MARCO DE GOBIERNO Y GESTIÓN DE TI PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO ORIENTADO A LA PRESTACIÓN DE SERVICIOS CRÍTICOS EN LAS HACIENDAS PÚBLICAS MUNICIPALES.

SOLÓRZANO GRIEGO IVETH ALICIA

TUTOR

WILSON NIETO

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
FUNDACIÓN UNIVERSIDAD DEL NORTE
BARRANQUILLA – COLOMBIA
2017

Tabla de contenido

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

Las administraciones municipales deben garantizar la calidad de los servicios que prestan a la ciudadanía y a través de la gestión de la continuidad del negocio se identifican los impactos potenciales que amenazan la continuidad de las actividades que apoyan la gestión en las secretarías de hacienda municipales. El diseño de un marco de gobierno de TI le da la capacidad a estas entidades de responder de forma efectiva a disrupciones, con base a herramientas de seguimiento y control, y es un referente para el cumplimiento de los objetivos de la administración pública mediante la preparación de las áreas de tecnología para la continuidad del negocio, elevando los niveles de competitividad y ofreciendo disponibilidad de los servicios a los ciudadanos.

El trabajo propuesto puede ser tomado como modelo de referencia por las oficinas TIC de los municipios, aplicado a procesos críticos de la Hacienda Municipal, para proteger los intereses de la entidad y para dar cumplimiento a las actividades definidas por el Gobierno Nacional, a través de la guía de continuidad del negocio del Modelo de Seguridad y Privacidad de la Información, como parte integral de la estrategia Gobierno en Línea - GEL, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Este componente estratégico es de obligatorio cumplimiento para entidades territoriales y nacionales, con implementaciones progresivas hasta el 2020, con el fin de fortalecer la seguridad de la información pública y garantizar el restablecimiento y recuperación de las operaciones y actividades esenciales.

La correcta implementación de un gobierno y una gestión que incluya la gestión de la continuidad del negocio es un reto para las administraciones municipales y resulta necesaria para disminuir la posibilidad de ocurrencia de incidentes y, en caso de producirse, estar preparada para responder en forma adecuada y oportuna.

2. DESCRIPCIÓN DEL PROBLEMA

La necesidad de reconocer la seguridad y privacidad de la información en las entidades territoriales y demás organizaciones en general, como un factor primordial para la apropiación de las TIC, hace que el Gobierno Nacional plantee un modelo de seguridad y privacidad de la información el cual debe ser respaldado por una gestión. Dicha gestión debe involucrar la implementación de un proceso de preservación de la información pública ante situaciones disruptivas para minimizar el impacto y recuperación por perdida de activos de información mediante la combinación de controles preventivos y de recuperación.

Las secretarías de hacienda en las administraciones locales son las responsables de los aspectos económicos y financieros de los municipios y son conscientes de que existen diferentes tipos de amenaza, cuyo origen puede ser natural, accidental o intencionado y puede repercutir en la operación tributaria y en el sistema de procesamiento de la información, impactando la continuidad del negocio, la imagen del gobierno local, en aspectos financieros y legales, y en las personas, como entidad y contribuyente, lo que crea la necesidad de recuperación del negocio en el menor tiempo posible, garantizando la continuidad de los servicios de TI.

2.1. OBJETIVO GENERAL

Diseñar un modelo de gobierno y gestión de TI que garantice la continuidad de los servicios que soportan los procesos críticos de la Hacienda Pública Municipal basándose en buenas prácticas internacionales ajustada a la infraestructura local.

2.2. OBJETIVOS ESPECIFICOS

1. Identificar los procesos de gobierno TI para soportar procesos de gestión de la continuidad en las secretarías de hacienda en administraciones municipales, basada en estudios de mejores prácticas internacionales y guías nacionales.

2. Proponer el marco de gobierno de TI para la gestión de la continuidad de procesos críticos en las Secretarías de Hacienda de administraciones públicas municipales.

3. Diseñar el plan de implementación y despliegue para el caso de estudio, Secretaría de Hacienda de la Alcaldía Municipal de Puerto Colombia, Departamento del Atlántico.

3. METODOLOGÍA

El diseño del modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios en las administraciones de hacienda pública municipales está compuesto por las siguientes fases:

Objetivo Específico	Fase	Descripción
Identificar los procesos de gobierno TI para soportar procesos de gestión de la continuidad en las secretarías de hacienda en administraciones municipales, basada en estudios de mejores prácticas internacionales y guías nacionales.	1. Revisión y análisis de conceptos de Gobierno y Gestión.	▪ Revisión de conceptos de Gobierno y Gestión. ▪ Estudio de marcos y mejores prácticas de Gobierno y Gestión: *Revisión de marcos y estándares existentes de Gobierno y Gestión y modelo de Gobierno y Gestión de TI del Ministerio de las Tecnologías de la Información y las Comunicaciones. Durante esta fase se realizan revisiones de marcos de trabajo de Cobit5, ITIL V3 y la Guía No.10 Preparación de las TIC para la Continuidad del negocio – MinTIC.* ▪ Revisión de guías y casos de éxito del gobierno y gestión de la continuidad del negocio.
	2. Revisión de componentes de Gestión de la Continuidad.	▪ Revisión de componentes asociados a la gestión de la continuidad en entidades territoriales.

Proponer el marco de gobierno de TI para la gestión de la continuidad de procesos críticos en las Secretarías de Hacienda de administraciones públicas municipales.	3. Diseño del modelo de gobierno y gestión de TI	▪ *Modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios de los procesos críticos en administraciones públicas municipales.* En esta fase se plantea el modelo de gobierno y gestión de TI con base a mapeos de procesos y metodologías revisadas en la fase anterior. Contiene por proceso, las prácticas, las actividades con las entradas y salidas, las métricas y los indicadores.
		Aplicación de una metodología para realizar el análisis de impacto del negocio de los riesgos en procesos críticos. El desarrollo de la metodología estará soportado por un documento guía de escenarios donde se definirán categorías de impacto de acuerdo al proceso crítico elegido.
Diseñar el plan de implementación y despliegue para el caso de estudio, Secretaría de Hacienda de la Alcaldía Municipal de Puerto Colombia, Departamento del Atlántico.	4. Elaboración de la guía de implementación del modelo propuesto.	Elaboración del plan de implementación del modelo propuesto. *En esta fase final se lleva a cabo el plan de implementación del modelo. Se toma como caso de estudio la Secretaría de Hacienda del Municipio de Puerto Colombia.*

4. MARCO TEÓRICO

4.1 CONCEPTOS Y DEFINICIONES

4.1.1. Gobierno Corporativo y Gobierno de TI

Hitt, Ireland y Hoskisson [1] definieron la estrategia como un conjunto de compromisos que indican lo que se pretende hacer y lo que no, de forma que se aproveche al máximo las competencias y se obtenga una ventaja competitiva. Determinar y controlar el direccionamiento de la estrategia, al igual que gestionar el desempeño y las relaciones de las partes interesadas es como se define el gobierno corporativo [2].
Los aspectos claves en las que se centra el Gobierno Corporativo incluyen principalmente: Funciones de la Junta Directiva y Ejecutivos, Cumplimiento normativo, Derechos de los accionistas, Operación y Control del negocio, Contabilidad Financiera y Reportes, Gestión de riesgos.

Así, gobierno de TI resulta ser una parte integral del gobierno corporativo y se refiere a alinear la estrategia de TI con la estrategia corporativa.

Gobierno de TI se define como una integración de la gestión, la planificación de políticas y prácticas y un proceso de revisión de desempeño, que permite alinear las inversiones y prioridades del negocio, mantiene una utilización responsable de recursos y activos, establece y aclara la responsabilidad y la toma de decisión, mejora el rendimiento de las organizaciones y defiende la innovación [3]. Su alcance abarca temas como: Principios de TI, arquitectura de TI, arquitectura orientada al Servicios (SOA), Infraestructura de TI, las necesidades de la aplicación del negocio, las inversiones de TI y su priorización, el desarrollo del talento humano y las políticas, procesos, mecanismos, herramientas y métricas.

Se debe reconocer la diferencia existente entre el Gobierno Corporativo, el Gobierno empresarial o del negocio y el Gobierno de TI:

Gobierno Corporativo	Gobierno Empresarial	Gobierno de TI
Separación de propiedad y control	Dirección y Control del Negocio.	Dirección y Control de TI.
Funciones del Directorio y Ejecutivos. **Cumplimiento normativo.** **Derechos de los Accionistas.** **Operaciones y Control de Negocios.** **Contabilidad financiera e Informes.** **Gestión de riesgos.**	Estrategia de negocios, Planes y Objetivos. Procesos y actividades empresariales. Innovación e Investigación. Capital intelectual. Gestión de recursos humanos. Métricas de rendimiento y Controles. Gestión de activos.	Estrategia de TI, Planes y Objetivos. Alineación con Planes de Negocios y Objetivos Recursos y recursos de TI. Gestión de la demanda. Entrega y Ejecución de Valor. Gestión (PM y ITSMD) Riesgo, Cambio y Rendimiento Administración.

Ilustración 1. Tomado de "Implementing IT Gobernance (2008) Dr Gad J Selig PMP COP. Varen Haren Publising.

De acuerdo a la ilustración, se puede observar que el Gobierno de TI es tarea de todos, la Junta Directiva y el CEO de la organización toman un lugar importante en cuanto al liderazgo, la estructura organizativa y los procesos que aseguren que la función de TI estén alineadas con las metas corporativas. Además, son los directivos los que toman decisiones en materia de inversiones y tienen la visión empresarial revisando y aprobando los planes estratégicos, programas y proyectos importantes que generan valor a la organización. El CIO además de aumentar la eficiencia y reducir costos, utilizan la TI como un estímulo principal para la innovación empresarial.

4.1.2. Gobierno y gestión de TI

Es necesario hacer una distinción de lo que es gobierno y gestión. Gobierno Corporativo de TI es el sistema por el cual se dirige y supervisa el estado actual y futuro del uso de TI (ISO/IEC 38500)[1]. El modelo de gobierno de TI presentado en ISO/IEC 38500 se enfoca en tres tareas claves de gobierno – evaluar, dirigir, controlar, como la clave para dar dirección y controlar el desempeñó de los roles de gestión en la conducción de la organización para la planificación, implementación y utilización operacional de TI. Por su parte, gestión se define como el sistema de controles y procesos para lograr los objetivos estratégicos establecidos por la dirección de la organización y está sujeta a monitorización establecida mediante el gobierno corporativo. Para tener una imagen visual de los conceptos, el modelo de gobierno de TI según la norma, lo representa claramente:

Ilustración 2. Modelo de Gobierno IT Tomado de ISO/IEC 38500

Los componentes principales del Gobierno de TI [3] son:

- Estrategia, Plan y Objetivos Corporativos

[1] ISO/ IEC 38500:2008 "*Corporate governance of information technology*". Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones lo utilicen al evaluar, dirigir y monitorizar el uso de las tecnologías de la información y comunicaciones (TICs). Está alineada con los principios de gobierno corporativo recogidos en el "Informe Cadbury" y en los "Principios de Gobierno Corporativo de la OCDE."

- Estrategia, Plan y Objetivos de TI
- Plan de Ejecución
- Gestión del Rendimiento y Controles de Gestión
- Gestión de Proveedores y Gestión de outsourcing
- Desarrollo de Talento Humano, Mejora Continua y Aprendizaje

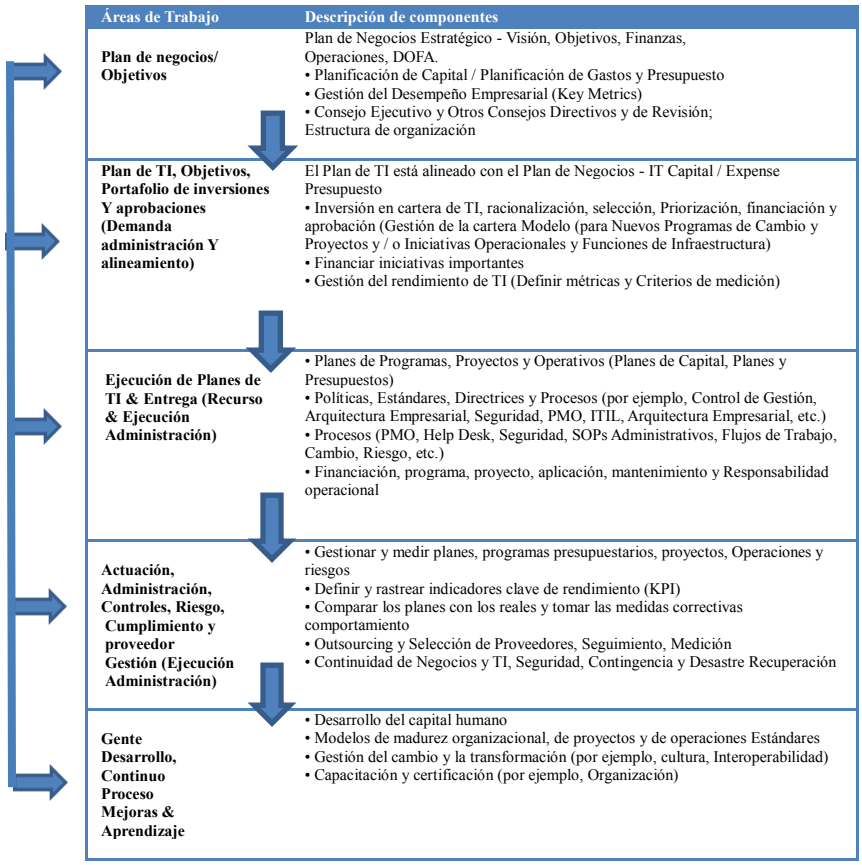


Ilustración 3. Framework integrado de Gobierno de Ti. Tomado de "Implementing IT Gobernance (2008) Dr Gad J Selig PMP COP. Varen Haren Publising [3]

El alcance del Gobierno de TI comprende [3]:

a. Principios de TI
b. Arquitectura de TI
c. Arquitectura orientada al Servicios (SOA)
d. Infraestructura de TI
e. Necesidades de aplicación del negocio

f. Inversiones de TI y su priorización
g. Desarrollo del talento humano
h. Políticas, procesos, mecanismos, herramientas y métricas.

Se plantea que el éxito de la implementación se basa en pilares fundamentales: **Liderazgo, organización y toma de decisiones, y que los procesos sean flexibles y escalables y tenga una tecnología innovadora**. Si alguno de los pilares anteriores falla o es ineficaz, la iniciativa del Gobierno de TI no será eficaz ni sostenible y puede atraer múltiples problemas que pueden desencadenar hasta el fin de una organización por pérdidas irrecuperables.

Asimismo, la aplicación de unas buenas prácticas sobre el Gobierno de TI obtendrá, además de los objetivos anteriormente expuestos, una serie de beneficios para la organización entre los que se puede destacar:

- La conformidad con los estándares de seguridad, de privacidad, de prácticas comerciales, de regulación medioambiental, y de responsabilidad social.
- Garantizar los derechos de propiedad intelectual, incluyendo acuerdos de licencia de software.
- Apropiada implementación y operación de los activos de TI.
- Clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización.
- Continuidad y sostenibilidad del negocio.
- Asignación eficiente de los recursos.
- Innovación en servicios, mercados y negocios.
- Buenas prácticas en las relaciones con las partes interesadas (stakeholders).
- Reducción de costes.
- Materialización efectiva de los beneficios esperados de cada inversión en TI.

4.1.3. Toma de decisiones.

Los roles indispensables en un modelo efectivo de Gobierno de TI son el director ejecutivo, Chief Executive Officer – CEO, y el director de tecnologías de la

información, Chief Information Officer – CIO.

El CEO es el responsable de hacer realidad el Gobierno de TI, es el encargado del establecimiento del direccionamiento estratégico, políticas, estructura global, presupuesto e inversión; el CEO debe conseguir que toda la organización comprenda y esté alineada con la visión estratégica, manteniendo siempre una buena comunicación interna.

El papel del CEO y el equipo de gestión ejecutiva requieren un equilibrio entre mantener el crecimiento y la rentabilidad mientras se optimiza la efectividad de la organización, además de cumplir con los requisitos regulatorios.

Ejecutar iniciativas estratégicas para toda la empresa y administrar operaciones comerciales efectivas es un negocio complejo que requiere un gobierno corporativo y de TI efectivo para que el CEO y el equipo ejecutivo implementan la estrategia de la organización [3].

El gobierno efectivo es un componente prominente para el crecimiento y la rentabilidad efectivos y los atributos que deben abordarse para cumplir estos objetivos respectivamente son:

Crecimiento (maximizar propuesta de valor)	Optimizar la efectividad y eficiencia
▪ Velocidad (reducir tiempo) al mercado. ▪ Minimizar los riesgos y la incertidumbre. ▪ Ejecución perfecta. ▪ Facilitación de mejores prácticas. ▪ Reducir costos. ▪ Reducir los gastos de capital. ▪ Reducir obstáculos. ▪ Reducir defectos. ▪ Aumentar la lealtad del cliente. ▪ Gobernabilidad e indicadores clave de rendimiento. ▪ Código ético.	▪ Aumentar la gestión / competencia / capacitación de los empleados. ▪ Implementar el cambio estratégico de una manera planificada, coordinada y controlada. ▪ Mejorar los resultados de los esfuerzos de implementación. ▪ Mejore la dinámica de creación de equipos y el comportamiento empresarial. ▪ Conformidad.

Tabla 1. Rol del CEO. Tomado de "Implementing IT Gobernance (2008) Dr Gad J Selig PMP COP. Varen Haren Publising [3]

El Gobierno de TI es tarea de todos, la Junta Directiva y el CEO de la organización toman un lugar importante en cuanto al liderazgo, la estructura organizativa y los

procesos que aseguren que la función de TI esté alineada con las metas corporativas. Además, son los directivos los que toman decisiones en materia de inversiones y tienen la visión empresarial revisando y aprobando los planes estratégicos, programas y proyectos importantes que generan valor a la organización. El CIO además de aumentar la eficiencia y reducir costos, utilizan la TI como un estímulo principal para la innovación empresarial.

El CIO es el líder de Tecnologías de la información dentro de la organización, es el encargado de establecer la estrategia de TI, obtener presupuestos, gestionar proyectos de TI, y definir la gestión de TI.

El CIO debe abordar aspectos claves y estratégicos, que incluyen:

- Cultura interna de la unidad de TI.
- Innovación, exploración de formas de tecnología actual y evolución, aprovechamiento de tecnologías emergentes.
- Gestión de Riesgos de TI.
- Identificación, valoración y gestión de activos.
- Planeación e implementación Estratégica de las TI.
- Aseguramiento del funcionamiento de operaciones dentro de la unidad de TI.
- Automatización de procesos y calidad de servicios, contribuyendo a la eficiencia y eficacia de la organización.
- Cumplimiento normativo.
- Seguridad y Privacidad de la Información.

5. MARCOS DE REFERENCIA

5.1. ESTÁNDARES Y MARCOS DE TRABAJO DE GOBIERNO Y GESTIÓN DE TI

Las organizaciones requieren adoptar buenas prácticas para las operaciones de TI, incluyendo la continuidad del negocio. La gestión de la continuidad del negocio puede ser diseñada a través marcos de referencia ampliamente utilizados que proporcionan

controles medibles. Para la propuesta de marco de gobierno de TI para llevar a cabo esa gestión, que sea compatible con los estándares y mejores prácticas de la industria, se consideran algunos marcos metodológicos internacionales y nacionales que ofrecen mayor probabilidad de garantizar un resultado exitoso, especialmente tras una interrupción no planificada de los servicios de TI.

5.1.1. Marco de referencia Arquitectura TI de Colombia - Ministerio de las Tecnologías y las Comunicaciones MinTIC.

Este Marco de Referencia es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea, liderado por el Ministerio de las Tecnologías y las Comunicaciones. Se busca habilitar las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad [8]. Está dirigido a las instituciones del Estado, las empresas privadas, la academia y los ciudadanos en general.

Principios

- ✓ **Excelencia del servicio al ciudadano:** Propender por fortalecer la relación de los ciudadanos con el Estado.
- ✓ **Inversión con buena relación Costo/beneficio:** Busca propender porque las inversiones de TI tengan un retorno medido a partir del impacto de los proyectos.
- ✓ **Racionalización:** Para optimizar el uso de los recursos, teniendo en cuenta criterios de pertinencia y reutilización.
- ✓ **Estandarización:** Para brindar un modelo estandarizado para la definición de los lineamientos, políticas y procedimientos de gestión de TI del Estado colombiano.
- ✓ **Interoperabilidad:** Para fortalecer los esquemas de Interoperabilidad que estandaricen y faciliten el intercambio de información entre entidades y sectores, manejo de fuentes únicas de información y la habilitación de servicios entre entidades y sectores.
- ✓ **Viabilidad en el mercado:** Busca motivar al mercado a plantear y diseñar soluciones según las necesidades del Estado colombiano.

✓ **Neutralidad tecnológica:** Busca garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, también busca garantizar la libre y leal competencia y que la adopción de tecnologías sea armónica con el desarrollo ambiental sostenible.

✓ **Federación:** Se debe definir y establecer, a través del Marco de Referencia de AE, estándares, lineamientos y guías para el gobierno y la gestión de TI.

✓ **Co-creación:** Permitir componer nuevas soluciones y servicios sobre lo ya construido y definido, con la participación de todas aquellas personas u organizaciones, que influyen o son afectadas por el Marco de Referencia AE.

✓ **Escalabilidad:** Permitir la evolución continua y adición de todos los componentes y dominios que integran el Marco de Referencia AE, sin perder calidad ni articulación.

✓ **Seguridad de la información:** Busca la definición, implementación y verificación de controles de seguridad de la información.

✓ **Sostenibilidad:** Aportar al equilibrio ecológico y cuidado del medio ambiente a través de las TI.

El Marco de Referencia está organizado en seis dominios, donde cada dominio tiene ámbitos, que agrupan lineamientos, además de roles, una normatividad, indicadores e instrumentos para la adopción. Estos dominios son [8]:

Dominios Arquitectura TI	Descripción
Estrategia TI	Apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para de manera que esté alineada con las estrategias organizacionales y sectoriales.
Gobierno TI	Brindar directrices para implementar esquemas de gobernabilidad de TI y para adoptar políticas que permitan alinear los procesos y planes de la institución con los del sector.
Información	Definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la

	misma.
Sistemas de Información	Planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución.
Servicios Tecnológicos	Gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.
Uso y Apropiación	Definir la estrategia y prácticas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI.

Ilustración 4. Dominios Marco de Referencia Arquitectura TI de Colombia - Tomado de MinTIC

El dominio de Servicios Tecnológicos busca gestionar la infraestructura tecnológica que sostiene los sistemas y servicios de información en las instituciones. Las direcciones de Tecnología y Sistemas de Información deben garantizar su disponibilidad y operación permanente, que beneficie a todos los usuarios.

La estrategia de servicios tecnológicos contempla el desarrollo de los siguientes aspectos:

- Arquitectura de infraestructura tecnológica.
- Procesos de gestión: capacidad, puesta en producción y operación.
- Servicios de conectividad.
- Servicios de administración y operación.
- Soporte técnico y mesa de ayuda.
- Seguimiento e interventorías.

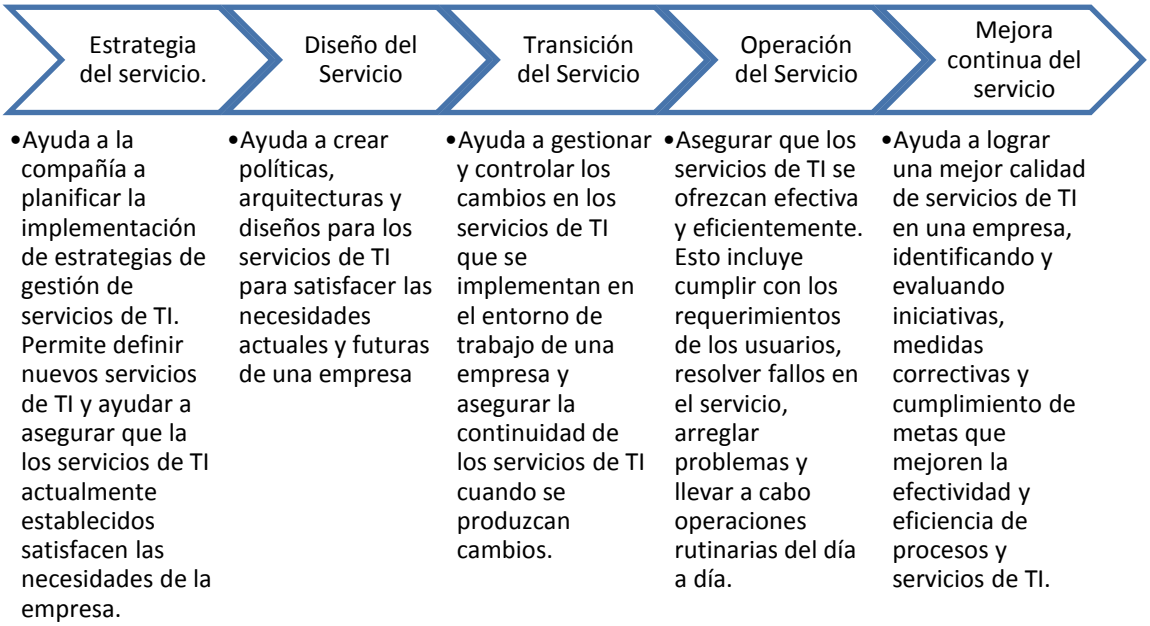
Dentro del ámbito de Operación de los Servicios Tecnológicos contiene el elemento de Operación y continuidad de los Servicios Tecnológicos que entrega un modelo de Seguridad y Privacidad de la Información y a su vez presenta una guía de preparación para la continuidad del negocio, que será considerada en esta propuesta de trabajo.

5.1.2. ITIL V3- Information Technology Information Library

ITIL V3 es un marco para la gestión de servicios de TI desarrollado en el Reino

Unido por la Oficina de Comercio del Gobierno (Office of Government Commerce - OGC), el marco de trabajo ITIL describe los métodos, funciones, roles y procesos sobre los que las organizaciones pueden desarrollar y evaluar sus propias actividades de TI [6].

ITIL implementa diferentes procesos de Gestión de Servicios de TI, tales como la gestión del ciclo de vida y solicitud de gestión para mejorar la calidad de los servicios de TI. El componente básico contiene cinco estrategias de gestión del marco de ITIL, que representan el ciclo de vida de servicios de TI. Las diferentes estrategias de manejo son:



ITIL avala un marco de trabajo denominado Gestión de la Continuidad del Servicio de TI (ITSCM TI Service Continuity Management). El ITSCM se ocupa de los riesgos que podrían causar un impacto en la infraestructura de TI, de manera que una interrupción de los mismos podría poner en peligro la continuidad del funcionamiento de la organización. La ITSCM se concentra en la protección de la infraestructura tecnológica, mientras que la continuidad del negocio se enfoca en los riesgos que podrían generar una interrupción de las operaciones de negocio.

5.1.3. COBIT 5 - Control Objectives for Information and related Technology

Es una guía de mejores prácticas para el control y supervisión de las tecnologías de la información - TI, mantenido por ISACA (Information Systems Audit and Control Association) y el ITGovernance Institute. COBIT es un marco de gobierno de las tecnologías de información que proporciona herramientas de control de las tecnologías en la organización y su alineamiento con los objetivos del negocio.

COBIT 5 provee de un marco de trabajo integral que plantea reglas claras apoyando a las organizaciones en la creación de valor desde TI lo cual significa generar beneficios a un coste óptimo de los recursos optimizando los niveles de riesgo [7]. COBIT 5 puede ser aplicado por diferentes modelos de negocio y sectores, ya sea en el público o privado y ayuda a la alta dirección y a ejecutivos a gestionar las inversiones en TI durante todo su ciclo de vida proporcionando un método para evaluar si los servicios de TI y las nuevas iniciativas están cumpliendo con las exigencias corporativas y si cumple con las expectativas de beneficios.

Los principios básicos de COBIT 5 habilitan a cualquier organización para construir un marco de gobierno y gestión para optimizar los recurso y hacer uso estratégico de las TI beneficiando a las partes interesadas, estos son:

Ilustración 5. Principios de Cobit 5. Tomado de COBIT® 5 - ISACA

COBIT 5 está organizado en 37 objetivos de control, agrupados en 5 dominios:

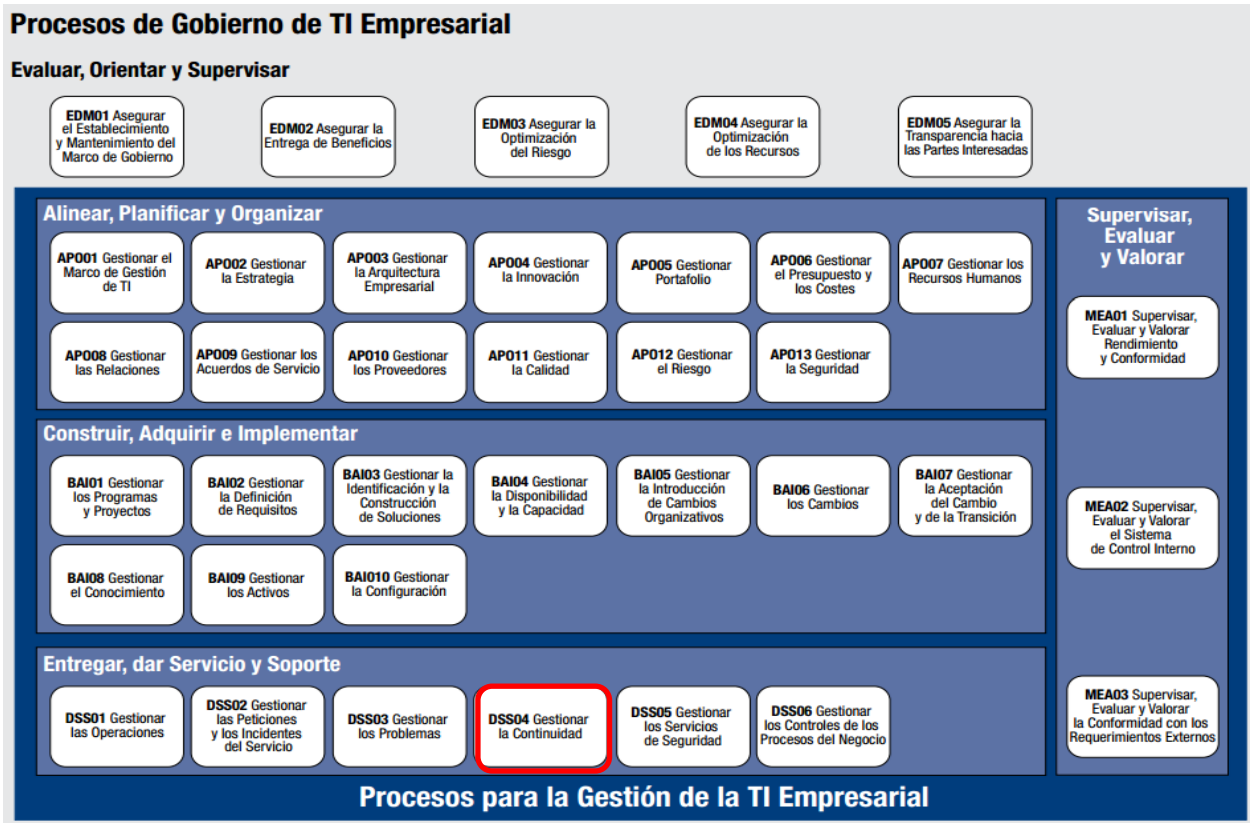


Ilustración 6. Procesos de Gobierno y Gestión TI - Tomado de Cobit 5 - ISACA

Dentro del marco está definido en el proceso Entregar, dar Servicio y Soporte DSS04, que se enfoca en establecer y mantener un plan para permitir al negocio y a TI, responder a los incidentes y las interrupciones del servicios para la operación continua de los procesos críticos para el negocio y los servicios TI, y mantener la disponibilidad de la información a un nivel aceptable para la empresa. De acuerdo a la definición de Cobit [5], es un proceso de gestión integral para establecer y mantener un plan que permita al negocio y a TI responder a incidentes e interrupciones de servicios para la operación continua de los procesos críticos para el negocio y los servicios de TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresas.

5.1.4. Gobierno en línea - GEL

En el año 2010, en el marco del congreso de ANDICOM, el Gobierno Nacional anunció el plan de Tecnologías de la Información y las Comunicaciones, denominada Vive Digital, cuyo objetivo es que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional en cuanto a infraestructura, los servicios, las aplicaciones y los usuarios. Dentro de las aplicaciones del plan Vive Digital se encuentra la estrategia de Gobierno en Línea, GEL, que es la estrategia de gobierno electrónico (e-government) en Colombia, y busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC y cuyos ejes temáticos son[4]:

1. TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.

2. TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.

3. TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.

4. Seguridad y privacidad de la información: Busca guardar los datos de los

ciudadanos, garantizando la seguridad de la información.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, el Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC, ha definido los lineamientos a través del decreto 1078 de 2015[2], único reglamentario del sector de tecnologías de información y las comunicaciones, como parte integral de la estrategia GEL, y es de obligatorio cumplimiento para las entidades del estado de orden territorial[3]:

Componente/Año	Entidades A (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	70%	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	80%	95%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	20%	45%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	35%	50%	80%	100%	Mantener 100%	Mantener 100%

Componente/Año	Entidades B (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

Componente/Año	Entidades C (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

Ilustración 7. Plazos implementación de actividades Manual de Gobierno en Línea.
Tomado de "Modelo de seguridad y privacidad de la Información" MinTIC.

El modelo está compuesto por lineamientos, políticas, normas, procesos en 16 anexos de apoyo y está basado en el ciclo PHVA, alineado con el estándar NTC: ISO/IEC 7001:2005 y complementado con otras iniciativas y estándares nacionales e internacionales, tales como MECI-Modelo Estándar de Control Interno; COBIT, ITIL, entre otros.

[2] Decreto 1078 de 2015. TITULO 9, POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPITULO 1, Estrategia de Gobierno en Línea - GEL, en la SECCIÓN 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES.
[3] Decreto 2573 de 2014, en el Articulo 10. Plazos. Sujetos Obligados del Orden Territorial: *A. Gobernaciones de categoría Especial y Primera*; alcaldías de categoría Especial, y demás sujetos obligados de la administración pública en el mismo nivel. *B. Gobernaciones de categoría segunda, tercera y cuarta*; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel. *C. Alcaldías de categoría cuarta, quinta y sexta* y demás sujetos obligados de la Administración Pública en el mismo nivel.

5.1.5. ISO 22301.

La ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas.

ISO 22301 identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. Esta norma proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de su organización y le da la confianza de negocio a negocio y de negocio a cliente. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente

.

ISO 22301 se compone de 10 cláusulas principales, las primeras corresponden al alcance, referencias normativas y términos y definiciones. Los capítulos principales de los que se compone la norma son:

- **4. Contexto de la organización.**

El primer paso es conocer la organización, sus necesidades internas y externas, y establecer límites para el alcance del sistema de gestión. Esto requiere que la organización entienda las necesidades de los stakeholders pertinentes.

- **5. Liderazgo**

ISO22301 hace especial énfasis en la necesidad de un liderazgo apropiado en la Gestión de la Continuidad del Negocio. Es útil para que la alta dirección asegure que se proporcionan los recursos necesarios, nombra a los responsables que implementan y mantienen el SGCN y establece la política.

- **6. Planificación**

Es necesario que la empresa identifique los riesgos para poder implementar el sistema de gestión e instaure los criterios y objetivos a seguir.

- **7. Soporte**

Para llegar al éxito en la continuidad del negocio, se debe tener en la organización personas con los conocimientos, experiencia y habilidades pertinentes, para que apoyen al SGCN y respondan a los incidentes, así como servicios de soporte, recursos de formación y toma de conciencia, comunicaciones internas y externas y control de la documentación.

- **8. Operaciones**

La empresa debe realizar el análisis de impacto en el negocio para comprender cómo su negocio se vería afectado por una interrupción y cómo cambia con el tiempo. Por otro lado, la evaluación de riesgos se encargará de tratar los riesgos para el negocio de forma estructurada e informar de éstos en el desarrollo de la estrategia de continuidad del negocio.

En esta cláusula se instauran los requisitos para la continuidad de negocio, hace referencia a los ejercicios y pruebas, parte esencial en el SGCN, ISO 22301.

- **9. Evaluación**

Es imprescindible contar con auditorías internas, con la revisión y seguimiento permanente de los SGCN por parte de la organización y actúe sobre dichas revisiones.

- **10. Mejora**

Ante el cambio constate de las organizaciones y sus entornos, aquí se definen las acciones para mejorar el SGCN para aumentar permanentemente la eficacia del sistema de continuidad del negocio.

La norma ISO 22301 trabaja sobre el ciclo dinámico PHVA: Planear – Hacer – Verificar – Actuar. Este ciclo nos ayuda a la realización de actividades, de una manera más organizada y eficaz. Por tanto aceptar la metodología de trabajo ofrecido por el ciclo PHVA es una guía básica para la gestión de actividades y procesos, ofreciéndonos una estructura ejemplar de un sistema que es aplicable para cualquier organización.

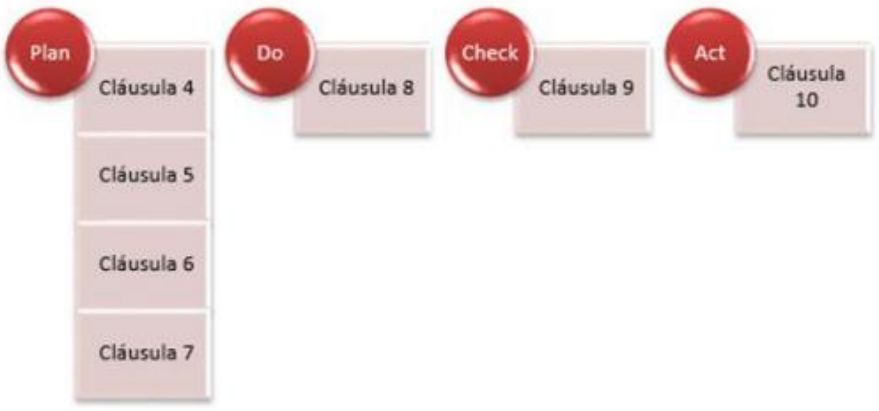


Ilustración 8. Cláusulas de la Norma ISO 22301 dentro del modelo PHVA. Adaptado ISO, 2012.

5.2. BUENAS PRÁCTICAS Y CASOS DE ÉXITO

5.2.1. Seguridad y Privacidad de la Información – Guía No. 10 Guía para la preparación de las TIC para la continuidad del negocio. Ministerio de las Tecnología y las comunicaciones MinTIC – Gobierno Nacional de Colombia. 2010.

La guía liberada por MinTIC es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones.

El modelo de operación de Continuidad del Negocio para el Modelo de Seguridad y Privacidad de la Información, contempla su implementación en las cuatro fases del ciclo del Modelo para que las Entidades puedan gestionar la seguridad y privacidad de la información, con el fin de fortalecer la protección de los datos y dar cumplimiento a lo establecido en la Estrategia de Gobierno en Línea, dentro del Marco de Referencia Arquitectura TI, cubriendo de una manera integral cada uno de sus componentes [10].

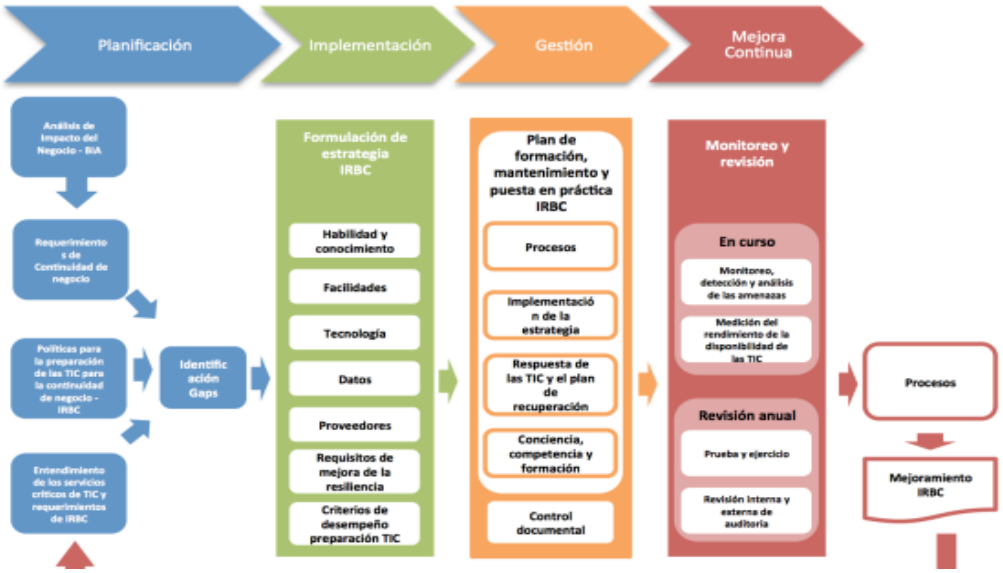


Ilustración 9. Marco Continuidad del Negocio para Seguridad y Privacidad de la Información – Tomado de MinTIC

Este modelo hace referencia a un sistema de gestión que complementa y suporta la continuidad del negocio de la organización y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI). Este marco indica lo que se debe hacer y cumplir, el cómo se debe hacer es criterio de la entidad, apoyándose en la adopción de mejores prácticas.

5.2.2. Adaptación COBIT 5 e ITIL en un municipio saudí. Govind Kulkarni, COBIT5, CSQA, Experto ITIL, PMP.

El artículo publicado en 2015 en ISACA [11], hace referencia al caso de estudio del municipio de Arabia Saudita, una institución estatal cuyo principal objetivo es servir a los ciudadanos en el ámbito de su región. La necesidad de gestionar un gran volumen de información que se genera con los servicios a los ciudadanos y cuya responsabilidad recae sobre el departamento de TI del municipio es un desafio que afrontaron con la adopción del marco de Cobit. Los principales motivadores de la implementación de un marco de gobierno y gestión de servicios eran los puntos débiles del municipio, en particular:

- Falta de continuidad del negocio
- Gestión de activos de TI que requería disciplina
- Incidentes importantes que causaban la falta de disponibilidad de servicios
- Insuficiente gestión de riesgos de TI y gestión de seguridad

- Creación de valor del negocio para las partes interesadas

Se conformó un equipo de implementación y definieron una estrategia abordando los puntos débiles en las fases iniciales. La implementación del proceso tuvo retos que incluyeron: Barreras interdepartamentales (superadas mediante el uso de talleres), Idioma, Experiencia en la implementación de las herramientas Logística, tales como visas de viaje para los consultores y reunir a las partes interesadas para los talleres, de acuerdo con la disponibilidad de todas ellas. Sin embargo, los apuntes finales de los beneficios logrados con la implementación describen que a pesar de estar aun en desarrollo, se ve la mejora en la manera de trabajar y las partes interesadas consideran que seguir el proceso y usar las herramientas de forma eficaz los ayuda a servir mejor, dar seguimiento a los estados, generar mejores informes y estar al tanto de los problemas. Concluyen que por primera vez, el departamento de TI está en la práctica de gestionar los problemas para reducir la recurrencia, realizar evaluaciones de riesgos para los activos de TI cruciales, y planificar e implementar la continuidad del negocio y que todo el proceso revela y asegura que las TI son un activo valioso que suministra los servicios necesarios, y se refleja en la satisfacción de los usuarios. Los resultados en términos de valor financiero no se cuantificaron en el artículo.

5.2.3. Metodología para la Gestión de la Continuidad del Negocio. Rodrigo Ferrer V.

Este artículo publicado en 2015 [12] expone los pasos requeridos para diseñar e implementar un proceso de Gestión de la Continuidad del Negocio orientado a diversas organizaciones en Colombia, basada en los estudios realizados por el Business Continuity Institute (BCI) y el Disaster Recovery Institute International (DRII) los cuales han sido las organizaciones líderes a nivel mundial en esta campaña de formación en los temas relacionados con la continuidad del negocio ante diferentes tipos de incidentes. La Gestión de la Continuidad del Negocio (GCN) se considera como parte fundamental del Gobierno y de la gestión del riesgo y se considera el proceso por fases de planeación, implementación, verificación y mejoras, conformando así el conocido ciclo PHVA. La norma internacional ISO 22301 sirvió de consulta permanente para la realización del artículo.

5.2.4. Plan de Continuidad de Negocio. Banco de la República. 2017.4

Una organización con experiencia en continuidad del negocio es el Banco de la República de Colombia, que cuenta con un Sistema de Gestión de Continuidad (SGC), el cual le brinda la las herramientas para continuar prestando las funciones asignadas al Banco por la Constitución Política, la Ley o sus Estatutos en niveles considerados como aceptables, garantizando la estabilidad al sistema financiero del país. Mediante un plan de continuidad proporciona el marco para construir la resiliencia organizacional, de manera que, después de un incidente perjudicial, se pueda continuar con la entrega de productos y servicios en los niveles considerados como aceptables. El SGC está conformado por: Marco de referencia, Sistema de prevención y atención de emergencias, Planes de contingencia tecnológicos y operativos, Plan de administración de crisis e Iniciativas de integración con sector financiero y Gobierno.

La información de estados de servicios, esquemas y pruebas de contingencia se encuentran publicados en la página web institucional.

5.2.5. Plan institucional de respuesta a emergencias "PIRE". Secretaría Distrital de Hacienda. Alcaldía Mayor de Bogotá D.C. 2013.

La Secretaría Distrital de Hacienda -SDH- de Bogotá publicó en 2013 el Plan institucional de respuesta a emergencias [13], el cual se encuentra en el proceso de implementación y desarrollo como parte del proyecto de Riesgo Operacional y Continuidad del Negocio que contempla, dentro de sus escenarios de evaluación, la falla total sobre las instalaciones físicas y tecnológicas de la entidad, generando repercusiones en la operación, en los sistemas de procesamiento de información y en el personal. Por lo anterior, adoptó como metodología las prácticas profesionales expuestas por el DRII (The Institute for Continuity Management) para garantizar la disponibilidad de estrategias de continuidad que permitan anticiparse a cualquier trastorno que pueda poner en peligro la supervivencia de la Secretaría. Para el efecto, teniendo en cuenta la metodología mencionada, las necesidades de la entidad y los

[4] Experiencia de organizaciones con sistemas de gestión de continuidad. http://www.banrep.gov.co/es/continuidad

requerimientos normativos, la -SDH- dentro de su Plan de Continuidad del Negocio -PCN- incluye el Plan Institucional de Respuesta a Emergencias -PIRE- en el cual se expone el esquema organizacional que operaría para la atención de la emergencia, y cuyo objeto principal es dar respuesta y cumplimiento a los protocolos Distritales que conforman el Plan de Emergencias de Bogotá -PEB-, adoptado mediante la resolución 004 de 2009.

5.3. MAPEO ENTRE ESTÁNDARES Y FRAMEWORKS ENFOCADOS A LA GESTIÓN DE LA CONTINUIDAD.

5.3.1. COBIT 5 e ITIL V3

- N/A – No Aplica

COBIT 5		ITIL V3	
Evaluar, Orientar y Supervisar (EDM)	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno	**N/A**	
	EDM02. Asegurar la entrega de beneficios	**Estrategia del Servicio**	Gestión del Portafolio de Servicios
	EDM03. Asegurar la optimización del riesgo	**N/A**	
	EDM04. Asegurar la optimización de recursos	**Estrategia del Servicio**	Gestión de la Demanda
	EDM05. Asegurar la transparencia hacia las partes interesadas	**Estrategia del Servicio**	Gestión de las relaciones de negocios
Alinear, Planificar y Organizar (APO)	APO01. Gestionar el marco de gestión de las TI	**Mejora Continua del Servicio**	Proceso de Mejora
	APO02. Gestionar la estrategia	**Estrategia del Servicio**	Gestión de la Estrategia del Servicio
	APO03. Gestionar la arquitectura empresarial	**N/A**	
	APO04. Gestionar la innovación	**N/A**	
	APO05. Gestionar el portafolio	**Estrategia del Servicio**	Gestión del Portfolio de Servicios
			Gestión del Catálogo de Servicios
	APO06 Gestionar el presupuesto y los costes	**Estrategia del Servicio**	Gestión Financiera de los Servicios
	APO07 Gestionar los Recursos Humanos	**Diseño del Servicio**	Gestión de la Capacidad
	AP008 Gestionar las relaciones	**Estrategia del Servicio**	Gestión de la Demanda
			Gestión de las Relaciones de Negocios
	AP009 Gestionar los acuerdos de servicio	**Estrategia del Servicio**	Gestión del Portfolio de Servicios
			Gestión de la Demanda Diseño del Servicio
			Gestión del Catálogo de Servicios
			Gestión de Niveles de Servicio

		Mejora Continua del Servicio	Gestión de Informes
	APO10 Gestionar los Proveedores.	**Diseño del Servicio**	Gestión de Proveedores
	APO11 Gestionar la calidad	**Mejora Continua del Servicio**	Proceso de Mejora
	APO12 Gestionar el riesgo	**Diseño del Servicio**	Gestión de la Seguridad de la Información
	APO13 Gestionar la seguridad.	**Diseño del Servicio**	Gestión de la Seguridad de la Información
Construir, adquirir e implementar (BAI)	BAI01 Gestión de programas y proyectos	**N/A**	
	BAI02 Gestionar la definición de requisitos	**Diseño del Servicio**	Gestión de Niveles de Servicio
	BAI03 Gestionar la identificación y construcción de soluciones	**N/A**	
	BAI04 Gestionar la disponibilidad y la capacidad	**Diseño del Servicio**	Gestión de la Disponibilidad
			Gestión de la Capacidad
	BAI05 Gestionar la facilitación del cambio organizativo	**N/A**	
	BAI06 Gestionar los cambios.	**Transición del Servicio**	Gestión del Cambio
	BAI07 Gestionar la aceptación del cambio y la transición	**Transición del Servicio**	Planificación y soporte a la Transición
			Gestión de Entregas y Despliegues
			Evaluación del Cambio.
			Gestión del Conocimiento
	BAI08 Gestionar el conocimiento	**Transición del Servicio**	Gestión del Conocimiento
	BAI09 Gestionar los activos	**Transición del Servicio**	Gestión de la Configuración y Activos del Servicio
	BAI10 Gestionar la configuración	**Transición del Servicio**	Gestión de la Configuración y Activos del Servicio
Entrega, Servicio y Soporte (DSS)	DSS01 Gestionar operaciones	**Operación del Servicio**	Gestión de Eventos
	DSS02 Gestionar peticiones e incidentes de servicio	**Operación del Servicio**	Gestión de Incidentes
			Cumplimiento de Solicitudes
	DSS03 Gestionar problemas	**Operación del Servicio**	Gestión de Problemas
	DSS04 Gestionar la continuidad	**Diseño del Servicio**	Gestión de la Continuidad del Servicio
	DSS05 Gestionar servicios de seguridad.	**Diseño del Servicio**	Gestión de Seguridad de la Información
	DSS06 -Gestionar controles de procesos de negocio	**Operación del Servicio**	Gestión de Acceso
Supervisar, Evaluar y Valorar (MEA)	MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad	**Mejora Continua del Servicio**	Gestión de Informes
	MEA02 -Supervisar, evaluar y valorar el sistema de control interno.	**Mejora Continua del Servicio**	Proceso de Mejora

	MEA03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	**Mejora Continua del Servicio**	Proceso de Mejora

5.3.2. COBIT 5 – ISO 22301

	PLANEAR				HACER	VERIFICAR	ACTUAR
Cláusulas ISO 22301 / Sub Procesos COBIT 5 - DSS04	**Cláusula 4: Contexto de la organización**	**Cláusula 5: Liderazgo**	**Cláusula 6: Planificación**	**Cláusula 7: Soporte**	**Cláusula 8: Operaciones**	**Cláusula 9: Evaluación de desempeño**	**Cláusula 10: Mejora**
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	X						
DSS04.02 Mantiene una estrategia de continuidad.		X	X				
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.			X	X	X		
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					X		
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.					X	X	
DSS04.06 Proporcionar formación en el plan de continuidad.						X	
DSS04.07 Gestionar acuerdos de respaldo							X
DSS04.08 Ejecutar revisiones pos reanudación.						X	X

5.3.3. COBIT 5 – ISO 27002:2013

Práctica COBIT 5 - DSS04	Control ISO27002:2013

DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	A.17.1.1	Planificación de la continuidad de la seguridad de la información.	17.1 Continuidad de la seguridad de la información
DSS04.02 Mantiene una estrategia de continuidad.	A.17.1.1	Planificación de la continuidad de la seguridad de la información.	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	A.17.1.2	Implantación de la continuidad de la seguridad de la información.	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
DSS04.06 Proporcionar formación en el plan de continuidad.	N/A		
DSS04.07 Gestionar acuerdos de respaldo	A.12.3.1	Copias de seguridad de la información.	12.3 Copias de seguridad
	A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	17.2 Redundancias.
DSS04.08 Ejecutar revisiones pos reanudación.	N/A		

6. MODELO PROPUESTO DE GOBIERNO Y GESTIÓN PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO ORIENTADO A LA PRESTACIÓN DE SERVICIOS CRÍTICOS EN LAS HACIENDAS PÚBLICAS MUNICIPALES.

6.1. COMPONENTES DEL MODELO

La guía para la Preparación de las TIC para la Continuidad de Negocio (MINTIC, Guía para la Preparación de las TIC para la Continuidad del Negocio, 2010), descrito en el

ítem 5.2.1., es fundamental para el desarrollo de este trabajo, donde se realizaron los cambios a las políticas generales de acuerdo a las necesidades corporativas y tecnológicas actuales de las entidades Colombianas.

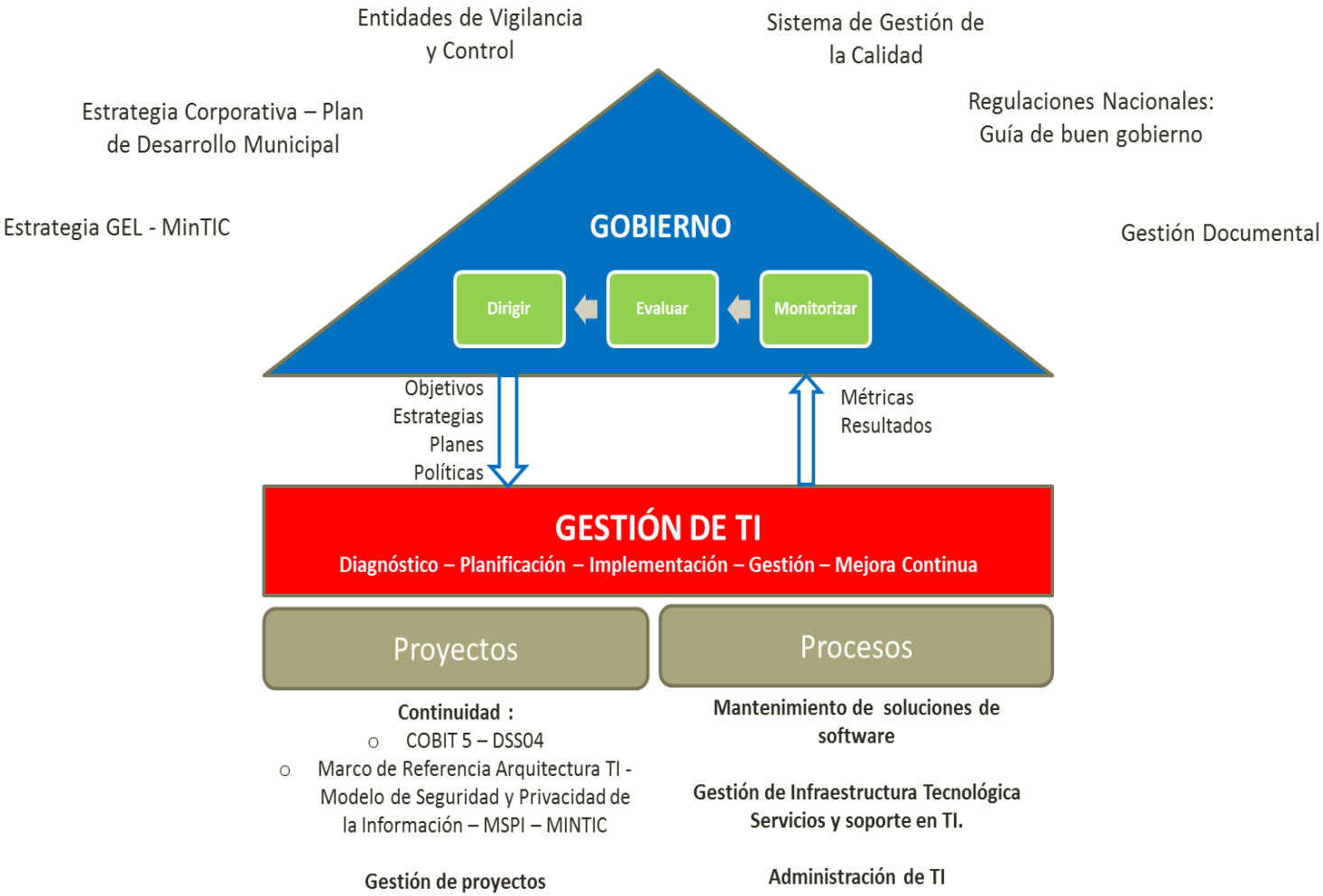
La guía fue diseñada con base al Marco de Seguridad y Privacidad de la Información, el cual define un ciclo de funcionamiento del modelo de operación de continuidad del negocio. Las fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema sostenible dentro de las entidades.

Las fases del modelo propuesto fueron desarrollas con base a los lineamientos de COBIT 5.0 en su dominio DSS - Entrega, Servicio y Soporte, proceso:

- DSS04 Gestión de la continuidad (Todas las prácticas)
- DSS05 Gestionar Servicios de Seguridad (Supervisar la Infraestructura de TI frente a eventos de seguridad)
- DSS06 Gestionar Controles de Proceso de Negocio (Asegurar los activos de información)

Para esto se definió un marco de continuidad para la recuperación de procesos de tecnología en las Haciendas Públicas Municipales, donde a cada fase o componente se le relacionan las prácticas aplicables del proceso de Gestión de la continuidad de Cobit5.

El modelo genérico de gobierno y gestión de TI está dado por:


Entidades de Vigilancia y Control
Sistema de Gestión de la Calidad
Estrategia Corporativa – Plan de Desarrollo Municipal
Regulaciones Nacionales: Guía de buen gobierno
Estrategia GEL - MinTIC
Gestión Documental
GOBIERNO
Dirigir
Evaluar
Monitorizar
Objetivos
Estrategias
Planes
Políticas
Métricas
Resultados
GESTIÓN DE TI
Diagnóstico – Planificación – Implementación – Gestión – Mejora Continua
Proyectos
Procesos
Continuidad :
COBIT 5 – DSS04
Marco de Referencia Arquitectura TI - Modelo de Seguridad y Privacidad de la Información – MSPI – MINTIC
Gestión de proyectos
Mantenimiento de soluciones de software
Gestión de Infraestructura Tecnológica
Servicios y soporte en TI.
Administración de TI

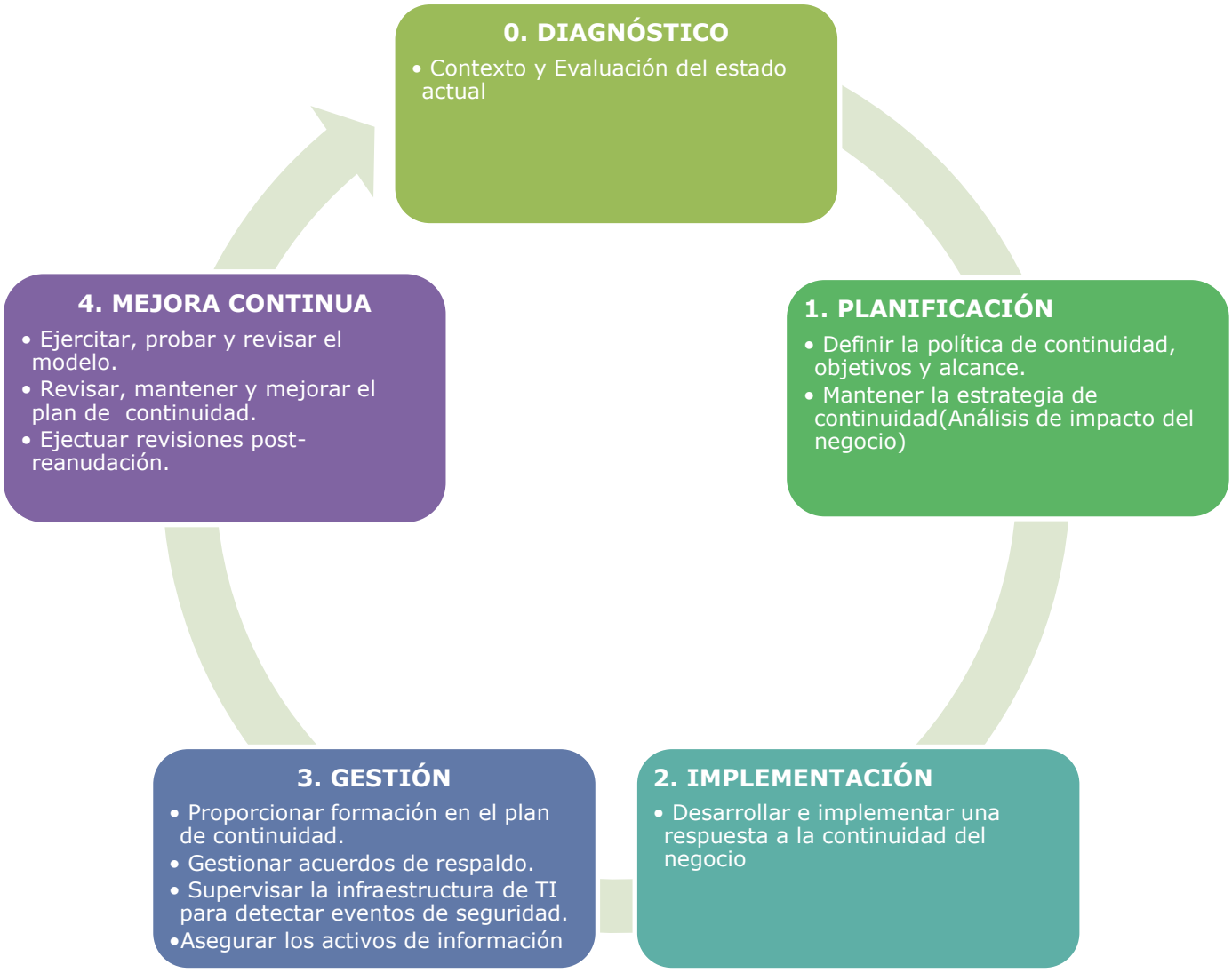


Ilustración 10. Modelo propuesto de gobierno y gestión de TI para garantizar la continuidad del negocio en las Haciendas Públicas Municipales.

De acuerdo al modelo planteado y teniendo como base el modelo de cascada de metas de Cobit5, se alinean las metas de TI, del negocio y los Objetivos de gobierno partiendo de los procesos que involucran la gestión de la continuidad:

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
GOBIERNO Y GESTIÓN DE LA CONTINUIDAD Procesos de COBIT 5		**Metas TI /**	Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de TI con las políticas internas	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			Financiera						**Cliente**		**Interna**							**Aprendizaje y Crecimiento**	
Entregar, Dar Servicio y Soporte	**DSS04**	Gestionar la Continuidad				**P**			**P**							**P**			
	DSS05	Gestionar los Servicios de Seguridad		**P**		**P**						**P**							
	DSS06	Gestionar los Controles de los Procesos del Negocio				**P**			**P**										

Ilustración 11. COBIT5 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

		Objetivos de Gobierno																	
		1. Valor para las Partes Interesadas de las Inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activo)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio
Dimensión	**Metas de TI**	**Financiera**					**Cliente**					**Interna**					**Aprendizaje y**	
Financiera	01 - Alineamiento de TI y la estrategia de negocio	P	P				P		P	P		P		P				
	02 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas				P											P		
	03 - Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P												P				
	04 - Riesgos de negocio relacionados con las TI gestionados			P				P			P							
Cliente	07 - Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P				P		P			P						
Interna	10 - Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	14 - Disponibilidad de información útil y fiable para la toma de decisiones							P		P								

Ilustración 12. COBIT5 Relación Primaria Metas Negocio con Metas TI

		Objetivos de Gobierno		
Dimensión	**Objetivo de negocio relacionado de Cobit 5**	**Entrega de beneficios**	**Optimización de riesgos**	**Optimización de recursos**
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio.	P		
	2. Cartera de productos y servicios competitivos	P	P	
	3. Riesgos de negocio gestionados (salvaguarda de activo)		P	
	4. Cumplimiento de leyes y regulaciones externas		P	
Cliente	6. Cultura de servicio orientada al cliente	P		
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		
	9. Toma estratégica de decisiones basadas en información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio			
	15. Cumplimiento con las políticas internas		P	

Ilustración 13. COBIT5 - Relación Objetivos de Negocio con Objetivos Gobierno

OBJETIVOS ESTRATÉGICOS DE GOBIERNO DE LAS SECRETARIAS DE HACIENDAS MUNICIPALES

Entrega de Beneficios	Optimización del riesgo	Optimización de recursos
▪ **Optimizar los procesos de la entidad y adoptar sistemas de información modernos, seguros, ágiles y bajo estándares internacionales que contribuyan a la efectividad del servicio.**	▪ Implementar nuevos estándares de gestión financiera y fiscal orientados a la eficiencia del ingreso, el gasto bajo parámetros de evaluación y seguimiento de riesgos en un ambiente de control.	▪ Implementar nuevos mecanismos de recaudo que faciliten el pago de las obligaciones. ▪ Orientar el talento humano al logro de los objetivos institucionales, fortaleciendo las competencia, la calidad de vida laboral y afianzando el sentido de pertenencia con la entidad.

6.1.1. Diagnóstico

Esta es el componente inicial o la fase preliminar para desarrollar el diagnóstico de la organización en cuanto a gobierno y gestión de la continuidad enfocada a servicios críticos. Se listaron las ocho prácticas de COBIT 5 del proceso DSS04 - Gestión de la Continuidad de Negocio, con las actividades mínimas para su cumplimiento y registro de cumplimiento. Cada actividad tiene un peso dentro de la práctica total, lo cual al final de la resolución de la encuesta genera un valor numérico porcentual de cumplimiento de la práctica.

La medición de la capacidad de la entidad, respecto a la gestión de la continuidad, fue desarrollada con el enfoque de evaluación de capacidad de procesos basado en el estándar ISO/IEC 15504. A cada subproceso se le genera una evaluación por rango y por niveles de capacidad.

Evaluación por Rango

ID	NOMBRE	RANGO
N	No alcanzado	0% al 15%
P	Parcialmente alcanzado	15% al 50%
L	Ampliamente alcanzado	50% - 85%
F	Completamente alcanzado	85% - 100%

Ilustración 14. Diagnóstico - Evaluación por Rango

Nivel de Capacidad

La evaluación por nivel de capacidad, está dada por el nivel de implementación de la práctica, en cuanto a las actividades del proceso. Está basada en la escala de evaluación utilizada en el MSPI.

Tabla de Escala de Valoración de la Práctica		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Secretaría no ha reconocido que hay un problema a tratar. No se aplican las prácticas de los procesos del GyG.
Inicial	20	Hay una evidencia de que la Secretaría ha reconocido que existe una situación y que hay que tratarla. No hay procesos estandarizados. La implementación de un actividad depende de cada individuo y es principalmente reactiva. Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y las actividades siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares.
Efectivo	60	Los procesos y las actividades se documentan y se comunican. Las actividades son efectivas y se ejecutan casi siempre. Es poco probable la detección de desviaciones cuando las actividades no se ejecutan oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Las actividades se monitorean. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Ilustración 15. Diagnóstico - Nivel de Capacidad

Así mismo, el cumplimiento de los atributos del proceso predeterminará el nivel de capacidad.

	Práctica		Diagnóstico Situación Actual Gobierno y Gestión de la Continuidad					
		Descripción	Actividades	Calificación Actual	Peso Actividad	Valor Práctica	Calificación Objetivo	GAP
PLANIFICACIÓN	DSS04.01	**Definir la política de continuidad del negocio, objetivos y alcance.**	¿Se encuentran identificados los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para la secretaría de hacienda?		30%	0	100	100
			¿Están identificados los roles y responsabilidades para definir la política de continuidad?		30%			
			¿La política de continuidad del negocio se encuentra definida y documentada?		40%			
	DSS04.02	**Mantener una estrategia de continuidad.**	¿Se realiza un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas de la secretaría y su efecto?		50%	0	100	100
			¿Se hace algún análisis de la probabilidad de amenazas que pueden causar pérdidas de continuidad de negocio y se identifican las medidas para reducir la probabilidad y el impacto?		25%			
			¿Se tiene aprobación del Secretario de Hacienda para implementar las estrategias identificadas?		25%			
IMPLEMENTACIÓN	DSS04.03	**Desarrollar e implementar una respuesta a la continuidad del negocio.**	¿Se encuentran definidos las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos críticos de la secretaría?		50%	0	100	100
			¿Los proveedores clave tienen implantados planes de continuidad efectivos?		20%			

			¿Están definidos y documentados los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI?		20%			
GESTIÓN	**DSS04.06**	**Proporcionar formación en el plan de continuidad.**	¿Existen planes de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes?.		100%	0	100	100
	DSS04.07	**Gestionar acuerdos de respaldo**	¿Se realizan copias de seguridad de los sistemas?		40%	0	100	100
			¿Las aplicaciones, sistemas o datos mantenidos por terceras personas se encuentran respaldadas?		30%			
			¿Se realizan pruebas periódicamente de las copias de seguridad?		30%			
	DSS05.07	**Supervisar la infraestructura TI para detectar eventos de seguridad.**	¿Se registró de los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura?		100%	0	100	100
	DSS06.06	**Asegurar los activos de información.**	¿Se aplican las políticas de clasificación de datos y seguridad y los procedimientos para proteger los activos de información bajo el control interno de la entidad?		100%	0	100	100

MEJORA CONTINUA	**DSS04.04**	**Ejercitar, probar y revisar el plan de continuidad.**	¿Se encuentran definidos los objetivos para probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio?		30%	0	100	100
			¿Existe un procedimiento de asignación de roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad?		30%			
			¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?		40%			
	DSS04.05	**Revisar, mantener y mejorar el plan de continuidad.**	¿Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?		50%	0	100	100
			¿Se comunican los cambios para la aprobación del Secretario de Hacienda?		50%			
	DSS04.08	**Ejectuar revisiones post-reanudación.**	¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?		40%	0	100	100
			¿ Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?		50%			

			¿ Se comunican los cambios para la aprobación del Secretario de Hacienda?		50%			
	PROMEDIO EVALUACIÓN DE PROCESOS					**0**	**100**	**100**

Ilustración 16. Instrumento para evaluar nivel de capacidad de los procesos de un modelo de gobierno y gestión de TI para garantizar la continuidad en las Hacienda Públicas Municipales tomando como Marco de Referencia de COBIT 5

6.1.2. Planificación

En este componente se definen la estrategia metodológica para establecer las políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la Entidad, la preparación de las TIC para la continuidad del negocio alineado a los objetivos de gobierno. Se basó en el proceso de Cobit 5:

- DSS04.01 Definir las políticas de continuidad de negocio, objetivos y alcance
- DSS04.02 Mantener una estrategia de Continuidad.

Las principales actividades son:

1. Identificar los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para las operaciones de la entidad o necesario para cumplir con las obligaciones legales y / o contractuales.
2. Identificar las partes interesadas y los roles y responsabilidades clave para definir y acordar la política de continuidad y alcance.
3. Definir y documentar los objetivos para la continuidad del negocio y la necesidad de integrar la planificación de la continuidad a la cultura empresarial.
4. Identificar posibles escenarios que puedan dar lugar a sucesos que podrían causar incidentes que afecten el normal funcionamiento de la entidad y por tanto la prestación de servicios al ciudadano.
5. Realizar un análisis de impacto de negocio (BIA) para evaluar el impacto en el tiempo de una interrupción de las funciones críticas o misionales de la entidad y el efecto que una interrupción podría tener en ellos.

El procedimiento para realizar el BIA es tomado de la Guía para realizar el Análisis de Impacto de Negocios[5]:

[5] Artículo 5482 del Modelo de Seguridad y Privacidad de la Información del Marco de Referencia Arquitectura de TI de MINTIC

Id	Fases	Descripción
1	Identificación de funciones y procesos	Identificar áreas y procesos apoyo a los procesos misionales de negocio y servicios de TI relacionados.
2	Evaluación de impactos Operacionales	El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio. Se hacen tablas de impacto, con esquemas de valoración, referente a la interrupción de la operación en los procesos listados en la fase anterior.
3	Identificación de Procesos críticos	La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según los valores de interpretación del proceso crítico: A - Crítico para el Negocio, la función del negocio no puede realizarse B - No es crítico para el negocio, pero la operación es una parte integral del mismo. C - La operación no es parte integral del negocio.
4	Establecimiento de tiempos de recuperación	Se establecen los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios: RPO - Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio. RTO - Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración. WRT - Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados, es

		decir, Tiempo de Recuperación de Trabajo. MTD - Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.
5	Identificación de activos	Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto es clave en este punto, la identificación de activos críticos de Sistemas de Tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades.
6	Identificación de procesos alternos	La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción.
7	Generación de Informe de Impacto del negocio	Listado de procesos críticos Listado de prioridades de sistemas y aplicaciones Listado de tiempos MTD, RTO y RPO Listado de procedimientos alternos

6. Evaluar la probabilidad de amenazas que podrían causar la pérdida de la continuidad del negocio y determinar las medidas que reduzcan la probabilidad y el impacto a través de una mejor prevención y una mayor capacidad de recuperación.
7. Identificar los requisitos de continuidad, analizar para identificar las posibles opciones estratégicas empresariales y técnicas.
8. Determinar las condiciones y los propietarios de las decisiones clave que hará que los planes de continuidad para ser invocados.

9. Obtener la aprobación del ejecutivo de negocios para las opciones estratégicas seleccionadas.

6.1.3. Implementación

Para la implementación del componente de planificación, se tiene en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia del Plan de Continuidad, las cuales deberán ser implementadas después de la aprobación de la alta dirección.

La implementación se gestiona como un proyecto a través del proceso de control de cambios formales de la Entidad y de los controles de gestión del proyecto de la Gestión de Continuidad del Negocio con el fin de asegurar visibilidad completa de la gestión y del reporte.

Las actividades generales a desarrollar en este proceso son:

1. Definir las acciones de respuesta a incidentes y las comunicaciones que deben adoptarse en caso de perturbación. Definir las funciones y responsabilidades relacionadas, incluyendo la rendición de cuentas de las políticas y su implementación.
2. Desarrollar y mantener operativos los procedimientos que deben seguirse para permitir la operación continua de los procesos críticos de negocio y / o régimen de temporales, incluyendo enlaces a los planes de los proveedores de servicios externalizados.
3. Asegurar que los proveedores clave tienen planes de continuidad de efectivos. Obtener evidencia auditada según sea necesario.
4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación del proceso de negocio, incluida la actualización y la recuperación de las bases de datos de información para preservar la integridad de la información.
5. Definir y documentar los recursos necesarios para apoyar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.

6. Definir y documentar los requisitos para las copias de seguridad de información necesarias para apoyar los planes, incluyendo los planes y documentos en papel, así como archivos de datos, y considerar la necesidad de seguridad y almacenamiento externo.
7. Determinar las habilidades necesarias para las personas involucradas en la ejecución del plan y los procedimientos.
8. Distribuir los planes y la documentación de apoyo debidamente autorizada a las partes interesadas y asegurarse de que son accesibles en todos los escenarios de desastre.

6.1.4. Gestión

Para el desarrollo de este proceso se tuvo como referencia Cobit 5.0 en sus prácticas:

- DSS04.06 - Llevar a cabo la formación y capacitación del plan de continuidad.
- DSS05.07 - Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
- DSS06.06 - Asegurar los activos de información.

En este proceso se determinan temas relacionados con la capacitación y sensibilización de todos los funcionarios de la entidad respecto a la continuidad del negocio, cuales son su roles y responsabilidades en caso de una emergencia.

En gestión también se definen cuáles son las habilidades y perfiles necesarios para restaurar las aplicaciones, sistemas y datos críticos de la organización en términos de conocimientos tecnológicos. Esto es en caso que sea necesario reemplazar en un momento dado a todos los miembros del equipo de TI, por ausencia o incapacidad.

Las principales actividades de esta práctica referentes a la práctica DSS04.06 son:

1. Definir y mantener los requisitos de formación y planes para los que realizan la planificación de continuidad, las evaluaciones de impacto, evaluaciones de riesgo, medios de comunicación y respuesta a incidentes. Asegúrese de que los planes de formación consideran la frecuencia y los mecanismos de entrega de capacitación y formación.

2. Desarrollar Competencias basados en la Formación Práctica, Incluyendo la Participación en Ejercicios y Pruebas.
3. Habilidades y competencias del líder en función de los ejercicios y resultados de pruebas.

De igual forma se agregaron prácticas adicionales de seguridad y protección de los datos que se manejan en la entidad, que es donde entran a jugar su papel el DSS05 Gestionar servicios de seguridad y DSS06 Gestionar Controles de Proceso de Negocio. Las principales actividades son:

1. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.
2. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.
3. Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse con base a la consideración de riesgo. Se debe retener por un periodo apropiado para asistir en futuras investigaciones.

En este proceso también se ejecuta la actividad que tal vez es la más importante en la Gestión de la Continuidad de Negocio, que es la gestión de backups. Para esto nos basamos en el subproceso de Cobit DSS04.06 Gestionar Copias de Seguridad. Las actividades generales son:

1. Documentación procedimiento de backup. Tener en cuenta:
    - Frecuencia (diario, semanal, mensual)
    - Modo de backup (ejemplo: duplicación de copias de seguridad en tiempo real)
    - Tipo de Backup (incremental, total)
    - Tipo de medios (cintas, DVD, Nube)
    - Tipos de datos

- Creación de registros
- Datos informáticos críticos de los usuarios (ejemplo: hojas de cálculo).
- Ubicación física y lógica de la fuente de datos.
- Seguridad y derechos de acceso
- Cifrado

2. Asegúrese de que los sistemas, las aplicaciones, los datos y la documentación que mantienen o son procesados por terceros están suficientemente apoyadas o aseguradas de otra manera. Considere la posibilidad de requerir devolución de las copias de seguridad de terceros. Considere la posibilidad de acuerdos de depósito en garantía o depósito.

3. Definir los requisitos para el almacenamiento en sitio y en custodia externa, de los datos de copia de seguridad que cumplen con los requerimientos del negocio. Tenga en cuenta la accesibilidad necesaria para realizar copias de seguridad de datos.

4. Formación y sensibilización. Establecer un control para asegurarse que el proceso se está llevando correctamente.

5. Realizar pruebas periódicas de recuperación de backup.

6.1.5. Mejora continua

Para definir el proceso de mejora continua, nos basamos en el numeral 10 de la norma ISO 22301:2012 y DSS04.4 probar y revisar el BCP; el DSS04.5 Revisar, mantener y mejorar el plan de continuidad y el DSS04.8 Revisión posterior a la reanudación.

La guía fundamenta la mejora continua en:

1. Administración del cambio de la organización. Cambios importantes de los procesos, estrategia, cambio del sector, cambio de políticas externas e internas, nueva regulación, cambios importantes a la infraestructura de tecnología, entre otros.

2. Capacitación del personal. Identificar oportunidades de mejora del plan mediante la participación activa los funcionarios de la entidad.
3. Resultados de las pruebas del plan de continuidad. Una vez ejecutadas las pruebas se definen los ítems o actividades que no se ejecutaron de acuerdo a lo planeado y los factores que contribuyeron al no cumplimiento, para definir oportunidades de mejora.

6.2. ROLES Y RESPONSABILIDADES DEL GOBIERNO Y LA GESTIÓN DE TI PARA GARANTIZAR LA CONTINUIDAD EN LAS SECRETARÍAS DE HACIENDA

Existen varios tipos de roles en la entidad, los cuales pueden ser de TI o de las diferentes áreas o dependencias, los cuales, de acuerdo al nivel de jerarquía, tienen distintos niveles de responsabilidad:

- R (responsable): La persona que está ejecutando la tarea.
- A (responsable de que se haga): Es la persona que rinde cuentas sobre el éxito de la tarea, es decir es el encargado de la correcta asignación de la misma.
- C (consultado): Es la persona que proporciona las entradas de información para la ejecución de las tareas.
- I (informado): Es la persona que recibe la información, este rol es el que recibe los entregables y/o logros de las tareas asignadas.

Las prácticas de los procesos junto con las responsabilidades y roles se especifican con base a la matriz RACI del proceso de Gestión de la Continuidad y Aseguramiento del Establecimiento y Mantenimiento del Marco de Gobierno:

Matriz RACI DSS04																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico Desarrollo Proyectos	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Mantener una estrategia de continuidad.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					I	R									I		R	R		C	R				A	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.				A	I	R					I							R		C	R				R	
DSS04.06 Proporcionar formación en el plan de continuidad.					I	R												R		R	R	R			A	
DSS04.07 Gestionar acuerdos derespaldo.																				C	A				R	
DSS04.08 Ejecutar revisiones post-reanudación.					C	R					I							R	C	C	R	R			A	

Ilustración 17. Matriz de Responsabilidades Prácticas clave del Proceso DSS04 COBIT5. Tomado de (ISACA, 2012)

6.3. MÉTRICAS

Tomando como referencia la cascada de metas de Cobit 5 se definieron las métricas por proceso, por las metas de TI relacionadas a los procesos y por las metas Corporativas alineadas a las metas de TI.

6.3.1. Métricas de los procesos

ÁREA	PROCESO	META	Métricas
GESTIÓN	DSS04 Gestionar la Continuidad	1. La información crítica está disponible para la Secretaría de Hacienda en línea con los niveles de servicio mínimos requeridos.	% de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
			% de medios de respaldo almacenados de forma segura.
		2. Los servicios críticos tienen resiliencia.	# de sistemas críticos para el negocio no cubiertos por el plan.
		3. Las pruebas de continuidad del servicio han sido efectuvas de acuerdo al BCP.	# de pruebas que han conseguido los objetivos de recuperación.
			Frecuencia de las pruebas
		4. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	% de mejoras acordadas que han sido reflejadas en el plan.
		5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	% de interesados internos y externos que han recibido formación.
			% de asuntos identificados que se han tratado subsecuentemente en los materiales de formación

Ilustración 19. Métricas de los Procesos. Elaborado con base a Métricas de Cobit 5

6.3.2. Métricas de las metas de TI de los procesos

ÁREA	PROCESO	META DE TI	Métricas
GESTIÓN	DSS04 Gestionar la Continuidad	04 Riesgos de negocio relacionados con las TI gestionados	% de servicios críticos de TI cubiertos por evaluaciones de riesgos.
		07 Entrega de servicios TI de acuerdo a los requisitos del negocio	% de usuarios satisfechos con la calidad de los servicios de TI entregados
		14 Disponibilidad de información útil y relevante para la toma de decisiones	Nivel de satisfacción de los usuarios del negocio y disponibilidad de la información de gestión.

Ilustración 20. Métricas de las metas de TI. Elaborado con base a Métricas de Cobit 5

6.3.3. Métricas de las metas Corporativas con las metas de TI de los procesos

Dimensión	Metas Corporativas relacionadas con las Metas de TI	Métricas
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio.	% de inversiones en las que la entrega cumple con las expectativas de los interesados
	2. Cartera de productos y servicios competitivos	% de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente
	3. Riesgos de negocio gestionados (salvaguarda de activo)	% de objetivos de negocio críticos y servicios cubiertos por gestión del riesgo
Cliente	6. Cultura de servicio orientada al cliente	# de quejas de clientes debido a incidentes relacionados con el servicio TI
	7. Continuidad y disponibilidad del servicio de negocio	# de interrupciones de servicio al cliente
	8. Respuestas ágiles a un entorno de negocio cambiante	Nivel de satisfacción del Consejo de Administración con la capacidad de respuesta corporativa a nuevos requerimientos del Estado o entidades externas.
	9. Toma estratégica de Decisiones basadas en información	Tiempo requerido para ofrecer información de apoyo que permita decisiones de negocio efectivas.
	10. Optimización de costes de entrega del servicio	Frecuencia de las evaluaciones de optimización del coste de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio	Frecuencia de las evaluaciones de madurez de la capacidad de los procesos
	13. Programas gestionados de cambio en el negocio	Número de programas cumplidos en tiempo y en presupuesto

Ilustración 21. Métricas de las metas Corporativas alineadas a las metas de TI. Elaborado con base a Cobit 5

7. MODELO DE MADUREZ

El cumplimiento de los atributos del proceso predetermina el nivel de capacidad, y de ahí el nivel de madurez viene determinado por los niveles de capacidad de todos los procesos asociados.

De acuerdo al nivel de capacidad definido en el componente de Diagnóstico (6.1), el modelo define las reglas de derivación para los Niveles de madurez, basados en el sistema de evaluación de la norma ISO/IEC 155045:

NIVEL DE MADUREZ	REGLA DE DERIVACIÓN	DESCRIPCION	CALIFICACIÓN DEL COMPONENTE (hasta)
0	La secretaría no tiene una implementación efectiva de los procesos[6].	**Organización**[7] **inmadura**. En este nivel no se han implementado los procesos, por consiguiente no se alcanza el propósito de la secretaría, ni se identifican productos o salidas de proceso. Por consiguiente no hay atributos que evaluar en este nivel.	**0**
1	Los procesos objeto de evaluación alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.	**Organización básica**. En este nivel la organización simplemente implementa y alcanza de manera básica los resultados del proceso y al alcanzar los resultados propuestos es posible identificar satisfactoriamente las salidas (resultados) del proceso evaluado.	**20**
2	Los procesos de nivel de	**Organización**	**40**

[6] Procesos hace referencia a los procesos que hacen parte del componente del modelo de Gobierno y Gestión de TI para garantizar la continuidad de las Secretarías de Hacienda Municipales.
[7] Organización hace referencia a las Secretarías de Hacienda

	madurez 2, tienen nivel de capacidad 2 o superior.	**gestionada**. La organización además de implementar los objetivos del proceso, demuestra una planificación, seguimiento y control 60tanto de los procesos, como de sus productos de trabajo asociados.	
3	Los procesos de nivel de madurez 2 y 3 tienen nivel de capacidad 3 o superior.	**Organización establecida**. En este nivel de madurez los procesos se estandarizan para toda la organización.	**60**
4	Uno o más de los procesos tienen nivel de capacidad 4 o superior.	**Organización predecible**. La organización gestiona cuantitativamente los procesos, es decir, se miden y se analiza el tiempo de su realización.	**80**
5	Uno o más procesos tienen nivel de capacidad 5.	**Organización optimizada**. Se lleva a cabo una monitorización continua de los procesos y se analizan los datos obtenidos.	**100**

Ilustración 22. Diagnóstico - Nivel de Madurez

8. GUÍA DE IMPLEMENTACIÓN DEL MODELO Y CASO DE ESTUDIO

Teniendo en cuenta el mapeo de la norma ISO 22301 con Cobit 5, se define una guía de implantación del modelo propuesto.

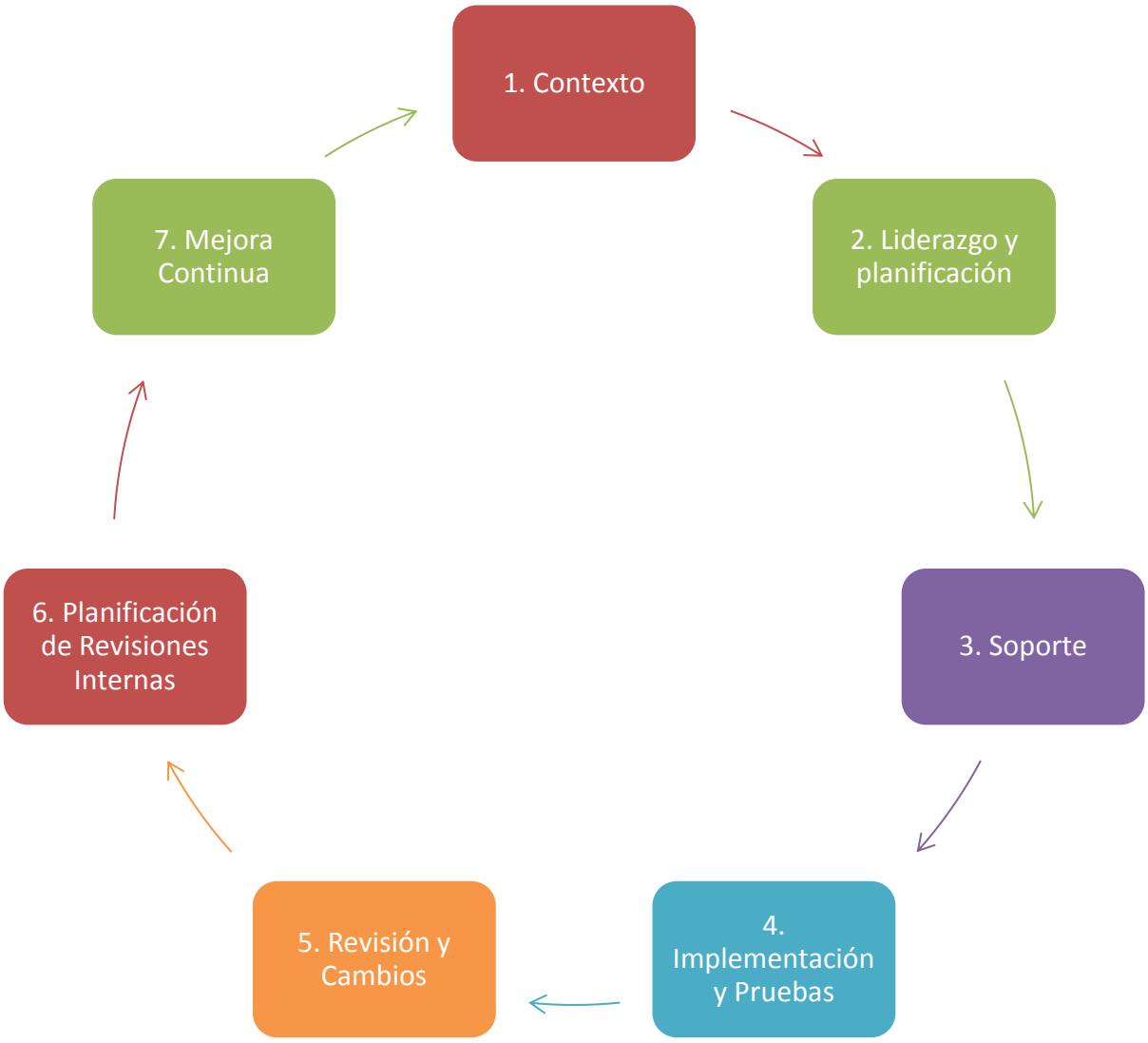


Ilustración 23. Fases de la implementación del ciclo de vida. ISO 22301.

Fase	Entregables	Componente del Modelo
1. Contexto	Conocimiento de la organización ▪ Identificación de stakeholders o responsables ▪ Procesos misionales ▪ Elección del proceso crítico ▪ Estado actual y objetivo – Herramienta de Diagnóstico	0. DIAGNÓSTICO
2. Liderazgo y planificación	Política de Continuidad del Negocio ▪ Creación de equipos ▪ Propósito y Alcance ▪ Identificación de activos: Se hace valoración del activo de información y la clasificación (Componente de Gestión - Asegurar activo de información– Práctica Cobit DSS06) ▪ Identificación de Riesgos ▪ Análisis de impacto del negocio	1. PLANIFICACIÓN 4. GESTIÓN
3. Soporte	Formulación del Plan de Continuidad del Negocio Definición de fases para la activación del plan de emergencias	2. PLANIFICACIÓN
4. Implementación y pruebas	Escenarios de pruebas del Plan de Continuidad del Negocio Cronograma de pruebas Plan de capacitación	3. IMPLEMENTACIÓN 4. GESTIÓN
5. Revisión y cambios	Cambios al plan de continuidad	5. MEJORA CONTINUA
6. Planificación de revisiones internas	Cronograma de capacitación al personal Plan de respaldo o copias de seguridad	4. GESTIÓN

7. Mejora continua	Revisión del modelo y Mejora Continua	5. MEJORA CONTINUA

8.1. CONTEXTO.

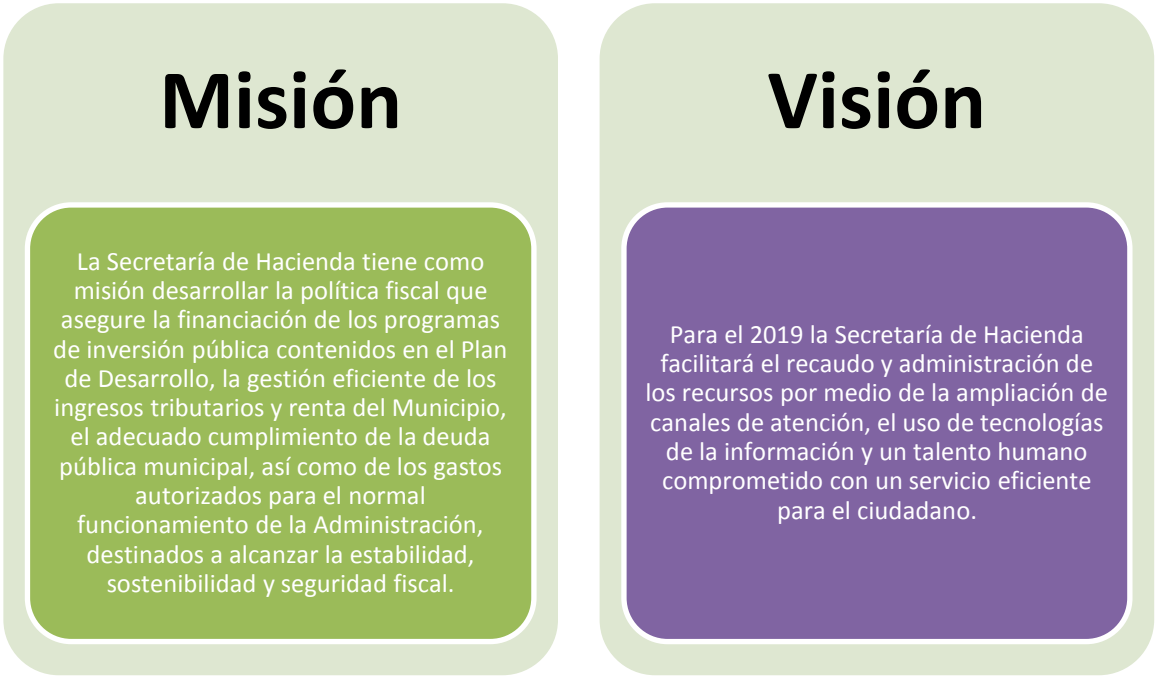
CASO DE ESTUDIO: SECRETARÍA DE HACIENDA DEL MUNICIPIO DE PUERTO COLOMBIA (ATLÁNTICO)

La alcaldía del municipio de Puerto Colombia, es una entidad pública del orden territorial, que al igual que sus entidades homólogas, debe estar comprometida con la implementación de herramientas y mejores prácticas, como parte de la estrategia nacional de gobierno electrónico, para fortalecer su gestión administrativa y cumplimiento de los objetivos de gobierno, mediante la apropiación de las tecnologías para la seguridad y privacidad de la información en los procesos críticos, como es la gestión tributaria, la gestión financiera, presupuestal y contable y , cuyo objetivo es dotar a la entidad de recursos propios para el cumplimiento de sus metas y el bienestar de la comunidad.

Así, es preciso que se establezca un marco de gobierno que ayude a dar un enfoque a la continuidad en este proceso y se alinee con la estrategia de continuidad del negocio, aplicando guías prácticas que han sido bien aceptadas por la industria, como lo es el marco de referencia Cobit 5, que presenta y cubre aspectos fundamentales como lo es la gestión de la continuidad del negocio, cubriendo aspectos generales del Modelo de Seguridad y Privacidad de la Información del Marco de referencia de Arquitectura de TI propuesto por el Gobierno Nacional a través de la guía de preparación para la continuidad del negocio.

El marco de gobierno debe garantizar la restauración oportuna de las operaciones esenciales como son los trámites en línea, servicios de webservice con entidades financieras, portal de impuestos, notificaciones, fiscalización, cobro coactivo, interoperabilidad, gestión presupuestal y contable, y convenio con la Ventanilla Única de Registro con la Superintendencia de Notariado y Registro, entre otros. La falta de disponibilidad de estos servicios, causados por diferentes incidentes, y la posible pérdida de información tiene consecuencia directa en la prestación de servicios de información al usuario y entidades externas, afectando el recaudo de los impuestos municipales, el acceso a los trámites por parte de los contribuyentes y la toma de decisiones en la gestión administrativa y financiera.

8.1.1. Información Institucional Secretaría de Hacienda del Municipio de Puerto Colombia.



Funciones

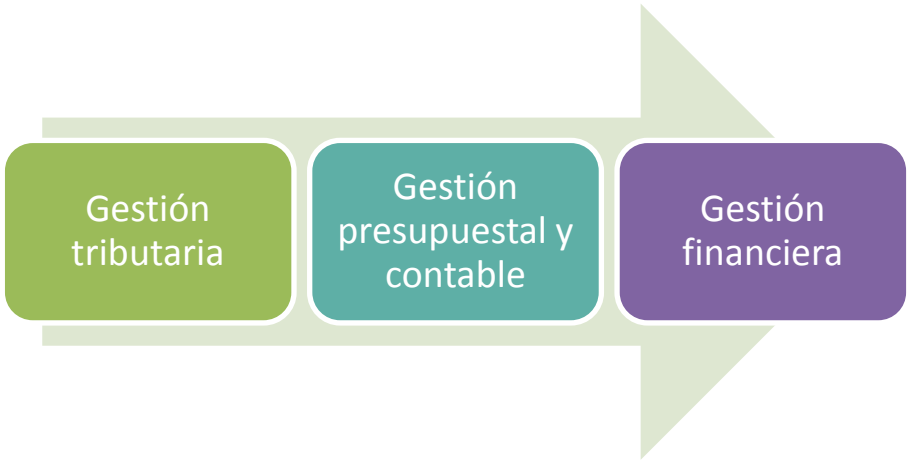
- Diseñar la estrategia financiera del Plan de Desarrollo y del Plan de Ordenamiento Territorial.
- Preparar el prepuesto anual de ingresos y de gastos.
- Formular, orientar y coordinar las políticas en materia fiscal y de crédito público.
- Gestionar los tributos del municipio mediante la actualización de la información sobre hechos generadores, sujetos pasivos, bases gravables y tarifas de impuestos, tasas y contribuciones; el desarrollo de los procesos de aforo, liquidación y facturación; la celebración de compromisos de pago, la presentación de informes del estado de las obligaciones y cartera del municipio y el ejercicio de la jurisdicción coactiva.
- Dirigir y controlar la gestión financiera, presupuestal y contable del Municipio.
- Proveer y consolidar la información, las estadísticas, los modelos y los indicadores financieros.
- Gestionar, hacer el seguimiento y controlar los recursos provenientes del orden

nacional.

Para gestionar los tributos los municipios cuentan con herramientas y procesos debidamente estructurados para el logro de las metas de recaudo de ingresos propios en la entidad territorial. Estas herramientas y procesos están soportadas por:

- Herramientas informáticas y de logística.
- Convenios de recaudo con entidades financieras.
- Sistemas de información de control tributario, fiscalización, determinación oficial y liquidación.
- Portal de pagos.
- Interface con otros sectores del Gobierno.
- Integración de sistemas de información con otros procesos.

➢ **Procesos misionales y funciones esenciales**



▪ **Gestión tributaria:**

Proceso Nivel A - Crítico para la Secretaría, la función del negocio no puede realizarse. Sus principales actividades son:

- Participar en la formulación y ejecución del plan estratégico.
- Formular la política tributaria en el marco del modelo tributario del municipio.
- Dirigir y controlar los procesos administrativos de inteligencia tributaria, recaudo, determinación, liquidación, discusión, cobro, devolución y servicio al

contribuyente, de los impuestos municipales.

- Definir y establecer los criterios de clasificación y gestión de los contribuyentes de los impuestos municipales.

- **Gestión presupuestal y contable:**

Proceso Nivel B - No es crítico para la Secretaría, pero la operación es una parte integral del mismo. Principales actividades:

- Participar en la formulación y ejecución del plan estratégico de la Secretaría de Hacienda.
- Dirigir el proceso de formulación, programación, ejecución, seguimiento y cierre presupuestal y fiscal.
- Dirigir el diseño de procedimientos, reglamentación y generación de información en materia presupuestal.
- Asesorar a la Administración Distrital en la priorización de recursos y la asignación presupuestal.
- Dirigir la administración del sistema de información presupuestal.

- **Gestión financiera**

Proceso Nivel B - No es crítico para la Secretaría, pero la operación es una parte integral del mismo. Principales actividades:

- Dirigir la evaluación financiera de los activos financieros a recibir.
- Coordinar la distribución, consolidación, seguimiento a la ejecución y control del programa anual mensualizado de Caja PAC.
- Administrar los Sistemas de Información de la dependencia.

8.1.2. Elección de proceso crítico

Gestión tributaria: El municipio constituye la célula básica de la organización estatal e interactúa de manera directa con el ciudadano en la prestación de servicios. Para tal

efecto requiere de ingresos propios para su funcionamiento por lo que la gestión tributaria es uno de los procesos críticos para garantizar la disponibilidad de los servicios y trámites para el logro de los objetivos estratégicos de la entidad en cuanto a recaudo y atención.

Las aplicaciones y plataformas que apoyan la Gestión Tributaria en la Alcaldía Municipal de Puerto Colombia son:

- Sistema web de impuesto predial e industria y comercio
- Portal web para trámites en línea
- Webservice de recaudo con Entidades Financieras
- Convenio de acceso con la Superintendencia de Notariado y Registro a información de estado de cuenta de contribuyentes del Impuesto Predial, a través de la Ventanilla única de Registro.
- Interconectividad con sistema administrativo y financiero de Hacienda.
- Sistema web para la gestión de cobro prejurídico y coactivo

8.1.3. Estado actual

De acuerdo a la fase preliminar del modelo, Diagnóstico, se realiza la evaluación del estado actual, con el instrumento diseñado, teniendo en cuenta el proceso crítico elegido de Gestión Tributaria.

Instrumento para evaluar nivel de capacidad de los procesos de un modelo de gobierno y gestión de TI para garantizar la continuidad en las Hacienda Públicas Municipales tomando como Marco de Referencia de COBIT 5

	Práctica		Diagnóstico Situación Actual Gobierno y Gestión de la Continuidad							
	Práctica	Descripción	Actividades	Calificación Actual	Peso Actividad	Valor Práctica	Calificación Objetivo	GAP	Nivel de Madurez del Componente	NIVEL DE MADUREZ
PLANIFICACIÓN	DSS04.01	**Definir la política de continuidad del negocio, objetivos y alcance.**	¿Se encuentran identificados los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para la secretaría de hacienda?	50	30%	21	100	79	22	GESTIONADA
			¿Están identificados los roles y responsabilidades para definir la política de continuidad?	20	30%					
			¿La política de continuidad del negocio se encuentra definida y documentada?	0	40%					

	DSS04.02	**Mantener una estrategia de continuidad.**	¿Se realiza un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas de la secretaría y su efecto?	10	50%	23	100	78		
			¿Se hace algún analisis de la probabilidad de amenazas que pueden causar pérdidas de continuidad de negocio y se identifican las medidas para reducir la probabilidad y el impacto?	10	25%					
			¿Se tiene aprobación del Secretario de Hacienda para implementar las estrategias identificadas?	60	25%					
IMPLEMENTACIÓN	**DSS04.03**	**Desarrollar e implementar una respuesta a la continuidad del negocio.**	¿Se encuentran definidas las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos	20	50%	26	100	74	26	GESTIONADA

			críticos de la secretaría?							
			¿Los proveedores clave tienen implantados planes de continuidad efectivos?	70	20%					
			¿ Estan definidos y documentados los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI?	10	20%					
GESTIÓN	**DSS04.06**	**Proporcionar formación en el plan de continuidad.**	¿Existen planes de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes?.	20	100%	20	100	80	45	ESTABLECIDO

	DSS04.07	**Gestionar acuerdos de respaldo**	¿Se realizan copias de seguridad de los sistemas?	80	40%	59	100	41		
			¿Las aplicaciones, sistemas o datos mantenidos por terceras personas se encuentran respaldadas?	70	30%					
			¿Se realizan pruebas periódicamente de las copias de seguridad?	20	30%					
	DSS05.07	**Supervisar la infraestructura TI para detectar eventos de seguridad.**	¿ Se registro de los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura?	50	100%	50	100	50		
	DSS06.06	**Asegurar los activos de información.**	¿ Se aplican las políticas de clasificación de datos y seguridad y los procedimientos para proteger los activos de información bajo el control interno de la entidad?.	50	100%	50	100	50		

MEJORA CONTÍNUA	**DSS04.04**	**Ejercitar, probar y revisar el plan de continuidad.**	¿Se encuentran definidos los objetivos para probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.?	10	30%	9	100	91	25	GESTIONADA
			¿Existe un procedimiento de asignación de roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad?	20	30%					
			¿Existe un plan de ejercicios y actividades de prueba, tal como esta definido en el plan de continuidad?	0	40%					
	DSS04.05	**Revisar, mantener y mejorar el plan de continuidad.**	¿ Se revisa el plan de continuidad regularmente teniendo en	10	50%	5	100	95		

			cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?							
			¿ Se comunican los cambios para la aprobación del Secretario de Hacienda?	0	50%					
	DSS04.08	**Ejectuar revisiones post-reanudación.**	¿Existe un plan de ejercicios y actividades de prueba, tal como esta definido en el plan de continuidad?	30	40%	62	100	38		
			¿ Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de	20	50%					

			aplicaciones?							
			¿ Se comunican los cambios para la aprobación del Seretario de Hacienda?	80	50%					
	PROMEDIO EVALUACIÓN DE PROCESOS					**32**	**100**	**68**	**29**	

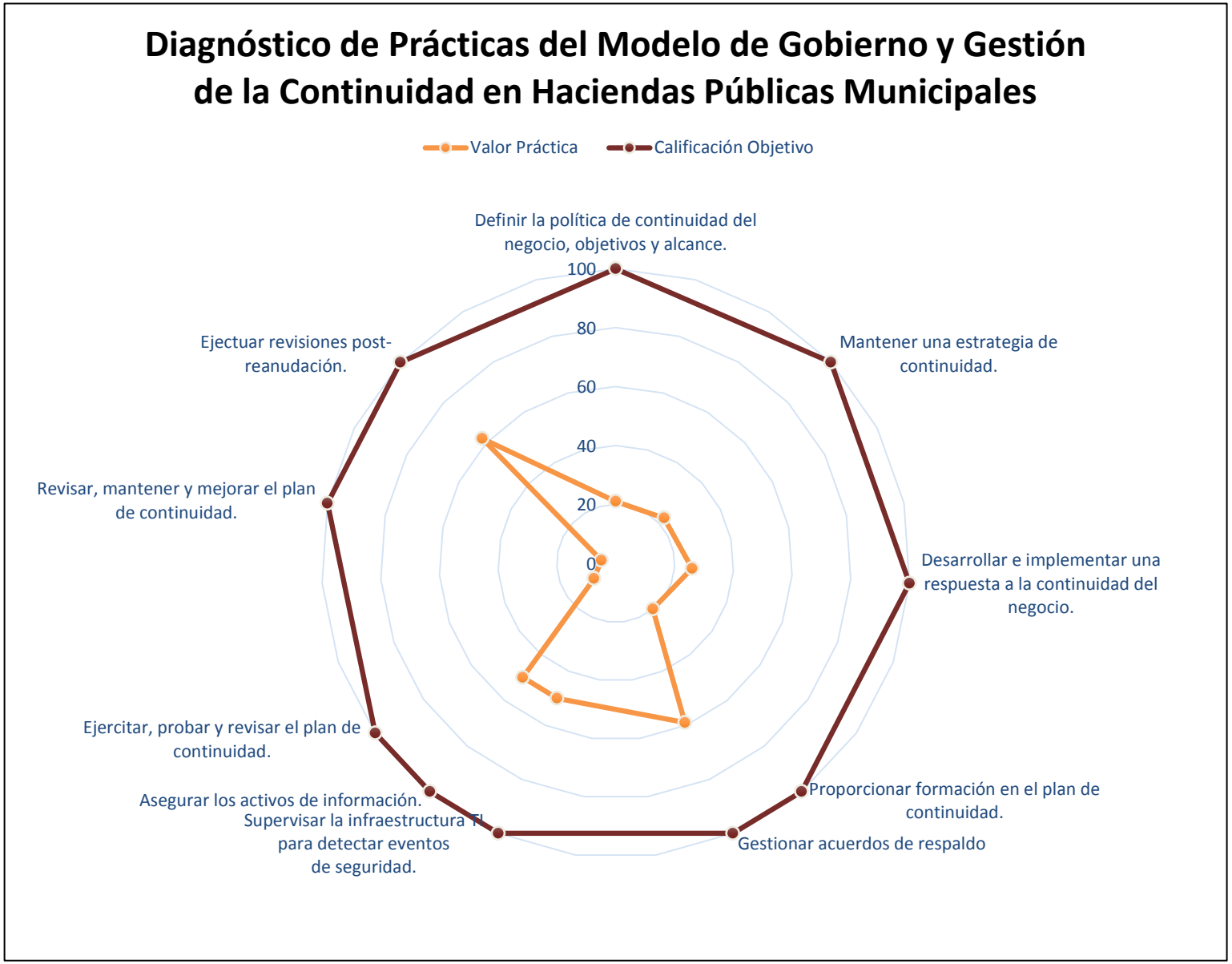


Ilustración 24. Diagnóstico Gestión de la Continuidad de la Secretaría de Hacienda de Puerto Colombia. Proceso Gestión Tributaria

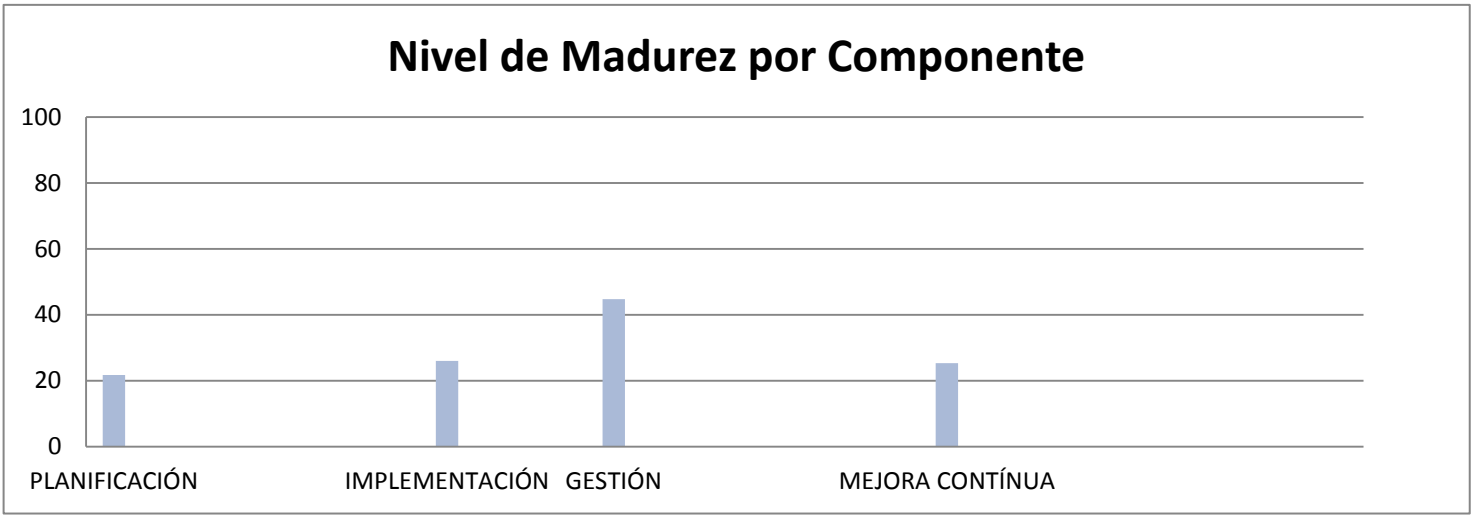


Ilustración 25. Diagnóstico por componente del modelo de Gobierno y Gestión

Para el desarrollo del componente de Seguridad y Privacidad de la Información, el Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC, ha definido los lineamientos a través del decreto 1078 de 2015[8], único reglamentario del sector de tecnologías de información y las comunicaciones, como parte integral de la estrategia GEL, y es de obligatorio cumplimiento para las entidades del estado de orden territorial.

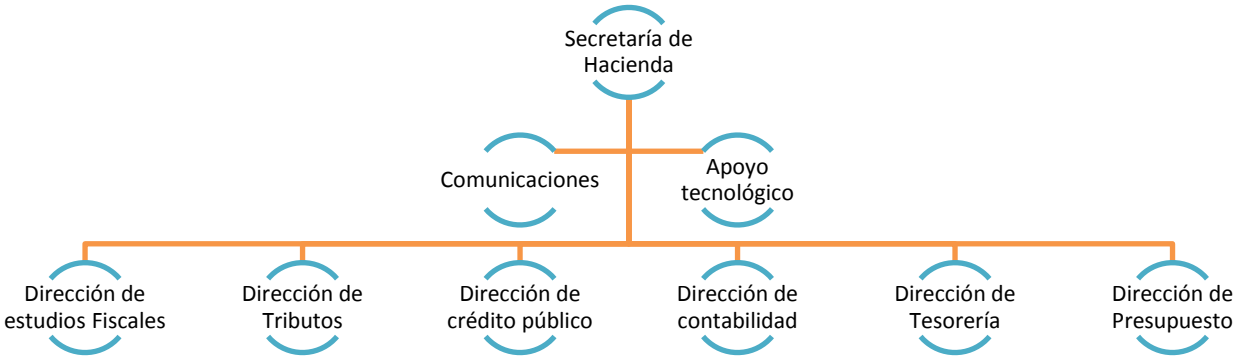
De acuerdo a los plazos establecidos según Decreto 2573 de 2014, en el Articulo 10. Plazos, las Alcaldías de categoría cuarta, quinta y sexta y demás sujetos obligados de la Administración Pública en el mismo nivel deberán tener un 100% de porcentaje de cumplimiento del modelo para el año 2020, siendo para el 2018 el 65%.

8.2. Liderazgo y planificación

8.2.1. Responsables de mayor nivel de la continuidad del negocio.

- **Organigrama Secretaría de Hacienda**

[8] Decreto 1078 de 2015. TITULO 9, POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPITULO 1, Estrategia de Gobierno en Línea - GEL, en la SECCIÓN 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES.



La oficina de Apoyo tecnológico es la Dirección de Informática y Tecnología de la Alcaldía de Puerto Colombia, donde algunas sus funciones enfocadas a la Secretaría de Hacienda son:

a. Participar en la formulación y ejecución del Plan Estratégico de la Secretaría de Hacienda.
b. Asesorar en los temas relacionados con las Tecnologías de la Información y las Comunicaciones.
d. Dirigir el Plan Estratégico de TIC y realizar su seguimiento y evaluación.
e. Formular y adoptar las políticas y estrategias tecnológicas para el buen uso, administración y explotación de la información de la Secretaría de Hacienda.
f. Proponer y adoptar las políticas de administración e implementación de TIC por parte de la Secretaría Hacienda.
g. Proponer y adoptar las políticas de seguridad informática que permitan el adecuado uso y acceso a las TIC de la Secretaría de Hacienda, buscando garantizar la integridad y privacidad de la información en un modo de operación seguro y de comunicación libre de intrusos, que permitan mantener la privacidad, disponibilidad, integridad y no repudio de la información.
h. Formular las políticas de custodia, administración, respaldo y seguridad de la información misional de la Secretaría de Hacienda.
i. Formular las políticas de administración, seguridad y control necesarias para garantizar la eficacia, eficiencia y confiabilidad de los recursos de las TIC de la Secretaría de Hacienda.
j. Garantizar la aplicación a nivel institucional de los estándares, buenas prácticas y

principios para la información de la Secretaría de Hacienda.

k. Formular el plan de contingencia y continuidad que garantice la disponibilidad y operación de los servicios de TIC de la Secretaría de Hacienda.

La oficina de Apoyo Tecnológico, Dirección de Informática y Tecnología, cuenta con 3 roles cuyas funciones alineadas a la Secretaría de Hacienda son:

Coordinador de Infraestructura de TI	Coordinador de Soluciones de TIC	Coordinador de Servicios de TIC
• Mantener actualizado los componentes de infraestructura y comunicaciones de la Secretaría de Hacienda y coordinar su ejecución. • Establecer y verificar el cumplimiento de políticas de servicios informáticos de conectividad y seguridad para el transporte de la información • Cumplir las políticas y estándares de control de seguridad de infraestructura de comunicaciones y de acceso a datos y aplicaciones de la Secretaría de Hacienda • Administrar la infraestructura tecnológica que se le asigne para garantizar la operación de los servicios de la Secretaría de Hacienda.	• Asesorar en la elaboración y ejecución del Plan de acción de la Dirección de Informática y Tecnología • Proponer la metodología de mantenimiento de software • Coordinar la adquisición, diseño y mantenimiento del software que hace parte de los Sistemas de Información de la Secretaría de Hacienda. • Gestionar los procesos de implementación del software desarrollado, teniendo en cuenta la integración de las plataformas e infraestructura de la Secretaría de Hacienda	• Mantener actualizado el catálogo de Servicios de la Dirección de Informática y Tecnología dispuestos tanto para los usuarios internos y externos • Realizar la gestión y administración de las garantías del inventario de los equipos de • escritorio, portátiles, impresoras y otros equipos informáticos a nivel de cliente y su correspondiente software • Resolver incidentes de tecnología reportados por funcionarios o usuarios externos.

- **Esquema organizacional para la continuidad**

  Se crea un esquema organizacional de manera que incluya los roles determinantes que intervienen en la planeación, el manejo de crisis, la respuesta, la recuperación y la logística.

- **Comité Directivo:**

  Es el comité de mayor nivel de la continuidad del negocio, que administra y verifica los recursos necesarios para recuperar las operaciones críticas de la Secretaría de Hacienda en caso de ocurrencia de una contingencia y/o emergencia. Está conformado por todas las direcciones, liderado por el responsable de la entidad, el Secretario de Hacienda y cuyo orden jerárquico es:

- Secretario de Hacienda – Líder del comité
- Director de tributos
- Director de estudios Fiscales
- Director de crédito público
- Director de Contabilidad
- Director de Tesorería
- Director de Presupuesto
- Asesor de comunicaciones
- Líder de apoyo tecnológico asignado (Coordinado de Servicios TIC)

✓ Cuando se presente una contingencia y/o emergencia se deberá contar como mínimo, con el líder del comité o suplente y con dos integrantes.

✓ El ordenador del gasto en caso de contingencia y/o emergencia es el Director de Tributos. Si no se encuentra presente, asume el lugar el que le sigue en la jerarquía.

✓ El Asesor de Comunicaciones es el responsable tanto de la notificación de la contingencia y/o emergencia a los medios externos e internos.

8.2.2. Política de continuidad de la Gestión Tributaria

Alcance

La presente Política de Continuidad de Negocio es de obligatorio cumplimiento en la Dirección de Tributos.

Objetivos

Mediante esta política se establece el marco para el desarrollo, implantación, revisión y mejora del plan de Continuidad del negocio en el proceso de gestión Tributaria, de manera que:

- Faciliten una respuesta apropiada y oportuna ante la materialización de un

riesgo de seguridad o del entorno con características catastróficas, que provoquen un escenario de falta de disponibilidad de alguno de los componentes básicos de la actividad de la gestión tributaria: personas, infraestructura, tecnología, información y procesos.

- Disminuir el impacto de las posibles catástrofes sobre las actividades de negocio, garantizando que se preservan las funciones esenciales y si no es el caso, que las funciones se recuperen paulatinamente.

Responsabilidades:

El Comité Directivo y, por delegación de éste, el Comité de Crisis, es el responsable de impulsar el desarrollo e implantación de los Planes de Continuidad de Negocio en la Secretaría de Hacienda, decidir y coordinar las actividades de continuidad de negocio, así como la revisión periódica de esta Política. Igualmente, asume la dirección ejecutiva y la gestión de aquellas situaciones de crisis derivadas de un desastre que tengan repercusiones en toda la entidad.

8.2.3. Identificación de Activos

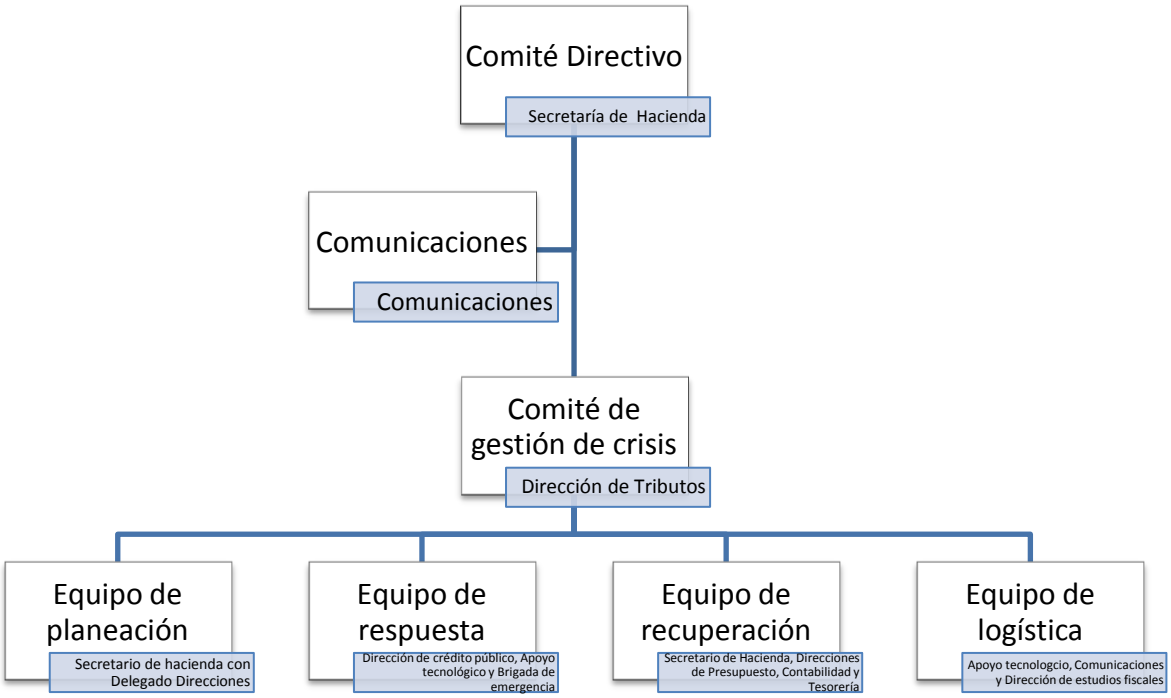
		Atributos del activo				Ubicación	Valoración del Activo de Información				Clasificación de la Información		
Tipo	Nombre Activo	¿El activo contiene datos personales?	¿El activo es susceptible de fraude o corrupción?	¿El activo es vital para la operación del proceso?	¿El activo es vital para la operación de la SDH?		Confidencialidad	Integridad	Disponibilidad	Criticidad	Confidencialidad	Integridad	Disponibilidad
Datos / Información	Procesos de Gestión tributaria	Si	Si	Si	Si	Dirección de Tributos	Alto	Alto	Alto	**Crítico**	**Pública Reservada**	**Crítica**	**Crítica**
Software	Portal de pagos	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Datos / Información	Conciliaciones Entidades Recaudadoras	Si	No	Si	No	Dirección de Tesorería	Bajo	Bajo	Bajo	**No Crítico**	**Pública**	**No Crítica**	**No Crítica**
Datos / Información	Declaraciones Tributarias	Si	No	Si	Si	Dirección de Tributos	Alto	Alto	Alto	**Crítico**	**Pública Reservada**	**Crítica**	**Crítica**

Hardware	Servidores	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Hardware	Equipos de escritorio	Si	Si	Si	Si	Dirección de Tesorería	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Hardware	UPS de servidor	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Hardware	Redes de comunicación y conectividad	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Datos / Información	Base de datos de contribuyentes	Si	No	Si	Si	Dirección de Tributos	Alto	Alto	Alto	**Crítico**	**Pública Reservada**	**Crítica**	**Crítica**
Software	Paltaforma de Procesos jurídicos	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**
Software	Plataforma de liquidación	Si	Si	Si	Si	Oficina de apoyo tecnológico	Alto	Alto	Medio	**Crítico**	**Pública Reservada**	**No Crítica**	**Crítica**

8.2.4. Equipos de continuidad

- **Equipos de emergencia**

El esquema organizacional para la atención de emergencias:



Comité Directivo

Es el comité de mayor nivel de la continuidad del negocio, que administra y verifica los recursos necesarios para recuperar las operaciones críticas de la Secretaría de Hacienda en caso de ocurrencia de una contingencia y/o emergencia. Está conformado por todas las direcciones, liderado por el responsable de la entidad, el Secretario de Hacienda y cuyo orden jerárquico es:

- Secretario de Hacienda – Líder del comité
- Director de tributos
- Director de estudios Fiscales
- Director de crédito público
- Director de Contabilidad

- Director de Tesorería
- Director de Presupuesto
- Asesor de comunicaciones
- Líder de apoyo tecnológico

Comité de Gestión de Crisis

Es el responsable de liderar la gestión de los incidentes materiales que impacten la función normal de las operaciones de la secretaría, asumiendo la toma de decisiones resultantes de la evaluación de daños. Conformado por el Director de Tributos, como líder, en caso de no estar el líder, lo suple el Director de estudios fiscales. En caso de no estar alguno de los Directores los suple algún Subdirector de la dependencia o en su defecto otro Director.

- **Equipo de Planeación**

Equipo responsable de elaborar el BRP, el cual define las actividades de respuesta y el uso de los recursos durante una emergencia. Los miembros que conforman el equipo de planeación son: Un funcionario delegado de las Direcciones y el Secretario de Hacienda. El equipo se complementa con la Oficina de Control Interno de la Alcaldía.

- **Equipo de Respuesta**

Equipo responsable de dar respuesta, evaluar los daños y estabilizar la situación después de un escenario de contingencia y/o emergencia en la secretaría. Los miembros que conforman el equipo de Respuesta son:

- Funcionario de la Dirección de Crédito Público, responsable de la vigilancia
- Funcionario de la Oficina de apoyo tecnológico, responsable del mantenimiento de planta y equipo y la gestión de la conectividad
- Brigada de emergencia, para primeros auxilios, incendio, evacuación y apoyo externo, conformado por funcionarios de la oficina de comunicaciones y la Dirección de Presupuesto.

- **Equipo de Recuperación y Operación**

Equipo responsable de restablecer los procesos u operaciones críticas de la secretaría de hacienda, teniendo en cuenta los tiempos de recuperación objetivo, la secuencia de recuperación y la información requerida por cada proceso para garantizar la continuidad.

Los miembros que conforman el equipo de Recuperación y Operación son:

- ✓ Secretario de Hacienda
- ✓ Dirección de Presupuesto
- ✓ Dirección de Contabilidad
- ✓ Dirección de Tesorería.

- **Equipo Logístico y de Soporte**

Equipo responsable de dar soporte administrativo y tecnológico al equipo de la Sección de Recuperación, de manera que se faciliten las labores de planeación, recuperación y retorno a la operación normal. Igualmente es responsable de facilitar la comunicación con el personal, sus familiares y dependientes.

Los miembros que conforman el equipo logístico son:

- o Funcionarios de la oficina de Apoyo Tecnológico para la gestión de la infraestructura tecnológica, la gestión de la conectividad y la gestión de soporte y atención a usuarios.
- o Funcionarios de la oficina de comunicaciones
- o Funcionario de Dirección de estudios fiscales responsable de archivo físico y administración de bienes.

8.2.5. Identificación de riesgos

Es importante identificar escenarios de riesgos de la continuidad del negocio para

hacer un análisis de impacto.

- **Escenarios**

  Algunos escenarios que pueden presentarse en la Secretaría de Hacienda impactando en la continuidad son:

Id	Escenario	Descripción
E1	Fallo de Infraestructura de red	Fallo o daño en cualquier dispositivo de infraestructura de red (Routers, Switch) debido a: 1. Cruce entre hilos(mala conexión) 2. Ruptura de los cables 3. Ruido o estática
E2	Fallo de servidores	Fallo o daño en los servidores que soportan el sistema de información de impuestos municipales. Puede ser causado por intervención humana o falla del dispositivo.
E3	Interrupción del fluido eléctrico	Fallas eléctricas debido a tormenta eléctrica que puede producir un corto circuito originando un apagón o un incendio
E4	Denegación del servicio de la plataforma de liquidación y pagos de impuestos municipales.	Como consecuencia de la denegación de acceso al sistema de liquidación y pago se trabaja de forma local mediante sistema ubicado solo en las instalaciones, durante el proceso de recuperación de la plataforma. En este evento puede presentarse que no se encuentre actualizada la base de datos de saldos de cartera de impuestos y pagos del día

Procedimiento de identificación de riesgos

Identificación de Riesgos	
R1	Impacto en la integridad de las personas debido a incendio en las instalaciones.
R2	Impacto en la continuidad de los servicios debido a fallas por falta de disponibilidad y contingencia de la infraestructura tecnológica
R3	Impacto en la confidencialidad debido a las vulnerabilidades detectadas en la infraestructura tecnológica
R4	Impacto en la imagen debido a fuga de información confidencial por parte del personal
R5	Impacto en la imagen debido a la no detección oportuna de operaciones fraudulentas en la plataforma de pagos y liquidación de los impuesto municipales
R6	Impacto financiero debido a la vulnerabilidad de la infraestructura de TI

Controles Existentes	
C1	Plan de evacuación y Sistema contra incendios instalado.
C2	Diseño de esquema de virtualización de servidores
C3	Tercerización de la fuerza de trabajo de TI
C4	Implementación de prácticas de desarrollo en tiempo real
C5	Creación de la división de Gestión del Riesgo
C6	Establecimiento de un mecanismo de análisis de comportamientos irregulares en liquidaciones de impuestos
C7	Centralización de la información generada por las diferentes oficinas regionales
C8	Implementación de una herramienta de visualización para el análisis de transacciones de recaudo

8.2.6. Análisis de Impacto del Negocio

Se definen las tablas de impacto y se aplican a los riesgos identificados para hacer el cálculo del Riesgo de exposición y residual en el proceso de Gestión Tributaria

Definición de impactos

Tabla de impacto Rangos acumulados de pérdidas en Millones de pesos (Tangible):

Determinada por el recaudo promedio mensual de la gestión tributaria de Puerto Colombia, que es de $1.000.000.000, que si se deja de percibir tendría consecuencias financieras para el municipio.

Score	Rango de pérdida financiera
0	Ninguna
1	< $100
2	≥ $100 < $400
3	≥ $401< $600
4	≥ $601< $800
5	≥ $801

Impacto acumulado por días usando la tabla de pérdida financiera:						
Categoría	1	3	5	10	20	30
Pérdida Financiera	1	2	3	3	4	5

Tabla de impacto en la Continuidad de los servicios:

La gestión tributaria salvaguarda la información diariamente.
La máxima cantidad de tiempo tolerable requerido para verificar integridad de los datos y los sistemas es de 12 horas.

MTD: 4 días = 96 horas
RTO: 1 día = 24 horas
WRT: ½ día = 12 horas
RPO: 1 día = 24 horas

Impacto en la continuidad de los servicios de TI

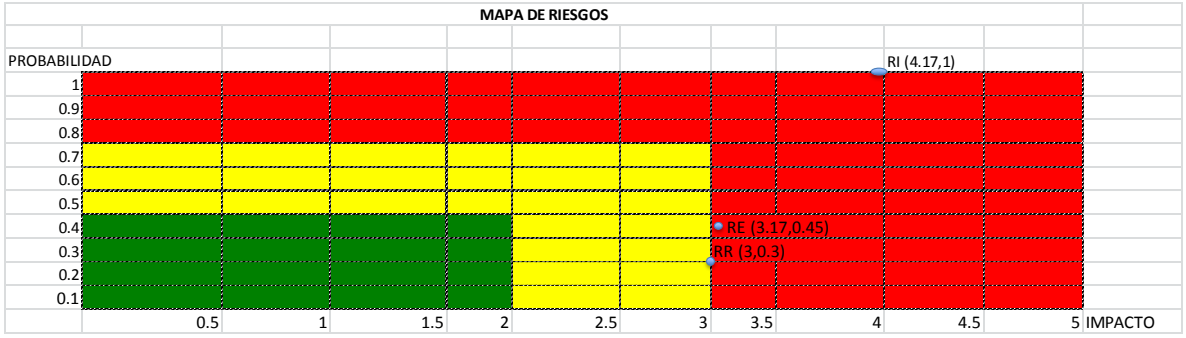
5 48 a 96 horas
4 24 a 48 horas
3 12 a 24 horas
2 1 a 12 horas
1 Menos de 1 hora

TABLAS FINALES DE VALORACIÓN DE IMPACTOS

Impacto Pérdida Financiera en Millones de pesos		Impacto en la continuidad de los servicios de TI		Impacto en la integridad de las personas	
5	>=801	5	48 a 96 horas	5	Crítico
4	>=601 < 800	4	24 a 48 horas	4	Importante
3	>=401 < 600	3	12 a 24 horas	3	Moderado
2	>=101 < 400	2	1 a 12 horas	2	Tolerable
1	< 100	1	Menos de 1 hora	1	Leve

	RIESGO INHERENTE		CONTROLES	RIESGO DE EXPOSICIÓN		CONTROLES	RIESGO RESIDUAL	
RIESGO	IMPACTO	PROBABILIDAD	EXISTENTES	IMPACTO	PROBABILIDAD	PROPUESTOS	IMPACTO	PROBABILIDAD
R1	5	1	C1	3	0.5		3	0.5
R2	4	1	C2	2	0.3	CP2	1	0.2
R3	5	1	C3, C4	3	0.8	CP3	3	0.5
R4	5	1	C1, C5	5	0.5	CP1	5	0.2
R5	3	1	C5, C6, C7, C8	3	0.2		3	0.2
R6	3	1	C3, C4	3	0.4	CP2	3	0.2
TOTAL	4.17			1.47			0.90	
PROMEDIO	4.17	1.00		3.17	0.45		3.00	0.30

Controles Propuestos	
CP1	Acuerdos de confidencialidad con pólizas de cumplimiento
CP2	Implementación de una infraestructura de alta disponibilidad y contingencia
CP3	Implementación de mejores prácticas de COBIT



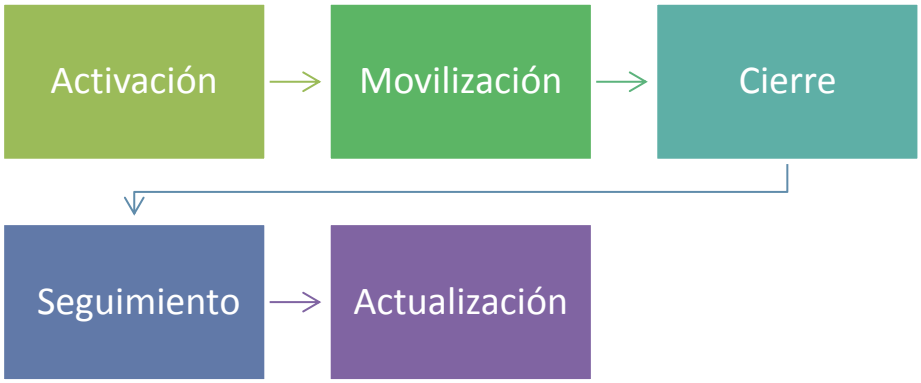
8.3. SOPORTE

Se formula el plan de continuidad cuyo objetivo es Salvaguardar la información financiera y de tributos de localidad y garantizar la disponibilidad de los servicios y trámites al ciudadano.

A continuación de define la matriz RACI en donde se definan las actividades y equipos que intervendrán , así como el rol (intercepción fila-columna) de cada área en la prevención, respuesta y recuperación ante la materialización del riesgo crítico con mayor impacto y probabilidad:

Denegación del servicio del sistema de facturación, nómina, archivos críticos y servicios de apoyo.		Roles / Responsabilidades									
ID	Actividad	comité directivo	Lider Equipo logística	Lider Equipo Recuperación de Direcciones	Lider Recuperación Dirección de Tributos	comité de crisis	Líder Apoyo tecnológico	Dirección de estudios fiscales	Lider Recuperación Unidades de Negocio	Asesor de comunicaciones	Lider Servicios
1	Aviso desde área de tributos para indicar la interrupción del servicio	C	I	I	I	A	R	I	I	I	R
2	Monitoreo del tráfico de red y y revisión de estado de servidor	A	I	I	I	R	C	I	I	I	C
3	Reportar diagnóstico de Denegación del Servicio	A	I	I	I	R	C	I	I	I	C
4	Evaluar el diagnóstico y activar Plan de continuidad	A	I	I	I	R	C	I	I	I	C
5	Notificar al personal de la secretaría de hacienda y Sistemas de activar plan de recuperación de acuerdo al escenario de Denegación de servicio	RA	I	R	R	C	I	I	R	R	I
6	Iniciar Plan local	C	I	I	A	I	R	I	A	I	R
7	Iniciar el Plan de recuperación del servicio (Servidor de respaldo)	A	I	I	R	C	I	I	R	I	I
8	Levantar el servicio - Mitigar el riesgo de denegación del servicio en el sistema	C	I	I	RA	R	I	I	RA	I	I
10	Documentar incidente y actualizar el Plan de continuidad	A	I	I	R	C	I	I	R	I	I

- **Fases para la operación del plan de continuidad**



En esta fase se define las fases para ejecutar plan de continuidad:

Activación

Con el fin de establecer los lineamientos para gestionar una comunicación efectiva y controlada para la activación de una emergencia de impacto al interior de la secretaría de hacienda se define un protocolo de Comunicación.

Movilización

Con el objetivo de minimizar el impacto de las operaciones, se toma como instalación alterna la Secretaría de Tránsito que cuenta con infraestructura suficiente y presentan menor riesgo de incendio, remoción e inundación. Esta escogencia se hace con base en el estudio sobre los mapas de riesgo entregados por Control Interno.

Operación

Con el propósito de responder exitosa y oportunamente ante eventos de interrupción de los servicios a los contribuyentes y ciudadanía en general, la secretaría ha identificado sus operaciones críticas.

Desmovilización

La secretaría de hacienda una vez concluya la operación en la Secretaría de tránsito, cuya notificación la hará el Comité de Gestión de Crisis, realizará un análisis y evaluación del resultado del desempeño de las labores ejecutadas, basados en la documentación generada. Una vez se confirma el cierre del plan alterno, un representante de cada Dirección hace entrega de los elementos y recursos asignados durante la emergencia.

Cierre

Finalizada la emergencia, se activa una nueva cadena de comunicación, siguiendo esquemas de comunicación, para informar la situación y las acciones a seguir para retornar a la normalidad, adicionalmente los miembros del Equipo de Recuperación deben generar un informe de trabajo en Contingencia, donde se citen los resultados obtenidos y los problemas presentados, para retroalimentar a los directivos de la secretaría.

Seguimiento

El plan de continuidad será monitoreado mediante un proceso sistemático, independiente y documentado de auditorías internas, cuya finalidad es realizar un examen objetivo e independiente de los procesos, procedimientos, actividades y operaciones que lo soportan, para formular recomendaciones.

La coordinación para la ejecución de las auditorías está a cargo la Oficina de Control Interno.

Actualización

El documento del plan de continuidad será revisado como mínimo 1 vez al año con los responsables y participantes de las diferentes dependencias, para identificar y realizar los ajustes.

8.4. IMPLEMENTACIÓN Y PRUEBAS

Se define el plan de pruebas del Plan de Continuidad (roles, tareas, etc).

Procedimiento de plan de prueba. TIPO SIMULACIÓN.

- ✓ Proceso: Gestión Tributaria

- ✓ Escenario: *Denegación del servicio de la plataforma de Liquidación y pagos*.

- ✓ Activos involucrados:
  - 1 servidor de pruebas con *Sistemas de Información de Impuestos*
  - 3 equipos clientes
  - Equipos de conectividad de la red de la entidad

- ✓ Periodicidad: Una vez al año

- ✓ Participantes:
  - Responsable y coordinador de la activación del BCP (Director de crisis)
  - Equipo TI
  - Secretario de Hacienda
  - Equipo de atención al usuario
  - Director de Tributos
  - 5 Usuarios críticos
  - Back up restaurado del sistema *Sistemas de Información de Impuestos*

Id	Descripción de la actividad
1	El Coordinador del BCP junto con el área de Apoyo TI debe reunir al Secretario de Hacienda, a los Líderes de Equipos y sus respectivos miembros. Una vez reunidos se les entrega copia de los procedimientos pertinentes a cada miembro y se le instruye sobre el alcance y los objetivos de la prueba a realizar.
2	El Coordinador del BCP da inicio de la prueba.
3	El equipo de atención inicia la prestación del servicio.
4	El equipo de TI monitorea el tráfico de red y mediante herramienta de software

	simula un ataque de Denegación de servicio sobre la plataforma donde se aloja el *Sistemas de Información de Impuestos*
5	Después de 5 minutos de interrupción, el personal de atención y los médicos usuarios del sistema, reportan al área de TI de la situación.
6	El equipo de TI realiza medición del tráfico de red y revisión de estado de servidor. Reporta el diagnóstico de Denegación del Servicio al Coordinador o Gerente de TI.
7	El Gerente de TI evalúa el diagnóstico y toma decisión de notificar al personal de atención, Líderes de equipo del área y al equipo de TI de activar plan de continuidad de acuerdo al escenario de Denegación de servicio. Por parte de TI involucra habilitar el servidor espejo que se encuentra en la sede alterna restablecer un back up ejecutado sobre el servidor de apoyo para garantizar que la información consultada una vez superada la falla es la más actualizada posible. Por parte del personal de atención y Director de Tributos, activan el Plan papel que consiste en usar formatos manuales donde se registra la información necesaria para ser luego registrada en el sistema una vez superada la falla, por medio de notas de calidad donde se especifique la extemporaneidad de la información.
8	El Gerente de TI inicia el Plan de recuperación del servidor afectado.
9	El Coordinador del BCP realiza medición de los tiempos de detección y respuesta.
10	El Coordinador del BCP da por terminada la prueba y debe generar un informe de lo relevante encontrado en esta prueba y debe anexar este documento al BCP y proceder a su actualización.

8.5. REVISIÓN Y CAMBIOS

En esta fase se debe evaluar si el plan de continuidad es efectivo cuando se realizan las pruebas. En caso de que no se cumpla con el procedimiento o se altere, se debe actualizar el plan.

Para el caso de estudio se debe tener especial cuidado en la actualización del procedimiento de Análisis de Impacto del Negocio de acuerdo a la identificación de

nuevos riesgos y amenazas ya que es fundamental para el desarrollo y procedimiento de la gestión de la continuidad.

La prueba es liderada por el equipo de Apoyo Tecnológico y debe contar con aprobación del Secretario de Hacienda.

8.6. PLANIFICACIÓN DE REVISIONES INTERNAS

Se identifican y describen el plan de entrenamiento para el personal involucrado (frecuencia y mecanismo utilizado)

Entrenamiento	Frecuencia
Capacitaciones de tipo recorrido del Plan de Continuidad con el fin de comprobar la efectividad del plan y revisar roles y responsabilidades	Una vez al año
Simulacro de escenarios	Una vez al año
Campañas con slogans y emails para concientizar al personal de los posibles escenarios de riesgo	Cada 2 meses
Para lograr retroalimentación, se habilita una dirección de correo electrónico, donde se consiga dirigir las sugerencias, en cuanto a las gestiones realizadas que vayan surgiendo por parte de los usuarios críticos.	Permanente

Igualmente se define el plan de copias de respaldo de la información del proceso seleccionado (tipo, periodicidad, medio, tiempo de retención, custodia).

Tipo	**Método**	**Periodicidad**	**Medio**	**Tiempo retención**	**Custodia**
Completo	Automático	Semanal	Disco/Nube	1 año	Director de TI/Proveedor
Incremental	Automático	Diario	Disco	1 año	Director de TI

- ✓ Se tienen datos personales de nivel medio-alto y de acuerdo a política de seguridad, se tiene un proveedor que custodia los respaldos en la nube y se ocupa con las debidas garantías legales de que nuestras copias de seguridad estén generadas.

- ✓ Se hacen pruebas de respaldo cada 2 meses.

8.7. Revisión del modelo y mejora continua

Se debe seguir el procedimiento:

- Aplicar los controles propuestos en la identificación de riesgos**.**
- Análisis de la brecha del estado actual con respecto al anterior análisis con la herramienta del componente de Diagnóstico.
- De acuerdo a la evaluación resultante, hacer revisión y actualización del modelo de gobierno si se requiere.
- Se elige el proceso crítico a evaluar para implementar el modelo.
- Revisar el presupuesto de continuidad.

8.8. RESULTADOS DEL CASO DE ESTUDIO

Fase	Observaciones	Oportunidades de Mejora
1. Contexto	Existe un Plan estratégico de TI.	El plan estratégico de TI está enfocado a mantenimiento y soporte y debe ser alineado a la estrategia del negocio.
	Existe un presupuesto aprobado de TI en el rubro Fortalecimiento Institucional.	
	Se tienen definidos roles del personal de área de Apoyo Tecnológico.	Diseñar, aplicar y mantener actualizado el plan de continuidad para procesos críticos como es la gestión tributaria
	Existen políticas de seguridad documentados y política de privacidad y protección de datos dentro del proyecto de ejecución actual de implementación del sistema de gestión de seguridad informática de acuerdo a los lineamientos del Modelo de Seguridad y Privacidad de MinTIC.	Hacer plan de pruebas del respaldo de información.
		Los procesos evaluados en la Secretaría de Hacienda obtuvieron como resultados un nivel de madurez del 29% en su estado inicial, un nivel Gestionado que implica que las actividades se están monitoreando. Sin embargo, es necesario que se documente toda la gestión.
	Existen manuales de entrenamiento de los sistemas de información.	
	Existen acuerdos de niveles de servicio	
	Se realiza mantenimiento preventivo de la infraestructura de TI	
	Los procesos misionales cuentan con sistemas de información estables. Cuentan con un sistema Administrativo y Financiero que integra todos los módulos de gestión. Además, la plataforma de impuestos es estable y la conectividad con Entidades Financieras está automatizada por webservice.	
	Los procesos están identificados según su nivel de criticidad están identificados	

2. Liderazgo y planificación	Se tienen identificados riesgos de TI	Dentro de la política de seguridad que están desarrollando se debe incluir los controles de continuidad del negocio de cada dependencia, incluyendo la Secretaría de Hacienda.
	Los equipos de emergencia y continuidad no están asignados oficialmente	Gestionar los riesgos.
	Se tienen identificado activos tecnológicos	Se debe actualizar la identificación de nuevas amenazas y vulnerabilidades dentro del análisis de impacto del negocio
	Existe una valoración y clasificación del activo de información por su impacto y criticidad dentro de la Secretaría.	
3. Soporte	No existe un procedimiento para la activación de un plan de continuidad.	Desarrollar e implementar la gestión de la continuidad que contemple el plan con roles y responsabilidades que involucre a la Dirección de la Secretaria de Hacienda.
	No existe un documento formal de gestión de la continuidad	
4. Implementación y pruebas	No se realizan pruebas de incidentes que puedan provocar una interrupción de los servicios de TI dentro de la Secretaría.	Incluir dentro de la gestión de la continuidad de los servicios TI dentro de la Secretaría de Hacienda, el escenario de pruebas, teniendo en cuenta que han recibido capacitación en respuestas frente a incidentes de seguridad.
	El personal es capacitado periódicamente en temas de seguridad informática.	
5. Revisión y cambios	El plan estratégico de TI se actualiza de acuerdo a los nuevos requerimientos de operación y mantenimiento de la Secretaría.	Incluir dentro del plan estratégico la implementación del modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios de TI en la Secretaría de Hacienda.

6. Planificación de revisiones internas	El personal es capacitado en lineamientos de la estrategia Gobierno en Línea, que incluye Modelo de Seguridad y Privacidad	Diseñar un cronograma de capacitación enfocado a la Guía de elaboración de Continuidad del Negocio de MinTIC.
	Se realizan copias de respaldo de las bases de datos de Contribuyentes e Impuestos con periodicidad aunque no se realizan copias del funcionamiento del respaldo	Diseñar cronograma de pruebas de los respaldo dentro del modelo de gobierno y gestión, componente de Gestión.
		Desarrollar e implementar Programa de concientización y entrenamiento del Plan de Continuidad.
7. Mejora continua	Se hacen revisiones post reanudación después de un incidente disruptivo pero no se documenta el incidente y la metodología de respuesta y reanudación	Coordinar y aprobar la definición de requerimientos, para los procesos tendientes a la adquisición o contratación de recursos técnicos y tecnológicos de las TIC.
	Existe compromiso y disposición de la Secretaria de Hacienda para mantener dentro de su estrategia el componente tecnológico para lograr las metas de gobierno. Es miembro del comité de gestión y control de plan de desarrollo.	Crear comité de continuidad involucrando a la alta dirección y oficializarla por medio de Decreto o documento administrativo avalado por el Alcalde y el responsable de la entidad, en este caso el Secretario de Hacienda. El modelo es flexible y puede replicarse en otras dependencias.

9. CONCLUSIONES

La gestión de la continuidad es la herramienta que las organizaciones deben implementar, para mantener sus operaciones y desarrollar la resiliencia frente a eventos disruptivos. Esta gestión debe estar alineada a los objetivos del negocio para que efectivamente se haga la entrega de los beneficios a los stakeholders, en el caso de las Secretarías de Haciendas Municipales, principalmente a los ciudadanos.

La aplicación de frameworks que involucran gobierno y gestión de TI, como lo es Cobit 5, hace que se mire la organización desde la perspectiva de la cascada de metas lo que facilita la identificación y alineación de los objetivos de TI con los objetivos del negocio y por ende se pueden implementar procesos y gestionar proyectos de manera efectiva apuntando siempre a las necesidades de la alta dirección.

Las políticas con respecto a la recuperación después de una emergencia deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y cumplimiento. El hecho de gestionar un plan de continuidad del negocio en entidades territoriales no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas y que pueden provocar grandes pérdidas, no solo materiales si no aquellas derivadas de la paralización del negocio durante un período más o menos largo. Además, el modelo cubre una práctica importante dentro del Modelo de Seguridad y Privacidad de la Información – MSPI - del Marco de Referencia Arquitectura Ti de MinTIC, el cual debe estar con el máximo cumplimiento dentro de tres años.

El modelo propuesto se alinea al MSPI en todos sus componentes por lo que las entidades pueden contar con algo más que la guía de elaboración del Plan de continuidad de manera que la gestión sea controlada y comprometida por la alta dirección. Esto es lo que realmente hace efectivo una gestión de continuidad en las entidades públicas.

El modelo de gobierno y gestión propuesto tiene diferentes niveles de complejidad y flexibilidad según las necesidades y características de las Secretarías de Hacienda Municipales. Igualmente no contempla todos los escenarios y los recursos suficientes para estar totalmente preparados, por tal razón es de vital importancia que el proceso

deba ser paulatino e ir evolucionando según el contexto, resaltando la fase preliminar de Diagnóstico y la Fase de Mejora Continua para la actualización del modelo de gobierno y gestión de la continuidad. El monitoreo y revisiones de las acciones es esencial para asegurar se estén llevando a cabo eficazmente. Además permite evidenciar los factores que pueden estar afectando negativamente la aplicación de controles.

La probabilidad que las amenazas externas, como efectos climáticos, se materialicen se minimizará diseñando y aplicando planes de emergencias de acuerdo a las fases especificadas en la guía de implementación.

La aplicación del modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios críticos en la Secretarías de Hacienda Públicas permitirá a la entidad estar preparados para identificar las posibles situaciones de disrupción y emergencia, los procedimientos para hacerles frente, las actualizaciones de dichos procedimientos y las alternativas disponibles.

10. REFERENCIAS

[1] Hitt, Ireland y Hoskisson. (2009). *Strategy Management*. USA: South-Western Cengage Learning.

[2] Hitt, Ireland y Hoskisson. (2009). *Strategy Management*. USA: South-Western Cengage Learning.

[3] Selig, G. (2008). *Implementing IT Governance - A Practical Guide to Global Best Practices in IT Management* (1St ed.). Zaltbommel: Van Haren Publising.

[4] Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno de Colombia. (2017). *Conoce la estrategia de gobierno en línea*. Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

[5] ISACA. (2012). *COBIT5: Procesos catalizadores*. ISBN 978-1-60420-285-4. USA.

[6] AXELOS. (2017). *What is ITIL® Best Practice.* Recuperado de https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[7] ISACA. (2012). *COBIT5: Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. USA.

[8] Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno de Colombia. (2017). *Arquitectura TI Colombia*. ISBN: 978-958-58786-6-2. Recuperado de http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html

[9] Instituto para el Desarrollo de Antioquia. (2015). *Gestión tributaria para municipios*. Recuperado de http://www.idea.gov.co/es-co/SalaDePrensa/Publicaciones/Gesti%C3%B3n%20tributaria%20para%20municipios.pdf

[10] Ministerio de la Tecnologías y las Comunicaciones. (2010) *Guía No. 10. Marco para la preparación de las TIC para la Continuidad del negocio*. Colombia.

[11] Kulkarni, G. (2012). *Adaptación COBIT 5 e ITIL en un municipio saudí*. Recuperado de http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-itil-adaptation-at-a-saudi-municipality-spanish.aspx.

[12] Ferrer V., R. (2015). *Metodología para la Gestión de la Continuidad del Negocio*. *Cintel Proyectos TIC innovadores*. http://cintel.org.co/wp-content/uploads/2013/05/Metodolog%23U00eda-para-la-Gesti%23U00f3n-de-la-Continuidad-del-Negocio.pdf

[13] Secretaría de Hacienda. Alcaldía Mayor de Bogotá D.C. (2013). *Plan institucional de respuesta a emergencias "PIRE"*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=3495&f_NORMFIL_FILE=X&inputfileext=NORMFIL_FILENAME

[14] Contenido de la Norma ISO 22301 [en línea]. [consultado 31 de Agosto de 2017]. Disponible en internet: http://normaiso22301.com/contenido-de-la-norma-iso-22301/