CONCEJO MUNICIPAL DE YUMBO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024-2027

Sistema Integrado de Gestión - SIG

Proceso Gestión Tecnologías de la Información – GTI
1-10-2024

CONTENIDO

1. 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.

2. MARCO REGULATORIO Y NORMATIVO

El Concejo Municipal de Yumbo, como entidad pública, está sujeta a un marco normativo y regulatorio relacionado con la seguridad de la información y a las buenas prácticas en la seguridad de la información definidas por entidades entes regulatorio en la emisión y normalización de metodologías y buenas prácticas a nivel mundial.

A continuación, se tienen las normas, decretos y disposiciones legales que aplican al Concejo municipal de Yumbo en lo establecido del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Ley 23 de 1982. Sobre derechos de autor.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 594 de 2000. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula

el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Decreto 2693 de 2012 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- Decreto 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Decreto 415 de 2016 “en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”
- Ordenanza departamental 430 de 2016 “Política TIC que busca convertir al departamento en un territorio inteligente e innovador”
- Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”
- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos”
- Guía Técnica Colombiana GTC-ISO/IEC 27002 “Tecnología de la información. Técnicas de seguridad. Código de Practica para Controles de Seguridad de la Información”
- Norma Técnica Colombiana NTC-ISO 31000 “Gestión del Riesgo. Directrices”

3. OBJETIVOS GENERALES Y ESPECÍFICOS

3.1. OBJETIVOS GENERALES

Garantizar la continuidad de las actividades de El Concejo Municipal de Yumbo, fundamentada de acuerdo al Modelo de Seguridad y Privacidad de la Información en el establecimiento de lineamientos que permitan proteger, asegurar y salvaguardar la integridad, confidencialidad, disponibilidad y privacidad de los activos de información del Concejo de Yumbo, que ponen en riesgo el normal funcionamiento de los procesos misionales asociadas a las Tic, a fin de minimizar, prevenir y responder de forma oportuna ante cualquier eventualidad. Con su información busca que todos los servidores públicos, contratistas, particulares y/o terceros, la política de seguridad de la información y contribuyan al aseguramiento un adecuado trato de los activos de información del Concejo de Yumbo.

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.)

4.1. 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. 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 PETI.
- Plan de Contingencias Informático.
- actividades de soporte técnico a los usuarios y equipos con que cuenta la entidad.

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

5.1. 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

5.2. 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
- 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.

- 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 del servicio a la comunidad.

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 centro de cómputo está provisto de una Temperatura autorregulada

6. IDENTIFICACION DE PROCESOS CRITICOS

6.1. FACTORES CRÍTICOS A CONSIDERAR

6.2. 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.

6.3. 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

6.4. 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.

7. 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.

7.1. 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 en la entidad.

7.2. 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.

7.3. Prioridad Baja

Se les 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.

Criticidad A: (Máxima)

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

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.

Criticidad C: (Mínima)

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

8. POLITICAS DE SEGURIDAD

8.1. 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.

8.2. 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**.**
- Alinear las Políticas en Seguridad Informática según lo establece las mejores prácticas de ISO/IEC: 27002:2013 así como la norma ISO 27001:2013.
- 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.

9. 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.

9.1. OBLIGACIÓNES DE LOS PROCESOS MISIONALES Y SUS INTEGRANTE

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

10. 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, 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.

11. 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 concejo 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 analenis@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.

- 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.
- 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.

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.

12. 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.

- 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.

- 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 del concejo municipal de yumbo debe ser reportado al ingeniero de sistemas de la entidad.
- 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.
- 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.
- 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.

13. 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, 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
- 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.
- 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.
- 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.

14. 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.

- 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.

- 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.

15. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

Se genera el plan de implementación de la seguridad de la información, se ejecuta de acuerdo al cronograma:

ESTRATEGIA	GESTIÓN	ACTIVIDAD	PROCESO	RESPONSABLE	Fechas	
					INICIO	FINAL
Seguridad de la información Privacidad de los datos	Activos de la información	Lineamientos para el levantamiento de activos de información	Actualizar los activos de información	TIC	FEB	MAR
		Publicación de activos de información	Consolidar el inventario de activos de Información.	TIC	ABR	ABR

	Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	TIC	MAY	MAY
		Sensibilización	Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	TIC	JUN	JUN
	Monitoreo	Revisión de los riegos	Seguimientos de los riesgos	TIC	JUL	DIC

16. CONTROL DE CAMBIOS

El concejo municipal de yumbo establece como única documentación vigente la ubicada en el sistema integrado de gestión - SIG en el drive establecido por la corporación, la cual entra en vigencia a partir de su aprobación, toda copia de este se considera COPIA NO CONTROLADA.
Los documentos obsoletos se les da de baja del Sistema Integrado de Gestión – SIG activo.

Versión	Fecha edición (dd/mm/aa)	Naturaleza del cambio
1	30/01/2024	Elaboración del Plan (Versión 1) 2024.
2	01/10/2024	Actualización del mapa de procesos de la corporación, ajuste del proceso de gestión de bienes y servicios, creando de manera independiente el nuevo proceso gestión tecnologías de la información, actualización del formato de caracterizaciones de procesos, estructuración del nuevo sistema integrado de gestión y actualización de la codificación para normalizar procesos, procedimientos y documentos relacionados.

17. RUTA DE APROBACION

Versión 2					
Elaboró o actualizó		**Revisión metodológica**		**Aprobó**	
Nombre	Diego Fernando Amaya M.	Nombre	Ana L. Lenis Zuluaga	Nombre	Uriel Urbano Urbano
Cargo	Profesional apoyo a la gestión - Proceso GTI (contratista)	Cargo	Auxiliar Administrativo	Cargo	Secretario General