2017

PLAN DE CONTINGENCIA Y POLÍTICAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

[Escriba el subtítulo del documento]

[Escriba aquí una descripción breve del documento. Normalmente, una descripción breve es un resumen corto del contenido del documento. Escriba aquí una descripción breve del documento. Normalmente, una descripción breve es un resumen corto del contenido del documento.]

s

Personeria Municipal de yumbo

01/03/2017

INTRODUCCION

La Personería 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.

1. OBJETIVOS GENERALES Y ESPECÍFICOS

1.1. OBJETIVOS GENERALES

Garantizar la continuidad de las actividades de la Personería Municipal de Yumbo, 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.

1.2. 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 la Personeria 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

2. 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 la Personería Municipal de Yumbo, asi cómo 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 la Personería Municipal de Yumbo; 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.).

El desarrollo de las actividades y proyectos, está condicionado a la aprobación del personero Municipal y del recurso que se asignen para tal fin.

3. 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.

3.1. 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 la Personería 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.

3.1.1. 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

3.1.2. 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 gestion Documental(Orfeo), el proceso contable(ASCII) y contratación de los 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 respectivo 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 la Personeria 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 computo del cuarto de sistemas. Sin embargo swe 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, la Personería Municipal de Yumbo 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 del 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.

.

4. IDENTIFICACION DE PROCESOS CRITICOS

4.1. FACTORES CRÍTICOS A CONSIDERAR

4.1.1. 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**.**

4.1.2. Personal

- Funcionarios que administran procedimientos de ingreso y altas en los 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

4.1.3. 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.

4.2. 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 la Personería Municipal de Yumbo.

4.2.1. Prioridad Alta

Corresponde a todas aquellas herramientas de la Personería 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.

4.2.2. Prioridad Media

Se le asigna a todas aquellas herramientas de la Personería Municipal de Yumbo, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de servicio, cuentan con procedimientos alternativos

4.2.3. Prioridad Baja

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

4.2.4. Criticidad A: (Máxima)

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

4.2.5. 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.

4.2.6. Criticidad C: (Mínima)

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

5. PLAN DE RESPALDO

Para asegurar que se consideran todas las posibles eventualidades, se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para la Personeria Municipal de Yumbo.

N°	**ACTIVIDAD**	**ELEMENTOS**	**RESULTADO**
1.	Copias de seguridad de la información y documentos residentes en los discos duros de los computadores	Documentos en formatos Word, Excel, PDF, artes, imágenes, audio y correos electrónicos	