PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020- 2023

CONCEJO MUNICIPAL DE YUMBO

INTRODUCCION

El Concejo Municipal de Yumbo considera que la información es el activo principal de toda Institución, a la cual se le deben aplicar medidas de seguridad con el propósito de protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Un plan de contingencia son un conjunto de procesos, procedimientos, recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro, teniendo como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto en la entidad, buscando una adecuada administración ante posibles riesgos que los afecten. Así mismo se hace necesaria la adopción de normas para la protección y utilización racional de los recursos que definan y documenten planes, normas y procedimientos que permitan la adecuada continuidad de las operaciones en caso de presentarse contingencias o situaciones de emergencia en los sistemas informáticos.

El Plan está basado en un proceso dinámico y continúo que incluye no sólo las actividades a realizarse en el evento de una interrupción de la capacidad de procesamiento de datos; sino además, en las actividades realizadas anticipando dicho evento.

Una actividad principal del plan, es evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un "desastre" ocurra.

Otra actividad es facilitar la recuperación en el evento de un desastre. Para lo cual, la fase de recuperación provee tres propósitos:

- **Tareas individuales (de ejecución, coordinación y toma de decisiones) deben ser socializados y de conocimiento general en la entidad.**

- **necesidad de establecer y mantener las descripciones de los procedimientos a ser realizados en el evento inesperado.**

- **El plan permite evaluar la perfección y exactitud de cada proceso y los procedimientos de recuperación sobre la marcha.**

3. OBJETIVOS GENERALES Y ESPECÍFICOS

3.1. OBJETIVOS GENERALES

Garantizar la continuidad de las actividades de El Concejo Municipal de Yumbo o, que ponen en riesgo el normal funcionamiento de los procesos misionales asociadas a las Tics, a fin de minimizar, prevenir, y responder de forma oportuna ante cualquier eventualidad.

3.2. OBJETIVOS ESPECIFICOS

- **Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante la eventual presencia de siniestros que los paralicen parcial o totalmente.**

- **Garantizar la continuidad en los procesos de los elementos críticos necesarios para el funcionamiento de las aplicaciones de El Concejo Municipal de Yumbo.**

- **Identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un siniestro que restrinja el acceso a los sistemas de información.**

- **Establecer las secuencias que se han de seguir para organizar y ejecutar las acciones de control de emergencias.**

- **Minimizar las pérdidas asociadas a la presencia de un siniestro relacionado con la gestión de los datos.**

- **Proveer una herramienta de prevención, mitigación, control y respuesta a posibles contingencias generadas en la ejecución del proyecto**

4. ALCANCE Y COBERTURA

En el presente documento se realiza un análisis de los posibles riesgos y eventuales siniestros a los cuales puede estar expuesto equipos de cómputo, programas, archivos y Bases de Datos de El Concejo Municipal de Yumbo, así como la minimización ante la posibilidad de ocurrencia y los procedimientos apropiados en caso de la presencia de cualquiera de tales situaciones.

El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman los sistemas de información que maneja la entidad, que se relacionan a continuación:

- **Datos: En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser Estructurados (Bases de Datos) o no**

estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colecciones de bits.

- **Aplicaciones: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.**

- **Tecnología: Incluye los equipos de cómputo como computadores de escritorio, servidores, cableados, Switch, etc. en general, conocidos como hardware y los programas, archivos, bases de datos, etc. denominados software para el procesamiento de información.**

- **Instalaciones: Lugares físicos de la Entidad donde se encuentren el software.**

Independientemente de la cobertura y medidas de seguridad que se encuentren implantadas, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia cuente también con un Plan de Recuperación en caso de desastres, el cual tendrá como objetivo restaurar los servicios de los sistemas de información de forma rápida, eficiente y con el menor costo y pérdidas de tiempo posible.

El impacto potencial que provoca la interrupción parcial o total de los servicios electrónicos y procesamiento de la información sobre el normal desarrollo de las actividades de El Concejo Municipal de Yumbo o; se hace necesario la adopción, desarrollo e implementación de un plan de contingencia relacionado con un eventual cese de actividades e inoperatividad de equipos.

Se debe considerar que los procedimientos planteados en este documento, debe ocuparse solamente de las acciones a realizar con relación al Hardware, Software y Equipos electrónicos involucrados en los procesos críticos definidos en el Plan.

Se consideran los riesgos y soluciones del ambiente físico en cada proceso así como en el Centro de Cómputo principal de la entidad.

Las actividades y procedimientos, se relacionan con las funciones que correspondan a cada uno de los grupos contingentes establecidos para la ejecución del Plan y colaboración de los procesos y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

5. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

DEFINICIÓN: Riesgo es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad, azar o exposición

TIPO DE RIESGO	FACTOR DEL RIESGO	PREVENCIÓN Y MITIGACIÓN
El Fuego: destrucción de equipos y archivos.	Bajo	Extintores, aspersores automáticos, detectores de humo, pólizas de seguros.
El robo común: pérdida de equipos y archivos.	Medio	Seguridad Privada, Alarma, Seguro contra todo riesgo y copias de respaldo (BackUp)
El vandalismo: daño a los equipos y archivos	Medio	Seguro contra todo riesgo, copias de respaldo...
Fallas en los equipos: daño a los archivos	Medio	Mantenimiento, equipos de respaldo, garantía y Copias de respaldo.
Acción de Virus: daño a los equipos y archivos	Bajo	Actualizaciones del sistema operativo, Antivirus Actualizados, copias de respaldo.

Terremotos: destrucción de equipo y archivos	**Medio**	**Seguro contra todo riesgo, copias de respaldo. Las sedes cumplen con las normas Antisísmicas.**
Accesos no autorizados: filtrado no autorizado de datos	**Medio**	**. Cambio de claves de acceso mínimo cada seis meses. Política de seguridad para acceso a personal competente.**
Robo de datos: difusión de datos sin el debido cubrimiento de su costo.	**Bajo**	**Cambio de claves de acceso mínimo cada seis meses, custodia de las copias de respaldo**
Fraude: modificación y/o desvío de la información y fondos de la institución.	**Bajo**	**Sistemas de información seguros con dos usuarios para autorizar transacciones, procedimiento de control y registro de transacciones en tablas de auditoría.**

5.1. DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos implica la valuación del impacto por interrupción del servicio, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones; esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

El proceso de Tecnología de El Concejo Municipal de Yumbo se encuentra conformado por un Ingeniero Informático contratista quien presta sus servicios tales como:

- **elaboración y puesta en marcha del Plan estratégico de las Tecnologías Y las comunicaciones PETIC.**

- **Plan de Contingencias Informático.**

- **actividades de soporte técnico a los usuarios y equipos con que cuenta la entidad.**

Por tal motivo se dificulta el avances significativos en cada proceso debido a que se debe de tener un diagnostico actual de la entidad en materia de tecnología para adopción de PETIC; de igual manera conocer y determinar las deficiencias en materia de seguridad en cada procesos que permita la formulación de planes y estrategias encaminadas a la adopción de un plan de contingencia acordes a las necesidades.

5.1.1. Riesgos con Incidencia Externa

- **Políticos**

Modificaciones a la constitución política ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión entidades

5.1.2. Riesgos con Incidencia Interna.

- **Posible incumplimiento de los contratistas**

  - **Este riesgo puede ocurrir a causa del posible atraso en la ejecución o violación.**

- **Estipulados en los contratos de actualización, modificación, mantenimiento de las plataformas, que se adjudicaron durante la vigencia del 2017; para el proceso de gestión Documental (Orfeo), el proceso contable (ASCII) y contratación del servicio de alojamiento del portal web de la entidad.**

➢ **Posibles retrasos en Procesos Administrativos**

La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos con exigencia en el cumplimiento de requisitos, ampliando el tiempo de ejecución de las actividades del Plan Emergente, de manera imprevista.

➢ **Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles**

Se relaciona con la carencia de procesos de análisis, evaluación, planeación y toma de decisiones para la elección de las alternativas tecnológicas a ser implementadas, y con el posible desconocimiento de las características y especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas.

➢ **pérdida de información.**

Este riesgo tiene alta probabilidad de ocurrencia, a pesar de que hayan empezado a realizar prácticas de respaldo de información, tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros) como a los archivos de bases de datos y resultados de las aplicaciones específicas en producción para cada una de las dependencias de la Entidad, se tiene un reto en la implementación de permiso para la administración de este recurso teniendo en cuenta que el desarrollo del presente manual se ha dificultado por que la plataforma tecnológica se encuentra desactualizada y existen unos niveles muy básicos en el control de acceso a la información y de los recurso tecnológico existentes en la entidad.

➢ **Posible falla de equipos electrónicos y Hardware fuera de inventario**

Este riesgo se presenta por la Falta de precaución, en el registro de los activos informáticos que soporten la inclusión en los inventarios de la entidad, por desconocimiento o por no haber sido reportados al proceso de Bienes y Tecnología tiempo a la Dirección de Informática para su respectiva asignación de código

➢ **Posibles Fallas en el Flujo de Energía Eléctrica.**

Este riesgo está relacionado con amenazas externas al control de la Entidad. Sin embargo, se presenta un riesgo alto porque los equipos para la mitigación del riesgo de corte temporal de energía eléctrica, UPS (Unidad de Poder interrumpido) no se ha realizado el respectivo mantenimiento provocando que no exista un debido proceso para tener la posibilidad de salvaguardar la información durante un tiempo prudencial para realizar el apagado de forma correcta de los equipos de cómputo. Si el corte es más prolongado no se cuenta con un sistema eléctrico independiente que genere el suficiente voltaje para la prestación de los servicios informáticos asociados a la atención y prestación de los servicio a la comunidad.

- **Posible Calentamiento de la Sala de Cómputo**

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que El Concejo Municipal de Yumbo ha implementado procedimientos para su mitigación, tales como: la instalación de un sistema de refrigeración que permite mantener una temperatura apropiada para los equipos de cómputo del cuarto de sistemas. Sin embargo se debe realizar inversión para la adquisición de sensores ambientales para el control y monitoreo de temperatura, humedad, flujos de corriente, filtros de aire, alarmas local y silenciosa. Además se debe instalar detectores de humo y fuego que accionan un sistema de alarmas y descarga automática de gases que apagan llamas originadas cuarto de computadores.

- **Posible Falla del Servicio Telefónico**

Este riesgo está relacionado con amenazas externas al control de la Entidad, El Concejo Municipal de Yumbo o es de nivel bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales implementada sobre cableado estructurado.

De otro lado, en lo que respecta al Centro de Cómputo de la entidad, se desarrolló un análisis del medio y los procedimientos de seguridad y control existentes.

El análisis indicó que la Entidad está en una posición favorable por lo siguiente:

- **la edificación no se encuentra en una zona que pueda presentar inundación.**
- **El centro de cómputo está ubicado estratégicamente en el piso 2 de la entidad.**
- **El acceso al software es restringido y se encuentra almacenado en un lugar seguro y adecuado.**
- **El cielo raso y pisos del centro de cómputo son de material no combustibles.**
- **El centro de cómputo está provisto de una Temperatura autorregulada y UPS.**

6. IDENTIFICACION DE PROCESOS CRITICOS

6.1. FACTORES CRÍTICOS A CONSIDERAR

6.1.1. Aplicaciones en Producción

- **Nivel de importancia de la aplicación en la entidad**
- **Impacto operativo, financiero o contable**
- **Oportunidad de procesamiento**
- **Programas críticos**
- **Comunicaciones: entrada y salida de datos**
- **Implicaciones para el usuario en caso de ausencia del recurso aplicativo.**
- **Documentación del sistema: manuales de usuario y procedimientos de Operación.**
- **Procedimientos de respaldo y recuperación a nivel aplicativo.**

6.1.2. Personal

- **Funcionarios que administran procedimientos de ingreso y altas en las cuentas de usuario y sus respectivas claves.**

- **Personal con alta dependencia en los sistemas automatizados**
- **Personal de que maneja el proceso de respaldo de la información y la cadena de custodia**
- **Entrenamiento al personal de planta de la entidad**

6.1.3. Parque computacional y aplicaciones en uso

- **Servidores, computadores personales, impresoras, periféricos, etc.**
- **Líneas de comunicación y equipos relacionados.**
- **Sistemas operativos y programas en producción.**
- **Suministros: papel, formas continuas, medios magnéticos y formas especiales**
- **Archivos maestros y de movimiento de información considerada crítica de respaldo de la misma.**

6.2. NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

Teniendo en cuenta los criterios y factores enunciados anteriormente, se han definido los siguientes niveles de prioridad y criticidad de los recursos informáticos con que cuenta El Concejo Municipal de Yumbo.

6.2.1. Prioridad Alta

Corresponde a todas aquellas herramientas de El Concejo Municipal de Yumbo que en el caso de no ser adaptadas oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar la actividad de servicio a la ciudadanía yumbeña.

6.2.2. Prioridad Media

Se les asigna a todas aquellas herramientas de El Concejo Municipal de Yumbo o, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de servicio, cuentan con procedimientos alternativos.

6.2.3. Prioridad Baja

Se le asigna a todas aquellas herramientas de El Concejo Municipal de Yumbo o, cuya falta de adaptación no representa graves traumatismos y sus modificaciones pueden aplazarse para la última parte del proyecto.

6.2.4. Criticidad A: (Máxima)

No puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas

6.2.5. Criticidad B: (Intermedia)

No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles.
Puede sustituirse parcialmente por un período, por un proceso manual.

6.2.6. Criticidad C: (Mínima)

Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles.
Puede sustituirse temporalmente por un proceso manual.

7. POLITICAS DE SEGURIDAD

7.1. OBJETIVOS GENERALES

Establecer y difundir las Políticas y Estándares de Seguridad Informática que deberán observar los usuarios de servicios de Tecnologías de la Información para proteger adecuadamente los activos tecnológicos y la información de El Concejo Municipal de Yumbo.

7.2. OBJETIVOS ESPECÍFICOS

Operar de una forma confiable en materia de Seguridad Informática a través de la definición de Políticas y Estándares Adecuados.

Evaluar y administrar los riesgos de la Seguridad Informática en base a Políticas y Estándares que cubran las necesidades de El Concejo Municipal de Yumbo.

Estructurar en 5 (CINCO) Políticas Generales de Seguridad para Usuarios de informática y cubrir:

- ✓ **Seguridad de Personal.**
- ✓ **seguridad física y ambiental.**
- ✓ **Administración de Operaciones de Cómputo.**
- ✓ **Controles de Acceso Lógico.**
- ✓ **Cumplimiento de Seguridad Informática.**
- ✓

Alinear las Políticas en Seguridad Informática según lo establece el Estándar Británico en sus mejores prácticas de ISO/IEC: 27002:2013 así como la norma ISO 27001:2013.

8. ALCANCE

El documento define las Políticas y los Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de Cómputo, aplicaciones y servicios informáticos El Concejo Municipal de Yumbo.

9. OBLIGACIÓNES DE LOS PROCESOS MISIONALES Y SUS INTEGRANTES

Cada supervisor de proceso tiene la responsabilidad de informar a los empleados de nuevo ingreso para que lean el Plan de Seguridad y Privacidad e la información y con ello conozcan las responsabilidades informáticas que implican ser nuevo empleado El Concejo Municipal de Yumbo o y a su vez se debe dejar evidencia que fue notificado de la existencia del material.

9.1. PRIMERA POLÍTICA GENERAL: POLÍTICAS Y ESTÁNDARES DE SEGURIDAD PERSONAL

POLÍTICA: Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de El

Concejo Municipal de Yumbo o, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

Obligaciones de los Usuarios: Es responsabilidad de los empleados y contratistas de El Concejo Municipal de Yumbo o, el estricto cumplimiento de las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

Acuerdos de uso y confidencialidad: Todos los empleados y contratistas de El Concejo Municipal de Yumbo o, deberán actuar conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de la entidad, así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

9.2. SEGUNDA POLÍTICA GENERAL: "POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL"

POLÍTICA: Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y área restringidas del Personería municipal de Yumbo, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes Centros de Cómputo del Poder Judicial.

Resguardo y protección de la información: El usuario deberá reportar de forma inmediata al proceso BIENES Y TECNOLOGÍA, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los CD-ROM, DVD, memorias USB, tarjetas de memoria, discos externos, computadoras, impresoras escáner y dispositivos portátiles que se encuentren bajo su resguardo, aun cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información de El Concejo Municipal de Yumbo o que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Seguridad en áreas de trabajo: Se prohíbe el consumo de alimentos en espacios de trabajo, eliminar objetos que impidan que los equipos puedan tener temperaturas ambientes adecuadas para el funcionamiento

Protección y ubicación de los equipos : Los usuarios no deben mover o reubicar los equipos de cómputo ni los de telecomunicaciones, ni instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del proceso de Bienes Y tecnología, en caso de necesitarlo, únicamente se requiere, a través de un correo electrónico martha.burbano@concejoyumbo.gov.co, o bien, a su supervisor del proceso para que pueda ser trasferido al personal encargado para esta actividad.

Administración de Bienes Informáticos de El Concejo Municipal de Yumbo se encargará de elaborar los resguardos de los bienes informáticos, para ello, cuando a un usuario se le instale un bien informático, el área de sistemas, se encargará de hacer entrega atreves de un acta donde el supervisor del proceso como el responsable de dicho activo y deberá conservarlos en la ubicación autorizada.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones que desempeña en la entidad.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información de archivos de programas, sistemas e información de El Concejo Municipal de Yumbo o, se recomienda que no almacenar información personal, música y videos lo cual permite que la capacidad de almacenamiento disminuya.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete, con el propósito de mantener el buen funcionamiento del equipo informático.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con de anticipación a proceso de bienes y tecnología detallado de movimientos debidamente autorizados por supervisor del proceso.

Queda prohibido que el usuario abra o desarme los equipos de cómputo, actividad que será realiza por el personal del área de sistemas.

Mantenimiento de equipo informático : Únicamente el personal del área de sistemas a cargo en el momento serán los en cargados prestar apoyo para los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría sistemas.

Mantenimiento preventivo de equipo informático: Esta actividad será realizada solo por el personal de sistemas el cual deberá de ser reportado al supervisor de proceso, el mantenimiento preventivo de los equipos informáticos tiene como finalidad de conservar su continua disponibilidad e Integridad.

Eliminación Segura y/o re-uso de equipo: Todas las computadoras, laptops y/o discos externos que contengan información almacenada y vayan a ser reasignadas a otro usuario o a otra adscripción distinta de la que actualmente se encuentra, deben ser revisadas por el usuario para que éste respalde su información, ya que el equipo cambie de usuario, se realizará la eliminación de la información que contenía.

Desaparición, pérdida, robo o extravío de equipo de cómputo: El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

En caso de desaparición, robo o extravío del equipo de cómputo o accesorios que estén bajo resguardo de un usuario, Auxiliar Administrativo, responsable del proceso de gestión de bienes y tecnologías, donde se llevara registro de la novedad y anexos de características técnicas y placa de los equipos, para iniciar el trámite interno e interponer la denuncia ante la autoridad competente.

Uso de dispositivos: El uso de los grabadores de discos compactos y/o dispositivos de almacenamiento tales como memorias USB, discos duros, etc. son exclusivos para respaldos de información que por su volumen así lo Justifiquen.

La asignación de este tipo de equipo será previa justificación por escrito y autorización supervisor del proceso correspondiente.

El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Daño del equipo: El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna falla por maltrato, descuido o negligencia por parte del usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso, se realiza previa consulta con el área de contabilidad para promediar el valor con respecto a los valores de compra.

9.3. TERCERA POLÍTICA GENERAL: "POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

POLÍTICA: **Los empleados y contratistas deberán utilizar los mecanismos institucionales para proteger la información generada en cada proceso la cual es uso exclusivo de El Concejo Municipal de Yumbo o. De igual forma, deberán proteger la información reservada o confidencial y no permitir su divulgación y tránsito de las mismas fueras de la entidad sin autorización por el supervisor de proceso y La Secretaria General.**

Los empleados y contratistas que haga uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. Y reportar de inmediato al área de sistemas para su respectiva evaluación y aplicación de las medidas correctivas de acuerdo al caso.

Uso de medios de almacenamiento: Cuando un empleado requiera usar o consultar la información que se tiene almacenada de otro compañero se deber realizar la autorización por parte del supervisor del proceso.

- ✓ **Explicará brevemente cuál es el fin de permitir compartir la información que se tiene en los medios de almacenamiento de un empleado a otro.**
- ✓ **Nombre y Puesto del empleado al que se le brindarán los derechos solicitados.**

Los usuarios deberán respaldar de manera periódica la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría al personal de soporte técnico, para que determinen el medio en que se realizará dicho respaldo.

En caso de que se requiera algún respaldo en un medio extraíble (USB, discos duros o DVD) debido a

que se tiene mucha información sensible, este servicio deberá solicitarse al supervisor del proceso y notificado al área de sistemas para que se deje evidencias y el uso que se dará a esta información.

Los empleados y contratistas de El Concejo Municipal de Yumbo deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

Para conservar la seguridad de la información, se llevará a cabo auditoría informática, es decir, se estarán realizando revisiones periódicas a las actividades informáticas que cada trabajador realiza, con la finalidad de detectar anomalías.

Instalación de Software que no es propiedad de El Concejo Municipal de Yumbo. Los usuarios que requieran la instalación de software que no sea propiedad El Concejo Municipal de Yumbo, deberán justificar su uso y solicitar su al supervisor del proceso para que remitas dicha solicitud al área de sistemas, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.

Si el dueño del software no presenta la factura de compra del software, procederá de manera inmediata a desinstalar dicho software porque se incurre en la violación sobre los derechos de autor que rigen en el territorio nacional.

Se considera una falta grave el que los usuarios instalen cualquier tipo de programa *(software)* en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la Personería municipal, que no tenga previa autorización para su uso.

Identificación del incidente: El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo de inmediato al superviso de proceso y/o al área de sistemas. Indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que la información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización se deberá dejar un registro del hallazgo y notificada al supervisor de proceso

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la personería municipal debe ser reportado al ingeniero de sistemas de la entidad.

Dicho incidente será reportado para que el personal de soporte se encargado de investigar la forma de solucionarlo.

Administración de la configuración: Los empleados y contratistas de El Concejo Municipal de Yumbo no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo si la autorización del supervisor del proceso y el área de sistemas.

Seguridad para la red: Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el área de sistemas o supervisor del proceso, en la cual los usuarios realicen la exploración de los recursos informáticos en la red la entidad, así como de las aplicaciones que operan sobre dicha red, con fines de detectar y mostrar una posible vulnerabilidad.

Uso del correo electrónico: Los usuarios no deben usar cuentas de correo electrónico asignadas por El

Concejo Municipal de Yumbo o se hacen responsable de la información que se maneje por este medio. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad El Concejo Municipal de Yumbo o Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó por la entidad.

El Concejo Municipal de Yumbo, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la entidad o realizado acciones no autorizadas.

Como la información del correo electrónico institucional personería municipal de yumbo es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

Los empleados y contratistas deben de utilizar el correo electrónico la entidad, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su cargo, quedando prohibido cualquier otro uso.

La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito o enviar un correo electrónico a supervisor del proceso el cual remitirá la orden atravesó del correo contacto @concejoyumbo.gov.co , señalando los motivos por los que se desea el servicio.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Controles contra código malicioso: Para prevenir infecciones por virus informáticos, los empleados y contratistas, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por personal de soporte.

Los empleados y contratistas, deben verificar que la información y los medios de almacenamiento como: memorias USB, discos duros externos y CD, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado proceso de bienes y tecnología evaluado por el personal de soporte.

El usuario debe verificar mediante el software de antivirus autorizado por la entidad que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

Ningún empleado y contratista de El Concejo Municipal de Yumbo debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autor replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software.

Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la entidad. El incumplimiento de este estándar será considerado una falta grave.

Ningún empleado y contratista o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de por el proceso de bienes y tecnología previamente evaluado por el personal de soporte.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo al personal de soporte, para la detección y erradicación del virus.

Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica al personal de soporte las actualizaciones del software de antivirus.

Los empleados y contratistas no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por personal de soporte.

Debido a que algunos virus son extremadamente complejos, ningún usuario de la entidad debe intentar erradicarlos de las computadoras, lo indicado es llamar al personal de soporte o el supervisor del proceso, para que sean ellos quienes solucionen esto.

Internet: El acceso a internet provisto a Los empleados y contratistas de El Concejo Municipal de Yumbo o es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el órgano interno de Control de la entidad.
Todos los accesos a internet tienen que ser realizados a través de los proveedores de internet pagados personería municipal de yumbo.

Los empleados y contratistas con acceso a Internet de El Concejo Municipal de Yumbo tienen que reportar todos los incidentes de seguridad informática a al personal de soporte o al supervisor del proceso, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

Obligaciones y/o monitoreo de usuarios que tienen el servicio de navegación en Internet

- **Serán sujetos de monitoreo de las actividades que realizan en internet.**
- **Saben que existe la prohibición al acceso de páginas no autorizadas.**
- **Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.**
- **Saben que existe la prohibición de descarga de *software* sin la autorización en proceso de bienes y tecnología atreves del personal de soporte.**
- **La utilización de internet es para el desempeño de su función y puesto en El Concejo Municipal de Yumbo o y no para propósitos personales.**

9.4. CUARTA POLÍTICA GENERAL: "POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO"

POLÍTICA: Cada usuario es responsable del mecanismo de control de acceso que le sea

proporcionado; esto es, de su identificador de usuario (UserID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica Personería municipal de yumbo, por lo cual deberá mantenerlo de forma CONFIDENCIAL.

Control de acceso lógico

Todos los consultores externos que realicen actividades de manera conjunta con el personal El Concejo Municipal de Yumbo en lo que respecta la Infraestructura tecnológica, requieren previamente obtener un permiso del supervisor del proceso donde estarán brindando la asesoría especializada o desempeñando la actividad por la cual fueron contratados, posteriormente, el Titular de esa Área, de soporte o proceso de bienes y tecnología, explicando:

- ✓ **El motivo por el cual se les debe dar acceso a la infraestructura Tecnológica**
- ✓ **El tiempo que requiere el acceso lógico**

Está prohibido que los usuarios utilicen la infraestructura tecnológica de la entidad para obtener acceso no autorizado a la información u otros sistemas de información de El Concejo Municipal de Yumbo o

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la entidad, a menos que se tenga autorización el supervisor de proceso respaldado por el proceso de bienes y tecnología.

Cada empleado y contratista que accede a la infraestructura tecnológica de El Concejo Municipal de Yumbo o debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de Usuario por varios usuarios.

Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

Los empleados y contratistas tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

Equipo desatendido: Activar protector de pantalla.

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados y autorizados por el personal de soporte, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

Apagar computadoras y recursos tecnológicos cuando termina la jornada laboral

Los usuarios deben pagar sus computadoras u otros recursos tecnológicos cuando hayan terminado su jornada laboral diaria con la finalidad de proteger los equipos ante eventuales cortes de energía eléctrica.

Administración y uso de Passwords: La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

Cuando un usuario olvide, bloquee o extravíe su contraseña deberá reportarlo por escrito al proceso de bienes y atreves del supervisor del proceso, o enviando un correo electrónico a contacto@concejoyumbo.gov.co, indicando si es de acceso a la red o a los recursos compartidos, para que se le proporcione una nueva contraseña.

Está prohibido que los identificadores de usuarios y contraseñas se encuentren en forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera que se permita a personas no autorizadas su conocimiento.

Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- **No deben ser números consecutivos**
- **Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos, o sea, números y letras.**
- **Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.**
- **Deben ser diferentes a las contraseñas (*passwords)* que se hayan usado previamente.**

La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

Los cambios o desbloqueo de contraseñas solicitados por el usuario a supervisor de proceso quien remitirla la solicitud al proceso de bienes y tecnología serán solicitados mediante oficio sellado y firmado por el jefe inmediato del usuario que lo requiere.

Control de accesos remotos: Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del personal de soporte.

La administración remota de equipos conectados a internet no está permitidos, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado el proceso de bienes y tecnología.

9.5. QUINTA POLÍTICA GENERAL: "POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD NFORMÁTICA

POLÍTICA: De acuerdo al Reglamento Interior de El Concejo Municipal de Yumbo "el proceso de bienes y tecnología tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

Derechos de Propiedad Intelectual: Está prohibido por las leyes de derechos de autor y por el Concejo municipal realizar copia no autorizadas de *software*, ya sea adquirido o desarrollado por El Concejo Municipal de Yumbo.

Revisiones del cumplimiento: El proceso de bienes y tecnología, realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Los empleados y contratistas.

El proceso de bienes y, podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

Violaciones de seguridad informática: Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el proceso de bienes y tecnología evaluados previamente por el personal de soporte y los fines de tal actividad.

Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del proceso de bienes y tecnología atreves del personal de soporte, con excepción de los Órganos Fiscalizadores.

Ningún empleado o contratista de El Concejo Municipal de Yumbo, debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el proceso de bienes y tecnología previamente evaluados por el personal de soporte.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, o similares diseñado para autor replicarse, dañar o afectar el desempeño o acceso a las computadoras del concejo municipal de yumbo