacitación Política TI.

Nombre del Indicador: Porcentaje de capacitados sobre la política de TI
Objetivo del Indicador: Cálculo porcentual de personal del IDPC que ha sido capacitada sobre la política de TI.
Frecuencia: Anual
Formula: (Cantidad de Personal Capacitado en el año sobre la Política de TI /Cantidad de Personal vinculado al IDPC en el año) * 100

7.2 Incidentes de Seguridad.

Nombre del Indicador: Cantidad de Incidentes de Seguridad de la Información.
Objetivo del Indicador: Calcular la cantidad de incidentes que sé que se presenten contra las políticas de seguridad de la información en el IDPC.
Frecuencia: Anual Formula: Cuantificación de incidentes contra la política de seguridad de la información.

8. Excepciones

Las excepciones al cumplimiento de la política de las TIC, deben ser aprobadas por Oficina de Gestión de Sistemas de Información y Tecnología para luego ser llevadas al comité institucional de gestión y desempeño para su aprobación. Todas las excepciones deben estar formalmente documentadas, registradas y revisadas por la dirección del grupo de Gestión de Sistemas de Información y Tecnología.

9. Sanciones

El incumplimiento de esta política de Tecnologías de la información y las comunicaciones traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere, así mismo la iniciación de las investigaciones y aplicación de las sanciones, de conformidad con las disposiciones legales vigentes.

10. Control de Cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
27/08/2021	01	Creación del documento.	Mejora	Política de Gobierno Digital
29/12/2023	02	Cambio de formato	Mejora	Resultados de revisión y autocontrol

11. Créditos

Elaboró	Revisó	Aprobó
Mary Rojas	Mary Rojas	Aura Herminda López Salazar
Cargo – Rol: Profesional Especializado código 222 grado 03 Subdirección de Gestión Corporativa	Cargo – Rol: Profesional Especializado código 222 grado 03 Subdirección de Gestión Corporativa	Cargo – Rol: Subdirectora de Gestión Corporativa
Aprobado	Memorando interno con N° 20235600183403 del 29-12-2023	