MANUAL POLITICA DE GESTION DE CONTINUIDAD RESPECTO A LOS SERVICIOS TIC

INDICE

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

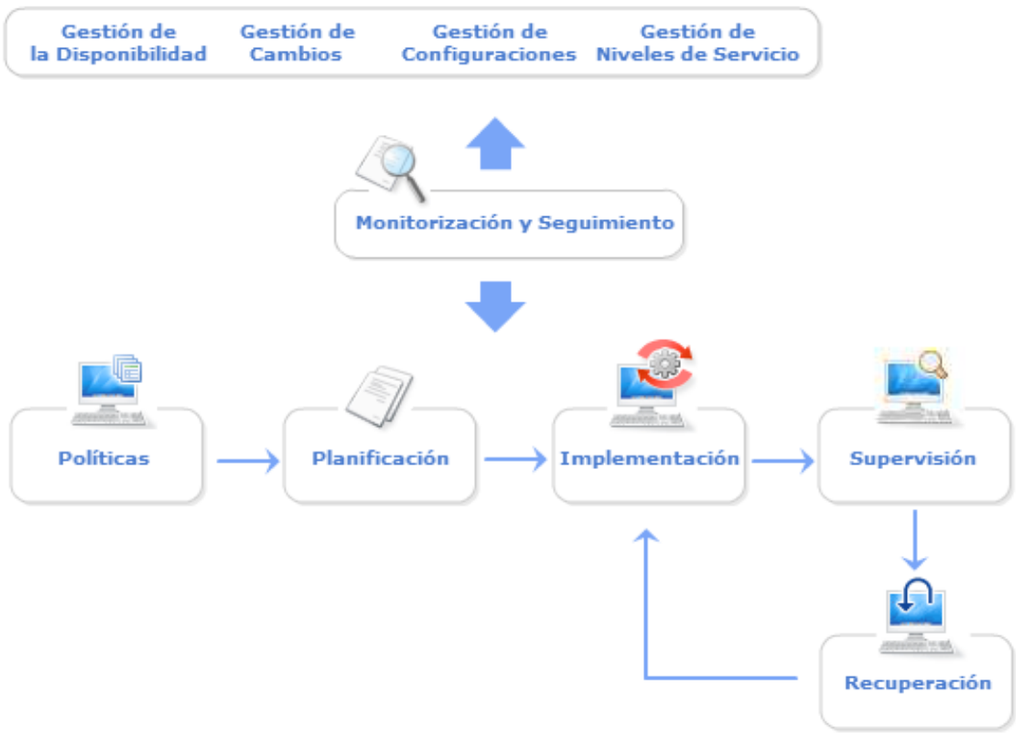
1. INTRODUCCION.

La Gestión de la Continuidad del Servicio se preocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para la Entidad.

La estrategia de la Gestión de la Continuidad del Servicio, debe combinar equilibradamente procedimientos:

- **Proactivos:** que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos:** cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

Visión General



2. OBJETIVO GENERAL

El objetivo de la Gestión de la Continuidad es actuar proactivamente preparando planes de contingencia para ocasiones de desastre, asegurando que la Infraestructura (técnica y de servicios) puede recuperarse cuando así se requiera y según los acuerdos y tiempos establecidos.

3. OBJETIVO ESPECIFICOS.

- Garantizar la continuidad de los servicios suministrados por la Oficina de Informática y Sistemas de la Entidad, previendo los riesgos ya sean a nivel de software, hardware, catástrofes naturales o causas de fuerza mayor.
- Incrementar la productividad en todas las áreas de la Entidad, garantizando la operación de los procesos apoyados por los servicios tecnológicos que actualmente se ofrecen.
- Controlar y mitigar los riesgos que se puedan materializar e impactar sobre los servicios de TI.
- Garantizar la pronta recuperación de los servicios (críticos) TI tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las consecuencias de un desastre o causa de fuerza mayor.

4. ALCANCE.

La presente política aplica para los servicios que actualmente brinda la Oficina de Informática y Sistemas.

5. DEFINICIONES.

Estrategia de Continuidad del Negocio: Es una guía general de acercamiento para asegurar la continuidad de funciones vitales para la Entidad en caso de eventos de desastre. La Estrategia de Continuidad del Negocio es preparada por la Entidad y sirve de punto de partida para la producción de la Estrategia de Continuidad de Servicios de TI.

Guía para Casos de Desastre: Es una guía producida por la Gestión de la Continuidad de los Servicios de TI, con instrucciones detalladas sobre cuándo y cómo recurrir al procedimiento para contrarrestar un desastre. La guía establece los primeros pasos que debe tomar el Servicio de ayuda tras sospechar o enterarse que ha ocurrido un desastre.

Índice de Datos Relevantes en Casos de Desastre: Es un catálogo con toda la información relevante en casos de desastre. Este documento es actualizado y puesto a circular por la Gestión de la Continuidad de los Servicios de TI entre todo el personal de la Oficina de Informática y Sistemas que esté a cargo de contrarrestar desastres.

Informe de Continuidad de Servicios de TI: Se crea cada cierto tiempo y provee información relacionada con la prevención de desastres a otros procesos de Gestión de Servicios y la dirección de TI.

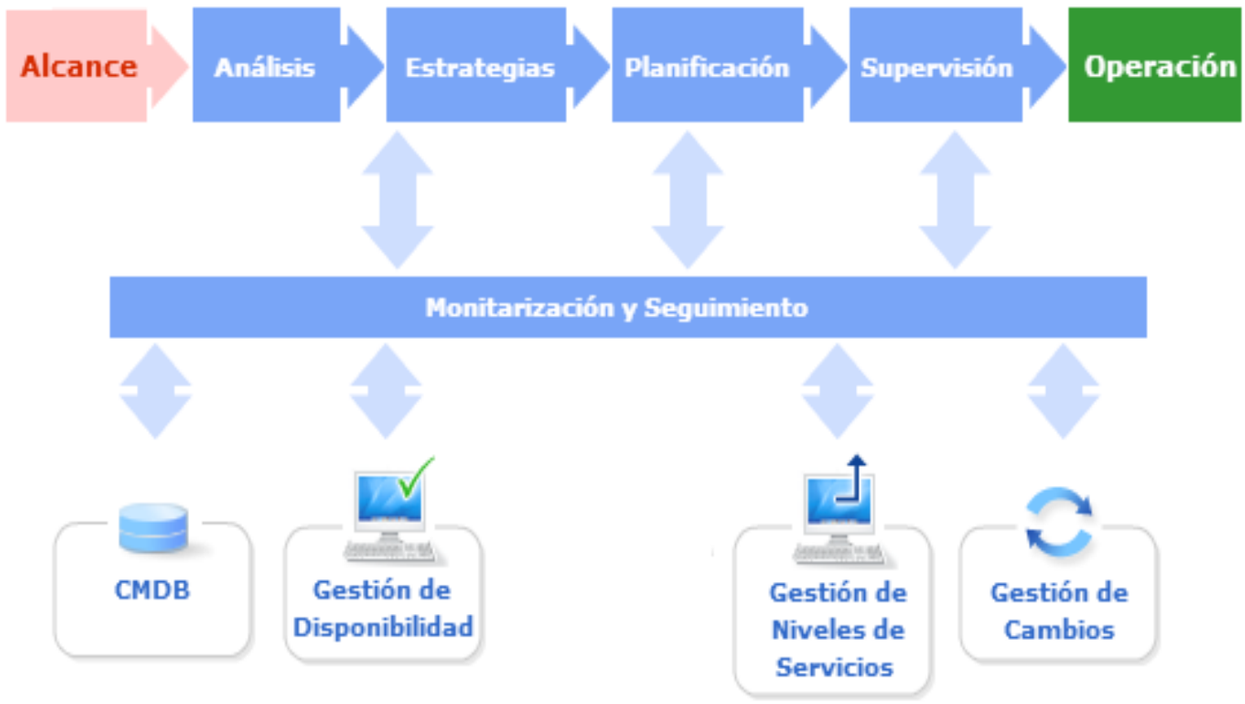
Estrategia de Continuidad de Servicios de TI: Contiene una guía de acercamiento para asegurar la continuidad de los servicios de TI en casos de desastre. Incluye una lista de Funciones Institucionales Vitales y opciones de aplicaciones para la reducción de riesgo (recuperación). La Estrategia de Continuidad de Servicios de TI debe basarse en una Estrategia de Continuidad del Negocio.

6. PROCESO

Las principales actividades de la Gestión de la Continuidad de los Servicios TI se resumen en:

- Establecer las políticas y alcance de la Gestión de la Continuidad del Servicio de TI (ITSCM por sus siglas en inglés).
- Evaluar el impacto en el negocio de una interrupción de los servicios TI.
- Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
- Establecer las estrategias de continuidad del servicio TI.
- Adoptar medidas proactivas de prevención del riesgo.
- Desarrollar los planes de contingencia.
- Poner a prueba dichos planes.
- Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co



7. CONTROL DEL PROCESO

La Gestión de la Continuidad del Servicio debe elaborar periódicamente informes sobre su gestión que incluyan información relevante para el resto de la TI.

Estos informes deben incluir:

- Análisis sobre nuevos riesgos y evaluación de su impacto.
- Evaluación de los simulacros de desastre realizados.
- Actividades de prevención y recuperación realizadas.
- Costos asociados a los planes de prevención y recuperación.
- Preparación y capacitación del personal TI respecto a los planes y procedimientos de prevención y recuperación.

Uno de los factores clave para el éxito de la Gestión de la Continuidad del Servicio es mantener la "concentración". Tras largos periodos en los que la prevención o, simple y llanamente, la suerte han impedido la existencia de graves interrupciones del servicio, se puede caer en un relajamiento que puede acarrear graves consecuencias.

Por esto es imprescindible llevar controles rigurosos que impidan que la inversión y compromiso inicial se diluyan y la Gestión de la Continuidad del Servicio no esté a la altura de la situación cuando sus servicios sean vitales para evitar que "un desastre se convierta en una catástrofe".

Pero si el control del proceso es importante en condiciones normales, éste se vuelve crítico durante las situaciones de crisis. La Gestión de la Continuidad del Servicio TI debe garantizar:

- La puesta en marcha de los planes preestablecidos.
- La supervisión de los mismos.
- La coordinación con la Gestión de Continuidad del Negocio.

8. DESARROLLO PLANEACION

ITEM	ACTIVIDADES	RESPONSABLE

1	Elaboración del plan de prevención y recuperación sobre los servicios de TI llamado plan de continuidad del negocio.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
2	Asignación de los recursos necesarios para cumplir con el plan de contingencia	Jefe de la Oficina de Informática y Sistemas.
3	Análisis de impacto del negocio ante una posible interrupción sobre los diferentes servicios suministrados.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
4	Elaboración y actualización de la matriz de riesgos y vulnerabilidades a los que está expuesta la infraestructura TI.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
5	Actualización del plan de continuidad del negocio.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
6	Evaluar el plan de continuidad del negocio.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.

9. DESARROLLO EJECUCION

ITEM	ACTIVIDADES	RESPONSABLES
1	Identificación del servicio afectado por la interrupción del servicio.	Funcionario o Contratista
2	Revisión del plan de continuidad, para verificar las directrices a ejecutar ante la interrupción presentada.	Funcionario o Contratista
3	De ser necesario revisar la base de datos de configuración.	Funcionario o Contratista
4	Creación de la incidencia en el sistema de gestión del servicio.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
5	Ejecución de la solución ante la interrupción del servicio.	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.
6	Actualización del plan de continuidad y de la matriz de riesgos	Funcionario o Contratista y Jefe de la Oficina de Informática y Sistemas.