ALCALDÍA MUNICIPAL DE
Ipiales

PLANES INSTITUCIONALES

PLAN DE TRATAMIENTOS
DE RIESGOS DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARIA GENERAL

SUBSECRETARIA DE BIENES Y SERVICIOS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA - 2025

MUNICIPIO DE IPIALES ENERO DE 2025

TABLA DE CONTENIDO

INTRODUCCIÓN

La Seguridad de la Información en las entidades tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio. Es por esto que la Alcaldía Municipal de Ipiales, dentro de su política de gestión del riesgo, vincula acciones para el control de la seguridad de la información y las actividades de valoración de actos inseguros bajo el objetivo de mantener la información de la administración municipal de manera mucho más confiable, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, gestión, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

Integridad: Propiedad que la información se mantenga exacta y completa.

Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

1. ALCANCE.

La gestión para el tratamiento de riesgos de seguridad y privacidad de la información debe aplicarse a todas las dependencias de la Administración Municipal, por ende, incluye a todos los funcionarios, contratistas, a toda la ciudadanía en general que interactúa con la entidad y a aquellas personas que por cumplimiento de los compromisos contractuales o en ejercicio de sus funciones realicen tratamiento de la información de la cual la alcaldía es responsable. La gestión incluye de manera explícita los diferentes activos de información que hacen parte del sistema de información. Para abarcar este alcance es primordial habilitar en primera instancia funciones de liderazgo para asesorar y apoyar el proceso de diseño, implementación y mantenimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información, seguido de una capacitación y generación de una cultura en la entidad para la gestión integral del riesgo.

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

2.3. 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.

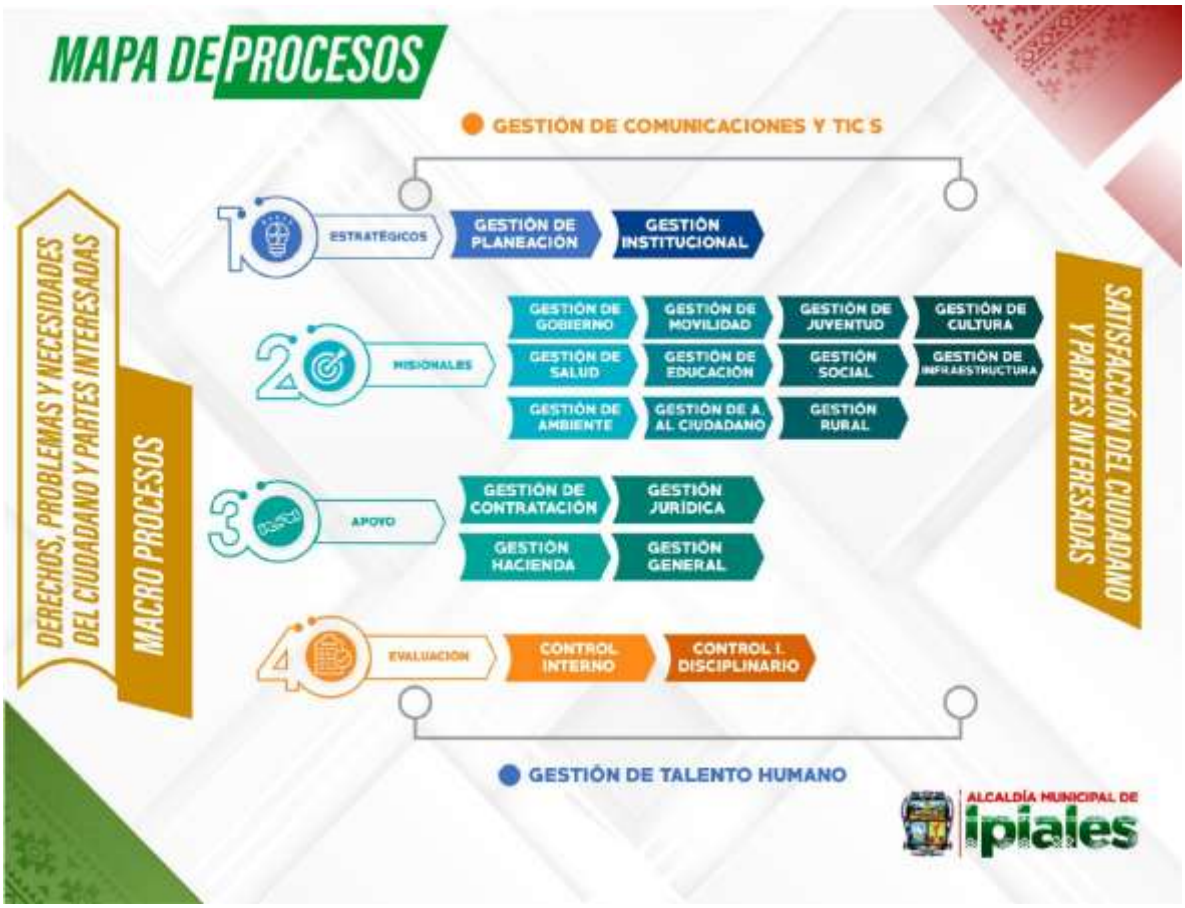
Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

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.

2.4 MAPA DE PROCESOS ALCALDÍA MUNICIPAL DE IPIALES



3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar, consolidar e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información para los procesos de la Administración Municipal y establecer parámetros para identificar y gestionar los riesgos de la información durante el periodo actual cumpliendo la normatividad vigente.

3.2. OBJETIVOS ESPECÍFICOS

- Determinar el alcance factible de la gestión integral del riesgo encaminados a la seguridad y privacidad de la información.
- Identificar y gestionar amenazas y vulnerabilidades en el hardware, software y recurso humano.
- Formalizar procedimientos, controles y pautas a cumplir para desarrollar la gestión de la seguridad y privacidad de la información.
- Generar conciencia y cultura enfocada a la identificación de los riesgos de seguridad y privacidad de la información.

4. TERMINOS CLAVE

Activo: Cualquier elemento que tenga valor para la organización.

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

Riesgo: efecto de la incertidumbre sobre los objetivos.

Gestión del Riesgo: actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

5. QUÉ ES LA SEGURIDAD

Se entiende como seguridad a una característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos. (Huerta, 2002, p. 2).

Aspectos relevantes que conforman la seguridad de la información:

6. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

7. SEGURIDAD FÍSICA Y LÓGICA

Desde el punto de vista de la naturaleza de la amenaza, se puede hablar de seguridad a nivel físico o material o seguridad a nivel lógico o software. (García y Hurtado, 2011, p. 6)

Física	Lógica
Desastres	Controles de acceso
Incendios	Identificación
Equipamiento	Roles
Inundaciones	Transacciones
Picos y ruidos E/M	Limitación a los servicios
Cableado	Control de acceso interno

7.1. Seguridad Física

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático, las amenazas físicas

se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales. Dentro de las provocadas por el ser humano, encontramos amenazas de tipo:

- **Accidentales**, como borrado accidental, olvido de la clave….

- **Deliberadas**: como robo de la clave, borrado deliberado de la información, robo de datos confidenciales, entre otras.

Dentro de las provocadas por factores naturales, se encuentran incendios, inundaciones. Otras medidas de seguridad física pueden variar desde el uso de veneno en el subsuelo para evitar que roedores rompan el cableado, hasta instalar suelo sintético para evitar que en un momento determinado una persona pueda recibir una descarga eléctrica causándole daños graves.

7.2. Seguridad lógica

La seguridad lógica se encarga de resguardar la parte de software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa usando una VPN (protocolos PPP, PPTP, la web HTTP, HTTPS, transmisión de ficheros FTP, conexión remota SSH, Telnet).

Dentro de la seguridad lógica, se tienen una serie de programas, o software, como el sistema operativo, que se debe encargar de controlar el acceso de los procesos o usuarios a los recursos del sistema.

Para ello debe tomar distintas medidas de seguridad. Cada vez los sistemas operativos controlan más la seguridad del equipo informático contrarrestando amenazas provenientes de errores del sistema, uso incorrecto del sistema operativo o del usuario, accesos no controlados físicamente o a través de la red, o por un programa malicioso, como los virus, espías, troyanos, gusanos, phishing. (Alfonso García-Cervigón Hurtado, 2011, pág. 8)

8. TIPO DE AMENAZAS.

En los sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos). Hay diferentes tipos de amanezcas de las que hay que proteger el sistema, desde las físicas como cortos electrónicos, fallos de hardware p riesgos ambientales hasta los errores intencionales o del

usuario, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información, las amenazas se clasifican en los siguientes cuatro grupos:

De interrupción: El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

De interceptación: Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, coma pueden ser datos, programas o identidad de personas.

De modificación: Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información, sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada. De fabricación: Agregarían información falsa en el conjunto de información del sistema.

8.1. AMENAZAS FÍSICAS Y LÓGICAS.

Amenazas físicas: En muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. (Huerta, 2002, p. 21).

Terremotos: No obstante, no se debe entender por terremotos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación; quizás sería más apropiado hablar incluso de vibraciones, desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos). Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. (Huerta, 2002, p. 22).

Inundaciones y humedad: Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica estaciones en los lugares más húmedos o que presenten situaciones extremas; no obstante, ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que se tengan dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de alta

disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial. (Huerta, 2002, p. 25).

Electricidad: Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta los equipos; cortocircuitos, picos de tensión, cortes de flujo a diario amenazan la integridad tanto el hardware como de los datos que almacena o que circulan por él.

Incendios y humo: Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio, o al menos en la planta, donde se encuentra invertido mucho dinero en equipamiento. (Huerta, 2002, p. 28).

Temperaturas extremas: Las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Centígrados, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de los sistemas. (Huerta, 2002, p. 28).

Amenazas Lógicas. Bajo la etiqueta de “amenazas lógicas” se incluyen todo tipo de programas que de una forma u otra pueden dañar a un sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). (Huerta, 2002, p.7).

Puertas traseras: Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar ‘atajos’ en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una ´única clave ‘especial’, con el objetivo de perder menos tiempo al depurar el sistema. (Huerta, 2002, p. 7).

Bombas lógicas: Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia

o presencia de ciertos ficheros, la ejecución bajo un determinado UID o la llegada de una fecha concreta. (Huerta, 2002, p. 8).

Virus: Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas. (Huerta, 2002, p. 8).

Gusanos: Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el Internet Worm, un gusano que en 1988 causo pérdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red. (Huerta, 2002, p. 8).

Programas conejo o bacterias: Bajo este nombre se conoce a los programas que no hacen nada ´útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina.

9. TIPOS DE ATACANTES DE LA RED.

Hackers: Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

Crackers ("blackhats"): Los crackers son individuos con interés en atacar un sistema informático para obtener de forma ilegal o simplemente para provocar algún daño a la organización propietaria del sistema, motivados por el interés económico, político, etc.

Sniffers: Los Sniffers son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por rede de ordenadores como internet.

Spammers: Los Spammers son los responsables del envío masivo de miles de correos electrónicos no solicitados a través de redes como internet, provocando el colapso de servidores y sobrecarga de los buzones de correo de los usuarios. Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa a través de internet.

Piratas informáticos: Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

Lamers: ("wannabes"): Los "lamers", también conocidos como "script-kiddies" o "Click-kiddies", son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas.

Ex- Empleados: Los Ex- Empleados pueden actuar contra su antigua empresa u organización por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización. También puede provocar la activación de "bombas lógicas" para causar determinados daños en el sistema informático (eliminación de ficheros, envió de información confidencial a terceros...) como venganza tras un despido.

10. PLANIFICACIÓN DE LA SEGURIDAD.

Se puede definir una Política de Seguridad como una "declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran " Así pues, se debe identificar qué es lo que se va a proteger, su valor y el grado de protección adecuado en función de las amenazas previsibles; por tanto, se tienen que ejecutar los siguientes pasos:

- Lista de objetos a definir (ordenadores, software, Routers, cables, etc).
- Categorizarlos.
- Asignar una métrica.
- Priorizar: asignar cual es el más importante.

La planificación se enfoca en cómo se va a lograr la protección y cuando se va a proteger; debe planificarse en conjunto, pero observando las características propias del software, hardware, recuperación en caso de desastres, la educación de los usuarios, las necesidades de crecimiento, la auditoria para todos los procesos del sistema de información, etc.

En la implementación se evalúa las opciones con base a diferentes niveles de servicio y operación de la empresa. Se debe incluir un periodo de prueba y entrenamiento del personal a todos los niveles.

La revisión deberá incluir estos puntos: monitorizar la red, la auditoria, la política de respaldo de archivos y la periodicidad necesaria para efectuar una revisión de las políticas. Se deberá tener en cuenta cuáles son las prioridades de la empresa, la seguridad que quiere o puede implementar.

11. METODOLOGÍA DE ANÁLISIS DE RIESGOS

1- Identificar los activos de Información de cada proceso

2- Identificación de los responsables y dueños de la información (dependencia que

produce el activo)

3- Identificar: Vulnerabilidades, Amenazas o Causas, Posibles consecuencias, Riesgo (Entrevistas, Observación directa, etc.)

4- Determinar la probabilidad de ocurrencia para cada riesgo.

5- Determinar nivel de valoración del impacto para cada riesgo materializado.

6- Determinar el nivel de riesgo basados en la probabilidad de ocurrencia y la valoración del Impacto.

12. DIAGNÓSTICO DE SEGURIDAD

12.1 INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN (HARDWARE, SOFTWARE Y DOCUMENTOS)

Se realizará un inventario y una clasificación de activos (formato) Inventario de activos, el cual permite a la entidad saber el estado en el que se encuentran los bienes adquiridos tener vigilancia y orden sobre ellos, para permitir al usuario una calidad de servicio adecuada y cumplir con la normatividad, dando el primer paso para crear un Modelo de Seguridad y Privacidad. Al momento de realizar el inventario y la clasificación de activos de la información se utilizará la plantilla de la entidad adaptando los lineamientos que indican en la guía No. 5 del MinTIC, así también un modelo de clasificación en cuanto a los tres principios fundamentales de la seguridad confiabilidad, integridad y disponibilidad de cada activo.

Tomando las indicaciones de la Guía No. 5 se definen los 3 niveles que permiten determinar el valor que genera el activo en la entidad: alta, media y baja (TIC, 2016). Criterios de Clasificación de activos de la información.

Confidencialidad	Integridad	Disponibilidad
Informacion Publica Reservada	Alta (A)	Alta (1)
Información Publica Clasificada	Media (M)	Media (2)
Información Publica	Bajo (B)	Baja (3)
No Clasificada	No Clasificada	No Clasificada

12.2. NIVELES DE CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

Alta	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
Media	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
Bajo	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Clasificación de acuerdo con la confidencialidad. La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, a manera de ejemplo en la guía se definieron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014) (ver tabla 4) (TIC, 2016).

Esquema de clasificación por confidencialidad.

Confidencialidad	
Información Publica Reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
Información Publica Clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Información Publica	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Clasificación de acuerdo con la integridad: La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles: Esquema de clasificación por integridad:

Integridad	
Alta (A)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
Media (A)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
Bajo (B)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Clasificación de acuerdo con la disponibilidad: La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. (TIC, 2016). En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

Esquema de clasificación por Disponibilidad

Disponibilidad	
Alta (1)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
Media (2)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
Baja (3)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

13. MEDICIÓN DE LA CULTURA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN POR PARTE DEL RECURSO HUMANO

Para determinar la cultura de seguridad de los funcionarios, contratistas y pasantes se realizará una encuesta anónima (Encuesta Seguridad y Privacidad de la Información), relacionada con el manejo de hardware, software, copia de seguridad y uso del internet. La encuesta se aplicará a las personas que se encuentren laborando.

14. EVALUACIÓN DE AMENAZAS Y VULNERABILIDAD EN EL HARDWARE, SOFTWARE Y RECURSO HUMANO

14.1. ESTADO DE LA INFRAESTRUCTURA FÍSICA

Planos generales de la Red.

El edificio tiene puntos de red en cada oficina mínimo 2 y el punto de red es usado por los funcionarios, la red se suministra por medios alámbricos e inalámbricos, los puntos de red que se encuentran en las oficinas se instalaron en canaletas sin estándares o improvisadas, los puntos de red no se encuentran debidamente marcados. Para el diagnostico de los puntos de red se realizará el levantamiento de los planos del cableado de red de la alcaldía, evidenciando los puntos de red de las plantas físicas.

14.2. RIESGOS DE SEGURIDAD DEL RECURSO HUMANO

Puertos USB expuestos.

Amenaza de factor humano en los equipos de cómputo. Los puertos USB de los equipos de cómputo están expuestos a personas inescrupulosas inserten dispositivos de almacenamiento, se muestra un equipo de una secretaria, el púbico visitante puede tener fácil acceso a los puestos USB facilitando la extracción de archivos por medio de virus.

Control de acceso en equipos de cómputo. El 30% de los usuarios de los equipos de cómputo no tienen como control usar contraseña para evitar el acceso de personas ajenas al computador, se puede observar que solo existe un perfil llamado usuario, al presionar enter accedemos al sistema operativo, estando expuesto a la extracción y/o manipulación de la información almacenada, donde cualquier persona puede entrar e instalar un exploit.

Consumo de alimentos en el área de trabajo. Por lo general en las oficinas se realizan pausas activas, o momentos cortos para compartir, no está bien comer cerca de los equipos de cómputo debido a que en cualquier momento el derrame de líquidos puede afectar el funcionamiento del equipo.

Documentación física. Durante la búsqueda de vulnerabilidades de hardware y software, se logró identificar un documento en la papelera de basura, para muchos funcionarios no son importantes los documentos que se desechan, creen que solo con arrugarlos ya se destruyen y la información se pierde. En el documento mencionado se encontró cifras de dinero de proyectos, nombre, cedula de funcionario responsable, datos que pueden ser utilizados para actos inescrupulosos, el control del documento se pierde al momento de ser arrojado sin destruirlo, hay personas que revisan la basura para obtener información privada y así lograr hacer daño a los que bien convenga.

15. PROCEDIMIENTOS, CONTROLES Y NORMAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

15.1. CONSTRUCCIÓN Y CREACIÓN DE POLÍTICAS, CONTROLES, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD.

Para la creación del manual de políticas, controles, normas y procedimientos se basa en los objetivos del plan, se realizará primero un diagnóstico del estado en el que se encontraba la entidad (ver anexo 5- Diagnóstico de Controles Norma NTC-ISO 27001:13).

16. MANUAL DE POLÍTICAS, NORMAS, PROCESOS Y CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Alcaldía Municipal de Ipiales, entendiendo la importancia de la gestión de la información, se ha comprometido con la implementación de un sistema integral de seguridad de la información y la red. buscando establecer un marco de confianza todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Tiene como propósito establecer reglas y lineamientos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, acceso no autorizado, divulgación no controlada, duplicación e interrupción intencional de la información para mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad.

17. ALCANCE FUNCIONAL

La política de seguridad y privacidad de la información de la alcaldía está diseñada para sus funcionarios públicos de planta, contratistas, terceros, pasantes, aprendices, proveedores y ciudadanía en general teniendo en cuenta los siguientes objetivos.

- Establecer normas, procesos y controles para la seguridad y privacidad de la información.
- Proteger los activos de información.
- Organizar, clasificar y valorar la información según el riesgo.
- Minimizar el riesgo de pérdida de datos.
- Realizar controles de acceso no autorizado.
- Generar cultura de seguridad y privacidad de la información en el personal de la Alcaldía.
- Preservar la integridad, confidencialidad y disponibilidad de los activos de información
- Mantener una red de internet segura.

Obligación. Es un deber de los funcionarios públicos de planta, contratistas, terceros, pasantes, aprendices y proveedores, de la alcaldía de Los Patios, conocer e implementar las políticas de seguridad y privacidad de la información para garantizar la integridad, confidencialidad y disponibilidad de los activos de información.

18. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

18.1. POLITICA DE SEGURIDAD DIGITAL

19. La Política de Seguridad Digital se refiere al conjunto de directrices, principios y acciones diseñadas para proteger la información digital y los sistemas de comunicación de una organización. A continuación, se presentan algunos de los principales objetivos de una política de seguridad digital.

19.1. SEGURIDAD DEL RECURSO HUMANO

- Antes de asumir el empleo, el empleador deberá leer el manual de Procedimientos, controles y normas de seguridad y privacidad de la información.
- Verificar por parte de los encargados de contratación los antecedentes de acuerdo con las leyes, reglamentos y ética pertinente, que deberían ser proporcionales a la clasificación de la información que se va a tener acceso.
- El empleador deberá firmar acuerdos contractuales donde se compromete velar por la confidencialidad, integridad y disponibilidad de los activos de la información de la alcaldía.

- Los pasantes deberán presentar una certificación de vinculación con la institución educativa a la que pertenece, especificando las áreas en las que se desempeñará.
- Los pasantes deberán firmar un acuerdo de confidencialidad, integridad y disponibilidad de los activos de la información de la alcaldía, en la secretaría que realizara las prácticas laborales.
- El personal de la alcaldía deberá recibir la educación y la formación para promover y fortalecer las políticas de seguridad de la información.
- Las responsabilidades y deberes de seguridad y privacidad de la información permanecerán vigentes después de la culminación o cambio del contrato.
- La oficina asesora TIC es la encargada de realizar campañas de seguridad y privacidad de la información.
- Si el usuario requiere de una capacitación deberá solicitarla en la oficina asesora TIC.
- La oficina asesora TIC programará capacitaciones periódicamente y dependiendo de la demanda de usuarios que la requieran.

19.2. CONTROL DE ACCESO

Política: Para garantizar la seguridad al acceso físico de la alcaldía se deben cumplir los mecanismos de control, donde garantiza el acceso de usuarios autorizados.

Circulación del personal de la Alcaldía.

• Los funcionarios de planta deberán portar distintivo que los acredite como empleados de la alcaldía.

• Secretaría general deberá proporcionar un distintivo con fecha de caducidad a los contratistas.

• En caso de pérdida, el empleador deberá reportar a la alcaldía la pérdida del distintivo.

Entrada y Salida de visitantes.

• Todo visitante deberá dejar registrarse en la portería con No. de cedula, Nombre, dependencia a la que se dirige.

Personal de Recepción.

• El personal de seguridad deberá solicitar al visitante un documento que lo identifique preferiblemente con foto.

• El personal de seguridad deberá brindar información acerca de la dependencia a la que desea llegar el visitante.

Restricción.

- Se impide a los visitantes o los funcionarios estar en las áreas de acceso no autorizado.
- Se impiden los préstamos o intercambio de distintivos.
- Si un empleador requiere trabajar fuera del horario laborar, el jefe de despacho deberá notificarle al personal de seguridad la novedad.

19.3. SEGURIDAD DE GESTIÓN DE ACTIVOS

Política: Se identifica los activos organizacionales y se definen los controles para la protección apropiada.

Controles:

- La oficina asesora TIC llevara el inventario de activos electrónicos por medio de un sistema operativo.
- Almacén deberá entregar inventario de activos electrónicos (computador, Access Paint, Reuter, impresoras, etc.) a la oficina asesoría TIC.
- Almacén deberá enviar un reporte cuando se adquieran un nuevo activo electrónico, con el propósito de mantener actualizado el sistema de gestión de inventario (GLPI).
- Un Ingeniero de la oficina asesora TIC deberá administrar el sistema de gestión de inventario (GLPI) y entregar un informe mensual de las incidencias reportadas.
- Cada dependencia tendrá un responsable de reportar la incidencia por medio del sistema de gestión de inventario (GLPI) por medio de un perfil asignado.
- Todo activo electrónico deberá tener un propietario, quien es el responsable del uso.
- Para dar de baja a un activo electrónico, se deberá dar el motivo y el concepto por parte de la oficina TIC, para ser entregado a la oficina de almacén.
- Cada dependencia deberá clasificar la información, determinar su sensibilidad y criticidad en los activos de la información.
- Todo activo electrónico debe tener una marquilla asignada por la oficina asesora TIC, para llevar un mejor control en el sistema de gestión de inventario (GLPI).
- Los activos de la información (documentos, actas, correspondencias), deberán estar en un lugar adecuado y clasificada según el nivel de sensibilidad, donde no corra peligro que se moje o este al acceso de personas inescrupulosas.

• Cuando un activo electrónico se notifica que será dado de baja, la oficina asesora TIC deberá eliminar toda información digital para entregar a la oficina de almacén y decidir el destino del activo.

19.4. SEGURIDAD FÍSICA Y DEL ENTORNO

Política: Prevención de daños y la interferencia a la información y a las instalaciones de procesamiento de información.

Controles:

• Antes de encender los equipos electrónicos se deberá revisar que las conexiones eléctricas estén seguras.

• Después de terminar la jornada laboral se deberá apagar los equipos de cómputo, impresoras y todo equipo electrónico alimentado por corriente y desconectar las UPS.

• Apagar equipos de cómputo e impresoras en casos de tormentas o descargas eléctricas.

• Todo lugar con acceso restringido deberá tener visible como restricción de personal no autorizado.

19.5. SEGURIDAD DE ACTIVOS ELECTRÓNICOS

Política: Se establecen controles para el uso de los activos electrónicos que permitan su operación correcta y segura, donde se establece las responsabilidades
de los usuarios, quienes son los encargados de salvaguardar la información que contiene cada uno de ellos.

Controles:
Computadores.

- El usuario o contratista será responsable del equipo de cómputo asignado.
- Los equipos de cómputo solo se usarán con fin laboral y no personal.
- Se le entregará el equipo de cómputo al usuario o contratista, de acuerdo con la función laboral que desempeñará en la alcaldía.
- La alcaldía suministrara el equipo de cómputo con sus periféricos básicos para el óptimo rendimiento del usuario.

- Los equipos de cómputo se asignan con hardware y software básico para el área que sea asigna al usuario o contratista.
- En caso de que el usuario o contratista requiera de un software en especial deberá notificar a la subsecretaria de bienes y servicios, para que el Ingeniero o Técnico encargado procesada a instalarlo.
- Si el equipo de cómputo presenta fallas físicas y/o lógicas deberá notificarse por el GLPI para que la subsecretaria de bienes y servicios atienda la incidencia.
- Los usuarios deberán tener conocimientos básicos del manejo de hardware y software del equipo de cómputo.
- Se prohíbe que el usuario instale software de entretenimiento.
- Se prohíbe el consumo de alimentos o líquidos que puedan derramarse alrededor de los equipos de cómputo.
- En caso cables en mal estado propensos a cortos circuitos informar inmediatamente a la subsecretaria de bienes y servicios.
- El usuario debe proteger las unidades de almacenamiento que estén a su cargo y que contengan información reservada.
- El equipo de cómputo no debe ser manipulado por otros usuarios, a menos que sea supervisado por el usuario asignado.
- Todo usuario que utilice equipo personal es responsable de la información que tiene almacenada y debe evitar cualquier forma de fuga de información.
- Para que un equipo de cómputo salga de las instalaciones de la alcaldía deberá tener visto bueno de la subsecretaria de bienes y servicios y permiso de la oficina de almacén.
- Es responsabilidad del usuario solicitar capacitación básica a la oficina asesora TIC sobre el uso del hardware y software para así evitar futuros riesgos. • Es responsabilidad del usuario solicitar capacitación básica a la oficina asesora TIC sobre el uso de herramientas informáticas para rendimiento del trabajo.
- Se prohíbe reubicar los equipos de cómputo de la institución, al momento que se requiera de una reubicación por motivos de la secretaría se debe pasar la incidencia a la subsecretaria de bienes y servicios para atender el requerimiento.
- Solo subsecretaria de bienes y servicios será la responsable de asignar al personal encargado para desarmar y arma r los equipos de cómputo.
- En caso de robo o extravío del equipo de cómputo o periféricos asignados deberá avisar a la subsecretaria de bienes y servicios y a almacén.
- Todo computador tendrá los puertos de almacenamiento deshabilitados, para evitar la transferencia de archivo por medio de memorias USB.

- En caso de que se encuentre un equipo de cómputo con daños, o descuidos por parte del usuario se levantará una incidencia por parte de la subsecretaria de bienes y servicios.
- Todo equipo de cómputo debe tener 2 perfiles de inicio de sesión, primer perfil con contraseña que solo domine la oficina asesora TIC para evitar la instalación de software por parte del usuario y el segundo perfil será el del usuario propietario del equipo.
- Todo equipo de cómputo deberá tener una contraseña segura, mínimo 8 caracteres combinado con mayúsculas minúsculas y caracteres.
- Se prohíbe tener contraseñas escritas cerca del equipo de cómputo o escritorio.
- Cuando sea necesario desplazarse a otro sitio de la entidad, se debe bloquear la pantalla, cerrar sesión o suspender.
- Se prohíbe la copia de archivos históricos que se encuentren en el equipo de cómputo sin la aprobación del jefe de despacho.
- Se debe utilizar un antivirus para revisar todo archivo que se descargue o se copie de dispositivos de almacenamiento.
- Se prohíbe la instalación de software sin licencia o de distribución gratuita a menos que sea aprobado por la subsecretaria de bienes y servicios.
- Los usuarios son responsables de la pérdida o daño de la información que está a su cargo.
- Los usuarios que utilizan computador personal no deben desatenderlo fuera la alcaldía debido a la información que maneja de la institución.
- Las contraseñas de los equipos de cómputo deberán ser cambiadas mínimo cada 3 meses o antes según la necesidad el usuario.

Impresoras.

- Todo documento que se imprima en las impresoras de la alcaldía debe ser de uso institucional
- El usuario debe capacitarse en el manejo de las herramientas básicas del uso de la impresora (escáner, impresión o fotocopiado) que se encuentre en la oficina asignada.
- Si la impresora presenta fallas físicas o lógicas deberá notificarse por el GLPI para la subsecretaria de bienes y servicios atender la incidencia.
- En caso cables en mal estado propensos a cortos circuitos informar inmediatamente a la subsecretaria de bienes y servicios.

- Se prohíbe reubicar la impresora al momento que se requiera de una reubicación por motivos de la secretaría se debe pasar la incidencia a la subsecretaria de bienes y servicios para atender el requerimiento.
- Solo la subsecretaria de bienes y servicios será la responsable de asignar al personal encargado para desarmar y armar los equipos de cómputo.
- En caso de robo o extravío de la impresora asignados deberá dar aviso a la subsecretaria de bienes y servicios y a la oficina de almacén
- No está permitido imprimir trabajos personales usando los recursos de la Alcaldía.
- Abstenerse de desatender las impresoras, sobre todo cuando se imprime documentos con información sensible.
- Para la instalación del software de la impresora se deberá solicitar a la oficina de bienes y servicios por medio de solicitud formal.

3. Dispositivos Móviles.

- Se recomienda evitar la conexión a las redes inalámbricas de la alcaldía por parte de los dispositivos móviles personales.
- Toda Oficina que requiera de conexión a internet en un dispositivo móvil de uso institucional deberá solicitar la conexión a la oficina que gestiona las conexiones de red, y su acceso.

19.6. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de La Alcaldía Municipal de Ipiales será reglamentado la SECRETARIA GENERAL, junto con la subsecretaria de bienes y servicios, considerando las labores realizadas por los funcionarios y su necesidad de uso.

Normas Dirigidas A la Oficina De Sistemas

La subsecretaria de bienes y servicios deben establecer las condiciones para el uso de periféricos y medios de almacenamiento de acuerdo a los lineamientos para tener una disposición segura de la información dentro de la organización

La subsecretaria de bienes y servicios debe autorizar el uso de periféricos y medios de almacenamiento dentro de la plataforma tecnológica de acuerdo a los perfiles de cada funcionario según se lo requiera

Normas Dirigidas A: Todos Los Usuarios

Los funcionarios y el personal provisto por terceras partes deben acoger las normas de uso de los periféricos y medios de almacenamiento establecidos por la Alcaldía Municipal de Ipiales. Por lo cual no se deben modificar las configuraciones de los periféricos y medios de almacenamiento establecidos por la alcaldía municipal de Ipiales.

Los funcionarios deben ser responsables de la custodiar la información al igual que el manejo de sus respectivos periféricos y medios de almacenamiento asignados a cada funcionario.

19.7. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La Alcaldía Municipal de Ipiales proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de plataformas tecnológicas en donde se procesa y almacena la información, adoptando los controles necesarios para evitar la pérdida o daños que puedan causar esto al igual que prevenir el contagio de software malicioso y prevenir daños a futuro los cuales pueden llegar a ser irreversibles, además de capacitar a los funcionarios para que puedan adoptar dichos mecanismos para poder mejorar la protección frente a estos ataques.

Normas de protección frente a software malicioso

Normas Dirigidas A la Oficina De Sistemas

La Oficina de Sistemas debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida dentro de La Alcaldía Municipal de Ipiales

La subsecretaria de bienes y servicios debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus

La subsecretaria de bienes y servicios, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de las plataformas tecnológicas.

Normas Dirigidas A todos los funcionarios

Los funcionarios deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera

vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

Los funcionarios no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Oficina de Sistemas; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al SAC, para que, a través de ella, la subsecretaria de bienes y servicios tome las medidas de control correspondientes.

19.8. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La subsecretaria de bienes y servicios certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Así mismo, la Organización velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta.

Normas Dirigidas A la Oficina De Sistemas o Quien Corresponda la Función

La subsecretaria de bienes y servicios, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
La subsecretaria de bienes y servicios debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

La subsecretaria de bienes y servicios debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

Normas dirigidas a todos los funcionarios

Es responsabilidad de los funcionarios de La Alcaldía Municipal de Ipiales identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

19.9. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La subsecretaria de bienes y servicios revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

Normas para la gestión de vulnerabilidades

Normas Dirigidas A la Oficina De Sistemas

La subsecretaria de bienes y servicios debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo.

La subsecretaria de bienes y servicios debe revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

La subsecretaria de bienes y servicios, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

19.10. POLÍTICA DE USO DEL CORREO ELECTRONICO

La subsecretaria de bienes y servicios entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y público en general, proporcionará un servicio dispuesto y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Normas Dirigidas A la Subsecretaria de Bienes y Servicios

La subsecretaria de bienes y servicios debe organizar y difundir un procedimiento para la administración de cuentas de correo electrónico, al igual diseñar estrategias para el buen uso de los servicios de correo electrónico. A demás de implementar controles que permitan detectar y proteger las plataformas de correo electrónico contra de códigos maliciosos y que se puedan ser trasmitidos a través de estos medios

Normas Dirigidas A Todos Los Usuarios

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la Administración debe proporcionar usuarios y claves de cuentas para ser utilizadas por terceros

Los mensajes y la información contenida en los buzones de correo son propiedad de La Alcaldía Municipal de Ipiales y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada uno de los usuarios con respecto a labores de la Alcaldía Municipal de Ipiales. El correo institucional no debe ser utilizado para actividades personales.

No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

Todos los mensajes enviados deben respetar el estándar de formato e imagen institucional definidos por La Alcaldía Municipal de Ipiales y deben conservar en todos los casos el mensaje legal.

19.11. POLÍTICA DE USO ADECUADO DE INTERNET

La Alcaldía Municipal de Ipiales consciente de la importancia del Internet como una herramienta para el desempeño de labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias dentro de la Organización.

Normas de uso adecuado de internet

Normas dirigidas a la Subsecretaria de Bienes y Servicios

La subsecretaria de bienes y servicios debe suministrar los recursos para lograr la, administración y ejecución de planes emplazados para la prestación segura del servicio de Internet, todo esto bajo las condiciones de cada uno de sus empleados

La subsecretaria de bienes y servicios debe perfilar e realizar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso que el proveedor principal de servicios de internet presente fallas en su servicio

La subsecretaria de bienes y servicios debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La subsecretaria de bienes y servicios debe concientizar a los funcionarios, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet. Tales como descargas de aplicaciones y software que pueda contener código malicioso.

Normas Dirigidas A Todos Los Usuarios

Los usuarios del servicio de Internet de La Alcaldía Municipal de Ipiales deben acceder a redes wifi en dispositivos móviles siempre y cuando sea en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea tales como redes sociales, que tengan como objetivo crear comunidades para intercambiar información con fines no laborales.

19.12. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La subsecretaria de bienes y servicios deberá de asegurar la protección de la información en el momento de ser transferida o intercambiada con otras dependencias de la entidad de tal manera que establecerá los procedimientos necesarios para dicho intercambio. De igual manera la oficina de sistemas propenderá el uso de recursos tecnológicos informáticos y de telecomunicaciones para llevar a cabo el intercambio de la información.

Normas de intercambio de información

Normas Dirigidas A la Subsecretaria de Bienes y Servicios

La subsecretaria de bienes y servicios debe definir y establecer el procedimiento de intercambio de información de las diferentes dependencias que hacen parte de La Alcaldía Municipal de Ipiales, las cuales contemplen la utilización de medios de trasmisión confiables, con el fin de proteger la confiabilidad y la integridad.

La subsecretaria de bienes y servicios debe velar por que el intercambio de información de las diferentes dependencias de la Alcaldía Municipal de Ipiales se realice cumpliendo las políticas de seguridad con respecto al intercambio de la información

Normas Dirigidas A Propietarios De Los Activos De Información

Los funcionarios responsables de los activos de información deben velar porque la información de La Alcaldía Municipal de Ipiales sea protegida de divulgación no permitida por parte de terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

Los responsables de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los jefes directos de las oficinas de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de La Alcaldía Municipal de Ipiales, así como del procedimiento de intercambio de información.

Normas Dirigidas A: Secretaria General y Correspondencia

La Coordinación de Correspondencia debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

La Coordinación de Correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por La Alcaldía Municipal de Ipiales, y que estos permitan ejecutar rastreo de las entregas.

Normas Dirigidas A la Subsecretaria de Bienes y Servicios

La subsecretaria de bienes y servicios debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas Dirigidas A Todos Los Usuarios:

Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Organización o de sus beneficiarios.

No está permitido el intercambio de información sensible de la Organización por vía telefónica.

19.13. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La Alcaldía Municipal de Ipiales asegurará que el software adquirido y desarrollado tanto al interior de la Organización, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información, La Alcaldía Municipal de Ipiales y la subsecretaria de bienes y servicios incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

Normas para el establecimiento de requisitos de seguridad

Normas Dirigidas a responsables de Sistemas de Información y Oficina de Sistemas

La Alcaldía Municipal de Ipiales debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

Las áreas propietarias de los sistemas de información, en acompañamiento con la Alcaldía Municipal de Ipiales y la subsecretaria de bienes y servicios deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

Las áreas responsables de los sistemas de información deben especificar qué información delicada puede ser eliminada de los sistemas y pedir que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

La oficina de sistemas debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas Dirigidas A Desarrolladores (Internos y/o Externos)

Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

19.14. POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

La Alcaldía Municipal de Ipiales protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

Normas para la protección de los datos de prueba

Normas Dirigidas A la Oficina De Sistemas

La subsecretaria de bienes y servicios debe documentar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

La subsecretaria de bienes y servicios debe borrar la información de los ambientes de pruebas, una vez estas han concluido.

19.15. POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

La Alcaldía Municipal de Ipiales establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los funcionarios responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas Dirigidas A: Oficina De Sistemas

La subsecretaria de bienes y servicios debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Organización.

La subsecretaria de bienes y servicios debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

La subsecretaria de bienes y servicios debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

19.16. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La Alcaldía Municipal de Ipiales promoverá entre los funcionarios y contratistas de eventualidades relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, tanto en la plataforma tecnológica como medios físicos de almacenamiento

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

Normas para el reporte y tratamiento de incidentes de seguridad

Normas Dirigidas a: Responsables de los Activos de Información

Los responsables de los activos de información deben informar a la subsecretaria de bienes y servicios, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de realización.

La subsecretaria de bienes y servicios debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

La subsecretaria de bienes y servicios debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y de esta manera informar a los jefes de la oficina o a quien se considere pertinente.

La subsecretaria de bienes y servicios debe crear una base de datos de conocimientos para los incidentes de seguridad. Prestados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas Dirigidas A Todos Los Usuarios

Es responsabilidad de los funcionarios de La Alcaldía Municipal de Ipiales y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Oficina de control interno para que se registre y se le dé el trámite necesario.

19.17. POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL PROCESO

POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

La Alcaldía Municipal de Ipiales suministrará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la Organización y que afecten la continuidad de sus albores

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La Alcaldía Municipal de Ipiales mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

La subsecretaria de bienes y servicios, deben reconocer las situaciones que serán identificadas como emergencia, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

La subsecretaria de bienes y servicios, deben liderar los temas relacionados con la continuidad de las labores y la recuperación ante eventualidades

La subsecretaria de bienes y servicios debe realizar los análisis de impacto a los procesos y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias

de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

La subsecretaria de bienes y servicios, deben asegurar la realización de pruebas periódicas del plan de recuperación ante daños y/o continuidad de los procesos, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

La subsecretaria de bienes y servicios deberá elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

Normas dirigidas a Subsecretarios, directores y jefes de Oficina

Los subsecretarios, directores y Jefes de Oficina deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser aprobados para certificar su efectividad.

19.18. POLÍTICA DE REDUNDANCIA

La Alcaldía Municipal de Ipiales propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Organización.

Normas de Redundancia

La subsecretaria de bienes y servicios debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la Organización y la plataforma tecnológica que los apoya.

La subsecretaria de bienes y servicios y debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de La Alcaldía Municipal de Ipiales.

La subsecretaria de bienes y servicios a través de sus funcionarios debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Organización.

19.19. POLÍTICAS DE CUMPLIMIENTO

POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La Alcaldía Municipal de Ipiales velará por la identificación, documentación y cumplimiento de la relacionada a la seguridad de la información, con respecto a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables vigentes.

Normas dirigidas a la Oficina De Sistemas

La subsecretaria de bienes y servicios debe certificar que todo el software que se ejecuta en las dependencias esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

La subsecretaria de bienes y servicios debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Organización para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas Dirigidas A Todos Los Usuarios

Los usuarios no deben instalar software o sistemas de información en sus lugares de trabajo o equipos móviles suministrados para el desarrollo de sus labores.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

20. 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**