



MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL

PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI

OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA

Código: STI-TIC-IIS-PR-003

Fecha: 21-09-2019

Versión: 001

Página: 1 de 12

PROCEDIMIENTO PLAN DE CONTINGENCIA

**SECRETARIA DE TECNOLOGIA,
INFORMACION, COMUNICACIONES,
CIENCIA E INNOVACION (SETIC-CeI)
BARRANCABERMEJA, ENERO 2020**

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 2 de 12

OBJETIVO

Proporcionar un plan de contingencia tecnológico que proporcione los procedimientos y las instrucciones necesarias que permitan el restablecimiento de la plataforma tecnológica (Servicios, procesos y operaciones TI) de la administración Municipal de Barrancabermeja en caso que se presente una eventualidad como un siniestró ocasionado por fenómeno natural o producto de actos terroristas, actos vandálicos etc.

ALCANCE

La información es el principal activo de cualquier organización, por eso la importancia de desarrollar procedimientos, normas y demás documentos que conlleven a la protección de la información de la organización. En mundo globalizado donde todos los procesos administrativos y de servicios son gestionados a través de la prestación de servicios eficientes donde la tecnología juega un papel importante. Surge la necesidad y responsabilidad de la protección de la información, medios tecnológicos y ambiente de operación. La administración Municipal cuenta con un Centro de datos gestionado por la Secretaria SETIC-CEI donde se centraliza toda La información que se maneja en la administración Municipal, materia prima para la toma de decisiones y cumplimiento de sus objetivos misionas y estratégicos de la entidad.

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 3 de 12

En el centro de datos se concentra todos los servicios la administración municipal tales como:

- Correo institucional
- Portal web
- Sistemas de información
- Directorio activo
- Telefónica IP
- DNS
- ISP
- Bases de datos
- Servidor de Dominio
- Copias de Seguridad

La cantidad de datos guardados en los medios y equipos de almacenamiento son considerados como la vida de nuestra entidad y su integridad va relacionada con su pérdida o destrucción intencional o no intencional. Todos los funcionarios que trabajan para la Administración Municipal tienen la responsabilidad directa o indirectamente de ayudar a garantizar el buen uso y operación de bienes informáticos. La Secretaria SETIC-CEI gestiona la apropiación y la adopción de medidas de seguridad para proteger su información.

PLAN DE ACCIÓN PARA EL RESTABLECIMIENTO DE SERVICIOS

En caso de un siniestro, ataque informático o terrorismo se debe contar con procedimiento con el fin que permita el restablecimiento de los servicios informáticos lo más pronto posible.



- a. **Identificar los servicios afectado y la gravedad:** Se debe hacer un inventario de los daños ocasionados y lo que se requiere para el restablecimiento e los servicios independiente del tiempo que tome.
- b. **Realizar un levantamiento de los servicios informáticos:** Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.
- c. **Identificar un conjunto de amenazas:** Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc. Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.
- d. **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 SETIC-CEI se cuente con los elementos necesarios para salvaguardar sus activos.
- e. **Identificar los servicios prioritarios:** Se deben identificar los servicios prioritarios o fundamentales para el funcionamiento de la Administración municipal, por medio de flujogramas de procesos específicos para medir el alcance de cada actividad.

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 5 de 12

PROCEDIMIENTO

1. Establecer un grupo de trabajo y definir roles

En caso de presentarse algún tipo de inconveniente que amerite iniciar el Plan de Contingencia Informático, los Líderes del proceso afectado o afectados de común acuerdo establecerán los roles y acciones a tomar para reactivar el servicio, corrigiendo de forma definitiva o parcial la inconsistencia. El Secretario SETIC-CEI es el responsable de aprobar la realización del Plan de contingencia Informático, dirigir un comunicado a los Jefes de Secretarías de las diferentes áreas involucradas informando el tiempo que toma restablecer los servicios. Al declararse una contingencia el Secretario TIC, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alternativo y autorizará las inversiones a realizar, así como el fondo de efectivo a asignarse para los gastos necesarios iniciales.

El Secretario TI mantendrá permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión. el Secretario TIC, Coordinará la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del Plan, de forma coordinada con el (los) Secretario (s) de Despacho involucrados en las acciones a tomar.

Al término de la realización de las pruebas, será el Secretario TIC, quien da visto bueno de la conclusión de éstas y de los resultados obtenidos, rindiendo un informe



de forma coordinada con los responsables de proceso involucrados, y en caso de ser necesario, convocar a la realización de una segunda prueba, corrigiendo previamente las fallas que se hubieran presentado. Una vez que se encuentre aprobado el Plan de Contingencia, será el líder de proceso quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal a la aplicación del Plan, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades, será el responsable de dar por concluida la declaración de contingencia por escrito o vía electrónica. A los Secretarios y todo el personal de la Administración Municipal. El Secretario SETIC-CEI será el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, servicios de internet, intranet, correo electrónico y red de la de la Administración Municipal, mantener actualizados dichos procedimientos en el plan de contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switches, antenas, etc). Así mismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica. El Secretario SETIC-CEI y el personal a su cargo, son los responsables de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan de Contingencia Informático. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total. El Secretario SETIC-CEI y el personal a su cargo son los responsables de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, CD Writer, escáneres, faxes, copadoras, etc., mantener los equipos en óptimas condiciones de funcionamiento; determinar la



cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la administración Municipal; todos los Usuarios deberán realizar el respaldo de la información en sus equipos de cómputo, El secretario SETIC-CEI es el responsable de la copia de respaldos de cada uno de los servidores o equipos en donde se procese la información, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático.

En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores. Para tal efecto deben participar en pruebas del Plan de Contingencia en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia. El Secretario TI, y el personal a su cargo serán los responsables de determinar los sistemas críticos, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Secretario TIC, deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación.

Los funcionarios de la Administración Municipal en coordinación con la Unidad de Riesgo, desastres y brigadistas, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 8 de 12

compañeros de trabajo, cuando la situación que se estuviera presentando sea grave (incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes de la Alcaldía Municipal (el propio inmueble, equipos, documentación importante, etc.).

2. Determinar los eventos que pueden afectar adversamente en la Alcaldía Municipal y su infraestructura, con interrupción o desastre en materia informática

Los desastres y crisis son eventos que pueden inhabilitar a la Alcaldía de Barrancabermeja de proveer normalmente sus servicios a los usuarios internos y la atención al público en general, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención.

Identificación de amenazas

- Terremoto
- Incendio
- Inundación y humedad
- Corte de energía
- Falla de la red de voz y datos
- Fallas en hardware o software
- Sabotaje o daño accidental
- Vandalismo y manifestaciones

Las operaciones de la administración Municipal, pueden ser afectadas en menor o mayor medida por los distintos siniestros tanto naturales, accidentales o

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 9 de 12

provocados. Tomando en cuenta los resultados del Análisis de Riesgos realizado y los riesgos residuales.

TERREMOTO

SIN PÉRDIDA O DAÑOS MENORES DE LAS INSTALACIONES:

El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto provocaría en la Alcaldía sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.

CON PÉRDIDA DE LAS INSTALACIONES:

La pérdida de las instalaciones afectaría gravemente a las operaciones de la alcaldía Municipal y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

INCENDIO (AREA DE CÓMPUTO):

Se tiene gran impacto en la información ya que los sistemas utilizados residen en los servidores y dispositivos de comunicación localizados en el Area de Cómputo y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de



instalar nuevamente el sistema, configurar el Servidor y restaurar los respaldos para continuar trabajando.

ÁREAS DISTINTAS AL AREA DE CÓMPUTO:

Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el Centro de Cómputo. En el caso de las primeras el impacto que tendría en la Alcaldía de Barrancabermeja es menor, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto.

CORTE DE ENERGÍA

Las operaciones informáticas de la Alcaldía de Barrancabermeja se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolonga por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos.

FALLAS EN HARDWARE O SOFTWARE

Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo, si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

SABOTAJE O DAÑO ACCIDENTAL

	MUNICIPIO DE BARRANCABERMEJA - ALCALDIA MUNICIPAL		
	PROCEDIMIENTO PLAN DE CONTINGENCIA SECRETARIA SETIC-CeI		
	OPERACIONES TI - INFRAESTRUCTURA TECNOLÓGICA		
Código: STI-TIC-IIS-PR-003	Fecha: 21-09-2019	Versión: 001	Página: 11 de 12

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran reprocesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles.

VANDALISMO Y MANIFESTACIONES

Un intento de vandalismo ya sea menor o mayor, podría afectar a las PC's, periféricos y servidores, así como las comunicaciones, si el intento de vandalismo es mayor, se presenta un grave riesgo dentro de las instalaciones debido que a palacio Municipal donde se encuentra el centro de datos hay ingreso de personal público ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado a la ciudadanía.

A continuación de menciona en forma enunciativa una serie de medidas preventivas:

- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación.

A continuación, se menciona en forma enunciativa una serie de medidas preventivas en caso de presentarse un paro total de las operaciones.

- Determinar lugares especiales, fuera del centro de datos, para almacenar los respaldos y una copia de la documentación de referencia.



3. Evaluar la efectividad de los controles y dispositivos de seguridad

Se debe contar con un sistema de seguridad en materia informática, realizando diversas actividades laborales, previniendo las posibles causas, condiciones de accidentes y siniestros, es necesario determinar las medidas más convenientes y llevarlas a cabo realizando inspecciones periódicamente.

Elaboró:	Ingeniero: Marino Rodríguez Palacios
Cargo:	Profesional Universitario – Coordinador de grupo funcional Operaciones TI - Plataforma tecnología
Responsable:	Ingeniero: Marino Rodríguez Palacios
Cargo:	Profesional Universitario – Coordinador de grupo funcional Operaciones TI - Plataforma tecnología

Aprobó:	Ingeniera. PATRICIA HELENA FIERRO VITOLA
Cargo:	Secretaria SETIC-Cel