ALCALDÍA MUNICIPAL DE
Ipiales

PLANES INSTITUCIONALES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARIA GENERAL

SUBSECRETARIA DE BIENES Y SERVICIOS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA - 2025

MUNICIPIO DE IPIALES ENERO DE 2025

TABLA DE CONTENIDO

INTRODUCCIÓN

La Alcaldía Municipal de Ipiales a través de la Subsecretaria de Bienes y Servicios, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información sea protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Mediante este documento se indicarán las medidas que implementará la Administración Municipal, para garantizar la seguridad y privacidad de la información que se maneja, según lo establecido en el decreto 1008 del 14 de junio de 2018; por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

La seguridad de la información es una prioridad para La Alcaldía Municipal de Ipiales y por tanto es responsabilidad de cada servidor público velar por que no se realicen actividades que puedan provocar perdida de la información.

1. CONTEXTO ESTRATÉGICO DE LA ENTIDAD.

El contexto estratégico que da soporte y el que permite determinar las cuestiones externas e internas, que son pertinentes para la Dirección Estratégica y la comprensión de la capacidad para lograr los resultados previstos por el Municipio de Ipiales es:

1. 2. CONTEXTO ESTRATEGICO DE LA ENTIDAD

2.1 MISIÓN DEL MUNICIPIO DE IPIALES

Concebimos a Ipiales como un municipio próspero, seguro, inclusivo y sostenible, donde la calidad de vida de sus habitantes sea prioritaria, promoviendo el desarrollo Integral y el bienestar de la comunidad.

Disponible en la web:

http://www.ipiales-narino.gov.co/alcaldia/mision-y-vision

2.2 VISIÓN DEL MUNICIPIO DE IPIALES

En el marco de la propuesta programática avalada por la ciudadanía: “Gobierno del Pueblo", nos convertiremos en un municipio modelo para el desarrollo humano, económico, turístico y ambiental en la región. Nos vemos como un municipio de oportunidades, donde la innovación, la diversidad cultural, la economía de frontera y el cuidado del medio ambiente son pilares fundamentales para alcanzar un municipio seguro, inclusivo, sostenible y próspero.

Disponible en la Web: http://www.ipiales-narino.gov.co/alcaldia/mision-y-vision

1.1. VALORES

La Administración del Municipio de Ipiales, expidió la resolución N° 141 del 18 de febrero de 2019 por medio del cual adopta código general de integridad y Ética, para los funcionarios y servidores públicos, con el fin de difundir en el contexto organizacional, el establecimiento de relaciones ecuánimes, respetuosas y diáfanas entre los servidores públicos y todos sus grupos de interés.

Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.

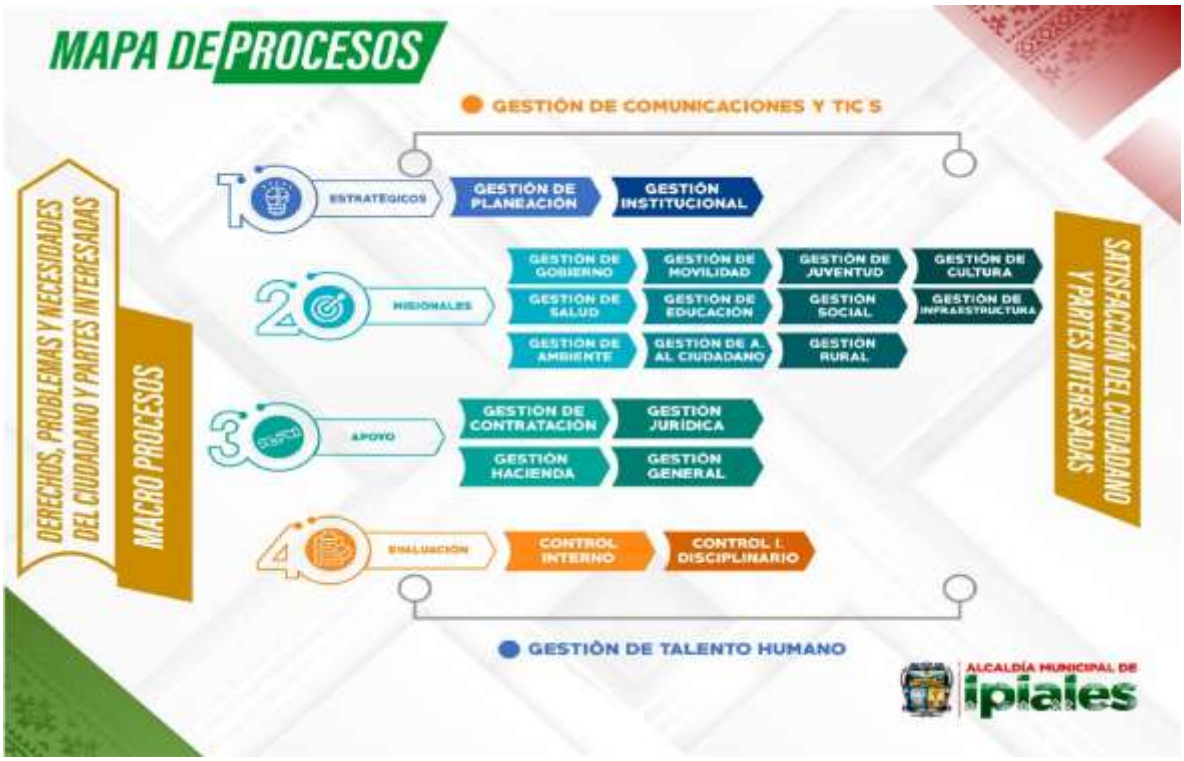
Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.

Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

1.2. MAPA DE PROCESOS ALCALDÍA MUNICIPAL DE IPIALES



2. OBJETIVO

2.1. OBJETIVO GENERAL

Establecer estrategias que garanticen la integridad y el manejo de la información de la Alcaldía Municipal de Ipiales.

2.2. OBJETIVOS ESPECIFICOS

El Plan de seguridad de la información implementa los siguientes objetivos:

- Minimizar la vulnerabilidad a partir del uso de software de ofimática licenciado.
- Apoyar la seguridad y privacidad de la información a partir del uso de usuarios estándar.
- Diligenciar un formato de hoja de vida de los equipos de cómputo para su respectivo control.

3. ALCANCE

Dentro de este documento se describen las estrategias y acciones en cuanto a tecnología que se ejecutará dentro de la Alcaldía Municipal de Ipiales, para el logro de sus objetivos.

4. DEFINICIONES

Activo de información
Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Organización y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad
Es un documento en los que los funcionarios de la Alcaldía Municipal de Ipiales o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Organización, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información
Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación
Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning
Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado
Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo
Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado
Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad
Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control
Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía
Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información
Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor
Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad
Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo
Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información
Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking Ético
Es el conjunto de actividades para ingresar a las redes de datos y voz de la Organización con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad
Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad
Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información
Es una lista ordenada y documentada de los activos de información pertenecientes a la Organización.

Licencia de software
Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible
Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario
Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual
Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información
Es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos
Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Alcaldía Municipal de Ipiales.

Registros de Auditoría
Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Alcaldía Municipal de Ipiales. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información
Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI
Sistema de Gestión de Seguridad de la Información.

Sistema de información
Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la

Alcaldía Municipal de Ipiales o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control humedad
Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso
Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros
Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades
Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Organización (amenazas), las cuales se constituyen en fuentes de riesgo.

5. CICLO DE OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI de acuerdo a los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones - Min TIC, se pretende adoptar las 5 fases de implementación de este, con las cuales se tendrá una mejor gestión de seguridad de la información en la Alcaldía Municipal de Ipiales.
La implementación del Modelo de Seguridad y Privacidad de la Información aumenta el nivel de transparencia de los funcionarios públicos, promoviendo un mejor uso de prácticas de seguridad de la información y riesgos digitales.

Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información. Fuente. Modelo de Seguridad y Privacidad de la Información MSPI. Versión 3.0.2 MinTIC

5.1. FASE DE DIAGNOSTICO

La Subsecretaria de Bienes y Servicios realizo un diagnóstico del estado actual de la información de la Alcaldía Municipal de Ipiales, donde se logra evidenciar:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	10	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	10	100	INICIAL
A.9	CONTROL DE ACCESO	15	100	INICIAL
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	INICIAL
A.18	CUMPLIMIENTO	20	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		13	100	INICIAL

Figura 2. Herramienta - Instrumento de Evaluacion MSPI- 2020

De acuerdo a los resultados obtenidos de la anterior figura, evaluacion de controles, la calificacion de la Alcaldia Municipal de Ipiales fue de 13, lo cual indica que la Administracion esta en la fase inicial de implementacion de medidas de seguridad y privacidad de la informacion

Por lo anterior en el Plan de Seguridad y Privacidad de la Información se plantean medidas para mejorar la implementación del MSPI en la Alcaldía Municipal de Ipiales.

5.2. FASE DE PLANIFICACION

Para el desarrollo de esta fase la Alcaldía Municipal de Ipiales utilizara los resultados obtenidos en el instrumento de evaluación, para proceder a elaborar un Plan de Seguridad y Privacidad de la Información con el fin de implementar medidas que aseguren la información que se presenta en la Administración.
Por lo anterior en el presente plan se propone la siguiente metodología para dar inicio al Plan de Información:
Meta 1. Diagnóstico de las dependencias pertenecientes a la Alcaldía Municipal de Ipiales.
Meta 2. Política de Seguridad y Privacidad de la Información.
Meta 3. Inventario de equipos tecnológicos de la Alcaldía Municipal de Ipiales.
Meta 4. Implementar y diligenciar formato de hoja de vida de los equipos de cómputo.
Meta 5. Inventario de licencias de software que se use en la Alcaldía Municipal de Ipiales.
Meta 6. Adecuado manejo del hardware y software de la entidad, bajo condiciones de seguridad.
Meta 7. Realizar Backup de áreas y puestos de trabajo donde la información este catalogada como importante.
Meta 8. Brindar soporte a las áreas encargadas de manejo y tratamiento de la información.

5.2.1. CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	RESPONSABLE	FECHA
Implementar la instalación de software de ofimática bajo licencia libre en puestos de trabajo con uso de nivel intermedio del mismo.	-Oficina asesora de Comunicaciones y TIC, en coordinación con secretaria general.	Febrero 2025 – junio 2025

Actualizar formato de hoja de vida de los equipos de cómputo para su respectivo control dentro de la Administración, Fortalecimiento del software institucional, sugerencias y capacitaciones con respecto a software malicioso	Oficina asesora de Comunicaciones y TIC, en coordinación con secretaria general.	Febrero 2025– junio 2025
Apoyar y brindar soporte a las dependencias en los sistemas de información internos, programas y proyectos de gobierno en línea de conformidad con la norma vigente	Oficina asesora de Comunicaciones y TIC, en coordinación con secretaria general.	Febrero 2025– diciembre 2025
Implementación del Servidor del Servidor de Alcaldía Municipal	Oficina asesora de Comunicaciones y TIC, en coordinación con secretaria general.	Febrero 2025– diciembre 2025
Terminación del Técnicos en desarrollo del Software	Oficina asesora de Comunicaciones y TIC, en coordinación con IDES	Febrero 2025 – diciembre 2025

5.3. FASE DE IMPLEMENTACIÓN

Para el desarrollo de esta fase la Alcaldía de Ipiales utiliza los resultados obtenidos en la fase anterior para dar continuidad al Plan de Seguridad y Privacidad de la Información, asegurando su correcta implementación y seguimiento.

Por tanto, se realizará un seguimiento de actividades, con el fin de tener un mejor control sobre la planificación estipulada por la Subsecretaria de Bienes y Servicios para salvaguardar la información de la Administración.

5.4. FASE DE EVALUACIÓN DE DESEMPEÑO

En esta fase del Plan de Seguridad y Privacidad de la Información, se hace con base al cumplimiento de las metas propuestas para el desarrollo de las actividades, por lo cual se dispondrá de indicadores de gestión para controlar el avance propuesto en el Plan de Información.

5.5. FASE DE MEJORA CONTINUA

La Alcaldía de Ipiales dentro del cumplimiento al modelo de seguridad y privacidad de la información debe diseñar un plan de mejoramiento continuo, articulándose con el plan de tratamiento de riesgos de la información para mitigar las debilidades presentes en la Administración.

6. REGLAMENTOS PARA LAS INFRACCIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información intentan establecer y fortalecer la cultura de seguridad de la información entre los servidores públicos, personal contratista y proveedores de la Alcaldía Municipal de Ipiales. Para lo cual, es preciso que las infracciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de designar medidas correctivas y frenar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7. POLÍTICAS EN CUANTO A TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN

Uso adecuado de la información y su seguridad al igual que la utilización de todas y cada una de las herramientas con las que cuenta la Alcaldía Municipal de Ipiales para el adecuado desarrollo de las actividades diarias. De esta forma, todo funcionario o proveedor de servicios de la Alcaldía Municipal de Ipiales debe tener en cuenta las siguientes disposiciones:

- La información y el conocimiento son recursos estratégicos y como tal deben administrarse institucionalmente.

- La adopción de nuevas tecnologías de información que se basan en un análisis realizado con tecnologías probadas, novedosas y de valor agregado para la entidad, en una visión propia de la prospectiva tecnológica.

7.1. POLÍTICAS SOBRE EL HARDWARE

a. Adquisición

La adquisición de hardware debe estar contemplada dentro de la entidad y debe estar sujeta a los procedimientos establecidos por la Alcaldía Municipal de Ipiales. No obstante, de acuerdo a necesidades de la Entidad, será posible la adquisición de hardware que no estuviera inicialmente previsto.

Cualquier adquisición es tramitada por la dependencia solicitante en coordinación con la Subsecretaria de Bienes y Servicios, previa observación del hardware existente para determinar la disponibilidad del mismo y no incurrir en gastos innecesarios.

El hardware debe ser adquirido a fabricantes con presencia directa en el país, que tengan reconocimiento nacional e internacional y capacidad de soporte técnico garantizada a nivel nacional. El hardware también podrá ser adquirido por empresas distribuidoras nacionales e internacionales debidamente autorizadas por sus fabricantes para igualmente garantizar la referida capacidad de soporte técnico.

La Subsecretaria de Bienes y Servicios junto con Sistemas autoriza previamente el suministro de equipos cuando se cumpla con los siguientes criterios:

- No exista suficiente disponibilidad de equipos propios.
- Existencia de contrato de arrendamiento con una firma especializada.
- Haya presupuesto.

b. Custodia

La Subsecretaria de Bienes y Servicios es el (la) responsable de la custodia de los activos físicos de cómputo, a través de los mecanismos que considere pertinentes.

La Subsecretaria de Bienes y Servicios debe mantener un inventario actualizado y completo de los activos físicos de cómputo. A su vez el asignado a Sistemas

diligencia el formato de hoja de vida de los equipos de cómputo para llevar el control de dichos equipos.

Los activos físicos de cómputo deben estar protegidos de las amenazas y riesgos del entorno. Esta protección es necesaria para reducir el riesgo contra la pérdida o avería del mismo y su cumplimiento es responsabilidad conjunta de las Subsecretaria de Bienes y Servicios.

El traslado de los activos de cómputo es responsabilidad conjunta de las Subsecretaria de Bienes y Servicios.

Los usuarios de los Equipos de Cómputo son responsables de su buen uso, especialmente de aquellos que estén a su cargo y deben atender para ello las normas establecidas por la Entidad.

Los equipos en uso pueden ser reasignados según las necesidades de procesamiento para la ejecución de las tareas de cada uno de los funcionarios de la Alcaldía Municipal de Ipiales.

La Subsecretaria de Bienes y Servicios determina los equipos, que por su nivel de obsolescencia no sean aptos para su adecuado funcionamiento ni para su efectivo mantenimiento correctivo y/o preventivo. La Subsecretaría de Bienes y servicios, es el responsable de entregar un informe de que equipos deben ser dados de baja.

El hardware que sea utilizado por los proveedores de servicio y no suministrados por la Alcaldía Municipal de Ipiales, es responsabilidad del proveedor del servicio. Esto para el caso de los equipos de cómputo que se arriendan.

c. Control y Mantenimiento

El hardware debe adquirirse con todas las normas dadas por la Oficina asesora de comunicaciones y TIC. Debe existir autorización, acompañamiento y coordinación por parte de la Subsecretaria de Bienes y Servicios, o quien se delegue para realizar cualquier labor

de mantenimiento, actualización o cambio sobre el hardware de la Alcaldía Municipal de Ipiales.

7.2. POLÍTICAS SOBRE EL SOFTWARE

a. Adquisición

La adquisición de cualquier software debe estar contemplado dentro de las normas regidas por la Oficina asesora de comunicaciones y TIC y debe estar sujeta a los procedimientos establecidos por la entidad. No obstante, de acuerdo a necesidades de la Entidad, será posible la adquisición de software que no estuviera inicialmente previsto.

Cualquier adquisición debe ser tramitada por la dependencia solicitante en coordinación con la Subsecretaria de Bienes y Servicios, previa autorización de la capacidad instalada para determinar la disponibilidad de productos y no incurrir en gastos innecesarios.

La adquisición de software debe realizarse a empresas, proveedora de productos de alta calidad y con respaldo técnico. En caso de ser necesario, el software a adquirir, debe someterse a aprobación por parte de la Oficina asesora de comunicaciones y TIC, según el tipo de aplicación de que se trate y de las áreas que involucre.

Las herramientas de administración de recursos informáticos son de carácter institucional y por lo tanto son definidas por la Oficina asesora de comunicaciones y TIC: Esto incluye soporte, gestión de redes, gestión de Inventarios, administración de copias de seguridad (backups), administración de la seguridad de la red, etc.,

El software operativo y aplicativo de uso particular en un área específica, debe ser adquirido, preferiblemente, con la cooperación y visto bueno de la Subsecretaria de Bienes y Servicios, preferiblemente el software adquirido debe integrarse con los Sistemas de Información ya existentes.

La adquisición de una solución de mercado primaria sobre un desarrollo a la medida, se realiza siempre y cuando se cubran los requerimientos y necesidades de la Alcaldía Municipal de Ipiales.

Cuando se requiera realizar la compra de un software nuevo, se debe verificar, mediante un estudio o análisis previo, que la solución no va a generar una duplicidad de tareas.

b. Custodia

La Subsecretaria de Bienes y Servicios, son responsables de la administración del software de uso institucional: sistemas operativos, aplicativos, utilitarios, administradores de bases de datos, lenguajes de programación, a la medida, etc. Debe mantener un inventario actualizado de dicho software y sus licencias.

c. Uso

Solo se encuentra permitido el software legalmente adquirido por la Alcaldía Municipal de Ipiales. 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.

1. Cada usuario es responsable por la instalación del software no licenciado que se encuentre en los equipos de cómputo a su cargo.
2. 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.
3. La instalación de cualquier software ya sea institucional, personal o de libre distribución debe contar con la autorización previa de Bienes y Servicios.
4. El software desarrollado a la medida es de propiedad de la Alcaldía Municipal de Ipiales y es responsabilidad de la Subsecretaria de Bienes y Servicios, adelantar, si es necesario, el debido registro del producto.

d. Manejo del Cambio

Los cambios de versiones del software deben ser planeados, analizados, evaluados y acordados conjuntamente entre el área responsable o solicitante del cambio y la Subsecretaria de Bienes y Servicios.

La actualización y configuración de un nuevo sistema operativo deberá realizarse únicamente por personal autorizado.

7.3. Políticas sobre el Correo Electrónico Institucional

La Alcaldía Municipal de Ipiales, por intermedio del Área de Sistemas, gestiona para sus servidores y proveedores, entre otros, los servicios de acceso al correo electrónico institucional y a Internet. Estos servicios apoyan la gestión personal, grupal e institucional, consolidándose como elementos facilitadores y dinamizadores en el desarrollo de la función pública. El uso de dichos servicios debe estar orientado exclusivamente hacia fines institucionales.

7.3.1. Sobre el uso del servicio de internet

En esta sección se establecen los controles que permiten minimizar el riesgo generado por el acceso a Internet y a redes públicas, exponiendo los sistemas de información de la Alcaldía Municipal de Ipiales a la propagación interna y externa de software con código malicioso o nocivo, el cual puede comprometer directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red, así como evitar que el acceso a dichas herramientas sea utilizada para actividades que no tengan relación directa con las funciones asignadas o las obligaciones contractuales.

7.3.2. Disposiciones Generales:

El Área de Sistemas es la encargada de proporcionar el servicio de acceso institucional a Internet, así como vigilar su correcto uso y funcionamiento. Para tal fin asigna una cuenta de usuario que tendrá asociados unos privilegios específicos y una clave de acceso.

Todos los usuarios están identificados independientemente con permisos de acceso. La utilización de la cuenta es personal e intransferible, por lo que, si se utiliza una cuenta y los privilegios que la misma le ofrece al usuario, para realizar acciones no permitidas, se asume inicialmente que fue el funcionario responsable y asociado a la cuenta quien las realizó, motivo por el cual se debe dar un uso responsable al manejo de claves de acceso evitando así la utilización de estas por personas no autorizadas.

El uso de Internet está permitido exclusivamente para actividades institucionales. Los usuarios deben utilizar únicamente los servicios para los cuales están autorizados. A través de herramientas de monitoreo y análisis de tráfico como estadísticas de Internet Aceleration Server, se detectan a los usuarios que hagan mal uso de los servicios de Internet.

El Área de Sistemas, se encuentra facultado para bloquear todos aquellos sitios de Internet que considere que no son compatibles con las labores de los servidores y contratistas. En caso de existir excepciones por causas debidamente justificadas, los jefes correspondientes deben presentar la solicitud mediante comunicación escrita, exponiendo las causas de la excepción ante la Subsecretaria de Bienes y Servicios y Oficina de Sistemas para su estudio y aprobación.

Se permite a los servidores públicos y contratistas que tengan acceso a Internet ingresar a las páginas de correos personales (Hotmail, Tutopia, Gmail, etc.). El Área de Sistemas determina los casos en los cuales sea necesario restringir el acceso a páginas y servicios que afecten negativamente el funcionamiento de la infraestructura tecnológica de la entidad y/o se detecte un mal uso de la misma.

7.4. Actividades prohibidas consideradas como faltas graves

Teniendo en cuenta el Código Disciplinario Único (Ley 734 de 2002), donde se establecen los deberes y prohibiciones para los servidores públicos, derivado de dicha Ley, La Subsecretaria de Bienes y Servicios y el Área de Sistemas considera pertinente establecer como faltas graves las siguientes:

1. Ingresar a páginas pornográficas, así como de personas u organizaciones al margen de la ley o de contenidos ilegales.
2. Descargar programas que permitan realizar conexiones automáticas, la utilización de los recursos asignados por la entidad para distribución o reproducción de este tipo de programas (Ej: software conexión ftp, p2p) ya sea vía Web o medios magnéticos.

3. Descargar música y video no aplicable a actividades del que hacer de la entidad, así como utilizar o participar en juegos de entretenimiento en línea.

4. Consultar material inapropiado, obsceno, pornográfico, de violencia explícita, indecente, ilegal o cualquier otro tipo de material que pudiera ofender a los usuarios de espacios de cómputo comunes. Se hace seguimiento a aquellos usuarios que incumplan esta directriz. Su omisión se reporta a la Oficina de Control Interno.

5. Utilizar los servicios de TV a través de Internet, salvo que dicha información se requiera para el ejercicio de las funciones a cargo. En este caso el Jefe

correspondiente debe presentar la solicitud mediante correo, exponiendo las causas de la excepción ante el Área de Sistemas su estudio y aprobación.

6. Descargar o instalar programas, modificar los paquetes y configuraciones ya instalados en los computadores de la Entidad, en pro de prevenir virus informáticos y reconfiguración de equipos personales. En caso de requerir algún software nuevo o la modificación de alguno ya instalado, el jefe o subdirector de la Oficina o Subdirección debe solicitar la respectiva instalación o modificación al Área de Sistemas.

7.5. Sobre el uso de las Cuentas de Correo Electrónico

Esta sección establece lineamientos para el buen uso de la plataforma de correo electrónico de la Alcaldía Municipal de Ipiales. Esta plataforma incluye tanto el servicio de correo interno como el externo y se constituye en un componente fundamental de información para la Administración, debiéndose garantizar la integridad, disponibilidad y confidencialidad de la información allí contenida.

7.5.1. Disposiciones Generales

Todos los servidores de la entidad tienen derecho a una cuenta de correo institucional, la que permite comunicarse al interior y exterior de la entidad. Este principio también aplica a las dependencias, proyectos y eventos oficiales de la Alcaldía Municipal de Ipiales.

La Oficina Asesora de Comunicaciones y Tic es la encargada de proporcionar el servicio de correo institucional, así como vigilar su correcto uso y funcionamiento. Para tal fin asigna una cuenta que tiene asociado un buzón de correo, en el cual se almacenan todos los mensajes enviados y recibidos. Cada usuario debe depurar continuamente su buzón de correo con el fin de mantener siempre espacio disponible para nuevos mensajes.

La información contenida en el correo ya sea institucional o electrónico se considera información privada y por lo tanto debe ser manejada como una comunicación privada y directa entre el remitente y su destinatario.

La cuenta de correo es intransferible. Por esto se deben tener claves seguras y no se puede compartir la cuenta, salvo en aquellos casos, en que las cuentas correspondan a una cuenta institucional compartida, como, por ejemplo: alcaldia@alcaldia.gov.co

Cada usuario es responsable de la información enviada o reenviada desde su cuenta de correo, aunque la entidad cuenta con un servicio de revisión de virus para los mensajes de correo electrónico entrante, los usuarios del correo deben ser cuidadosos al decidir abrir los archivos anexos colocados en mensajes de remitentes desconocidos o sospechosos. Si llegan mensajes con esta característica, se debe informar al Área de Sistemas.

Le corresponde a cada usuario verificar que todos los archivos que se copien a su computador no contengan virus. Para tal fin debe ejecutar el antivirus que está instalado en cada equipo y verificar los archivos correspondientes.

Las cuentas de correo y acceso a la red son desactivadas a partir de la fecha en la cual la persona termine oficialmente su vinculación con la entidad por solicitud del Jefe o Subdirector de la Oficina o Subdirección correspondiente.

La Oficina Asesora de Comunicaciones y Tic puede cancelar las cuentas de correo que no demuestren su uso durante más de dos (2) meses consecutivos, excepto aquellos usuarios que se encuentren en vacaciones o licencias de trabajo. También el mal uso del correo ocasiona la cancelación de la cuenta. Los funcionarios de la Alcaldía Municipal de Ipiales no pueden emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad.

7.6. ACTIVIDADES PROHIBIDAS

En desarrollo de los postulados legales contenidos en el Código Disciplinario Único, quedan prohibidas las siguientes actividades:

1. Enviar correos a "Todas las dependencias" cuyo contenido no sea de carácter institucional; si se trata de propósitos institucionales la información que se incluya en dichos mensajes no debe ser mayor a 25 Mb; si se tienen archivos de mayor tamaño, debe realizarse la publicación a través de la Intranet de la entidad, mediante solicitud al Área de Sistemas.
2. En el caso que los correos que requieren ser enviados no cumplan con alguna de las condiciones anteriores se debe contactar al Área de Sistemas para definir la forma de distribución, estos pueden ser casos esporádicos en los que se requiere envío de correos a través de Yousendit, web transfer.

3. Enviar o contestar cadenas de mensajes a una persona o grupo de personas, que no sean de carácter institucional.
4. Enviar correo con material o información que transgreda las normas nacionales o internacionales referentes a los Derechos de Autor.
5. Enviar o reenviar correos que contengan de propaganda o cualquier otra información de carácter político partidista.
6. Enviar correo externo o interno a la Entidad con material o información que vaya en contra de la moral y buenas costumbres, o que constituya o fomente un comportamiento que dé lugar a responsabilidades civiles, administrativas o penales.
7. Promocionar a través del correo interno o externo bienes o servicios particulares que no tengan relación con los objetivos institucionales.
8. Utilizar el correo electrónico para fines diferentes a los objetivos de la Entidad.
9. Usar el Servicio en relación con mensajes no deseados, correos molestos (spam) u otros mensajes duplicativos o no solicitados (comerciales o de otro tipo).
10. Difamar, insultar, acosar, amenazar o infringir de cualquier otra forma los derechos de terceros (tales como el derecho a la intimidad o a la propia imagen).
11. Publicar, distribuir o divulgar cualquier información o material inapropiado, obsceno, indecente o ilegal.
12. Recopilar o de cualquier otro modo recabar información sobre terceros, incluidas sus direcciones de correo electrónico, sin su consentimiento.
13. Transmitir o cargar archivos que contengan virus, "caballos de Troya", "gusanos" u otros programas perjudiciales o nocivos.
14. Intentar obtener acceso de forma no autorizada al Servicio, a otras cuentas, a sistemas informáticos o a redes conectadas con el Servicio, a través de búsqueda automática de contraseñas o por otros medios. Interferir o interrumpir redes conectadas con el Servicio o infringir las normas o directivas.

8. POLÍTICAS SOBRE LAS REDES Y LAS TELECOMUNICACIONES

La adquisición de elementos físicos para las redes de servicios profesionales y sistemas de comunicaciones debe estar incluida en la Adquisición de elementos por parte de la Alcaldía Municipal de Ipiales. No obstante, de acuerdo a necesidades de la Entidad, será posible la adquisición de elementos que no estuvieran inicialmente previstos.

Cualquier adquisición de servicios profesionales relacionada con las redes de datos o de comunicaciones debe ser tramitada por el área solicitante y en coordinación con Sistemas.

La gestión, es decir administración, configuración, monitoreo, y funcionamiento de los sistemas institucionales de redes y telecomunicaciones utilizados por la Alcaldía Municipal de Ipiales está coordinado por la Oficina de Sistemas.

Toda solicitud para la obtención de frecuencias, licencias y permisos de uso del espectro electromagnético debe ser canalizada a través de la Oficina de Sistemas, en coordinación con el área solicitante del servicio.

En caso de requerirse una conexión con un ente externo, ésta debe tener el visto bueno previo y realizarse con el apoyo del asignado a Sistemas. Las conexiones de red, tanto local como remota, deben contar con definiciones y requerimientos específicos y claros, con características técnicas y de seguridad definidas por la Alcaldía Municipal de Ipiales y sus políticas de seguridad de la información.

El buen uso de las aplicaciones, la administración de la utilización y de la operación, así como la especificidad de los parámetros y roles de usuarios es responsabilidad de las áreas usuarias.
Las conexiones de equipos externos a la red institucional de la Alcaldía Municipal de Ipiales, deben ser autorizadas por el Área de Sistemas.

9. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

9.1. SEGURIDAD FÍSICA

Los responsables de cada dependencia de la Alcaldía Municipal de Ipiales, deben aplicar normas mínimas de seguridad física en los lugares en donde existan equipos de cómputo, equipos de comunicaciones, equipos de documentación y en general cualquier activo de información.

El control de acceso a los equipos de cómputo, es responsabilidad del funcionario que tenga a su cargo cada uno de los equipos. El funcionario debe establecer como medidas mínimas de prevención una contraseña y de protector de pantalla. Este protector de pantalla debe estar configurado para que se ejecute en un tiempo no superior a tres minutos. El equipo de trabajo de Sistemas apoya el proceso de configuración de protectores de pantalla, protegido por contraseña.

Los usuarios de equipos de cómputo portátiles suministrados por la entidad deben reforzar las medidas de protección física en todo lugar. En todos los casos estos equipos deben

contar con pólizas y seguros contra todo daño y cuya suscripción debe ser de responsabilidad conjunta entre la Subsecretaria de Bienes y Servicios, Control Disciplinario y la Oficina de Sistemas.

Todo servidor de bases de datos, de aplicaciones y/o de archivos debe localizarse en un centro de cómputo.

9.2. SEGURIDAD LÓGICA

Todo usuario de recursos informáticos, debe ser autorizado formalmente de acuerdo con los procedimientos establecidos dentro de la Alcaldía Municipal de Ipiales. El uso y mantenimiento de las claves de acceso a los recursos informáticos es de total responsabilidad de cada uno de los usuarios.

Los responsables de cada área son quienes definen los roles, privilegios y accesos a cada una de las aplicaciones que soporten los procesos a su cargo.

Cada usuario tiene definido y asignado el ambiente de trabajo y configuración informática para el uso de las aplicaciones y sistemas de información. La pérdida de información y el no funcionamiento de las aplicaciones por modificación del ambiente de trabajo es responsabilidad del usuario.

La información debe ser clasificada según criterios de disponibilidad, integridad, y confiabilidad para efectuar su custodia, conservación, necesidad, prioridad y grado de operación.

Se deben hacer copias de seguridad con la periodicidad sujeta a los criterios de riesgo y volumen de información esencial de la entidad con propósitos de recuperación en caso de una eventual pérdida.

Para el caso de proveedores y contratistas del de la Alcaldía Municipal de Ipiales que tengan acceso a la información de la entidad, el acuerdo de confidencialidad se establece mediante cláusula del contrato. Todos los usuarios de activos informáticos deben acoger las normas, procedimientos y políticas que en materia de seguridad informática se promuevan desde el Área de Sistemas.

10. POLÍTICAS SOBRE LOS EQUIPOS Y SERVICIOS DE CÓMPUTO

Estas políticas son adoptadas en cada dependencia perteneciente a la Alcaldía Municipal de Ipiales donde se hace necesaria la utilización de elementos de cómputo (computadores e impresoras) contribuyendo a una educación, para el cuidado y adecuado funcionamiento de cada uno de estos equipos.

10.1. CONDICIONES GENERALES DE USO

Los usuarios de la red y equipo de cómputo de la Alcaldía Municipal de Ipiales deben solicitar apoyo u orientación a la Oficina de Sistemas o a quien este designe ante dudas específicas en el manejo de los equipos de cómputo, acceso a la información de los servidores internos y manejo de datos.

Los equipos de cómputo y de la red de datos deben ser operados por personal de área, administrativo y/o personal previamente autorizado por los responsables de los equipos, en ninguna circunstancia deben ser operados por personas ajenas a la Alcaldía Municipal de Ipiales.

Las actividades realizadas en los equipos de cómputo de la Alcaldía Municipal de Ipiales deben acoplarse a los programas y proyectos misionales y administrativos de la Administración y no para fines personales u ociosos. Los equipos de cómputo cuentan con los programas necesarios para las actividades de administración, investigación y capacitación. Está prohibido el uso, almacenaje, copiado y reproducción de software sin el consentimiento del propietario de los derechos de autor.

10.2. USO ACEPTABLE DE LOS RECURSOS DE CÓMPUTO Y RED

Los siguientes son los usos aceptables de los recursos de cómputo y red de datos que la subsecretaria de bienes y servicios contempla para la Alcaldía Municipal de Ipiales:

- La investigación apoyada en el uso de recursos de software.
- Presentaciones, talleres, congresos y seminarios virtuales y en general todas las actividades que promuevan la cultura informática entre los funcionarios de la Alcaldía Municipal de Ipiales.

- Realización de cursos internos para capacitación de acuerdo a los requerimientos de cada una de las Dependencias y/o usuarios de la Alcaldía Municipal de Ipiales. (Programados por los responsables).
- Actividades de gestión y administración que requiera el uso de medios electrónicos y sistemas distribuidos.

Los usuarios deben tener bien definidas las actividades que van a realizar con los equipos de cómputo y red de datos de la Alcaldía Municipal de Ipiales, con el fin de lograr un buen desempeño y optimización de los recursos de cómputo.

10.3. RESTRICCIONES Y OBLIGACIONES DE LOS USUARIOS

Todos los usuarios deben respetar la integridad de los equipos y las instalaciones de cómputo del Área de Sistemas de la Alcaldía Municipal de Ipiales, además de la confidencialidad y los derechos individuales de los demás, cumpliendo los siguientes ítems:

- Se recomienda no fumar, consumir alimentos y/o bebidas en sitios donde se encuentre ubicados los equipos de cómputo (computadores, impresoras, escáner, etc), es obligación de los usuarios mantener limpias las áreas donde se encuentren los equipos, tirando la basura en los botes destinados para este fin.
- Se debe evitar conectar y/o desconectar componentes de hardware de los equipos de cómputo, cualquier falla de los equipos de cómputo se deberá reportar al personal del Área de Sistemas para que solucionen el inconveniente.
- No se permite la ejecución de sistemas de mensajería como MSN.
- Deben, abstenerse de realizar actividades ociosas tales como juegos, chat, descargar archivos MP3, DIVx, MPEG o ejecución de software desde páginas de Internet y otras actividades que saturen el ancho de banda de la red del Instituto Distrital de Turismo; bajo ninguna circunstancia la infraestructura de cómputo debe ser utilizada para lanzar ataques a otros equipos conectados en red.
- Se debe respetar la configuración original de los equipos, evitando personalizar el aspecto y contenido de los mismos, así como la instalación de cualquier tipo de software ajeno al instalado por el personal técnico del área de sistemas.
- No se permite la modificación de configuración de:
  - Conexiones de red.
  - Escritorio.
  - Protector de Pantalla.
  - Sonido.

- Hora y fecha del sistema.
- Firewall de Windows.
- Cuentas de Usuario.

- Todos los computadores deben manejar la "Hora Legal de la República" (Hora Internacional) de acuerdo a la directiva 013 de 2005 emitida por la Procuraduría General de la Nación.
- Cada usuario responsable de cualquier equipo tecnológico o equipo electrónico debe dejarlo apagado al momento de la salida al medio día y al terminar la jornada laboral, si el usuario dentro del horario laboral deja su equipo por alguna circunstancia debe guardar sus archivos y dejarlo bloqueando para prevenir perdida de información.

10.4. MODIFICACIONES AL SERVICIO

La subsecretaria de bienes y servicios de la Alcaldía Municipal de Ipiales se reserva el derecho para modificar las condiciones aquí establecidas cuando lo considere necesario. También puede modificar o incluso suspender el servicio o partes del mismo cuando sea necesario, por razones administrativas, de mantenimiento de los equipos o por causas de fuerza mayor.

11. POLÍTICAS ANTIVIRUS Y MANEJO DE INFORMACIÓN

Estas son algunas normas que debe tener en cuenta para proteger los equipos de cómputo ante algún ataque por virus informáticos. Es importante que todo el personal de la Alcaldía Municipal de Ipiales sea consciente sobre su responsabilidad.

11.1. Cuidado con los archivos VBS

No se debe abrir archivos cuya extensión sea VBS (Visual Basic Script es un lenguaje que permite ejecutar rutinas dentro de los PC), a menos que se esté absolutamente seguro que el mail viene de una persona confiable y que haya indicado previamente sobre el envío.

11.2. No esconder extensiones de archivos tipos de programas conocidos

Todos los sistemas operativos Windows, por predeterminación, esconden la extensión de archivos conocidos en el explorador de Windows. Esta característica puede ser usada por los diseñadores de virus y hackers para disfrazar programas maliciosos como si fueran otra extensión de archivo. Por eso los usuarios pueden ser engañados, y dar clic sobre el archivo de "texto" y sin darse cuenta ejecutar el archivo malicioso.

11.3. Instalación de un Firewall

La Oficina de Sistemas debe considerar la utilización de un firewall bien sea a nivel de hardware o nivel software, este tiene la función de minimizar el riesgo de ataques a la red y equipos conectados a ella, de igual forma el filtrado de contenidos y manejo de políticas de Internet.

11.4. COPIAS DE SEGURIDAD

Nunca se debe trabajar un archivo directamente sobre un medio magnético, especialmente sobre memorias USB y otros medios extraíbles ya que si estos se dañan por virus u otro problema la mayoría de las veces se puede recuperar la información.

Debe realizarse Backup de los archivos exclusivamente laborales (excluye fotos, imágenes o archivos de texto personales) de cada una de las estaciones de trabajo.

11.5. ACTUALIZACIÓN DEL SISTEMA OPERATIVO

Se realizan actualizaciones periódicas por parte del personal del Área de Sistemas con el fin de aumentar al máximo la seguridad ante eventuales ataques víricos, puesto que algunos de los gusanos que recorren el mundo buscan especialmente los agujeros de seguridad de muchos de los productos de Microsoft. Para ello la empresa Microsoft ofrece periódicamente actualizaciones "críticas “para descargar, de igual forma el administrador del sistema puede configurar el sistema operativo para que se descarguen en forma automática en horas poco críticas para la red.

11.6. APLICACIÓN DE ANTIVIRUS

Se debe crear la cultura de vacunación, siempre revisando con el antivirus sus discos removibles o memorias USB antes de usarlas.

Preferiblemente una vez por semana se debe vacunar el disco duro del computador, la asesoría cuenta por parte de la Oficina de Sistemas. Para realizar esta operación simplemente ingrese al antivirus y utilice la opción analizar Unidad C; en caso que el disco tenga dos particiones o el equipo tenga discos, se deben analizar ambos discos.

11.7. DESARROLLO, SOPORTE Y MANTENIMIENTO

El soporte de primer nivel a nivel técnico y operativo se provee mediante el ingeniero y personal técnico contratado mediante prestación de servicios.

El mantenimiento preventivo de los equipos de cómputo fuera de garantía se Realiza a través de una empresa especializada en mantenimiento, los demás requiere la contratación a medida que expira la garantía para cada equipo. El mantenimiento correctivo se realiza a través del personal técnico contratado mediante prestación de servicios.

12. EVALUACIÓN DE LOS SISTEMAS E INFRAESTRUCTURA TECNOLOGICA DE LA ALCALDIA MUNICIPAL DE IPIALES

12.1. EVALUACIÓN DEL ENTORNO

- Automatización del proceso de generación de Copias de Seguridad en los PC, a través de un Disco portátil de 2tb.
- Re potenciamiento de los equipos de cómputo.

12.2. AMENAZAS

- Aumento de riesgos informáticos debido a procedimientos y procesos de informática.
- Siniestros en las instalaciones de la entidad en servicios de tecnología
- Incumplimiento por parte de los proveedores en la prestación de los servicios contratados.

12.3. EVALUACIÓN INTERNA

- No se cuenta con una adecuada red de cableado estructurado y una red de comunicaciones suficiente para la cantidad de usuarios del sistema.
- Se cuenta con algunos equipos de Cómputo nuevos con características funcionales suficientes y acorde a cada cargo.
- Deficiente Infraestructura tecnológica adecuada para los sistemas actuales.
- Falta de una planta eléctrica para garantizar la continuidad del servicio ante fallas o suspensión del fluido eléctrico.
- Carencia de cuarto frio para centro de cómputo y servidores con su respectivo rack para distribución de la red.

13. ESTRATEGIAS DEL PLAN

13.1. ESTRATEGIAS QUE CONTRIBUYEN AL CUMPLIMIENTO DE LOS PROCESOS DE LA ENTIDAD

ESTRATEGIA 1.
Mantener los sistemas de información, aplicaciones y herramientas ofimáticas actualizadas (versión y actualidad de la información) y completamente funcionales para los usuarios finales.

ESTRATEGIA 2.
Optimizar la infraestructura de las tecnologías de información.

ESTRATEGIA 3.
Optimizar las configuraciones de los servidores existentes, creado cuentas de usuario y control de acceso.

13.2. ESTRATEGIAS QUE CONTRIBUYEN A OPTIMIZAR LOS PROCESOS ADMINISTRATIVOS Y DE CONTROL DE LA ENTIDAD

ESTRATEGIA 1.
Garantizar el acceso, óptimo funcionamiento y oportuna actualización de los aplicativos existentes para la rendición de cuentas e informes de gestión dirigidos a las diferentes entidades de control.

ESTRATEGIA 2.
Mantener licencias actualizadas

14. FICHA DE RESPONSABILIDADES

RESPONSABLES	NOMBRE	CARGO	FIRMA
ELABORÓ:	**Darío Acosta Parra**	**Jefe Oficina Asesora de Comunicaciones y TIC**	
APROBÓ:	**Darío Acosta Parra**	**Jefe Oficina Asesora de Comunicaciones y TIC**	
REVISÓ E INTEGRO AL SIGC:	**Claudia Marcela Yaguapaz Pantoja**	**Jefe Oficina Asesora de Gestión Institucional**