FACULTAD DE ESTUDIOS EN AMBIENTES VIRTUALES

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN Y PROYECTOS TECNOLÓGICOS

TRABAJO DE GRADO

“MODELO DE GESTIÓN DE LA DISPONIBILIDAD, RESPALDO, RECUPERACIÓN DE LOS SISTEMAS DE INFORMACIÓN Y DE LA GESTIÓN DEL RIESGO, PARA LA SECRETARÍA DISTRITAL DE HACIENDA DE BOGOTÁ”

Ing. JOSÉ FLORENTINO AYALA CUERVO
Ing. NICOLÁS RODRÍGUEZ MEDINA
Autores

Ing. LUIS ARMANDO COBO CAMPO
Director de la tesis

BOGOTÁ D.C., JULIO DE 2019

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

En la era actual, el área de tecnología ha tenido un valor fundamental en el desarrollo de las organizaciones públicas y privadas, impulsando el desarrollo adecuado de todos los procesos, brindando la ayuda necesaria para alcanzar eficiencias operativas y soportando eficazmente la operación del negocio a través de prácticas seguras que protegen la confidencialidad, integridad y disponibilidad de la información.

El objetivo de este documento es presentar un modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo, alineado con estándares mundialmente conocidos como la norma NTC-ISO-IEC 27001:2013, NTC-ISO-IEC 20000:2018 y NTC-ISO-IEC 31000:2011 que aplique a cualquier área de TI, sin importar a que se dedica la organización.

Dicho modelo se aplica a la Secretaría Distrital de Hacienda, quien es la entidad del distrito encargada de garantizar la sostenibilidad de las finanzas de Bogotá, es decir, asegurar que la capital de Colombia cuente con los recursos suficientes para cumplir con sus obligaciones y hacer las inversiones necesarias en la ciudad.

Los hallazgos encontrados y los resultados obtenidos en la aplicación del modelo en la entidad fueron satisfactorios, permitiendo a la Secretaria Distrital de Hacienda conocer y analizar el estado actual que presenta el área de la Subdirección de Infraestructura de Tecnología, de acuerdo con los requisitos y objetivos de control que se establecen en las tres normas mencionadas. Adicionalmente, se definieron los sistemas de información críticos, una solución de respaldo de información, un procedimiento para la gestión de riesgos, se formularon indicadores e identificaron los riesgos que pueden afectar los activos más importantes del área.

Palabras Claves: modelo, seguridad, información, activos, riesgos.

1 INTRODUCCIÓN

La carta política de Colombia contempla a Bogotá como único distrito capital, ciudad que durante años se ha visto inmersa en una transformación social, política y económica, mostrando la necesidad de integrar todos los actores sociales en una sola sociedad a través de las 16 entidades que hoy forman el distrito capital (Ley No 1423, 1993). La Secretaría Distrital de Hacienda hace parte del nivel central de la Alcaldía mayor de Bogotá, cuya misión es la de gestionar recursos y distribuirlos entre los sectores de la administración distrital, para cumplir con las metas establecidas en el plan de desarrollo bajo el principio de sostenibilidad física. Optimizando los procesos de la entidad, a partir de la adopción de sistemas de información modernos, seguros, ágiles y bajo estándares internacionales que contribuyan a la efectividad del servicio. (Secretaría Distrital de Hacienda, 2019)

En el presente trabajo, se diseña un modelo para la gestión de la disponibilidad, respaldo y recuperación de los sistemas de información y la gestión del riesgo (DRRGR), de manera que la Secretaría Distrital de Hacienda dé cumplimiento al plan estratégico de la "Bogotá Mejor Para Todos" (Secretaría Distrital de Planeación, 2016). Lo cual implica la reorganización de los sistemas y tecnologías de información que en la actualidad posee.

La implementación de este modelo le permitirá a la entidad optimizar y asegurar los servicios internos y externos, garantizando la identificación y el análisis de riesgo, el mejoramiento de los procesos de calidad, las copias de seguridad de los datos, la generación y optimización de nuevos indicadores de gestión, enmarcados en metodologías de buenas prácticas y estándares reconocidos en el mercado, que al final se traduce en altos niveles de calidad e integridad de la información.

Este modelo se entregará en etapa de diseño y se aplicará inicialmente a la Subdirección de Infraestructura de Tecnología de la Secretaría Distrital de Hacienda, no obstante, por la metodología estándar utilizada, se podrá implementar en otras áreas de la entidad sin generar mayor impacto y esfuerzo.

A lo largo de este trabajo se expondrán los casos encontrados en las áreas intervenidas y de la misma manera se mostrarán otros hallazgos que puedan estar afectando el desarrollo de las actividades de la Secretaría Distrital de Hacienda, como es el caso de la conectividad, los sistemas

de información, tanto administrativos, financieros y tributarios, y de esta manera buscar mitigar la problemática a través del diseño de un modelo de gestión de la disponibilidad, respaldo y recuperación de los sistemas de información y la gestión del riesgo, de tal forma que se cumplan los objetivos planteados en el plan de desarrollo de la Bogotá Mejor para todos.

El trabajo está alineado con el grupo, campo y líneas de investigación de la Universidad EAN, tiene la aprobación de la Secretaría Distrital de Hacienda y cuenta con los permisos de la Dirección de Informática y Tecnología de la SDH[1] para el acceso operativo y procedimental de los sistemas de información.

El contenido del trabajo se desarrolla en cuatro secciones o capítulos:

1. Introducción, en la primera parte del documento se especifica la identificación del problema detectado en la organización, se definen los objetivos, la justificación del trabajo, el alcance donde se delimita el ámbito para el cual tiene validez los resultados aportados y la metodología utilizada.

2. Marco Teórico, en la segunda sección se presenta los conocimientos y conceptos necesarios para el desarrollo del modelo y finalmente la descripción de la empresa a la que va encaminada el presente trabajo dirigido.

3. Modelo, en la tercera sección de presenta el modelo propuesto de Gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión de los riesgos en 3 fases para su implementación, (diagnóstico, planeación y preparación).

4. Modelo Aplicado, en esta sección se desarrolla el modelo propuesto en el capítulo anterior en la Secretaría Distrital de Hacienda.

5. Conclusiones y Recomendaciones, finalmente se hace una síntesis de las recomendaciones realizadas a la organización, las conclusiones del trabajo y las líneas de investigación o mejoras que puede tener el modelo.

[1] SDH (Secretaría Distrital de Hacienda)

1.1 Formulación del problema

Los nuevos servicios implementados en la SDH hacen que se incrementen las probabilidades de tener fallas críticas en la infraestructura, afectando la disponibilidad de los sistemas de información y el cumplimento de los acuerdos de niveles de servicio con los usuarios internos y externos, afectando la imagen de la entidad y la del Distrito Capital, de otra parte, la entidad no tiene documentados los procedimientos para el crecimiento y disponibilidad de los sistemas de información. Esta situación degrada considerablemente los tiempos de respuesta en la atención de los servicios, así mismo se ve el incremento significativo del uso de los diferentes recursos en componentes como: Almacenamiento, procesamiento y conectividad, para atender los servicios nuevos y actuales que tiene la Secretaría Distrital de Hacienda.

La SDH ha tenido varios incidentes correspondientes a la perdida del servicio por consecuencia de la ineficiente gestión de la disponibilidad de la infraestructura de TI.

Tabla 1. Informe mensual de incidentes de infraestructura reportados por la mesa de servicios en el mes de Julio de 2019

ALERTA	Área o Sistema Afectado	Cuenta de ALERTA	Incidente
Critica	Aire Acondicionado	2	Alarma de sobrecalentamiento Datacenter
	Aplicación WEB	55	Falla en url de aplicaciones
	Bases de Datos	62	Indisponibilidad de la Base de Datos
	Servidores	109	Indisponibilidad de los servidores por causa de

			llenado de unidad o filesystem
Total, general		228	

Fuente. Propia a partir de (Secretaría Distrital de Hacienda, 2019)

En la tabla número 1 se puede observar que el 48% de los incidentes reportados en el mes de julio de 2019 por la mesa de servicios corresponde a problemas asignados a los servidores específicamente en temas relacionados con almacenamiento, lo cual ocasiona el llenado de los espacios de disco y la caída de las aplicaciones de servicio.

La entidad cuenta con un procedimiento para la realización de copias de seguridad de los sistemas de información, sin tener presentes las normas técnicas o estándares; no hay una política clara para el servicio y operación del sistema de copias de respaldo de la entidad, por tal motivo se han presentado inconvenientes y quejas por parte de los funcionarios cuando se requieren restauraciones de archivos que se eliminaron accidentalmente o que perdieron su integridad. Adicionalmente, el inadecuado respaldo de información está generando problemáticas que se ven reflejadas en tiempo y consumo de recursos para la entidad.

De otro lado, no se ha desarrollado un modelo de gestión del riesgo aplicado a los sistemas de información que permita identificar las diferentes vulnerabilidades y posibles ataques que puedan llegar a comprometer la integridad de la información vital para la entidad, así mismo se requiere un plan de continuidad del negocio con el objeto de asegurar la disponibilidad y la recuperación rápida y efectiva de toda la operación.

La Secretaría Distrital de Hacienda centraliza la información financiera, presupuestal, de terceros, contabilidad, tesorería y nómina de empleados, de las entidades del distrito; el manejo de altos volúmenes de información y de datos es procesado mediante 11 sistemas de información de cara al ciudadano y a las entidades adscritas a la alcaldía mayor de Bogotá (6 de carácter administrativo, 4 financieros y 1 de carácter tributario). Además, cuenta con 30 aplicaciones que ofrecen información al interior de la entidad con el objeto de que los funcionarios las utilicen para el desarrollo de las actividades propias; una necesidad indiscutible está en la actualización permanente de sus sistemas de información dando cumplimiento a nuevos diseños de

funcionabilidad, normas técnicas y jurídicas de tal manera que los servicios que se ofrecen al ciudadano sean de calidad y oportunos.

La Secretaría Distrital de Hacienda ha venido desarrollando diferentes actividades para garantizar la información y el uso diario de los recursos internos y externos, así también como para verificar los procesos y subprocesos que estén alineados a la metodología del riesgo. Un logro importante para la entidad es que contará con un modelo de gestión que permitirá a la dirección de informática y tecnología manejar la información de manera oportuna y eficaz, garantizando la seguridad, la gestión de la disponibilidad, el respaldo, la recuperación de la información y la gestión del riesgo.

1.1.1 Pregunta general

¿Cuáles son los elementos que se deben tener en cuenta para realizar un modelo de gestión de la disponibilidad, respaldo y recuperación de los sistemas de información y la gestión del riesgo, para la Secretaría Distrital de Hacienda?

1.1.2 Preguntas específicas

¿Cuál es el estado actual de las actividades de disponibilidad, respaldo, recuperación de los sistemas de información de la Secretaría Distrital de Hacienda?

¿Cuáles son los sistemas de informaciones claves y más importantes en la Secretaría Distrital de Hacienda?

¿Existe una identificación, análisis y evaluación de los riesgos asociados a la seguridad de la información de los sistemas de información en la Secretaría Distrital de Hacienda?

¿Cuál es el diseño y la arquitectura que soporta el respaldo y recuperación de los sistemas de información en la Secretaría Distrital de Hacienda?

¿Cuál es la percepción de los usuarios con respecto a la restauración de las copias de seguridad?

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un modelo de gestión de la disponibilidad, respaldo y recuperación de los sistemas de información y la gestión del riesgo para la Secretaría Distrital de Hacienda de Bogotá

1.2.2 Objetivos específicos

- Diagnosticar el estado actual de los sistemas de información "administrativos, financieros y tributarios" disponibles en la Secretaría Distrital de Hacienda respecto a la gestión de la disponibilidad, respaldo y recuperación de la información y la gestión del riesgo.

- Definir un conjunto procedimientos aplicados a los procesos de gestión de la disponibilidad, respaldo y recuperación de la información y la gestión del riesgo basado en las buenas prácticas de ISO20000, ISO27001 e ISO 31000.

- Definir los elementos del modelo para la gestión de la disponibilidad, respaldo y recuperación de la información y la gestión del riesgo de la Secretaría Distrital de Hacienda

- Realizar las recomendaciones necesarias para la implementación del modelo de gestión de la disponibilidad, respaldo y recuperación de la información y la gestión del riesgo para la Secretaría Distrital de Hacienda.

1.3 Justificación

La presente investigación contribuirá a la mejora continua de la gestión de servicios, la disponibilidad, la seguridad, respaldo, recuperación de la información y la gestión del riesgo en la Secretaría Distrital de Hacienda, a través de la adopción, documentación e implementación de las mejores prácticas y modelos de la industria, los cuales deben cumplir con estándares de calidad para soportar los servicios dispuestos a los procesos de la Secretaría Distrital de Hacienda, en materia de gobierno y gestión de TIC[2].

La ejecución del modelo permite tener como resultado una base estandarizada, normalizada, y soportada de aplicaciones y sistemas de información, una mejora sustancial de aspectos críticos como la recuperación, la disponibilidad, el desempeño y el control de los recursos de TI, impactando directamente la prestación de servicios a los usuarios internos y a los ciudadanos.

Con la adopción del modelo planteado la Secretaría Distrital de Hacienda tendrá una visión completa de cada uno de los sistemas de información, es decir, observara el proceso de inicio a fin. Implementar controles a lo largo del flujo. Adicional de contar con indicadores desde el punto de vista de disponibilidad, seguridad, respaldo y gestión del riesgo.

De acuerdo con las características del distrito, y mediante el desarrollo de este trabajo se analizarán los sistemas de información, necesidades, caracterización de datos, proyectos tecnológicos, metodología y modelos de gestión de la información. Siendo pertinente el trabajo de grado cuyo objetivo es diseñar un modelo para la gestión, disponibilidad, respaldo y recuperación de la información y la gestión del riesgo en la Secretaría Distrital de Hacienda.

1.3.1 Contribuciones esperadas

Un modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo, para la secretaría Distrital de Hacienda es un elemento muy importante en el plan estratégico de tecnología de la información, debido a que le permite respaldar y operar

[2] TIC (Tecnologías de la Información y las Telecomunicación)

adecuadamente sus servicios, y sirve como sustento en la obtención del certificado en la norma NTC[3]-ISO[4]-IEC[5]20000-1:2018.

A continuación, se presenta las contribuciones esperadas.

- El modelo planteado permitirá la organización de los procesos, optimizando aspectos como la operación de backups y restauración de los diferentes sistemas de información, e identificación de los riesgos asociados a los diferentes sistemas de información de la Secretaría Distrital de Hacienda.

- El modelo permitirá optimizar la gestión de los recursos tecnológicos mediante la implementación de mejores prácticas y estándares alineados a las nuevas tecnologías.

- Realizar el análisis de riesgos para identificar los más críticos, y poder generar estrategias de mitigación en aspectos como pérdida de conocimiento, sabotaje, robo de información, creación de puertas traseras, entre otras.

- Garantizar el mejoramiento de los procesos de gestión que permitan dar cumplimiento a las políticas establecidas en la estrategia de gobierno en línea y en los planes estratégicos de la "Bogotá mejor para todos".

- Permitirá a la entidad mejorar los servicios con el uso de las buenas prácticas gerenciales vinculando la tecnología como estrategia de negocio en la Secretaría Distrital de Hacienda.

- Permitirá a la entidad mejorar sus indicadores de gestión e incrementará la percepción del área por parte de los usuarios finales.

- Valorar el impacto económico que puede tener un incidente grave dentro de la infraestructura de TI

[3] NTC (Norma Técnica Colombiana)
[4] ISO (Organización Internacional de Normalización)
[5] IEC (Comisión Electrotécnica Internacional)

1.4 Alcance y limitaciones

1.4.1 Alcance

El presente trabajo de grado comprende la etapa de diseño y generación de un modelo de un Sistema de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo. El modelo aplica al área de Subdirección de Infraestructura de Tecnología de la Secretaría Distrital de Hacienda, con sede en Bogotá Colombia.

1.4.2 Limitaciones

El presente trabajo dirigido no incluye las fases de implementación, revisión, mantenimiento y mejora del modelo, únicamente aplica a la etapa de diagnóstico, diseño y generación del modelo de Disponibilidad, Respaldo, Recuperación y Gestión del Riesgo (DRRGR).

La identificación, valoración y tratamiento de riesgos no aplica a todas las áreas y procesos que tiene la Secretaría Distrital de Hacienda.

No se tuvieron en cuenta todos los requisitos de las normas NTC-ISO-IEC 27001:2013, NTC-ISO-IEC 20000:2018, únicamente los referentes a la capacidad, disponibilidad, recuperación y gestión del riesgo.

1.5 Metodología

1.5.1 Diseño general

La metodología planteada busca cumplir los objetivos específicos, con el fin de lograr el objetivo principal del trabajo, teniendo en cuenta el marco de referencia de la norma NTC-ISO-IEC 20000:2018, NTC-ISO-IEC 27000:2013 y NTC-ISO-IEC 31000:2011, que especifica los requerimientos que se deben desarrollar para el diseño del modelo de gestión DRRGR.

Es importante considerar en el diseño metodológico que el orden en que trabajan las diferentes normas no refleja su importancia ni el orden en el que se deben implementar.

1.5.2 Enfoque

Para el trabajo dirigido, se utiliza el enfoque de investigación cualitativo, el cual nos permite obtener respuestas de las preguntas específicas y poder tomar de decisiones exactas y efectivas que ayuden a alcanzar el objetivo planteado, según el planteamiento de Hernández, Fernández y Baptista (2015), este tipo de enfoque cuenta con características, procesos y algunas bondades que se encuentran en nuestro tema de estudio:

Tabla 2. Enfoque

Enfoque cualitativo		
Características	**Procesos**	**Bondades**
Los significados se extraen de los datos	Inductivo	Profundidad de significados
Se conduce básicamente en ambientes naturales	Recurrente	Amplitud
Explora los fenómenos en profundidad	Analiza múltiples realidades subjetivas	Riqueza Interpretativa
No se fundamente en la estadística.	No tiene secuencia lineal	Contextualiza el fenómeno”

Fuente: (Hernández, Fernandez, & Baptista, 2015)

1.5.3 Tipo de investigación

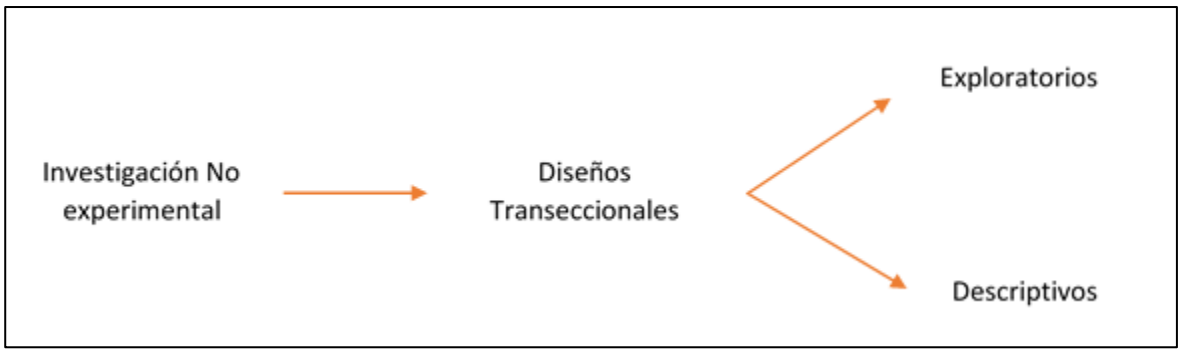
El desarrollo de este trabajo de investigación se realiza como tipo descriptiva y aplicativa, toda vez, que nos permitirá tener un acercamiento con la Secretaría Distrital de Hacienda para familiarizarnos con los procesos y procedimientos de la entidad, examinar las características del tema a investigar, definir la metodología para la recolección de datos y explicar las causas que originaron la situación analizada. Van Dalen y William J. Meyer (1986) especifican como el objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas.

Para el desarrollo de la investigación tomamos como referencia los autores Hernández, Fernández, & Baptista (2015), quienes nos dan las bases para hacer el estudio del tema propuesto en el proyecto.

1.5.4 Tipo de estudio

El estudio realizado es de tipo transversal o transaccional, de acuerdo con los autores Hernández, Fernandez, & Baptista (2015). Los diseños de investigación transaccional o transversal recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado.

Figura 1. Diseño de Investigación



Fuente. (Hernández, 2015)

Exploratorios: (Hernández, Fernandez, & Baptista, 2015) lo define como:

> Los diseños transaccionales exploratorios identifican una variable o un conjunto de variables, una comunidad, un contexto, un evento, una situación. Se trata de una exploración inicial en un momento especificó. Por lo general, se aplican a problemas de investigación nuevos o poco conocidos, además constituyen el preámbulo de otros diseños (no experimentales y experimentales).

Descriptivos: (Hernández, Fernandez, & Baptista, 2015) Plantea que:

> Los diseños transaccionales descriptivos tienen como objetivo indagar la incidencia de las modalidades o niveles de una o más variables en una población. El procedimiento consiste en ubicar en una o diversas variables a un grupo de personas u otros seres vivos, objetos, situaciones, contextos, fenómenos, comunidades, y así proporcionar su descripción. Son, por tanto, estudios puramente descriptivos y cuando establecen hipótesis, éstas son también descriptivas (de pronóstico de una cifra o valores).

1.5.5 Instrumentos de recolección de Información

Para el diseño del modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo, para la Secretaría Distrital de Hacienda, se utilizaron los siguientes recursos para la recolección de los datos:

- Entrevistas
- Cuestionarios
- Revisión de los resultados de los indicadores
- Revisión de la documentación existente
- Levantamiento de procesos
- Observación

1.6 Glosario

Activo de información: Es todo aquello que tiene valor para la Entidad y que gestiona información, hacen parte de los activos de información el hardware, el software, la información en cualquier medio en que se encuentre, así como las personas y sus conocimientos. (ICONTEC, 2013)

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en el daño a un activo de información a toda la organización. (ICONTEC, 2011)

ANS: Acuerdos de Niveles de Servicios

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ICONTEC, 2013)

Criptografía: Técnica que se ocupa del cifrado o codificado de un mensaje, destinada a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. (MINTIC, 2016)

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ICONTEC, 2013)

DRRGR: Disponibilidad, Respaldo, Recuperación y Gestión del Riesgo.

Evento de Seguridad de la Información: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias o una situación anterior desconocida que podría ser relevante para la seguridad. (ICONTEC, 2013)

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (ICONTEC, 2011)

Incidente de Seguridad de la Información: Un evento o serie de eventos de seguridad de la información no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. (ICONTEC, 2013)

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. (ICONTEC, 2013)

Mejora Continua: Actividad recurrente para aumentar la capacidad para cumplir con los requisitos. (ICONTEC, 2018)

Riesgo Residual: Nivel restante de riesgo después del tratamiento de riesgo. (ICONTEC, 2013)

Seguridad de la Información: Proceso que busca preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. (ICONTEC, 2013)

Sistema de Información: Se refiere a un conjunto de recursos y métodos organizados para: recopilar, procesar, mantener, transmitir y difundir la información según, determinados procedimiento. (Baca, 2015)

SDH: Secretaría Distrital de Hacienda.

SGS: Sistema de Gestión de Servicios.

SGSI: Sistema de Gestión de Seguridad de la Información, parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar operar hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (ICONTEC, 2013)

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. (ICONTEC, 2011)

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las Políticas y procedimientos de la entidad. (MINTIC, 2016)

2 MARCO TEÓRICO

El siguiente marco teórico se desarrolla en 4 partes significativas, iniciando de lo general a lo específico. La primera parte describe el tema de gestión de tecnologías de información y disponibilidad, la segunda se dirige directamente sobre el respaldo y recuperación de los sistemas de información, la tercera se enfoca en la gestión de riesgos, y en la última parte se describe el marco institucional donde se realizará el trabajo dirigido.

2.1 Ciclo de vida de la información

Como marco de referencia se encuentra la alcaldía de Santiago de Cali, que implemento un modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información, los cuales cumplen con parámetros y buenas prácticas de seguridad y funcionalidad que son definidas por el departamento administrativo de las TICS; adicionalmente, como referencia el uso de las arquitecturas IT(IT4+), ITIL y la Norma ISO/IEC 20000 como estándar específico para la Gestión de Servicios de TI, con el objetivo de aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita a una organización proveer servicios de TI gestionados, de calidad y que satisfagan los requisitos de sus clientes, COBIT 5 Marco de Negocio para el Gobierno y la Gestión de las TI, la Norma ISO/IEC 38500 - Gobierno TI sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI), la Norma ISO/IEC 27000 - Marco de Gestión de seguridad de la información

Figura 2. Gestión tecnológica de información Alcaldía de Santiago de Cali

Fuente. (Alcaldía Santiago de Cali, 2019)

2.2 Gestión de tecnologías de información y disponibilidad

Sin importar el tipo de organización, sea pública o privada, cada vez se tiende a depender más de los sistemas y las tecnologías de la información, para administrar los datos, la información y el conocimiento, en donde no tener la disponibilidad necesaria representa graves afectaciones económicas y legales. Diseñar estrategias para gestionar las tecnologías de información y asegurar la disponibilidad de los sistemas de información es fundamental para mantener los niveles de servicios y la operatividad de toda la empresa.

2.2.1 Tecnologías de la información

En este tiempo estamos rodeados de objetos tecnológicos que permiten al ser humano realizar investigación, desarrollo e innovar en diferentes productos tecnológicos, esto con el fin de mejorar y optimizar los procesos y procedimientos, para atender más rápido y eficientemente las necesidades de este mundo cambiante y globalizado.

En un tiempo en que lo único permanente es el cambio, la sociedad del conocimiento plantea una nueva revolución de la información, que no es tecnológica. No se trata de nuevas máquinas, nuevo software o de aumentar la velocidad de los dispositivos. Es una revolución de conceptos, que plantean sobre todo una nueva relación del espacio y el tiempo, dimensiones fundamentales de la experiencia humana y que están cambiando por completo las estructuras sociales y nuestra forma de vivir. (Andrada, 2004)

La humanidad se encuentra en los albores de una nueva era, caracterizada entre otras grandes tendencias, por una nueva transformación radical de la interacción social, y sustentada de manera especial en la aplicación de intensiva de las nuevas tecnologías es determinante para la emergencia de los nuevos riesgos y nuevas oportunidades. (Leonel, 2002)

2.2.2 Sistemas de información

Actualmente las organizaciones están generando constantemente información en todos los procesos y procedimientos, lo cual demanda que sus sistemas de información estén actualizados y acordes con las necesidades del negocio, esto se requiere para que la información se pueda

clasificar, optimizar y darle la confiabilidad pertinente. Según Peralta (2009), los sistemas de información deben cumplir tres objetivos básicos y define los siguientes tipos de información:

Objetivos básicos

- Automatización de procesos operativos
- Proporcionar información que sirva de apoyo al proceso de toma de decisiones
- Lograr ventajas competitivas a través de implantación y uso.

Tipos de sistemas de información:

- Sistemas transaccionales
- Sistemas de apoyo a las decisiones
- Sistemas estratégicos

2.2.3 Arquitectura de la información

El concepto de arquitectura de la información fue utilizado por Richard Saul Wurman, en 1975, tal como lo indica López (2012), el cual describía la necesidad de transformar los datos en información para que las personas los consultaran rápidamente, debido al crecimiento exponencial de internet y las nuevas tecnologías, la cantidad de información en la red se multiplico, lo que originó una preocupación por la correcta clasificación y recuperación de la información.

En otras palabras, arquitectura de la información es la forma particular que la tecnología de la información toma en una organización para alcanzar las metas o funciones seleccionadas Es un diseño para los sistemas de aplicaciones de negocios fundamentales de la empresa y de las formas especificas en que se utilizan en cada organización. (Laudon Kenneth C & Laundon Jane P, 2018)

2.3 Respaldo y recuperación de los sistemas de información

2.3.1 Plan de Continuidad del Negocio

De acuerdo con lo plateado por Martínez (2010), no existe un modelo fijo de estrategia para establecer la continuidad de negocio, depende del grado de criticidad de los sistemas de información, pero si indica que para conseguir una estrategia de continuidad de negocio aceptable

debe basarse en la disponibilidad de un centro alterno propio o subcontratado que permita definir los umbrales de respuesta y recuperación.

Por otro lado, existen diferentes categorías de desastre:

- Desastre menor: Definido como una parada no mayor a 4 horas
- Desastre mayor: Supera las 4 horas, pero no sobrepasa un día.
- Desastre Catastrófico: Cuando el servicio esta indisponible por un día, pero no supera la semana.

De acuerdo con lo plateado por Martínez (2010) no existe un modelo fijo de estrategia para establecer la continuidad de negocio, depende del grado de criticidad de los sistemas de información, pero si indica que para conseguir una estrategia de continuidad de negocio aceptable debe basarse en la disponibilidad de un centro alterno propio o subcontratado que permita definir los umbrales de respuesta y recuperación.

2.3.2 Seguridad Informática

Para una empresa la parte más importante de la informática son los datos, porque un equipo dañado o perdido se puede volver a comprar y podemos volver a instalar y configurar todas las aplicaciones que tenía. Pero la información y los datos no los podemos recuperar fácilmente. En este caso nuestra única esperanza son las copias de seguridad y el almacenamiento redundante. (Roa, 2013) Por lo anterior, las empresas deben realizar un esfuerzo mayor en asegurar su infraestructura y sistemas de información con el objetivo de mejorar la integridad y disponibilidad de los datos, para esto debemos identificar los diferentes activos que se deben proteger en orden de criticidad y tomar las diferentes medidas de aseguramiento en cada uno de ellos.

Las amenazas que afectan a la seguridad informática pueden derivar de diferentes fuentes externas e internas. Externas como un delincuente cibernético, que salta los protocolos de seguridad a través de explotar una vulnerabilidad en la red local de la empresa, o interna como los trabajadores de la organización, que conoce las debilidades de la compañía y se aprovecha para acceder a información privilegiada a la cual no debe tener acceso (Gómez, 2011). A continuación, se presentan las principales amenazas:

Virus: son programas maliciosos que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior de un archivo de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus ocasionado una nueva fuente de infección (Gómez , 2007)

Ramsonware: Es un código malicioso que cifra la información del ordenador, secuestrándola, para que el usuario no pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero. Desde el 2017 esta modalidad se hizo popular, registrado recientemente en casi 80 países alrededor del mundo (Surhone, 2018).

Spyware: También conocido como software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento (Benavides, 2012).

Ataque de denegación de servicio: También llamado DOS, es un ataque informático que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, provocando la pérdida de la conectividad de las redes por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima (Benavides, 2012).

2.3.3 Sistemas de Gestión de Seguridad de la Información

Las organizaciones han reconocido la información como el activo más importante para su operación; su protección y seguridad tiene una importancia primordial en el desarrollo de su gestión. En tal sentido, para disminuir los riesgos y proteger este y otros activos de información, los cuales abarcan entre otros al conocimiento de las personas, es necesario implementar un conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad en el manejo, transformación y operación de la información y de igual forma administrar estos controles para mantener este nivel a lo largo del tiempo.

Un Sistema de Gestión de Seguridad de la Información, en su abreviación en español SGSI, es una herramienta de la que dispone las organizaciones para dirigir y controlar la seguridad de la información. Está conformado por un proceso sistemático y conocido por toda la empresa, con el fin de proteger tres principios fundamentales, la confidencialidad, disponibilidad e integridad de

la información. Una gran ventaja que tiene un SGSI es la identificación de riesgos, la gestión de incidentes y los controles a implementar. Brindando confianza a las partes interesadas, como clientes internos y externos, proveedores, junta directiva, etc. Un aspecto muy importante que menciona la norma ISO27001 en su versión 2013 es que el sistema de gestión de la seguridad de la información debe ser parte directa en los procesos y en la estructura de la gestión total de la información de la organización, teniendo en cuenta que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. (ICONTEC, 2013)

2.3.4 Organización de la Información

La evolución y desarrollo de internet ha generado cambios importantes en cuanto a la creación, distribución, almacenamiento y modos de acceso de los recursos de información. “El desarrollo de las tecnologías de la información y las comunicaciones ha hecho que cualquiera pueda publicar en la red” (Daudinot, 2007), pero las personas suben todo tipo de información a la nube sin ninguna descripción que permita la organización y posteriormente su recuperación, en consecuencia, los usuarios no pueden localizar rápidamente información importante, esto debido a la falta de tratamiento documental en la red.

Baeza-Yates incorpora la siguiente Reflexión: “la representación y organización debería proveer al usuario un fácil acceso a la información en la que se encuentre interesado. Desafortunadamente, la caracterización de la necesidad informativa de un usuario no es un problema sencillo de resolver” (Baeza-Yatesa & Ribeiro-Neto, 2009). Es importante generar consultas de forma rápida y eficaz, que facilite la obtención de información relevante que satisfaga las necesidades de los clientes.

2.4 Gestión del riesgo de los sistemas de información

2.4.1 Proyectos de sistemas de información

De acuerdo con lo planteado por Baca (2015), la norma ISO 27000 nos brinda un conjunto de estándares de buenas prácticas sobre la Seguridad de la Información que pueden ser implementadas en cualquier tipo de empresa. De otra parte, las empresas, deben preocuparse por la información que poseen; es considerada como el activo más valioso que poseen, por esta razón, debe ser

protegido adecuadamente para evitar el deterioro o perdida. Con la adopción de la norma ISO 27000 las partes interesadas pueden definir los riesgos de seguridad de la información y establecer controles para mitigarlos o eliminarlos.

Es necesario tener en cuenta:

- Realizar un análisis óptimo del uso de la red y sus recursos
- Identificar los roles a nivel de usuario.
- Tener el control del uso de las contraseñas

2.4.2 Norma Técnica Colombiana NTC-ISO 31000

Las organizaciones actualmente se enfrentan constantemente a situaciones de riesgo internas y externas producto de las dinámicas propias del mercado al cual pertenecen, para lo cual deben buscar nuevos métodos de mitigación y aseguramiento de la información, esto hace que necesariamente tengan que evolucionar en el uso de nuevas tecnologías que les permitan gestionar de una manera eficiente y efectiva los diferentes riesgos que puedan llegar en algún momento a impactar drásticamente el negocio.

La norma NTC-ISO 31000 nos muestra un marco de referencia con una metodología de mejores prácticas donde nos permite integrar el proceso de la gestión del riesgo con los procesos de negocio y cultura organizacional. Esta norma brinda los principios y las directrices genéricas sobre la gestión del riesgo y puede ser utilizada por cualquier empresa pública, privada o comunitaria asociación, grupo o individuo. (ICONTEC, 2011)

2.4.3 Seguridad y privacidad de la información

De acuerdo con la guía de gestión del riesgo del (MINTIC, 2016) la seguridad y privacidad es necesaria para que las entidades documenten cada una de las etapas de los procesos de la Gestión del Riesgo, de esta forma la entidad y las partes interesadas podrán definir la guía de riesgos y replicarla cada vez que se requiera.

La norma ISO 27005A propone varias etapas para realizar el análisis de riesgos de entidad sin importar su naturaleza.

- **Identificación del riesgo:** Determina que podría suceder si se perdiera la información.
- **Identificación de los activos** Un activo es todo aquello que tiene valor para la entidad.
- **Identificación de las amenazas** Las amenazas pueden ser de origen natural o humano.
- **Identificación de controles existentes** Los controles existentes para evitar trabajo o costos innecesarios,
- **Identificación de las vulnerabilidades** Es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes
- **Identificación de las Consecuencias** Es necesario tener en cuenta:
    - Lista de activos de información y su relación con cada proceso de la entidad.
    - Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

2.4.4 Seguridad de la información

De acuerdo con lo planteado por Areito, (2008), la seguridad es un proceso continuo y multidimensional, también considerada como una disciplina en continua evolución, persigue que se cumpla todos los objetivos estratégicos y misionales de una empresa. Aplica medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y adicionalmente tiene en cuenta activos como la información impresa y el conocimiento de las personas.

Las organizaciones deben crear y asegurar un ambiente que permita proteger los tres principios fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad. Los cuales se presentan con más detalle en la siguiente tabla.

Tabla 3. Principios Fundaméntales de la Seguridad de la Información

Principio	Descripción
Confidencialidad	La información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para las partes interesadas.

Integridad	Garantiza a las partes interesadas a que los datos no se modifican sin autorización.
Disponibilidad	Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

Fuente. Elaboración propia

2.5 Descripción de la Secretaría Distrital de Hacienda

El nacimiento de la Entidad se produjo gracias a la Ley 72 de noviembre 29 de 1926 "Sobre atribuciones del municipio de Bogotá", expedida por el Congreso de Colombia durante la presidencia de Miguel Abadía Méndez y la alcaldía de José María Piedrahita.

Además de establecer la creación de una entidad especializada en el manejo de las finanzas del todavía municipio y del perfil del funcionario a cargo, la Ley no entrega más detalles sobre la estructura o funcionamiento de la misma. Su estructura y funciones vendrían a establecerse unos meses después en el Decreto 106 de junio 30 de 1927, cuando también se posesionaría el primer Secretario de Hacienda: Alipio Pabón G.

Se afirma que la creación de la Secretaría Distrital de Hacienda se dio en un momento en que la capital se consolidaba como centro financiero, cultural y político del país, respondiendo a necesidades administrativas específicas como el crecimiento urbano, la explosión demográfica y nuevas exigencias sociales que demandaron asistencia por parte del Estado y en participar del Ejecutivo Municipal. Estas demandas solo podrían ser solucionadas por una entidad que se encargará exclusivamente de la administración de los recursos económicos y financieros, a través del sistema tributario, del recaudo de las rentas y la asignación de recursos para toda la administración municipal.

2.5.1 Misión de la Entidad

La Secretaría Distrital de Hacienda tiene la misión de gestionar recursos y distribuirlos entre los sectores de la Administración Distrital, para cumplir con las metas establecidas en el Plan de Desarrollo, bajo el principio de sostenibilidad fiscal. (Secretaría Distrital de Hacienda, 2019)

2.5.2 Visión de la Entidad

Para 2020 la Secretaría Distrital Hacienda facilitará el recaudo y administración de los recursos a través de la ampliación de canales de atención, el uso de tecnologías de la información y un talento humano comprometido con un servicio amable y eficiente de cara al ciudadano. (Secretaría Distrital de Hacienda, 2019)

2.5.3 Servicios que ofrece la Secretaría Distrital de Hacienda

- Atención al contribuyente a través de los canales establecidos
- Certificación de pagos
- Consulta de pagos
- Certificación de saldos, deudas o de cuenta
- Facilidad de pago
- Devolución y/o compensación de pagos en exceso y pagos de lo no debido
- Corrección de declaraciones que afectan la liquidación (corrección por menor valor)
- Corrección de errores e inconsistencias en declaraciones y recibos de pago (saneamiento)
- Registro de contribuyentes del impuesto de industria y comercio
- Registro de los sujetos pasivos o responsables de impuesto al consumo
- Cancelación del registro de contribuyentes del impuesto de industria y comercio
- Impuesto predial unificado
- Impuesto vehículos automotores
- Impuesto de industria y comercio y su complementario de avisos y tableros
- Impuesto de delineación urbana
- Impuesto a la publicidad visual exterior
- Impuesto unificado fondo de pobres, azar y espectáculos
- Sobretasa municipal o distrital a la gasolina motor
- Impuesto de loterías foráneas y sobre premios de lotería
- Impuesto al consumo de cervezas, sifones, refajos y mezclas nacionales
- Impuesto al consumo de cigarrillos y tabaco elaborado de origen extranjero
- Certificación del pago de participación en plusvalía
- Tornaguía de Tránsito y Reenvíos

- Recaudo de ingresos tributarios y no tributarios
- Pago a personas naturales y/o jurídicas
- Certificados de retención

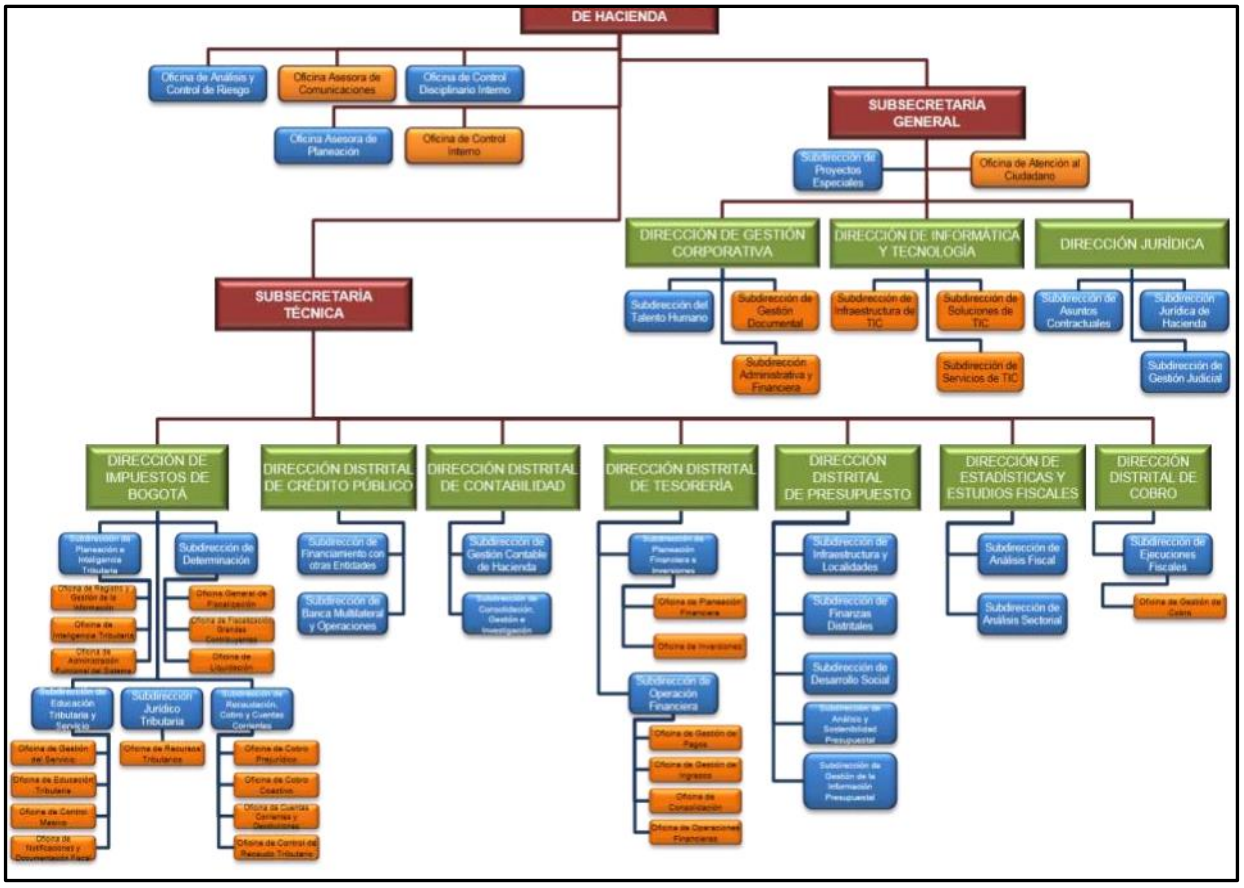
2.5.4 Áreas de la Secretaría Distrital de Hacienda

- Despacho del secretario
- Subsecretaría Técnica
- Subsecretaría General
- Dirección de Gestión Corporativa
- Dirección de Informática y Tecnología
- Dirección Jurídica
- Dirección Distrital de Presupuesto
- Dirección de Impuestos de Bogotá
- Dirección Distrital de Crédito Publico
- Dirección de Estadísticas y Estudios Fiscales
- Dirección Distrital de Contabilidad
- Tesorería Distrital
- Oficina Asesora de Planeación
- Oficina de Análisis y control de Riesgos
- Oficina de Atención al Ciudadano
- Oficina de Control Disciplinario Interno
- Oficina de Control Interno

2.5.5 Organigrama de la Secretaría Distrital de Hacienda

A continuación, se presenta el organigrama que muestra la organización interna de la Secretaría Distrital de Hacienda lo cual va a permitir identificar las áreas a intervenir y los procesos misionales y de soporte que se requieran para el desarrollo de la investigación.

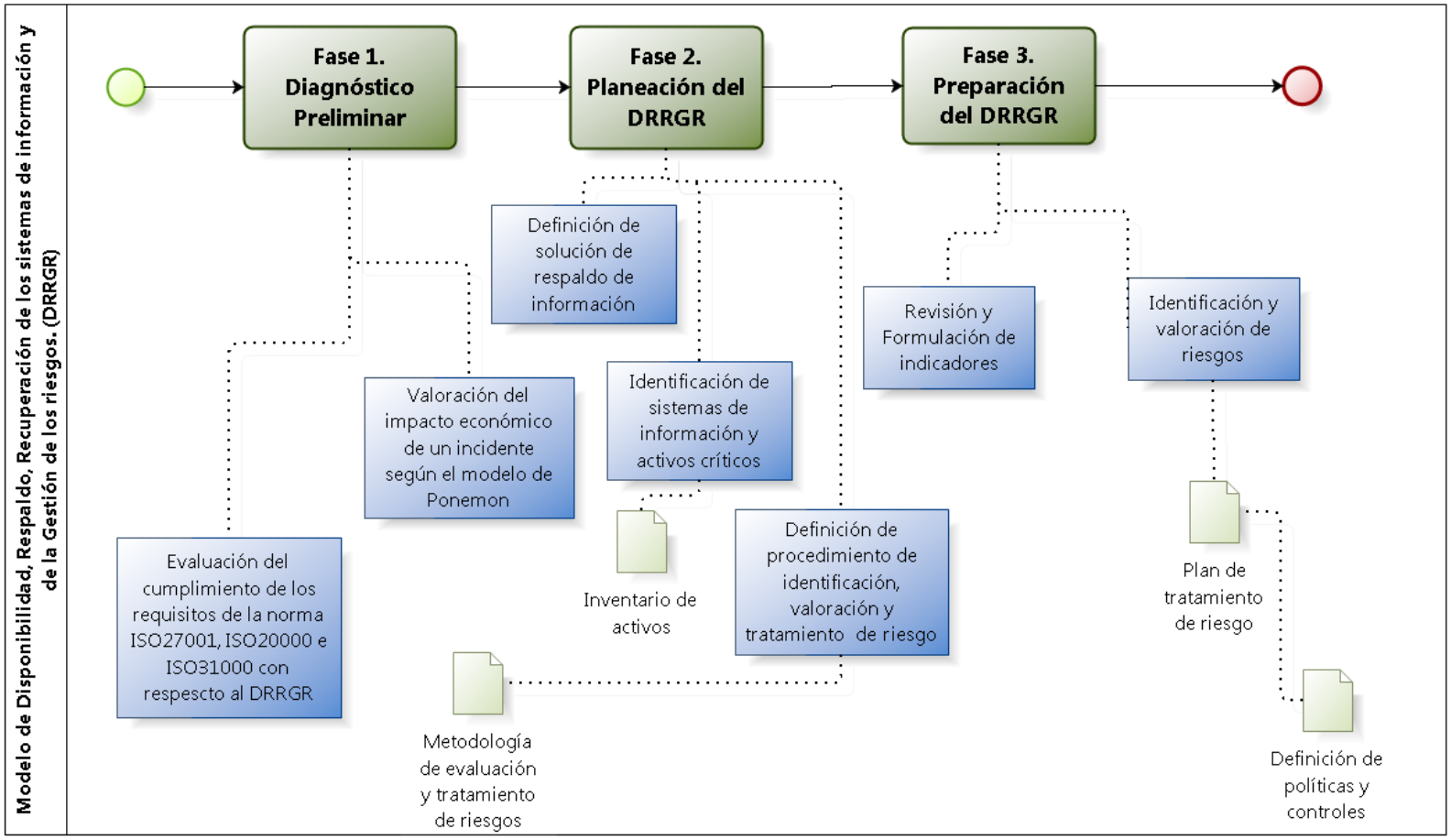
Figura 3. Organigrama de la Entidad



Fuente. Propia basado en (Secretaría Distrital de Hacienda, 2019)

3 MODELO DEL DISPONIBILIDAD, RESPALDO, RECUPERACIÓN Y GESTIÓN DEL RIESGO (DRRGR)

Figura 4. Modelo general del DRRGR



Fuente. Propia

En la figura 3 presentada anteriormente, se puede visualizar el modelo completo de la gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo. El cual fue diseñado de acuerdo con los marcos de referencia de las normas o buenas prácticas descritas en el marco teórico para el DRRGR. En la figura 4 se presentan y establecen 3 fases específicas:

Figura 5. Fases del modelo del DRRGR

Fuente. Propia

En la Fase 1, Diagnóstico preliminar del DRRGR, se identificará el nivel actual de la entidad con respecto a evaluar la disponibilidad ofrecida, su esquema de respaldo y recuperación de los sistemas de información y la gestión de riesgos basados en las mejores prácticas de las normas NTC-ISO-IEC 20000:2018, NTC-ISO-IEC 27000:2013, NTC-ISO-IEC 31000:2011. En esta fase se revisarán los indicadores actuales de operación del área, la valoración del impacto económico de un incidente que afecte la operación de acuerdo al modelo de Ponemon, y se inspeccionará el cumplimiento de unos requisitos de los marcos de referencia, con el fin de determinar el estado real y actual del área de sistemas analizada. (Instituto Ponemon, 2016)

En la Fase 2, Planeación del DRRGR, se determinarán los sistemas de información y los activos críticos, se especificará una solución para el respaldo y disponibilidad de los sistemas de información y se generará un procedimiento de identificación, valoración y tratamiento de los riesgos. En la Fase 3, Preparación del DRRGR se establecerán indicadores adecuados de gestión, se identificarán y valorarán los riesgos de acuerdo al modelo de la fase 2

3.1 Fase 1: Diagnóstico Preliminar del DRRGR

3.1.1 Evaluación del cumplimiento de los requisitos

El diagnóstico preliminar de la gestión que realiza una organización con respecto a la gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo consiste en realizar una evaluación completa de los siguientes requisitos, objetivos de control y controles de cada norma respectiva referenciados en la tabla 3.

Tabla 4. Requisitos, Objetivos de Control y Controles a evaluar

NORMA	NUMERAL	ASPECTO	REQUISITO
ISO270001:2013	A.12.1.3	CAPACIDAD	Gestión de capacidad: se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
ISO270001:2013	A.11.2.4	DISPONIBILIDAD	Mantenimiento de los equipos: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
ISO270001:2013	A.17.2.1	DISPONIBILIDAD	Disponibilidad de instalaciones de procesamiento de información: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

NORMA	NUMERAL	ASPECTO	REQUISITO
ISO270001:2013	A.17.1	RECUPERACIÓN	Continuidad de seguridad de la información: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad del negocio.
ISO270001:2013	A.17.2	RECUPERACIÓN	Redundancias: Asegurar la disponibilidad de instalaciones de procesamiento de información.
ISO270001:2013	6.1	RIESGOS	Acciones para tratar riesgos y oportunidades.
ISO270001:2013	8.2	RIESGOS	Valoración de los riesgos de la seguridad de la información.
ISO270001:2013	8.3	RIESGOS	Tratamiento de riesgos de la seguridad de la información.
ISO31000:2011	Toda la norma	RIESGOS	Gestión del riesgo, principios y directrices
ISO20000:2018	8.7.1	DISPONIBILIDAD	Aseguramiento del servicio, Gestión de la disponibilidad del servicio.
ISO20000:2018	8.7.2	RECUPERACIÓN	Aseguramiento del servicio, Gestión de la continuidad del servicio.
ISO20000:2018	8..4.3	CAPACIDAD	Oferta y Demanda, Gestión de la capacidad.

Fuente. Elaboración propia

Los anteriores requisitos, objetivos de control y **c**ontroles se deben evaluar a partir del uso de los siguientes recursos para la recolección de los datos:

- Entrevistas con los directivos del área de TIC o sistemas.
- Cuestionario con 27 preguntas orientadoras para evaluar el estado de cumplimiento de los requisitos de las tres normas (Ver Anexo 1).

Para determinar el nivel de cumplimiento que presenta la entidad con respecto a los temas relacionados del DRRGR, realizamos una entrevista utilizando el cuestionario del anexo 1 a los directivos de la Dirección de Informática y Tecnología con el fin de evaluar todos los requerimientos de los numerales de las tres normas. La Tabla 4 presenta los estados con los cuales se debe evaluar cada numeral:

Tabla 5. Criterios de validación en el diagnóstico preliminar

ESTADO	DETALLES
Cumple	Existe, está documentado, se está cumpliendo y gestionando de acuerdo a lo requerido por la norma. Cumple entre 80% y 100%.
Cumple Parcialmente	De acuerdo a lo requerido por la norma, se está realizando de manera parcial, no está completamente documentado, se definió, pero no se gestiona, ni se conoce en la organización. Puede ir desde 21% hasta 79%.
No Cumple	No existe, y/o no se está realizando, y/o no se había determinado su necesidad. Cumple entre 0% y 20%.

Fuente. Propia

Esta fase termina con la entrega del informe final de diagnóstico donde se determina el porcentaje de cumplimiento de los requisitos especificados en la Tabla 3, discriminado por tres temas básicos: gestión de disponibilidad, gestión de respaldo y recuperación, y gestión de riesgos. Dicho informe incluye un análisis de los hallazgos detectados, y da fin a la Fase 1, para iniciar con la etapa de planificación del DRRGR.

3.1.2 Valoración del impacto económico de un incidente

El diseño de un modelo DRRGR es un elemento clave en las estrategias generales de las organizaciones del sector de la tecnología. No obstante, para muchos directivos, todas las iniciativas asociadas al área de TI son vistas como un gasto, jamás como un ahorro y mucho menos como una inversión. Según la firma Ponemon Institute, los costos en promedio por pérdida de algún activo de información pueden ser superiores a los 63 millones de pesos. (Instituto Ponemon, 2016)

Un correcto diseño de un modelo de DRRGR impacta positivamente el área económica, a través de la reducción de costos directos como la pérdida de los activos o las inversiones innecesarias en seguridad y tecnología e indirectos como el aumento en los pagos de primas de seguros. Según el Instituto Ponemon el ahorro que pueden tener las empresas que contratan soluciones digitales enfocadas en seguridad puede ir hasta los $1.9 millones de dólares al año (Instituto Ponemon, 2016).

En esta última etapa de la fase 1 el objetivo es demostrar el valor de las buenas prácticas de protección de la información y los factores que se deben evaluar en cuanto los costos económicos causados por la afectación de un incidente que interrumpa totalmente la operación de los servicios que ofrece el área, segregándolos en los siguientes aspectos especificados en la figura 5:

Figura 6. Gama de Costos de un incidente

Fuente. Propia

En la tabla5 se presenta la plantilla de evaluación que se debe utilizar para medir efectivamente todos los costos asociados que pueden generarse cuando se presente un incidente que interrumpa la operación total del área.

Tabla 6. Plantilla de evaluación de Costos de un Incidente

Tipo de Costo	Costos Internos				Costos directos		Costos Indirectos		
Costos asociados a	Detección	Investigación	Contención	Recuperación	Pérdida de clientes	Multas y Sanciones	Afectación de la imagen de la empresa	Aumento en la prima del seguro	Interrupción en la operación
Costos (Millones de Pesos Colombianos $)									

Fuente. Propia

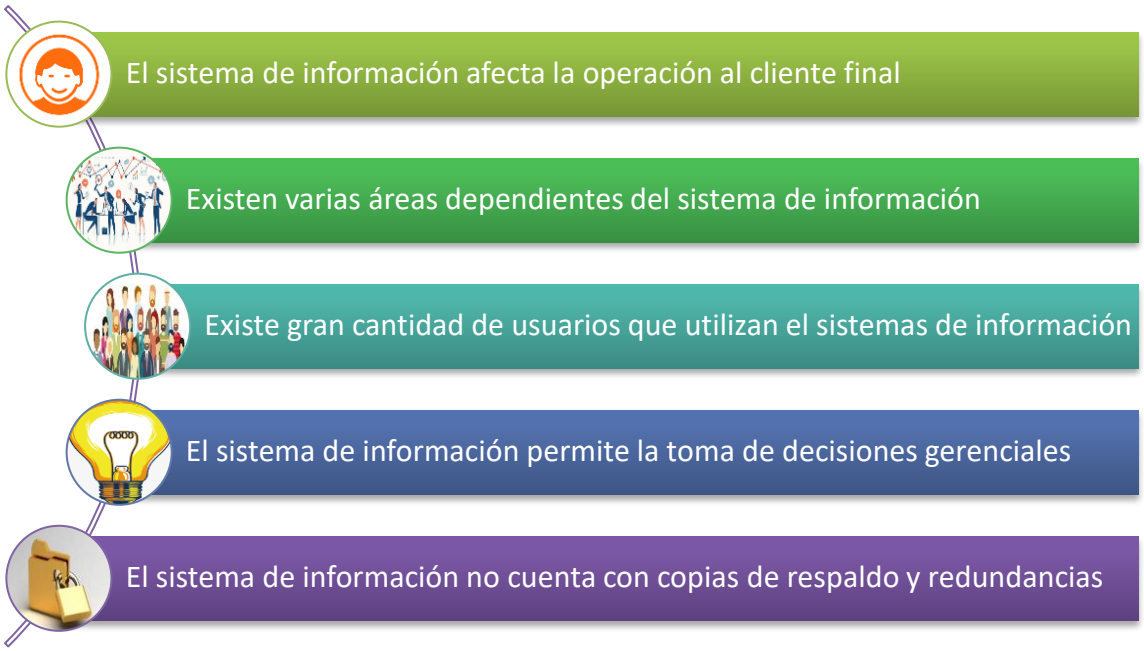
3.2 Fase 2: Planificación del DRRGR

3.2.1 Identificación de sistemas de información

Una vez culminado el diagnóstico, se inicia la etapa de planificación con la identificación y clasificación de los sistemas de información críticos en la operación.

Para identificar correctamente los sistemas de información que son claves en la operación se recomienda tener en cuenta los siguientes cinco aspectos mencionados en la figura 6.

Figura 7. Aspectos para determinar la importancia de un sistema de información



Fuente. Propia

3.2.2 Definición de la solución de respaldo de información

Nos encontramos en una era tecnológica, en donde sin importar el tipo o el tamaño de la empresa se generan grandes cantidades de información, cuyo valor es muy importante para la continuidad del negocio. Dentro y fuera de la organización, la información está expuesta a muchos riesgos y amenazas como desastres naturales, delincuentes informáticos, errores humanos o empleados descontentos que pueden afectar la disponibilidad de la información. En consecuencia, cualquier empresa o entidad necesita generar mecanismos que garanticen que, si los datos o la información

son borrados, se puedan recuperar, independientemente de la causa que originó la pérdida de información.

Una actividad muy importante dentro del modelo del DGRRR es obtener copias de respaldo de la información que soporta el Sistema de Información para mejorar los niveles de preparación de la Entidad en caso de una contingencia o emergencia. En esta Actividad de la fase 2 se debe identificar la situación actual que tiene la organización con respecto a la infraestructura para las tareas de respaldos de información. Para posteriormente definir una nueva solución que se adecue a las necesidades actuales de la compañía.

3.2.3 Definición de procedimientos de identificación, valoración y tratamiento de riesgo

La última etapa de la fase 2, correspondiente a la gestión de riesgos, es un aspecto muy importante, ya que aquí se establecen las acciones para identificar, evaluar, clasificar y convenir la estrategia para mitigar los riesgos a niveles aceptables. A continuación, se presenta la metodología propuesta con la cual se debe construir el procedimiento de gestión de riesgos, el cual se basa en la norma ISO27001 y en la norma ISO31000, y se alinea perfectamente al ciclo PHVA (planear, hacer, verificar y actuar). En la figura 7 se presentan las cuatro etapas fundamentales que debe tener la metodología de gestión de riesgos:

Figura 8. Metodología Gestión de Riesgos

Fuente. Propia

3.3 Fase 3: Preparación del DRRGR

3.3.1 Revisión y formulación de indicadores

Según Salgueiro (2001), la manera más eficaz de mejorar los resultados del área de sistemas de la organización es midiendo y controlando los aspectos correctos, ya que a tavés de estos, se puede controlar la evolución del área, indicar a los directivos y empleados lo que realmente importa.

En esta segunda parte de la fase 1, adicional de revisar la gestión que tiene el área con respecto a los indicadores de gestión, es importante validar que estén midiendo los aspectos importantes y no únicamente en los que el área está fuerte. Para el modelo del DRRGR es importante verificar la existencia mínima de los siguientes indicadores:

- Disponibilidad de los servicios soportados por el área
- Apreciación de los usuarios respecto a la prestación del servicio
- Cumplimiento de los acuerdos de niveles de servicio establecidos
- Recurrencia de incidentes por usuario y servicio

3.3.2 Identificación y valoración de riesgos

Una vez establecido el procedimiento solicitado en el numeral 3.2.3 de la fase 2, se deben identificar los riesgos teniendo en cuenta como mínimo los campos establecidos en la tabla 6.

Tabla 7. Campos mínimos del registro del análisis de riesgos

Objeto del análisis del riesgo	Integrantes del equipo de identificación	Riesgos Identificados	Vulnerabilidades	Valoración	Tratamiento del Riesgo	Controles	Riesgo Residual

Fuente. Propia

Adicionalmente, se deben analizar las causas o vulnerabilidades que producen estos riesgos, la severidad del riesgo inherente y el residual.

IDENTIFICACIÓN Y VALORACIÓN

3. RIESGOS	4. VULNERABILIDADES	5. VALORACIÓN DE LA CAUSA INHERENTE							Severida Inherente d Causa
Descripción	Descripción	Probabilidad	Criterio	P	Impacto	Criterio	I	PI	

4 MODELO DEL DRRGR APLICADO A LA SDH

4.1 Fase 1: Diagnóstico Preliminar del DRRGR

4.1.1 Evaluación del cumplimiento de los requisitos

En este capítulo se presenta el diagnóstico realizado en la Secretaría Distrital de Hacienda con el fin de conocer el estado actual de cumplimiento de los requisitos de la norma ISO27001, ISO20000 e ISO31000, con respecto a la disponibilidad, respaldo, recuperación de los sistemas de información y la gestión del riesgo. Dicha validación se realizó bajo los criterios de evaluación establecidos en la Tabla 3 del capítulo 3.

En la tabla 7 se presentan los resultados del estado de cumplimiento evidenciados en la Secretaría Distrital de Hacienda.

Tabla 8. Estado de Cumplimento de requisitos

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO270001:2013	A.12.1.3 CAPACIDAD	¿La Secretaría Distrital de Hacienda hace seguimiento al uso de recursos?	Cumple Parcialmente	30%	La Secretaría Distrital de Hacienda cuenta con un contrato de monitoreo en el Datacenter en un modelo 7*24*365 días del año.
ISO270001:2013	A.12.1.3 CAPACIDAD	¿La Secretaría Distrital de Hacienda identifica los requisitos de capacidad teniendo en cuenta la criticidad que tiene para el negocio cada sistema?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO270001:2013	A.12.1.3 CAPACIDAD	¿La Secretaría Distrital de Hacienda hace proyecciones de los requisitos sobre la capacidad futura, teniendo en cuenta los nuevos servicios, sistemas y las tendencias actuales y proyectadas?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO270001:2013	A.11.2.4 DISPONIBILIDAD	¿La Secretaría Distrital de Hacienda realiza mantenimientos preventivos a intervalos planificados a los equipos para asegurar su disponibilidad?	**Cumple**	90%	La Entidad cuenta con un cronograma donde se definen las fechas de los mantenimientos preventivos y correctivos con el objetivo de no impactar el negocio.

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO270001:2013	A.11.2.4 DISPONIBILIDAD	¿Se lleva registros de todas las fallas reales o sospechadas, y de todos los mantenimientos preventivos realizados?	**Cumple**	100%	Se lleva control mediante los informes de los proveedores y las bitácoras que llevan los operadores de Datacenter
ISO270001:2013	A.17.2.1 DISPONIBILIDAD	¿Las instalaciones de procesamiento de información cuentan con redundancias suficientes para cumplir con los requisitos de disponibilidad?	**Cumple**	100%	Actualmente toda la infraestructura ubicada en el Datacenter de la Entidad cuenta con alta disponibilidad para los diferentes dispositivos como; las UPS, aires, Planta eléctrica, servidores, almacenamiento, conectividad entre otras.
ISO270001:2013	A.17.2.1 DISPONIBILIDAD	¿La SDH tiene identificado los requisitos del negocio para la disponibilidad de los sistemas de información?	Cumple Parcialmente	50%	Este requisito se cumple parcialmente debido a que la SDH si tiene alta disponibilidad en el DataCenter para toda la infraestructura, incluyendo UPS, Aire Acondicionado, plantas eléctricas, entre otros. Pero no se evidencia que conozcan ni hayan

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
					identificado los requisitos del negocio
ISO270001:2013	A.17.2.1 DISPONIBILIDAD	¿Los sistemas de información redundante se ponen a prueba regularmente para asegurar que después de una falla, la conmutación?	Cumple Parcialmente	21%	No existe el procedimiento, pero cuando se generan apagados controlados del Datacenter se realizan pruebas de alta disponibilidad sobre alguna infraestructura.
ISO270001:2013	A.17.1 RECUPERACIÓN	¿Existe un plan de continuidad que aplique a los sistemas de información que son soportados por el área de Subdirección de Infraestructura de Tecnología de la SDH?	Cumple Parcialmente	21%	Actualmente la entidad cuenta con un contrato para el envío de cintas de Backup a un sitio alterno por medio de un operador de correo pero no se realizan pruebas de recuperación de estos medios.
ISO270001:2013	A.17.1.1 RECUPERACIÓN	¿Los requisitos de continuidad de seguridad de la información se formulan explícitamente en los procesos de negocio o de gestión de recuperación de desastres?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO270001:2013	A.17.1.2 RECUPERACIÓN	¿La Secretarías Distrital de Hacienda tiene establecido, documentado e implementado procesos, procedimientos y controles paras asegurar el nivel continuidad requerido de los sistemas de información?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO270001:2013	A.17.1.3 RECUPERACIÓN	¿La SDH verifica a intervalos planificados los controles de continuidad establecidos, con el fin de asegurar que son válidos y eficaces durante situaciones adversas?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO270001:2013	6.1 RIESGOS	¿En la Subdirección de Infraestructura de Tecnología de la SDH, la organización ha identificado riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de los sistemas de información y de su infraestructura?	Cumple Parcialmente	70%	La entidad tiene construida e implementada una matriz de riesgos asociados al proceso y los procedimientos, pero la actividad de identificación y evaluación no se realiza de forma periódica, ni se evalúa el riesgo residual.

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO270001:2013	8.2 RIESGOS	¿En la Subdirección de Infraestructura de Tecnología de la SDH existe un proceso de valoración de riesgos?	**Cumple**	100%	La SDH si cuenta con un proceso de valoración de riesgos.
ISO270001:2013	8.3 RIESGOS	¿En la Subdirección de Infraestructura de Tecnología de la SDH se ha definido un proceso de tratamiento de los riesgos? ¿Existe una valoración del riesgo residual?	Cumple Parcialmente	70%	La entidad tiene construida e implementada una matriz de riesgos asociados al proceso y los procedimientos, y tiene asociado planes para mitigar los riesgos. Pero no se evidencia la valoración del riesgo residual.
ISO31000:2011	RIESGOS	¿En proceso de identificación, valoración y tratamiento de los riesgos, se tiene considerado el análisis del contexto, la identificación, el análisis, la evaluación y el tratamiento del riesgo?	Cumple Parcialmente	70%	Actualmente solo está documentada una matriz de riesgo para la continuidad del negocio alineada solamente a desastres físicos en el Datacenter. Falta identificar más riesgos que puedan afectar la continuidad del negocio
ISO20000:2018	8.7.1 DISPONIBILIDAD	¿En la Subdirección de Infraestructura de Tecnología de la	Cumple Parcialmente	70%	Actualmente solo está documentada una matriz de riesgo

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
		SDH se ha evaluado, y documentado los riesgos para la continuidad del servicio?			para la continuidad del negocio alineada solamente a desastres físicos en el Datacenter.
ISO20000:2018	8.7.1 DISPONIBILIDAD	¿La SDH ha identificado los requisitos y los objetivos de disponibilidad del servicio?	Cumple Parcialmente	50%	Este requisito se cumple parcialmente debido a que la SDH si tiene alta disponibilidad en el DataCenter para toda la infraestructura, incluyendo UPS, Aire Acondicionado, plantas eléctricas, entre otros. Pero no se evidencia unos objetivos claros en la disponibilidad del servicio
ISO20000:2018	8.7.1 DISPONIBILIDAD	¿Los requisitos acordados para la gestión de la disponibilidad de los servicios, tienen en cuenta los requisitos de negocio pertinentes, los requisitos del servicio, los ANS y los riesgos?	Cumple Parcialmente	50%	Se identifican Acuerdos de niveles de servicio para mantenimientos correctivos y preventivos, pero no para la disponibilidad, no existen acuerdos definidos con los clientes internos de las otras áreas de la entidad. Pero si se evidencia ANS en los contratos con los acuerdos de mantenimiento con los

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
					proveedores, service desk, entre otros.
ISO20000:2018	8.7.2 RECUPERACIÓN	¿En la Subdirección de Infraestructura de Tecnología de la SDH se ha evaluado y documentado los riesgos para la continuidad del negocio?	No Cumple	15%	Se evidencia una matriz de riesgos, pero no se tienen identificados riesgo que afecten completamente la continuidad del negocio, ni tampoco riesgos una vez se haya iniciado un plan de continuidad
ISO20000:2018	8.7.2 RECUPERACIÓN	¿En la Subdirección de Infraestructura de Tecnología de la SDH existe un plan de continuidad del negocio?	No Cumple	15%	Actualmente la entidad cuenta con un contrato que incluye el envío de cintas de Backup a un sitio alterno por medio de un operador de correo, pero no se realizan pruebas de recuperación de estos medios, ni se cuenta con un plan de continuidad.
ISO20000:2018	8.7.2 RECUPERACIÓN	¿Dentro del plan de continuidad del negocio, se tiene definido los criterios y las responsabilidades para invocar la continuidad del servicio?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.

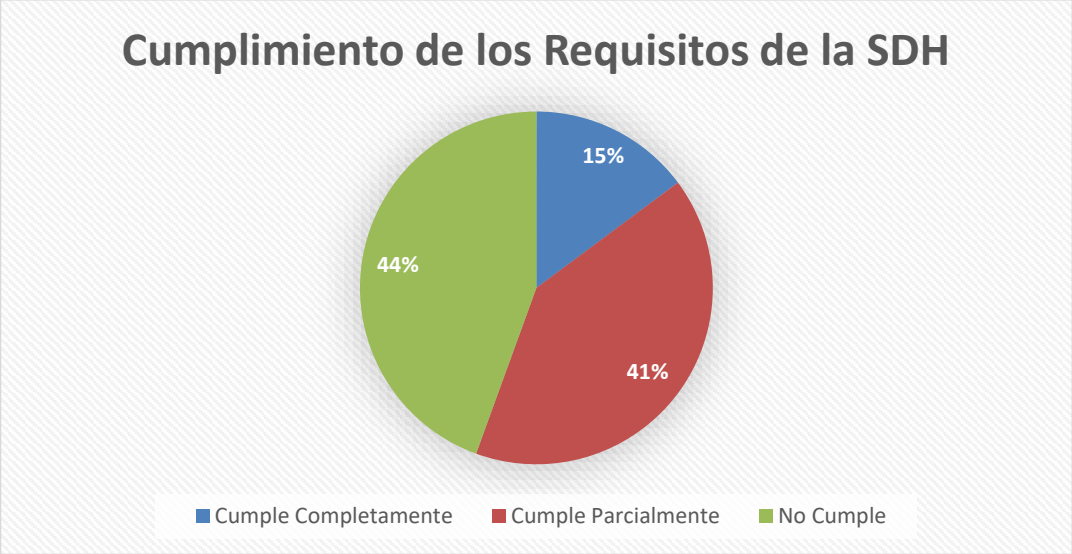
Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO20000:2018	8.7.2 RECUPERACIÓN	¿Dentro del plan de continuidad del negocio, se tiene definido los procedimientos por implementar en caso de una pérdida importante en el servicio?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO20000:2018	8.7.2 RECUPERACIÓN	¿Dentro del plan de continuidad del negocio, se tiene definido los procedimientos para regresar a las condiciones normales del trabajo?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral.
ISO20000:2018	8.4.3 CAPACIDAD	¿En la Subdirección de Infraestructura de Tecnología de la SDH se ha determinado los requisitos de capacidad en relación con los recursos humanos, técnicos, de información y financieros?	Cumple Parcialmente	75%	La entidad cuenta con la planta de personal para la administración de los sistemas y tiene la infraestructura para soportar los diferentes servicios.
ISO20000:2018	8.4.3 CAPACIDAD	¿La Subdirección de Infraestructura de Tecnología de la SDH ha planificado su capacidad actual y prevista en función de la demanda de servicios?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral. La entidad va creciendo de acuerdo a los problemas que vayan surgiendo.

Norma	Requisito	Pregunta	Estado de Cumplimiento	%	Evidencia
ISO20000:2018	8.4.3 CAPACIDAD	¿La Subdirección de Infraestructura de Tecnología de la SDH ha planificado su capacidad para incluir cronogramas de tiempo y umbrales para cambios en la capacidad del servicio?	No Cumple	0%	No se evidencia ningún cumplimiento de este numeral. La entidad va creciendo de acuerdo a los problemas que vayan surgiendo.

Fuente. Propia a partir de (ICONTEC, 2018), (ICONTEC, 2013), (ICONTEC, 2011)

De acuerdo con el cuestionario realizado para evidenciar el cumplimiento de cada uno de los requisitos de las tres normas guías estipuladas en la fase del diagnóstico, en la figura 8 se presenta el resumen del nivel de cumplimiento y madurez de la SDH con respecto a la Disponibilidad, Capacidad, Recuperación y gestión del Riesgo:

Figura 9. Estado de cumplimiento de los requisitos establecidos

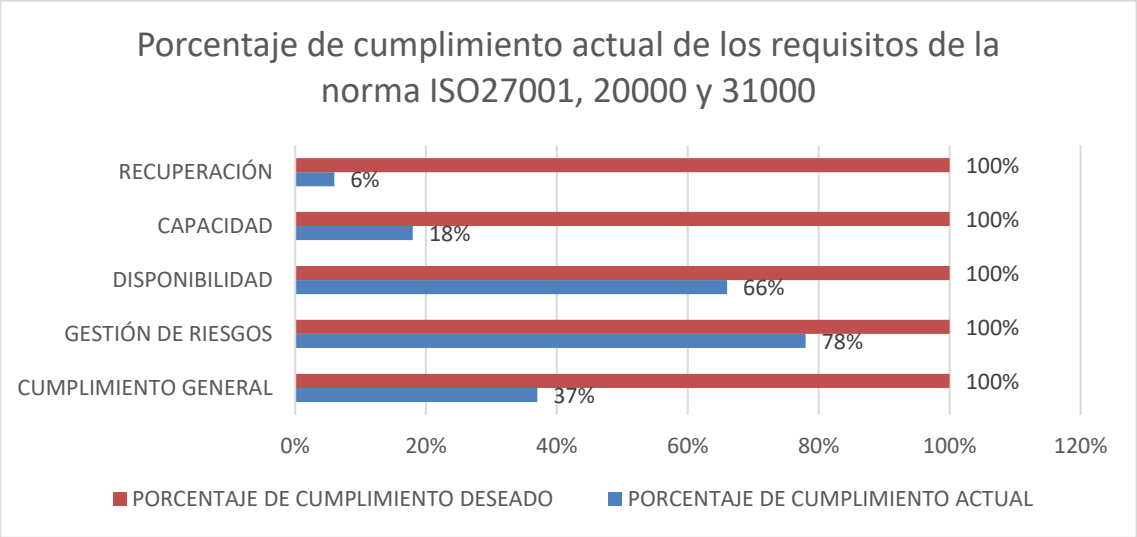


Fuente. Propia

Como se observa en la figura 8 la SDH está incumpliendo completamente en 12 de los 27 requisitos, debido a que no se evidencia ningún cumplimiento de 8 numerales de Recuperación y 4 de gestión de capacidad. Adicionalmente existen 11 requisitos que se cumplen parcialmente y únicamente cumplen totalmente 4 requisitos de la norma ISO27001 enfocados a Disponibilidad.

En la figura 9, se presenta el estado de madurez que tiene la entidad con respecto a la Disponibilidad, Capacidad, Recuperación y Gestión del Riesgo:

Figura 10. Estado de cumplimiento actual de los requisitos de las normas ISO27001, 20000 y 31000



Fuente. Propia

Como se puede observar en la figura 9 el porcentaje total de cumplimiento de los 27 requisitos evaluados es del 37%, el cual es apalancado por dos aspectos que la compañía cumple positivamente (Disponibilidad 66% y Gestión de riesgos 78%). No obstante, el cumplimiento con respecto a la recuperación y la gestión de capacidad es muy bajo, con solo 6% y 18% respectivamente. A continuación, se detalla las fortalezas y debilidades detectadas.

Disponibilidad: La SDH sí tiene alta disponibilidad en el Data Center con respecto a toda la infraestructura, incluyendo UPS, servidores, aire acondicionado, conectividad, plantas eléctricas, entre otros. Adicionalmente, la entidad cuenta con un cronograma donde se definen las fechas de los mantenimientos preventivos y correctivos. Con el objetivo de no impactar el negocio y siempre asegurar la disponibilidad, se llevan registros de todas las fallas reales o sospechadas, y cuando se generan apagados controlados del Datacenter, se realizan pruebas de alta disponibilidad sobre alguna infraestructura. Pero no se evidencian los Acuerdos de Niveles de Servicio (ANS) para la disponibilidad, ya que no existen objetivos claros, ni acuerdos definidos con los clientes internos y con las otras áreas de la entidad.

Gestión del Riesgo: La SDH cuenta con un procedimiento para la identificación, evaluación y tratamiento de los riesgos de la entidad y tiene una matriz de riesgos asociados a los procesos de

TI. No obstante, la actividad de identificación y evaluación no se realiza de forma periódica, ni se evalúa el riesgo residual.

Gestión de Capacidad: Como aspecto positivo la Secretaría Distrital de Hacienda cuenta con un contrato de monitoreo en el Datacenter bajo un modelo de 7×24 para los 365 días del año. Pero no se evidencia que la entidad identifique los requisitos de capacidad teniendo en cuenta la criticidad que tiene para el negocio cada sistema, ni las proyecciones de capacidad futura. Como lo dijo el Director de Sistemas en una reunión de comité directivo de la Dirección de Informática y Tecnología: "La entidad va creciendo de acuerdo a los problemas que vayan surgiendo".

Recuperación: Este el aspecto más negativo detectado en el diagnóstico realizado, debido a que la SDH no tiene un Plan de Recuperación de Desastres (PRD) para el área, ni mucho menos un plan de continuidad. La entidad cuenta con un contrato para el envío de cintas de copias de respaldo a un sitio alterno por medio de una empresa de mensajería, pero no se realizan pruebas de recuperación ni pruebas de estos medios.

4.1.2 Valoración del impacto económico de un incidente

En este punto se realiza la evaluación de los costos por la afectación de un incidente causado por un incendio en el Data Center. Este incendio va a interrumpir totalmente la operación de los servicios que ofrece la Subdirección de Infraestructura de Tecnología de la Secretaría Distrital de Hacienda.

Actualmente la SDH no ha sido víctima de un ataque de denegación de servicio, no obstante, se realizó una investigación de posibles costos internos, directos e indirectos como simulación de consecuencias

Costos internos:

Detección: Actualmente la SDH tiene su infraestructura ubicada en un Data Center que cuenta con un servicio de monitoreo en un modelo 7×24 los 365 días del año para la capa de aplicación bases

de datos y servidores, estos ingenieros son los encargados inicialmente de la detección y escalamiento cuando se identifique un ataque dirigido a la SDH.
Costo mensual: Contrato de monitoreo de la capa de aplicaciones, bases de datos e infraestructura tecnológica: 85 millones de pesos

Investigación: Debido a la criticidad de la operación de la SDH, se requiere contratar una firma consultora para identificar la causa raíz y análisis forense de la infraestructura y las aplicaciones comprometidas en el ataque.
Costo: Contrato con firma consultora 50 millones de pesos

Contención: Como medida de contención y recuperación rápida del servicio, se debería montar la infraestructura en el sitio alterno de operación con las copias de respaldo que se tendrían en cintas magnéticas
Costo: 130 millones de pesos

Recuperación: La SDH, para recuperar nuevamente su operación a condiciones normales, debería invertir en los gastos de volver a montar el Data Center con toda su infraestructura.
Costo: 200 millones de pesos

Costos directos:

Multas y Sanciones: El Gobierno Nacional puede imponer multas o sanciones económicas causadas por no cumplir adecuadamente sus obligaciones de seguridad.
Costo Aproximado: 1.000 millones de pesos

Pérdida de equipos: La SDH, para recuperar nuevamente su operación a condiciones normales, debería invertir en los equipos de volver a montar el Data Center con toda su infraestructura.
Costo: 2.000 millones de pesos

Costos indirectos:

Afectación de la imagen de la entidad: De llegarse a presentar algún incidente en la prestación del servicio entregado por la SDH en una fecha de vencimiento de impuestos, y su recuperación tardara un tiempo mayor a una semana, se tendría pérdidas catastróficas que podrían llegar a representar un monto alrededor de los 5.000 millones de pesos.

Aumento en la prima del seguro: La SDH actualmente cuenta con póliza contra todo riesgo con cobertura de daños en sus aplicaciones e infraestructura, de tal manera que cuando se presenta el incidente se activan estos protocolos cumpliendo la póliza y atendiendo la emergencia. De presentarse un incidente los costos en las pólizas serán de $500 millones de pesos.

Interrupción en la operación: Toda entidad distrital, que presenta interrupción en sus operaciones tiene consecuencias, el impacto de la interrupción en la operación puede alcanzar los 5.000 millones de pesos ya considerados en la afectación de la imagen.

En la tabla 8 se presenta el resumen de todos los costos anteriormente analizados

Tabla 9. Costos Incidente de Seguridad de la Información en SDH

Tipo de Costo	Costos Internos				Costos directos		Costos Indirectos		
Costos asociados a	Detección	Investigación	Contención	Recuperación	Pérdida de equipos	Multas y Sanciones	Afectación de la imagen de la empresa	Aumento en la prima del seguro	Interrupción en la operación
Costos (Millones de Pesos Colombianos $)	85	150	130	200	2000	1000	2500	500	2500

Fuente. Propia

Costos Totales: 9065 millones de pesos colombianos.

4.2 Fase 2: Planificación del DRRGR

4.2.1 Identificación de sistemas de información y activos críticos

En esta fase se presentan los once sistemas de información críticos identificados en la SDH, diferenciados por administrativos, financieros y tributarios:

Administrativos:

- **PERNO**

  El Sistema de Personal y Nomina Permite apoyar el procesamiento y control del pago de los salarios del personal de planta y supernumerarios. También permite apoyar la gestión del recurso humano en cuanto a bienestar, capacitación, planta de personal, hoja de vida y salud ocupacional.

- **SISCO**

  El Sistema de Contratación permite controlar y gestionar procesos de adquisición de bienes y servicios, mediante la contratación, con y sin las formalidades plenas establecidas en la Ley 80 de 1993 y sus decretos reglamentarios, controlando el plan de contratación, la etapa precontractual y la etapa contractual.

- **TERCEROS**

  El Sistema de Información Terceros permite almacenar y centralizar la información de todas las personas naturales y jurídicas que es procesada por el Sistema de Información SICAPIT@L, eliminando de esta forma la duplicidad de los registros y garantizando la integridad y calidad de la información que es utilizada por todos los sistemas de información.

- **CORDIS**

  Aplicación desarrollada para la administración, manejo y control de documentos que emite y recibe la Secretaría de Hacienda del Distrito, en las diferentes dependencias que la conforman. Permite la interconexión de los usuarios a través de una red Internet - Intranet.

El sistema se concibió con la posibilidad de un manejo centralizado, mixto o descentralizado, asociado a la planta de personal de la entidad, mediante la cual se controlan los funcionarios autorizados para recibir y suscribir correspondencia interna o externa.

- **SAE**

  Sistema de Administración de Elementos "SAE" registra todos los ingresos de consumo y devolutivos, igualmente permite efectuar la distribución de los elementos de consumo en cada una de las áreas, de acuerdo con la programación mensual de sus necesidades y genera la identificación o placa de inventario de los bienes devolutivos. Administra los bienes y servicios de propiedad, planta y equipo. Mediante la gestión de traslados, ingresos, egresos, cálculo de depreciación y amortización.

- **SAI**

  El sistema de administración de elementos devolutivos "SAI", apoya las funciones de administrar el catálogo de elementos, registrar y controlar los procesos de ingreso, egreso y traslado de elementos, administrar y controlar el kárdex, bodegas y el inventario de elementos.

Financieros:

- **LIMAY**

  El Sistema Libro Mayor permite la generación y control de la contabilidad, a partir de los movimientos generados por los módulos de gestión de las dependencias de la SHD y las transacciones manuales requeridas. Mediante procesos de parametrización, cierres y reportes contables.

- **PREDIS**

  El Sistema de Presupuesto Distrital apoya el proceso de programación ejecución, control y seguimiento del presupuesto Distrital.

- **PAC**

  El Sistema Programa Anual de Caja apoya la programación y reprogramación mensual de los gastos de vigencia, reservas y cuentas por pagar del presupuesto distrital.

- **OPGET**

  El Sistema Operación y Gestión de Tesorería automatiza las gestiones de recaudo, pagaduría y planeación financiera de la Dirección Distrital de Tesorería. Incluye módulos de ingresos, egresos y conciliaciones bancarias.

Tributarios:

- **SIT II**

  El Sistema información Tributaria – SIT apoya la gestión de los tributos de la ciudad, permitiendo el control de la información relacionada con los contribuyentes, entidades financieras y otras instituciones, para el intercambio de información.

4.2.2 Definición de la solución de respaldo de información

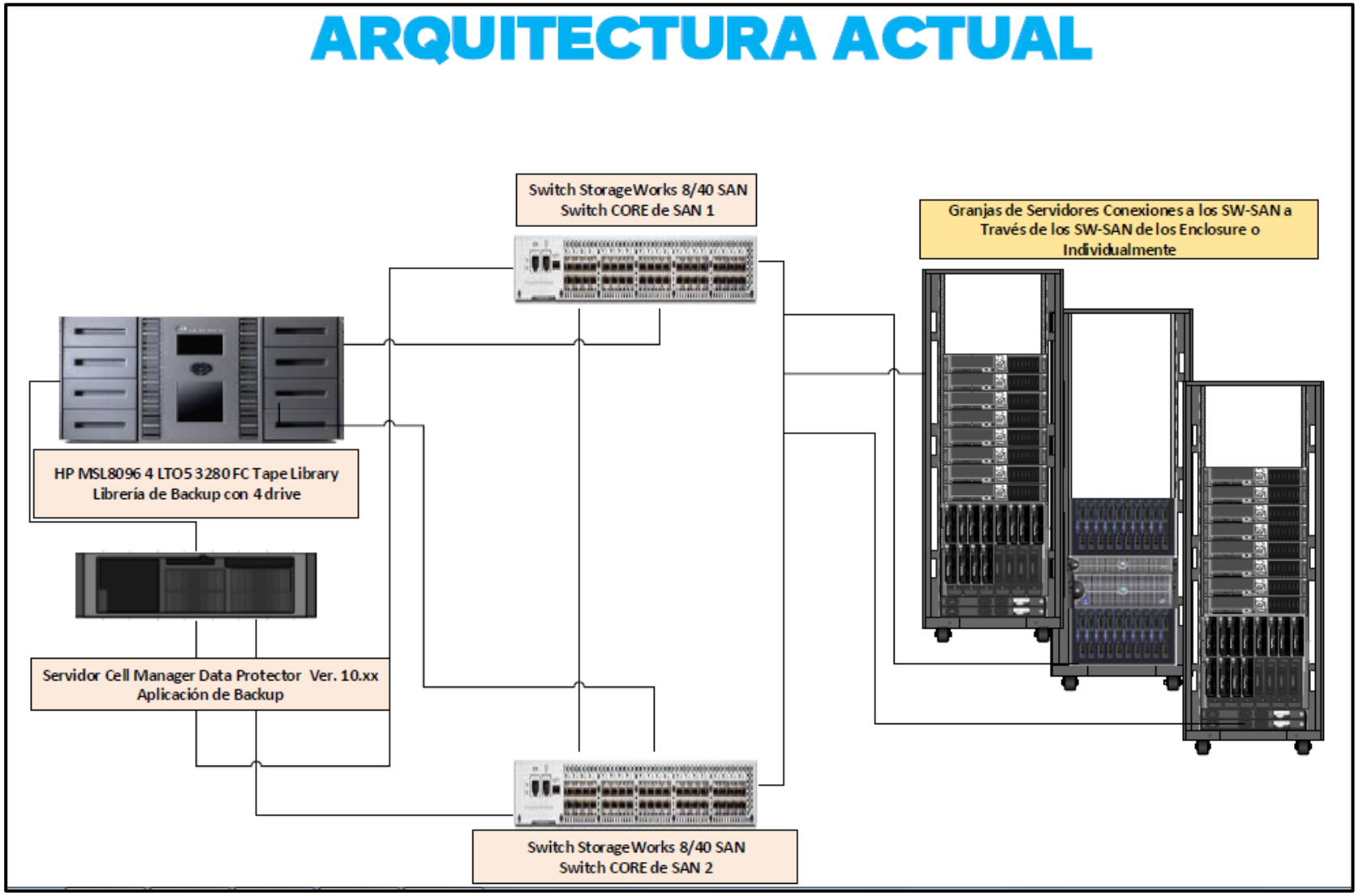
A continuación, se presenta el estado actual que tiene la organización con respecto a la infraestructura usada para las tareas de respaldos de información. Los siguientes diagramas fueron construidos a partir de la información adquirida en la etapa del diagnóstico.

En la Secretaría Distrital de Hacienda, el proceso de copias de respaldo inicia con la programación de las copias de respaldo o con la solicitud de usuario y termina con la creación de la copia y la comunicación al usuario.

Es importante mencionar que el procedimiento de copias de respaldo aplica a la información vital para el funcionamiento de la Secretaria Distrital de Hacienda la cual esta almacenada en los servidores y bases de datos presentados al sistema de almacenamiento de la entidad.

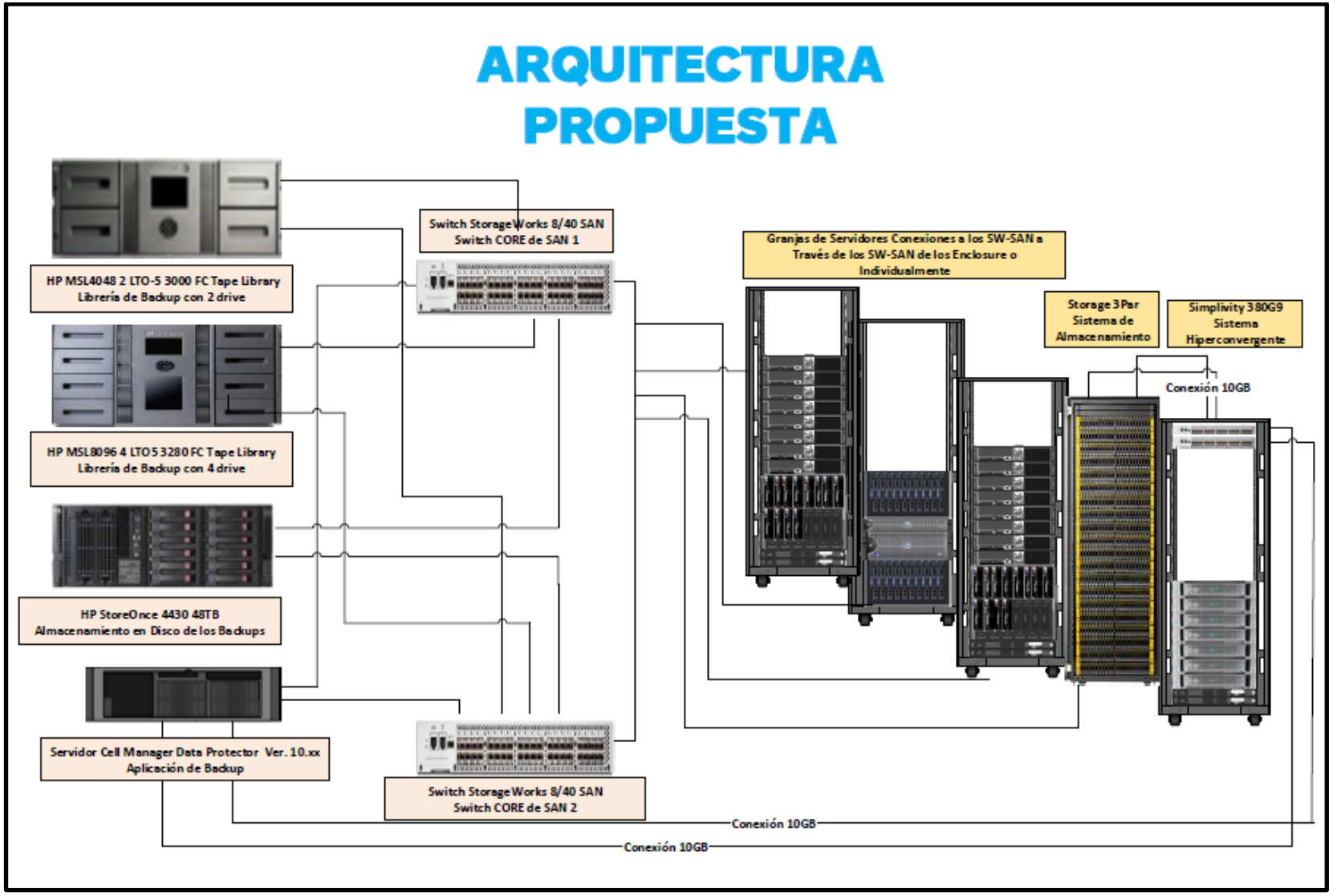
En la figura 10 se presenta el estado actual de la infraestructura de la SDH, y en figura 11 se detalla la propuesta de mejora de la infraestructura para las copias de respaldo.:

Figura 11. Estado Actual de la infraestructura para las copias de respaldo



Fuente. Propia

Figura 12. Propuesta de infraestructura para las copias de respaldo



Fuente. Propia

Es importante mencionar que la infraestructura que actualmente tiene la SDH no tiene toda la cobertura para asegurar todos los sistemas de información, ni capacidad suficiente en recuperación y respaldo de la información. Con la arquitectura propuesta se pretende crecer y mejorar todos los dispositivos o elementos de configuración que hacen parte de esta, obteniendo mayor cobertura, consolidando todas las librerías y optimizando los tiempos en la toma y restauración de backups. La anterior infraestructura tendría un costo aproximado de 300 millones de pesos, lo cual no se compara con los costos asociados que podría tener un incidente.

4.2.3 Definición de procedimientos de identificación, valoración y tratamiento de riesgo

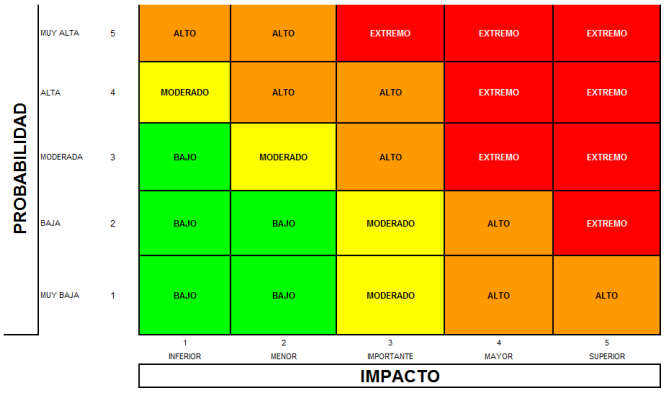
En la tabla 9, se presenta el procedimiento de gestión de riesgos, a utilizar en la identificación, valoración y tratamiento del riesgo, el cual se alinea perfectamente con la norma ISO31000 e ISO27001:

Tabla 10. Procedimiento de Gestión del Riesgo

No.	ACTIVIDAD	DESCRIPCIÓN	SALIDAS
PLANEACIÓN			
1	Establecer el objetivo de la gestión del análisis de los riesgos	Como primera actividad se debe determinar el objetivo del análisis del riesgo, es decir establecer el alcance, puede ser a todo el departamento, al área, a un servicio o a un proceso.	Objetivo del análisis de riesgo en el Registro de Riesgos.
2	Establecer los integrantes del equipo identificador	En esta segunda actividad se debe especificar cuál es el equipo que será parte de la identificación, valoración y tratamiento del riesgo. Para tener una visión más objetiva se debe procurar que el equipo esté compuesto por personal de diferentes áreas, de diferentes cargos, para que a partir de sus experiencias y visiones distintas realicen una gestión más objetiva.	Definición de los integrantes del equipo de trabajo y fecha de identificación en el Registro de Riesgos

No.	ACTIVIDAD	DESCRIPCIÓN	SALIDAS
		Se recomienda utilizar como fuentes de información los eventos e incidentes ocurridos, los riesgos identificados en áreas similares o en contextos parecidos, la lista de riesgos especificados en la pestaña 4 del registro de riesgos y las vulnerabilidades comunes que se encuentran en la pestaña 5 del registro de riesgos. Una herramienta a considerar para la identificación de riesgos puede ser las siguientes: • Entrevistas con el personal técnico u operativo. • Lluvia de Ideas con el personal relevante.	
IDENTIFICACIÓN			
3	Identificar los riesgos	En esta tercera actividad se debe identificar los riesgos a nivel de personas, servidores, sistemas de información, áreas y/o procesos según corresponda.	Riesgos identificados en el Registro de Riesgos.
4	Identificar las vulnerabilidades	En esta cuarta actividad se debe identificar las vulnerabilidades o causas que permiten que se dé dicho riesgo. Es importante mencionar que un riesgo puede tener varias causas, en este caso el riesgo se repite por cada una. Y cada vulnerabilidad o causa debe tener su propia valoración.	Vulnerabilidades identificadas en el Registro de Riesgos.

<table>
<tr><th>No.</th><th>ACTIVIDAD</th><th>DESCRIPCIÓN</th><th>SALIDAS</th></tr>
<tr><td colspan="4">VALORACIÓN</td></tr>
<tr><td>5</td><td>Valoración de la Causa Inherente</td><td>En la quinta actividad se debe evaluar el impacto y la probabilidad que tendría que un riesgo se materialice, obteniendo la severidad del riesgo inherente.

A continuación, se presenta las posibles combinaciones que originan los anteriores valores

<table>
<tr><th>PROBABILIDAD</th><th>P</th><th>IMPACTO</th><th>I</th><th>PI</th><th>SEVERIDAD</th></tr>
<tr><td>MUY BAJA</td><td>1</td><td>INFERIOR</td><td>1</td><td>11</td><td>BAJO</td></tr>
<tr><td>BAJA</td><td>2</td><td>INFERIOR</td><td>1</td><td>21</td><td>BAJO</td></tr>
<tr><td>MODERADA</td><td>3</td><td>INFERIOR</td><td>1</td><td>31</td><td>BAJO</td></tr>
<tr><td>ALTA</td><td>4</td><td>INFERIOR</td><td>1</td><td>41</td><td>MODERADO</td></tr>
<tr><td>MUY ALTA</td><td>5</td><td>INFERIOR</td><td>1</td><td>51</td><td>ALTO</td></tr>
<tr><td>MUY BAJA</td><td>1</td><td>MENOR</td><td>2</td><td>12</td><td>BAJO</td></tr>
<tr><td>BAJA</td><td>2</td><td>MENOR</td><td>2</td><td>22</td><td>BAJO</td></tr>
<tr><td>MODERADA</td><td>3</td><td>MENOR</td><td>2</td><td>32</td><td>MODERADO</td></tr>
<tr><td>ALTA</td><td>4</td><td>MENOR</td><td>2</td><td>42</td><td>ALTO</td></tr>
<tr><td>MUY ALTA</td><td>5</td><td>MENOR</td><td>2</td><td>52</td><td>ALTO</td></tr>
<tr><td>MUY BAJA</td><td>1</td><td>IMPORTANTE</td><td>3</td><td>13</td><td>MODERADO</td></tr>
<tr><td>BAJA</td><td>2</td><td>IMPORTANTE</td><td>3</td><td>23</td><td>MODERADO</td></tr>
<tr><td>MODERADA</td><td>3</td><td>IMPORTANTE</td><td>3</td><td>33</td><td>ALTO</td></tr>
<tr><td>ALTA</td><td>4</td><td>IMPORTANTE</td><td>3</td><td>43</td><td>ALTO</td></tr>
<tr><td>MUY ALTA</td><td>5</td><td>IMPORTANTE</td><td>3</td><td>53</td><td>EXTREMO</td></tr>
<tr><td>MUY BAJA</td><td>1</td><td>MAYOR</td><td>4</td><td>14</td><td>ALTO</td></tr>
<tr><td>BAJA</td><td>2</td><td>MAYOR</td><td>4</td><td>24</td><td>ALTO</td></tr>
<tr><td>MODERADA</td><td>3</td><td>MAYOR</td><td>4</td><td>34</td><td>EXTREMO</td></tr>
<tr><td>ALTA</td><td>4</td><td>MAYOR</td><td>4</td><td>44</td><td>EXTREMO</td></tr>
</table></td><td>Estimación del impacto y la probabilidad en el Registro de Riesgos.

Valoración del riesgo inherente</td></tr>
</table>

<table>
<tr><th>No.</th><th>ACTIVIDAD</th><th>DESCRIPCIÓN</th><th>SALIDAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>MUY ALTA</td><td>5</td><td>MAYOR</td><td>4</td><td>54</td><td>EXTREMO</td></tr>
<tr><td>MUY BAJA</td><td>1</td><td>SUPERIOR</td><td>5</td><td>15</td><td>ALTO</td></tr>
<tr><td>BAJA</td><td>2</td><td>SUPERIOR</td><td>5</td><td>25</td><td>EXTREMO</td></tr>
<tr><td>MODERADA</td><td>3</td><td>SUPERIOR</td><td>5</td><td>35</td><td>EXTREMO</td></tr>
<tr><td>ALTA</td><td>4</td><td>SUPERIOR</td><td>5</td><td>45</td><td>EXTREMO</td></tr>
<tr><td>MUY ALTA</td><td>5</td><td>SUPERIOR</td><td>5</td><td>55</td><td>EXTREMO</td></tr>
</table>

Es importante mencionar que para su valoración se debe tener en cuenta que:
• Para cada fila de riesgo la probabilidad del riesgo es única.
• Para valorar el impacto se debe considerar el peor de los escenarios.

Como ya se mencionó en la actividad 4, van a surgir riesgos que tengan diferentes causas, cada una de ellas se debe ser evaluada separadamente.
Al final se promediarán las calificaciones de las causas, para tener una sola valoración del riesgo inherente</td><td></td></tr>
<tr><th colspan="4">TRATAMIENTO</th></tr>
<tr><td>6</td><td>Selección del Tratamiento del riesgo y establecimiento de controles</td><td>En esta actividad se debe generar los planes de respuesta para tratar cada riesgo, las opciones posibles son

• Reducir el riesgo
• Transferir el riesgo
• Evitar el riesgo
• Aceptar el riesgo

Un riesgo puede ser aceptado únicamente por el responsable del riesgo cuando su calificación sea baja.

En esta misma actividad se puntualizarán los controles que deben implementarse o ejecutarse con el fin de tratar adecuadamente el riesgo.</td><td>Planes de tratamiento en el Registro de Riesgos.

Controles a implementar</td></tr>
</table>

No.	ACTIVIDAD	DESCRIPCIÓN	SALIDAS
		Es importante mencionar que cada causa debe tener un control a implementar, es decir que un riesgo puede tener varios controles.	
7	Evaluar el riesgo residual	En esta última actividad se debe valorar nuevamente el riesgo con el supuesto de la implantación de los controles generados.	Valoración del riesgo residual

Fuente. Propia

4.3 Fase 3: Preparación del DRRGR

4.3.1 Identificación y Formulación de indicadores

En la tabla 11, se presenta la validación de los indicadores mínimos que debería tener el modelo del DRRGR en la SDH:

Tabla 11. Verificación de Indicadores en la SDH

Indicador	Existe o es Adecuado en la SDH
Disponibilidad de los servicios soportados por el área	SI
Apreciación de los usuarios respecto a la prestación del servicio	SI
Cumplimiento de los acuerdos de niveles de servicio establecidos	NO
Recurrencia de incidentes por usuario y servicio	NO

Fuente. Propia

4.3.1.1 Indicadores Identificados

En la tabla 12, se presentan el indicador de disponibilidad identificado en la Secretaría Distrital de Hacienda y el análisis respectivo de su desempeño

Tabla 12. Indicador de Disponibilidad

INDICADOR DE DISPONIBILIDAD	
Nombre del Indicador:	DISPONIBILIDAD DE INFRAESTRUCTURA TECNOLOGICA
Año Indicador:	2019
Frecuencia del Análisis:	MENSUAL
Tipo de indicador:	EFICIENCIA
Objetivo del Indicador:	MEDIR LA DISPONIBILIDAD DE LOS SERVICIOS SOPORTADOS POR LA SITIC - MENSUALMENTE
Proceso:	CPR-46 GESTION DE LA INFRAESTRUCTURA TECNOLOGICA
Definiciones	DAPADM: DISPONIBILIDAD DE APLICACIONES ADMINISTRATIVAS DAPFIN: DISPONIBILIDAD DE APLICACIONES FINANCIERAS DAPTRI: DISPONIBILIDAD DE APLICACIONES TRIBUTARIAS DLIQUI: DISPONIBILIDAD DE LIQUIDADORES DSRCOL: DISPONIBILIDAD DE SERVICIOS DE COLABORACIÓN DBAFUN: DISPONIBILIDAD DE BASES FUNCIONALES
Área:	DIRECCIÓN DE INFORMATICA Y TECNOLOGIA

INDICADOR DE DISPONIBILIDAD	
Definición de la meta :	0 - 80% 80 - 90 90 - 100%
Acumulado Meta:	98.5
Fórmula:	(DAPADM+DAPFIN+DAPTRI+DLIQUI+DSRCOL+DBAFUN)*100

Fuente. Propia a partir de (Secretaría Distrital de Hacienda, 2019)

En la tabla 12 se observa los resultados del indicador de Disponibilidad en los primeros 4 meses del 2019:

Tabla 13. Resultados del indicador de Disponibilidad

Año - Periodo	2019 - 01	2019 - 02	2019 - 03	2019 - 04	**Promedio**
Resultado Indicador	**99.7**	**99.69**	**99.7**	**99.69**	**99.69**
METAS	98.5	98.5	98.5	98.5	**98.5**
% Cumplimiento	100	100	100	100	**n**

Fuente. Propia a partir de (Secretaría Distrital de Hacienda, 2019)

Análisis: Como se puede observar en la tabla 12 la Entidad cumple satisfactoriamente este indicador, lo cual va de la mano con el buen desempeño que se identificó en el diagnóstico con respecto a la Disponibilidad de sus sistemas de información. Adicionalmente el indicador es adecuado y tiene en cuenta los sistemas de información identificados en la fase 2.

En la tabla 13, se presentan el indicador de apreciación de los usuarios respecto a la prestación del servicio identificado en la Secretaría Distrital de Hacienda con su análisis respectivo de desempeño

Tabla 14. Indicador de apreciación de los usuarios respecto a la prestación del servicio

INDICADOR APRECIACIÓN DE LOS USUARIOS RESPECTO A LA PRESTACIÓN DEL SERVICIO	
Nombre del Indicador:	MEDICION DE LA EXPERIENCIA DE SERVICIO DE SOPORTE TECNICO OFRECIDO
Año Indicador:	2019
Frecuencia del Análisis:	MENSUAL
Tipo de indicador:	EFECTIVIDAD
Objetivo del Indicador:	MEDIR LA APRECIACION DE LOS USUARIOS RESPECTO A LA PRESTACION DEL SERVICIO DE SOPORTE TECNICO
Proceso:	SERVICIOS Y SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
Definiciones	NSCMI4: NUMERO DE SERVICIOS CALIFICADOS MAYOR A 4

INDICADOR APRECIACIÓN DE LOS USUARIOS RESPECTO A LA PRESTACIÓN DEL SERVICIO	
	NTSECA: NÚMERO TOTAL DSE SERVICIOS CALIFICADOS
Área:	DIRECCIÓN DE INFORMATICA Y TECNOLOGIA
Unidades:	PORCENTAJE
Definición de la meta:	0 - 80% 80 - 90 90 - 100%
Acumulado Meta	95%
Periodicidad:	MENSUAL
Fórmula:	(NSCMI4/NTSECA) *100

Fuente. Propia a partir de (Secretaría Distrital de Hacienda, 2019)

En la tabla 14 se observa los resultados del indicador de Disponibilidad en los primeros 4 meses del 2019:

Tabla 15. Resultados del indicador apreciación de los usuarios

Año - Periodo	2019 - 01	2019 - 02	2019 - 03	2019 - 04	**Acumulado**
NSCMI4	327	320	327	265	309.75
NTSECA	335	333	335	265	317.00
Resultado Indicador	**97.61**	**96.1**	**97.61**	**100**	**n**
METAS	95	95	95	95	**95**
% Cumplimiento	100	100	100	100	**n**

Fuente. Propia a partir de (Secretaría Distrital de Hacienda, 2019)

Análisis: El indicador es adecuado para medir la apreciación de los usuarios con respecto a la prestación de los servicios. Como se puede observar en la tabla 14, la SDH cumple satisfactoriamente este indicador, aunque se debe trabajar más en la cultura de los usuarios, debido a que la mayoría no responde las encuestas para poder tener una data más objetiva.

4.3.1.2 Indicadores Propuestos

Debido a que no fueron detectados 2 de los 4 indicadores mínimos, en la tabla 15 y 16 se presentan los indicadores de mejora propuestos a la Secretaría Distrital de Hacienda. Es importante mencionar que el modelo debe adecuarse a las fichas técnicas que tenga la organización.

Tabla 16. Indicador de cumplimiento de los acuerdos de niveles de servicio establecidos

INDICADOR DE CUMPLIMIENTO DE LOS ACUERDOS DE NIVELES DE SERVICIO ESTABLECIDOS	
Estado:	Propuesto
Nombre del Indicador:	CUMPLIMIENTO DE LOS ACUERDOS DE NIVELES DE SERVICIO ESTABLECIDOS
Frecuencia del Análisis:	MENSUAL
Tipo de indicador:	EFECTIVIDAD
Objetivo del Indicador:	MEDIR EL CUMPLIMIENTO DE LOS ACUERDOS DE NIVELES DE SERVICIO ESTABLECIDOS
Proceso:	SERVICIOS Y SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
Área:	DIRECCIÓN DE INFORMATICA Y TECNOLOGIA
Unidades:	Porcentaje
Definición de la meta:	0 - 80% | 80 - 90 | 90 - 100%
Meta:	95%
Fórmula:	(NUMERO DE SERVICIOS SOLUCIONADOS EN EL TIEMPO ESTIMADO/NUMERO TOTAL DE SERVICIOS CERRADOS) *100

Fuente. Propia

Tabla 17. Recurrencia de incidentes por usuario y servicio

INDICADOR RECURRENCIA DE INCIDENTES POR USUARIO Y SERVICIO	
Estado:	Propuesto
Nombre del Indicador:	RECURRENCIA EN INCIDENTES REPORTADOS
Frecuencia del Análisis:	MENSUAL
Tipo de indicador:	EFECTIVIDAD
Objetivo del Indicador:	ANALIZAR LA RECURRENCIA DE INCIDENTES POR USUARIO Y SERVICIO
Proceso:	SERVICIOS Y SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
Área:	DIRECCIÓN DE INFORMATICA Y TECNOLOGIA
Unidades:	PORCENTAJE
Definición de la meta:	0 - 80% | 80 - 90 | 90 - 100%
Meta:	2
Fórmula:	(NUMERO DE INCIDENTES RECURRENTES SOLUCIONADOS/NUMERO TOTAL DE INCIDENTES) *100

Fuente. Propia

4.3.2 Identificación y valoración de riesgos

De acuerdo con el procedimiento establecido en el numeral 4.2.3 de la fase 2, se identificaron siete riesgos que afectan el modelo de disponibilidad, respaldo y recuperación de los sistemas de información, para la Secretaría Distrital de Hacienda, los cuales pueden consultarse en el Anexo 2 Registro de Riesgos.

En la tabla 17 se presenta el resumen de los siete riesgos identificados

Tabla 18. Valoración de los Riesgos identificadas

RIESGOS	1. Actos malintencionados en el manejo de la información por parte de terceros	2. Fallas de conectividad.	3. Fallas de hardware o software en servidores, equipos de seguridad y telecomunicaciones	4. Fallas en la prestación del servicio	5. No disponibilidad de los servicios de infraestructura tecnológica.	6. Pérdida de elementos de infraestructura tecnológica.	7. Pérdida de la seguridad de la información (Disponibilidad, integridad, confidencialidad).
Severidad del Riesgo Inherente	**EXTREMO**	**BAJO**	**MODERADO**	**MODERADO**	**MODERADO**	**ALTO**	**MODERADO**

Fuente. Propia

En la tabla 18 se presenta la relación de los riesgos identificados y las cincuenta y ocho causas u vulnerabilidades identificadas en la SDH:

Tabla 19. Riesgos y vulnerabilidades identificadas

Riesgos identificados	Causas - Vulnerabilidades
1. Actos malintencionados en el manejo de la información por parte de terceros	Incumplimiento de la reserva en el manejo de la información.
	Accesos no autorizados (Físico y/o Lógico)
2. Fallas de conectividad.	Caída del Core switch de comunicaciones.
	Manipulación inadecuada del enrutamiento, direccionamiento y reglas de configuración del Core y los firewalls.
	Desconexión física del cableado.

Riesgos identificados	Causas - Vulnerabilidades
3. Fallas de hardware o software en servidores, equipos de seguridad y telecomunicaciones	Fallas en el suministro eléctrico regulado.
	Defectos de fábrica.
	Falta de mantenimiento de la infraestructura tecnológica.
	Manipulación indebida de hardware y software.
	Falla de actualizaciones de hardware y software.
4. Fallas en la prestación del servicio	Recurso humano no calificado.
	Tipo de contratación insuficiente a la necesidad.
	Inadecuada supervisión de contrato.
	Fallas de hardware.
	Capacidad insuficiente de los equipos.
	Falta de renovación de licencias.
	No disponibilidad de la herramienta de Mesa de Ayuda
	No disponibilidad del correo electrónico
	No disponibilidad de las bases de datos
	Falta de mantenimiento de la infraestructura tecnológica.
5. No disponibilidad de los servicios de infraestructura tecnológica.	Obsolescencia de Hardware o Software.
	Fallas en el suministro eléctrico regulado.
	Falta de monitoreo 7x24
	Fallas en el sistema de control de acceso.
	Falta de capacitación del personal.
	Fallas en los enlaces de comunicaciones.
	Inadecuada definición de los Planes de Mantenimiento
	Inadecuada supervisión de contrato.
	Fallas en el Proceso de Copias de Respaldo.
	Falta de Planeación para la renovación de contratos de mantenimiento

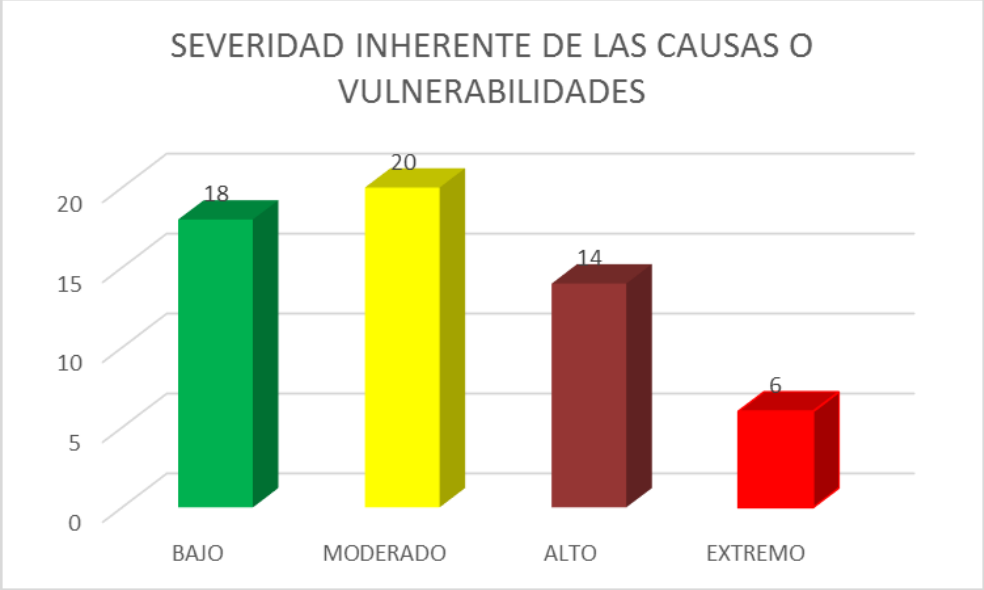
Riesgos identificados	Causas - Vulnerabilidades
	Daño o falta del software de monitoreo.
	Inadecuada gestión en la solución de incidentes.
6. Pérdida de elementos de infraestructura tecnológica.	Manipulación indebida de hardware y software.
	Accesos no autorizados (Físico y/o Lógico)
7. Pérdida de la seguridad de la información (Disponibilidad, integridad, confidencialidad).	Obsolescencia de Hardware o Software.
	Fallas en el Proceso de Copias de Respaldo.
	Inadecuada prestación del servicio.
	Fallas en la gestión de acceso lógico a los recursos de software.
	Asignación inapropiada de roles.
	Ataques informáticos internos o externos.
	Aumento significativo de temperatura en el centro de datos
	Error humano.
	Falla en el servicio de correo electrónico.
	Fallas de hardware.
	Fallas en el Proceso de Copias de Respaldo.
	Carencia de copias de seguridad de la configuración de los equipos y de los datos contenidos en los mismos.
	Fallas en el suministro eléctrico regulado.
	Falta de capacitación del personal.
	Falta de ética profesional.
	Fallas de hardware.
	Falta de mantenimiento de la infraestructura tecnológica.
	Falta de protocolos de cifrado en ambiente de pruebas
	Incidentes técnicos presentados durante el apagado y/o encendido.

Riesgos identificados	Causas - Vulnerabilidades
	Incumplimiento de las políticas del uso de las contraseñas.
	Inexistencia de políticas para la generación de backup
	Tiempos de retención establecidos en TRD muy altos.

Fuente. Propia

En total se detectaron 58 causas asociadas a los 7 riesgos. En la figura 12 se presenta su segregación de acuerdo con el nivel severidad inherente

Figura 13. Severidad Inherente de las Causas Identificadas



Fuente. Propia

Dentro de las causas identificadas, obtuvieron una mayor calificación las fallas en el suministro eléctrico regulado, la falta de ética profesional, la falta de protocolos de cifrado en ambiente de pruebas y el incumplimiento de las políticas de seguridad de la información en el uso de las contraseñas.

5 CONCLUSIONES Y RECOMENDACIONES

5.1.1 Recomendaciones

La Secretaría Distrital de Hacienda tiene procedimientos muy burocráticos, con demasiada tramitología para requerimientos de bajo nivel de complejidad. Se recomienda diseñar Acuerdos de Niveles de Servicio (ANS) más cortos para atender los requerimientos sencillos y desarrollar un esquema de servicio de requerimientos de baja complejidad en donde la prioridad sea la rapidez en la atención. Estas solicitudes no deberían entrar a la misma cola de los requerimientos más complejos, lo cual va a mejorar la percepción que tienen los usuarios con respecto a la atención de requerimientos.

Es clave que la dirección del área trabaje en la arquitectura global de los sistemas de copias de respaldo de la SDH, buscando la articulación y el aprovechamiento de los diferentes desarrollos y aplicativos de la entidad. Debe existir alguien con la visión total del negocio que lidere este esfuerzo.

Se recomienda revisar los indicadores actuales de la organización, ya que no se está evaluando correctamente el cumplimiento de los acuerdos de niveles de servicio establecidos, ni la recurrencia de incidentes por usuario y servicio. De esta forma, detectar cuellos de botella y acercarse más con la operación real de la entidad, con miras a profundizar en el conocimiento de sus necesidades y expectativas y direccionar las acciones de mejora hacia aspectos concretos.

La infraestructura que actualmente tiene la SDH no tiene toda la cobertura, ni capacidad suficiente para gestionar adecuadamente las copias de respaldo. Se recomienda implementar la arquitectura propuesta con miras de mejorar y optimizar los tiempos en la toma y restauración de backups.

Con respecto al sistema de información financiero LIMAY, se identificaron debilidades en cuanto a su parametrización, ya que solo lo está haciendo el área de sistemas, y es necesario tener conocimientos contables y el apoyo de otras áreas. Se recomienda adicionalmente contar con el apoyo de otras entidades distritales que ya están utilizando este sistema de información

En el proceso de construcción de los diferentes sistemas de información que fueron identificados, no se priorizó el proceso de documentación, como resultado muchos de los sistemas se encuentran parcialmente documentados, dejando a voluntad de quien tuviese el conocimiento, su transferencia. Esta situación genera riesgos significativos para la entidad, algunos ya materializados, como reproceso para mantenimientos e incumplimientos frecuentes en la entrega de soluciones. Se recomienda establecer en los desarrollos próximos, acuerdos de documentación y verificación de la correcta entrega de la gestión del conocimiento incluyendo comentarios en el código fuente, vídeos explicativos, diagramas arquitectónicos, presentaciones, etc.

La Secretaria Distrital de Hacienda cuenta con una seguridad perimetral, la cual protege todos los perímetros vulnerables como son el Internet, la red extranet (conexión dedicada de las entidades del Distrito), conexión de las sedes de la Entidad, Cades, Supercades y la red interna de la SDH. Pero no se detecta estos niveles de seguridad de la información directamente en las áreas, se recomienda definir un conjunto de políticas que aplique a todas las áreas, sean aprobadas por la dirección, publicadas y comunicadas a todos los empleados y partes externas pertinentes.

Se recomienda establecer adecuadamente una gestión de capacidad, especialmente para atender los picos que se presentan en el consumo de los servidores de base de datos, para los meses de abril a julio, fechas de vencimientos de impuestos.

Dentro de las medidas a introducir en el corto plazo se recomiendan aquellas relacionadas con la gestión del riesgo, el nivel de satisfacción sobre los sistemas implementados, clasificar y medir el tipo de incidentes reportados, el tiempo de resolución de problemas y el cumplimiento de los niveles de servicio.

Se recomienda tener reuniones periódicas para realizar seguimiento y definir acciones a los incidentes de infraestructura presentados mensualmente por la mesa de servicios.

La Secretaría Distrital de Hacienda tiene un centro de procesamiento de datos que cumple con los estándares de seguridad física y lógica establecidos en las mejores prácticas. La entidad tiene procesos de desarrollo bien definidos, un departamento de análisis de riesgo, un sistema de gestión de recursos humanos que garantiza contar con el personal del área de TI adecuado. Pero no están preparados para una adecuada recuperación ante un desastre que interrumpa completamente la

operación, se recomienda generar un plan de continuidad y evaluarlo a intervalos planificados para determinar su idoneidad y que los conozca todo el personal interesado.

Para hacer frente a las limitaciones identificadas en esta evaluación, se recomienda que la organización establezca un plan estratégico de al menos cinco años en el que se especifique como la dirección va a tomar en cuanto el mejoramiento de los sistemas de información e infraestructura, siendo coherente con las necesidades actuales de operación. Por ejemplo, entre las decisiones a tomar por la institución se incluye aquella relacionada con el software: adquirir uno nuevo para reemplazar el actual, corregir los potenciales problemas en los sistemas actuales de recuperación de datos. No obstante, debe considerar acciones inmediatas para solucionar los problemas de gobierno tecnológico a corto plazo.

Con base en el avance realizado en la aplicación del modelo propuesto de gestión de la disponibilidad, recuperación de los sistemas de información y de la gestión del riesgo en la Secretaría Distrital de Hacienda, se propone el siguiente plan de acción, con las siguientes actividades a realizar para su correcta implementación en los siguientes 6 meses. Es importante aclarar que el siguiente plan de acción aplica al modelo propuesto y no al plan estratégico de tecnologías de la información, el cual abarca muchos más procesos, sistemas de información y es a más largo tiempo.

Tabla 20. Plan de acción, actividades y cronograma

Implementación completa del modelo de DRRGR en la SDH			**Responsable**	**Semana de realización**	**Tiempo del proyecto en meses (6 meses)**																															
Fase	**Acciones a ejecutar**				**Mes 1**				**Mes 2**				**Mes 3**				**Mes 4**				**Mes 5**				**Mes 6**											
Fase 1 Diagnóstico Preliminar del DRRGR	1	Realizar la divulgación del estado actual de la de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y de la gestión del riesgo.	Administrador Virtualización Almacenamiento	2																																

Implementación completa del modelo de DRRGR en la SDH			Responsable	Semana de realización	Tiempo del proyecto en meses (6 meses)																													
Fase	**Acciones a ejecutar**				**Mes 1**				**Mes 2**				**Mes 3**				**Mes 4**				**Mes 5**				**Mes 6**										
	2	Socializar los resultados del cuestionario del anexo 1, respecto al estado de cumplimiento de lo requerido por las normas ISO27001, ISO20000 E ISO31000	Administrador Virtualización Almacenamiento	0.5																														
Fase 1. Diagnóstico Preliminar del DRRGR	3	Socializar los resultados cuantificados de la valoración del impacto económico de un incidente.	Administrador Virtualización Almacenamiento	0.5																														
Fase 2. Planificación del DRRGR	4	Validación y actualización de los sistemas de información	Administrador Virtualización Almacenamiento	0.5																														
	5	Aprobar el alcance y los objetivos del DRRGR por parte de la dirección	Jefe de área	0.5																														
	6	Aprobación de la solución de respaldo de información y disponibilidad	Jefe de área	1																														

Implementación completa del modelo de DRRGR en la SDH			Responsable	Semana de realización	Tiempo del proyecto en meses (6 meses)																							
Fase	Acciones a ejecutar				Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	7	Divulgación de la metodología de Gestión de identificación, valoración y tratamientos de los riesgos por parte de todos los responsables de los activos y de los actores involucrados	Administrador Virtualización Almacenamiento	1																								
Fase 3 Preparación del DRRGR	8	Aprobación de los indicadores propuestos en este documento por parte de la dirección	Jefe de área	0.5																								
	9	Piloto y pruebas de la ejecución de los nuevos indicadores	Jefe de área	1																								
	10	Identificar los activos de información para una correcta gestión de riesgos	Administrador Virtualización Almacenamiento	2																								
	11	Identificar, valorar los riesgos por parte de los dueños de los procesos bajo la metodología divulgada en la semana 6	Administrador Virtualización Almacenamiento	4																								

Implementación completa del modelo de DRRGR en la SDH			Responsable	Semana de realización	Tiempo del proyecto en meses (6 meses)																							
Fase	Acciones a ejecutar				Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	12	Formular los planes de acción pertinentes para tratar los riesgos de SI	Administrador Virtualización Almacenamiento	2																								
	13	Ejecutar los planes de acción pertinentes para tratar los riesgos de SI	Administrador Virtualización Almacenamiento	4																								
	14	Definición de políticas de SI en todos los procesos con respecto al DRRGR	Jefe de área	1																								
Revisión y seguimiento	17	Realizar una identificación de vulnerabilidades desde un ente externo	Proveedor Externo	1																								
	18	Realizar el análisis causa raíz de los hallazgos detectados	Administrador Virtualizac	1																								
	19	Cerrar los hallazgos respectivos	Administrador Virtualizac	1																								
	20	Realizar la retroalimentación a las partes interesadas.	Administrador Virtualización	1																								

Fuente. Elaboración propia

En el anexo 3 se presenta el presupuesto para el año 2020 destinado a la implementación del DRRGR, para la SDH

5.1.2 Conclusiones

En el diagnóstico realizado se identificó como la entidad se aferra a la premisa de adaptar el software o los sistemas de información a los procesos institucionales, alejándose de lo que ocurre en el mercado, en donde la tendencia es acogerse a las mejores prácticas, en la cual los procesos se adaptan al estándar del mercado, respetando los principios de confidencialidad, integridad y disponibilidad de la información, interoperabilidad y economías de escala.

Conocer los riesgos es fundamental para estar preparados con el fin cumplir con las expectativas que la Entidad, el Sector y el Distrito tienen. Los riesgos más relevantes que se encuentran con el análisis de la situación actual de los sistemas de información de la SDH son:

- Actos malintencionados en el manejo de la información por parte de terceros.
- Fallas de conectividad.
- Fallas de hardware o software en servidores, equipos de seguridad y telecomunicaciones
- Fallas en la prestación del servicio
- No disponibilidad de los servicios de infraestructura tecnológica.
- Pérdida de elementos de infraestructura tecnológica.
- Pérdida de la seguridad de la información (Disponibilidad, integridad, confidencialidad).

Entender y reconocer que la Secretaria Distrital de Hacienda cada vez más depende de la Tecnología para alcanzar sus objetivos estratégicos, mediante la implementación de metodologías agiles y buenas prácticas, lo cual va a permitir a la entidad mejorar la disponibilidad de la información y optimizar la calidad de los servicios de cara al ciudadano y funcionario interno.

Los datos obtenidos en la aplicación del modelo propuesto en la Secretaria Distrital de Hacienda han permitido determinar que la entidad está incumpliendo completamente 12 de los 27 requisitos evaluados de las normas ISO27001 e ISO20000, debido a que no se evidencia ningún cumplimiento de 8 numerales de Recuperación y 4 de gestión de capacidad. Adicionalmente existen 11 requisitos que se cumplen parcial y únicamente cumplen totalmente 4 requisitos enfocados a Disponibilidad, A continuación, se detalla las fortalezas y debilidades detectadas:

Disponibilidad: Como gran fortaleza se identifica que la SDH si cuenta con alta disponibilidad con respecto a toda la infraestructura del Data Center, incluyendo aspectos directos en la operación como son servidores y su conectividad, y de apoyo al correcto funcionamiento como las plantas eléctricas, UPS, Aire acondicionado, entre otros. Pero no se evidencia ANS para la disponibilidad, ya que no existen objetivos claros, ni acuerdos definidos con los clientes internos y con las otras áreas de la entidad, simplemente se tiene un indicador.

Gestión del Riesgo: Como fortaleza se identifica que la SDH cuenta con una adecuada gestión para la identificación, evaluación y tratamiento de los riesgos de los diferentes procesos de la entidad. No obstante, la debilidad detectada es con respecto a que no se realiza la evaluación del riesgo residual, ni de forma periódica se realiza la identificación y evaluación nuevos riesgos.

Gestión de Capacidad: Como fortaleza se identifica que la SDH cuenta con un contrato de monitoreo en el Datacenter las 24 horas durante los 365 días del año. Pero no se evidencia que la entidad identifique los requisitos de capacidad futura de acuerdo con la demanda que se prevé. La organización crece de acuerdo con los problemas en las necesidades que van presentándose

Recuperación: No se encontró ninguna fortaleza significativa en este aspecto, lo único que tiene considerado el área para su recuperación por una afectación total es un contrato para el envío de cintas de copias de respaldo a un sitio alterno, pero no se realizan pruebas periódicas de recuperación del correcto funcionamiento de estos medios. Adicionalmente no está considerado un Plan de Recuperación de Desastres ni un Plan de Continuidad

Con respecto al modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y la gestión del riesgo aplica de una forma adecuada a todos los procesos TI que se quisieran evaluar y mejorar. Dicho modelo puede aplicarse a cualquier empresa sin importar su sector o tamaño, y es totalmente ajustable a una nueva actualización de las normas ISO27001, ISO20000 e ISO31000. Por tanto, el modelo responde de una manera eficaz a los cambios que se puedan presentar.

El modelo de gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y la gestión del riesgo es un elemento clave dentro del plan estratégico de las organizaciones públicas. Debido a que más allá, de cumplir requisitos contractuales y proteger sus

sistemas de información, le permite brindar la seguridad adecuada al distrito y a la nación de una operación adecuada de sus servicios e incrementa la percepción positiva del público en general.

Se logró el cumplimiento de todos los objetivos planteados inicialmente, diseñando un modelo compuesto por tres fases fundamentales. En la fase 1 se especifica la realización de un diagnóstico y la valoración del impacto económico de un posible incidente; en la fase 2 se realiza la planificación del DRRGR, el cual se compone de la identificación de los sistemas de información, la definición de una solución para la toma de backups y la definición de un procedimiento para la gestión del riesgo; y en la fase 3, mencionada como preparación del DRRGR, se inicia con la identificación y formulación de indicadores, y se termina con la identificación y valoración de los riesgos.

La metodología planteada en la fase 1 del modelo fue todo un éxito, ya que los datos obtenidos determinaron el estado actual del área en cuanto a sus sistemas de disponibilidad, recuperación, respaldo y gestión del riesgo. No obstante, se ha identificado que la fase 3 está sujeta a mejoras en cuanto a la inclusión y definición de una propuesta para realizar el plan de continuidad y la gestión de capacidad.

Los resultados de nuestra investigación apoyarán estudios futuros realizados en la Secretaría Distrital de Hacienda, respecto al Sistema de Gestión de Seguridad de la Información y al Sistema de Gestión de Servicios de Tecnología de la Información internos. Adicionalmente, se puede derivar de esta investigación, estudios de gobiernos de TI en empresas públicas, y diseño y generación de mejores prácticas en empresas colombianas.

Es importante decir que como funcionarios del sector público en este caso de la Secretaria Distrital de Hacienda del área TI, observamos las dificultades que a diario se presentan en relación con la gestión de la disponibilidad, respaldo, recuperación de los sistemas de información y la gestión del riesgo; de allí, la necesidad de presentar nuestro modelo, que seguramente será el punto de partida para el uso y puesta en marcha de las buenas prácticas al interior de la entidad en beneficio de los usuarios internos, externos y partes interesadas.

REFERENCIAS

Alcaldía Santiago de Cali. (13 de 09 de 2019). Obtenido de http://www.cali.gov.co/tic/publicaciones/32728/plan_estratgico_de_tic/:

Andrada, A. M. (2004). *Nuevas tecnologias de la Información y la comunicación.* Buenos Aires: Maipue.

Areito, B. J. (2008). *Seguridad de la Información, Redes, Informática y Sistemas de Información.* Colombia: Paraninfo.

Baca, G. (2015). *Proyectos de Sistemas de Información.* México.

Baeza-Yatesa & Ribeiro-Neto. (2009). *Modern information retrieval.*

Benavides, M. L. (2012). *Módulo Riesgos y Control Informático.* Pasto: UNAD.

Daudinot. (2007). *Organización y recuperación de información en internet*.

Gómez, A. (2007). *Enciclopedia de la seguridad Informática.* México: Alafaomega.

Gómez, V. (2011). *Seguridad Informática Básica.* Colombia: ECOE.

Hernandez, R., Fernandez, C., & Baptista, P. (2015). *Metodologia de la Investigación.* Mexico: McGraw-Hill Interamericana, S.A.

ICONTEC. (2011). *Norma Técnica Colombiana NTC-ISO 31000.* Instituto Colombiano de Normas Tecnicas y Certificación.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001 Técnicas de Seguridad y Requisitos para un Sistema de Gestión de Seguridad de la Información. Colombia.* Colombia.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27002 Técnicas de Seguridad, Código de Práctica para Controles de Seguridad de la Información.* Colombia.

ICONTEC. (2018). *NTC-ISO/IEC 20000-1 Tecnología de la Información. Gestión del Servicio Parte 1: Requisitos del Sistema de Gestión del Servicio.* Colombia.

Instituto Ponemon. (2016). *Modelo de Costos de Ponemon.* Global Analysis.

Laudon Kenneth C & Laundon Jane P. (13 de 09 de 2018). *Sistemas de Información.* Pearson.

Leonel. (2002). *Los desafios de las tecnologías de la información.*

LEY No 1423. (1993).

Lopez, X. (2012). *Arquitectura de la información.* Madrid.

Martínez, J. G. (2010). *El plan de continuidad del negocio. Guía práctica para su elaboración.* Madrid: Diaz de Santos.

MINTIC. (2016). *Modelo de Seguridad y Privacidad de la Información.*

Peralta, M. (2009). *Sistemas de información.* El cid.

Roa. (2013). *Seguridad Informática.* Graw Hill.

Salgueiro, A. (2001). *Indicadores de Gestión y Cuadros de Mando.* Madrid: Diaz de Santos.

Secretaría Distrital de Hacienda. (2019). *http://www.shd.gov.co*.

Surhone. (2018). *Lo nuevo del Ransomware.* USA: Betascript.

Van Dalen y William J Meyer . (1986). *Manual de Técnica de la Investigación Educacional.* España.

LISTA DE ANEXOS