PLAN DE CONTINUIDAD TECNOLÓGICA

OFICINA TIC Tecnologías de la Información y las Comunicaciones

Contenido

1. INTRODUCCION

El plan de contingencia de la oficina TIC es una estrategia planificada, con una serie de actividades que nos facilitan o nos orientan, a restablecer los servicios TI ante un evento o incidente que los afecte de forma parcial o total.

Este documento establece los lineamientos de respuesta para atender de forma efectiva, eficiente y eficaz, daños en la infraestructura TI ante desastres producto de eventos naturales u otros, que le causen algún incidente tanto interno como externo.

Durante el desarrollo del presente Plan, se presentan aspectos conceptuales que permitan un mayor panorama acerca del entendimiento de las contingencias y que servirán como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencia.

2. OBJETIVO

- Garantizar la continuidad de la operación de la infraestructura TI de la Alcaldía Municipal de Acacías Meta, estableciendo procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- Identificar al personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Identificar los riesgos presentes para la continuidad.
- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

3. ALCANCE

El Plan de Contingencia TIC que se desarrolla en el presente documento cubre a la infraestructura TI (Hardware y Software) de la Alcaldía Municipal de Acacías Meta, Instalada

en el Data Center ubicado en la sede principal en la Carrera 14 # 13 – 30 del municipio de Acacias Meta, administrado por la Oficina TIC donde se centraliza toda La información que se maneja en la administración Municipal, materia prima para la toma de decisiones y complimiento de sus objetivos misionales y estratégicos.

Servicios:

1. Sistema de Información
2. Página web de la entidad.
3. Sistema control Documental
4. Servidor de Dominio
5. Plataformas de Monitoreo de Red
6. Telefonía IP
7. Internet
8. Firewall
9. Almacenamiento.

4. DEFINICIONES

AMENAZA: Se refiere a la potencialidad que tiene un evento natural, una actividad humana o una acción mecánica, de causar daños o destrucción independiente de la existencia en el área amenazada de habitantes y/o bienes materiales.

EMERGENCIA: Situación que aparece cuando, en la combinación de factores conocidos, surge un fenómeno o suceso que no se esperaba, eventual, inesperado y desagradable por causar daños o alteraciones en las personas, los bienes, los servicios o el medio ambiente, sin exceder

IMPACTO: Acción directa de una amenaza o riesgo en un grupo de personas.

MITIGACIÓN: Son todas aquellas medidas de prevención conducentes a disminuir total o parcialmente el grado de vulnerabilidad a que están sometidos elementos bajo riesgo.

PLAN: Documento que permite organizar, dirigir y desarrollar una actividad de manera controlada.

PREVENCIÓN: Es equivalente a decir que mediante la intervención directa del peligro puede evitarse su ocurrencia, es decir impedir la causa primaria del desastre.

PROCEDIMIENTO: Una manera especificada de efectuar una actividad. (NTC ISO 8402). Un procedimiento escrito o documentado generalmente contiene: los propósitos y el alcance de una actividad, lo que se debe hacer, quien lo debe hacer, como se debe hacer, que documentos se deben usar, y como se controlara y registrara dicho procedimiento.

REDUCCIÓN: Término que agrupa los conceptos de prevenir la ocurrencia, mitigar las pérdidas, prepararse para las consecuencias y alertar la presencia.

RIESGO: Se refiere a las consecuencias esperables al ocurrir un fenómeno natural o una actividad humana, en término de muertes o heridas causadas a la población y a la destrucción de propiedades o de cualquier tipo de pérdida económica.

ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA – BUSINESS IMPACT ANALYSIS): mediante la definición de los servicios críticos de la Entidad, se realiza una priorización de los mismos, con el fin de asignar el tiempo de recuperación, en caso de presentarse algún tipo de interrupción. De tal manera que si el servicio tiene mayor prioridad, su tiempo de recuperación debe ser menor con respecto a los servicios que tienen menor prioridad.1

EVENTO DISRUPTIVO: son los sucesos que se pueden presentar, como por ejemplo pérdida de servicio, falla de seguridad, desastres naturales.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO: es el proceso mediante el cual se identifican las amenazas potenciales y el impacto que pueden causar en caso que se materialicen; de tal forma que busca que la Entidad tenga una mayor capacidad de resistencia, dando una respuesta oportuna a salvaguardar la información y lo más importante, la reputación que tiene hacia las partes interesadas.

PLAN DE CONTINGENCIA: en estos planes se definen las actividades realizadas a diario, las cuales en el momento que se requiera puedan ser restauradas, de acuerdo al evento o incidente que se pueda presentar.

SERVICIOS TECNOLÓGICOS CRÍTICOS DE LA ENTIDAD: estos servicios son aquellos que se encuentran en la plataforma tecnológica, los cuales son usados como medio de trabajo, por los procesos para desarrollar algunas de las actividades que permiten el desarrollo de la misión de la Entidad.

5. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Manual de Políticas de Seguridad la información GTIC-M-01 se describe la gestión de la continuidad del negocio, a partir de Seguridad de la Información y enfocado en los servicios que se encuentra bajo la responsabilidad y gestión del Área de Tecnologías y Sistemas de Información.

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

6. RESPONSABLE

El Jefe de la Oficina TIC o quien haga sus veces es el responsable de la ejecución del Plan de Contingencia y, además:

1. Deberá definir la ubicación para instalar el Data Center alterno.
2. Definir las actividades para la configuración y/o instalación de los nuevos servicios.
3. Dirigir las pruebas necesarias hasta el correcto funcionamiento de los servicios.
4. Mantener informados a los Jefes de Secretarias, Jefes de Oficina y comunidad sobre la ejecución del Plan de Contingencia (tiempo que toma restablecer los servicios, estado del Plan de contingencia)
5. Aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la ejecución del Plan Contingencia.
6. Mantener actualizado el Plan de Contingencias de TI.

7. REQUISITOS DE GESTIÓN DE CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Se define en el Manual de Políticas de Seguridad de la Información GTIC-M-01, la Gestión de continuidad del negocio, de tal forma que indica:

“Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Prevenir interrupciones en las actividades de la plataforma informática de la Alcaldia de Acacias que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de la Alcaldía de Acacias podrán ser restaurados dentro de escalas de tiempo razonables.

La alcaldía de Acacias deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de la Alcaldia de acacias de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La continuidad del negocio deberá ser gestionada por la Dirección de la Alcaldia de Acacias.

La alta dirección de la alcaldía de Acacias será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La alta dirección, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

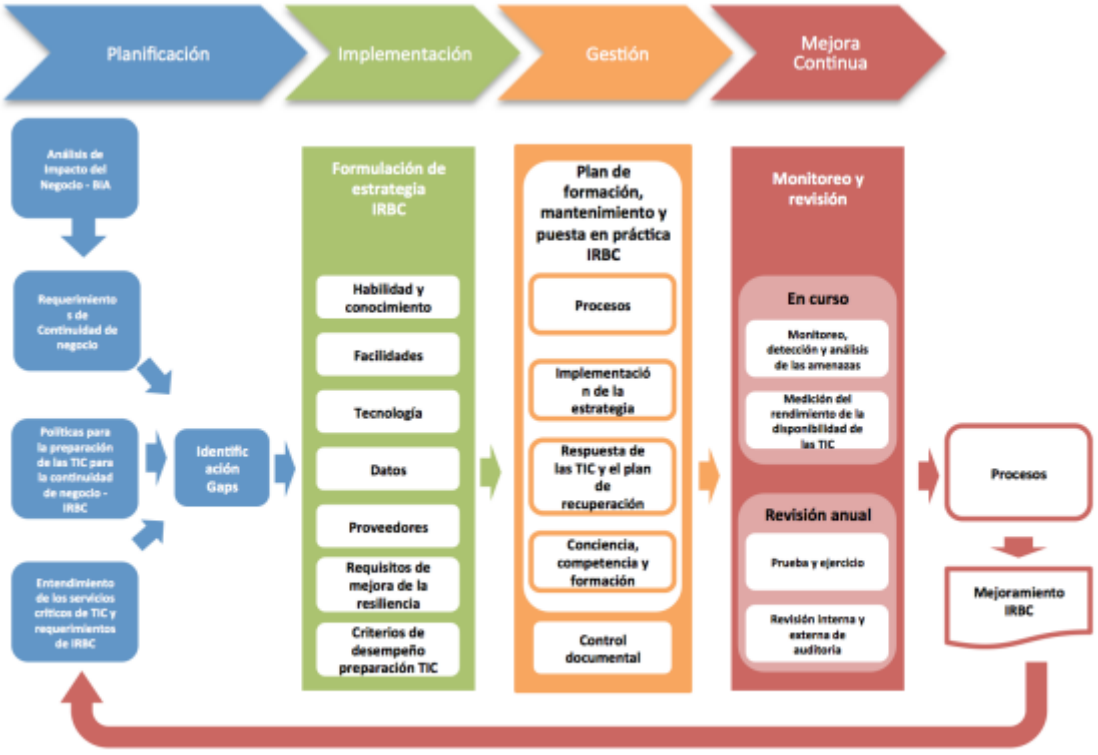

Ilustración 2 – Marco Continuidad del Negocio para Seguridad y Privacidad de la Información

8. SERVICIOS TECNOLOGICOS CRITICOS

Los Servicios Tecnológicos críticos de la Entidad, se denominan de esa forma por la importancia que se deriva de ellos en el desarrollo de las labores de la entidad a diario, permitiendo ser de ayuda en la consecución de la misión, mediante el desarrollo de las actividades realizadas por los funcionarios, contratistas y colaboradores de la Alcaldia de Acacias; Estos sistemas de misión crítica son aquellos a los cuales se les asigna una mayor prioridad para el momento que se requiera la activación de los planes de contingencia, por su importancia, dado que les facilita a los usuarios de la plataforma tecnológica el desarrollo de sus actividades.

Los servicios que están contemplados para el análisis de impacto, son algunos de los que se encuentran definidos en el Catálogo de Servicios TI:

Sitio Web principal de la Entidad
Internet
Correo electrónico – google Workspace
Sistema Financiero

Estos servicios son elegidos por la razón, que en caso que suceda alguna interrupción de los mismos, la importancia para la Entidad de su disponibilidad tiene un margen alto y medio.

8.1 Prioridad de los servicios

Se define el orden de atención de los servicios de misión crítica que brinda el proceso de tecnología de información y comunicaciones, definidos de esa forma por su importancia para el desarrollo de las actividades encaminadas al desarrollo de la misión de la Entidad, por parte de los funcionarios, contratistas y colaboradores de la alcaldía de Acacias.

A continuación, se visualiza la prioridad de atención de los servicios críticos:

SERVICIO	PRIORIDAD
Sitio Web principal de la Entidad	Alta
Internet	Alta
Correo electrónico – google Workspace	Media
Sistema Financiero	Alta
Sistema Contable	Alta
Sistema de Gestión Documental	Media

9. POSIBLES EVENTOS O AMENAZAS

Estos eventos son las amenazas naturales, accidentales o provocados que pueden afectar el normal servicio de la infraestructura TI de la Alcaldía de Acacias Meta, poniendo en riesgo los servicios ofrecidos a través de ella a los usuarios internos y externos de la entidad.

1. **Ataque Informático:** Por ser una empresa del sector oficial y debido a su actividad económica, se convierte en posible blanco de ataques de ciberseguridad.

2. **Incendio:** Se podría dar por actos inseguros, por condiciones inseguras de las redes eléctricas (cableado sin empotrar, tomas sobrecargadas), por cortos circuitos, conexiones hechizas, entre otros.

   Se aprecia presencia de carga combustible representada en papelería, archivos, escritorios y sillas de madera. Posibles condiciones inseguras en el almacenamiento de líquidos inflamables (combustible de la planta eléctrica).

3. **Inundación:** Se puede presentar a causa de lluvias torrenciales que por su intensidad y duración puedan causar inundación en las oficinas del piso superior del Edificio principal de la ALCALDÍA MUNICIPAL DE ACACÍAS o en las áreas expuestas a ventanales, también se puede presentar inundaciones por daños en tuberías. Se calificó esta amenaza como Probable**.**
4. **Terremoto:** El municipio de Acacías se encuentra ubicado en el departamento del Meta, cuyo territorio en un 79,30% se encuentra en una zona que está amenazada por fenómenos sísmicos de alta y mediana intensidad, fenómeno dado por estar ubicado sobre dos grandes fallas geológicas.

5. **Terrorismo:** Por ser una empresa del sector oficial y debido a su actividad económica, se convierte en posible blanco de organizaciones y grupos delictivos al margen de la ley. Se puede presentar esta amenaza a través de la instalación de paquetes bomba o carros bomba o cualquier tipo de elemento susceptible de ser cargado con explosivos. Su calificación es probable**.**

6. **Tormenta eléctrica**: No se descarta la posibilidad de descargas eléctricas, se calificó esta amenaza como posible. La edificación es vulnerable a la acción de este fenómeno atmosférico, por la complejidad de equipos y redes eléctricas.

7. **Hurto, robo, atraco:** Es probable, teniendo en cuenta las características del servicio público de la Alcaldía de Acacías y por la visita de gran número de personas que se presenten robo de equipos y/o bienes de la empresa y los trabajadores. Existen antecedentes de hurto en el edificio principal. Se calificó esta amenaza como Probable.

10. ACCIONES PREVENTIVAS

ITEN	ACTIVIDAD	PERIDICIDAD
1	Actualizaciones de Aplicativos (Sistemas operativos, Antivirus, Firewall, etc)	SEMANAL
2	Garantizar la temperatura del centro de datos.	SEMANAL
3	Realizar Backup de los servicios TI	SEMANAL
4	Tener los extintores recargados	TRIMESTRAL
5	Realizar mantenimientos preventivos de equipos (servidores, switch, AA, UPS, etc)	ANUAL
6	Realizar Inspecciones locativas (revisión de goteras, humedades)	SEMANAL
7	Participación de los funcionarios de la Oficina TIC en los simulacros de emergencias.	TRIMESTRAL
8	Control de acceso de visitantes al centro de datos.	DIARIO
9	Circuito cerrado de televisión	MENSUAL

11. PLAN DE CONTIGENGIA

En caso de un evento se debe realizar como mínimo las siguientes actividades con el fin de restablecer lo más rápido posible los servicios ofrecidos por la infraestructura TI.

1. **Desenergizar los Equipos:** Desconectar los equipos afectados de la energía eléctrica, apagar breaker de alimentación de energía si es necesario.
2. **Desconectar equipos de la Red:** Con el fin de evitar de que falla afecte a mas equipos de la Red en necesario desconectar el equipo afectado de la intranet.
3. **Revisión Técnica:** Se procede a la revisión técnica del hardware y software afectado.
4. **Identificar los equipos y servicios afectado:** Realizar un inventario de los equipos y sus servicios afectados, con los elementos necesarios para restablecerlos en el menor tiempo posible.
5. **Identificar los servicios prioritarios:** Se deben identificar los servicios prioritarios con el fin de que sean los primeros restablecidos.
6. **Construir un plan de Trabajo:** Realizar un plan que tengas las actividades para restablecer los servicios TI de acuerdo a su importancia.
7. **Adquisición para las partes dañadas:** Según el caso se procede a la solicitud de adquisición o al proceso contractual para la compra de los elementos dañados.
8. **Revisar la seguridad:** Revisar los controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles. Se deben estar preparado para cualquier percance, verificando que dentro de datos de la Secretaría de TIC se cuente con los elementos necesarios para salvaguardar sus activos.
9. **Verificación de Backup**: Se debe validar que se tenga copia de seguridad de los servicios o equipos afectados con el fin optimizar la reparación.
10. **Instalación y configuración**: Instalación de los equipos, sistemas operativos, y restauración de las bases de datos con último Backup realizados.
11. **Pruebas de los servicios:** Verificación de puesta en marcha de los equipos y los servicios restablecidos después del plan de contingencia.
12. **Envió de Comunicación:** Enviar comunicado informando la superación de las fallas.

12. REGISTROS

DOCUMENTOS Y REGISTROS RELACIONADOS	
Código	**Nombre**
GTIC - F - 08	Reporte ingreso para servicio manto a cuarto de comunicaciones
GSIG – PL – 03	Plan de Emergencias
GTIC - F - 23	Bitacora Backup

14 CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Fecha de aprobación	**Código**	**Versión**	**Descripción y razón del cambio**
02/110/2021	GTIC – PL – 03	1	Creación de Documento

ELABORÓ	REVISÓ	APROBÓ
Edwin Rafael Coba Saldaña Cargo: Profesional Seguridad y Privacidad de la informacion	Esther Rodríguez Garavito Cargo: Profesional Especializado SIG	Edilberto Romero Trujillo Cargo: Jefe Oficina de Tecnologías de la Información y las Telecomunicaciones