

Diseño de un modelo de gestión tecnológica para fortalecer la operación de los servicios críticos de tecnologías de información ante posibles desastres naturales en el Instituto Nacional de Metrología de Colombia

Richard Alexander Rodríguez Martínez

Jhon Alexander Díaz Moreno

Universidad Nacional Abierta y a distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnologías de la Información

Bogotá, Colombia

2020

Diseño de un modelo de gestión tecnológica para fortalecer la operación de los servicios críticos de tecnologías de información ante posibles desastres naturales en el Instituto Nacional de Metrología de Colombia

Richard Alexander Rodríguez Martínez

Jhon Alexander Díaz Moreno

Director (a):

Carmen Emilia Rubio Vanegas

Universidad Nacional Abierta y a distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnologías de la Información

Bogotá, Colombia

2020

Agradecimientos

A la Universidad Nacional Abierta y a distancia UNAD y al Ministerio de tecnologías de información y Comunicaciones MinTIC, por darnos la oportunidad de realizar nuestros estudios de maestría.

Resumen

En la actualidad las entidades públicas y privadas carecen de elementos necesarios para soportar fenómenos naturales, fallas intencionales y/o involuntarias a las que está expuesta toda organización y que además pongan en riesgo los activos tecnológicos y de información críticos para una entidad, por esta razón se pretende resaltar su importancia y además establecer el diseño práctico que debe tener una solución que incluya un plan de recuperación de desastres, que determine la continuidad de operaciones y servicios críticos de la entidad pública Colombiana Instituto Nacional de Metrología (INM). La adaptación contempla como componente fundamental la posibilidad de ofrecer continuidad de servicios tecnológicos y su operación ante diferentes factores internos o externos dentro de los que se encuentran los fenómenos naturales que se puedan presentar. Inicia con la identificación de modelos tecnológicos enfocados en la mejora de servicios críticos, posteriormente se basa en un levantamiento de información que permita conocer el estado actual de la infraestructura tecnológica y los servicios que soporta la entidad, luego se registran e identifican los servicios críticos de manera clara y precisa para su posterior intervención. Con los elementos descritos anteriormente se aplica y adapta el modelo de gestión tecnológica basado principalmente en el análisis de activos críticos de TI mediante una investigación que hace uso de datos para mejorar las condiciones de disponibilidad y continuidad de operación institucional, donde se articulan diversas tecnologías y nuevos procesos que permiten generar un entorno más seguro, organizado y fácilmente gestionable.

Palabras clave: Modelo de gestión tecnológica, Gobierno de TI, Plan de recuperación de desastres, disponibilidad, Infraestructura Tecnológica.

Abstract

Currently, public and private entities lack the necessary elements to withstand natural phenomena, intentional and / or involuntary failures to which every organization is exposed and that also put at risk the technological and information assets critical for an entity, for this reason It is intended to highlight its importance and also to establish the practical design that a solution must have, including a disaster recovery plan, which determines the continuity of operations and critical services of the Colombian public entity National Metrology Institute (NMI). The adaptation considers as a fundamental component the possibility of offering continuity of technological services and their operation in the face of different internal or external factors that may represent a negative impact on their availability, among which are possible natural phenomena. As part of the methodology, the identification of technological models focused on the improvement of critical services is carried out, subsequently it is generated in a survey of information that allows knowing the current state of the technological infrastructure and the services that the entity supports, then they are registered and identify the critical services clearly and precisely for subsequent intervention. With the elements described above, the technology management model based mainly on the analysis of critical IT assets is applied and adapted through an investigation that makes use of data to improve the conditions of availability and continuity of institutional operation, where various technologies and technologies are articulated. new processes that allow generating a more secure, organized and easily manageable environment.

Keywords: Technological management model, IT Government, Disaster recovery plan, availability, Technological Infrastructure.

Tabla de contenido

	<u>Pág.</u>
Introducción	11
1. Planteamiento del problema.....	15
1.1 Descripción de la realidad problemática	15
1.2 Identificación y formulación del problema	16
1.2.1 Problema General	18
1.2.2 Problemas Específicos	18
1.3 Objetivos de la investigación	19
1.3.1 Objetivo General.....	19
1.3.2 Objetivos Específicos	19
1.4 Justificación de la investigación.....	20
1.5 Limitaciones de la Investigación:.....	21
1.5.1. Delimitación Teórica	21
1.5.2 Delimitación Geográfica.....	24
2. Marco teórico	25
2.1 Antecedentes de la investigación	25
2.1.1 A nivel mundial	25
2.1.2 A nivel nacional.....	26
2.2 Bases teóricas	27
2.2.1 ¿Gestión tecnológica o gestión de conocimiento?.....	27
2.2.2 Modelo Nacional de gestión de tecnología.....	31
2.2.2 Modelo Gestión tecnológica COTEC.....	32
2.2.3 Modelo Nonaka y Takeuchi	33
2.2.4 Modelo de Andersen.....	35
2.2.5 Modelo de Ray Gehani	38
2.2.6 Modelo de gestión tecnológica de Hidalgo Nuchera.....	38
2.2.7 Modelo de gestión y gobierno de TI.....	39
2.2.8 Relación norma ISO/IEC 27001 con un modelo de gestión tecnológica	40
2.2.9 Antecedentes desastres naturales.....	42
2.3 Bases Legales	47

2.3.1 Normas nacionales.....	47
2.3.2 Normas Internacionales	48
2.4. Definiciones de Términos	49
3. Metodología.....	53
3.1 Tipo y nivel de la Investigación	55
3.2. Diseño de la Investigación	55
3.3 Fases de la Investigación.....	56
3.3.3 Fase I: Diagnóstico.	56
3.3.1.1 Técnicas de recolección de datos.	56
3.3.1.2 Instrumentos de recolección de datos.	57
3.3.4 Fase II. Procesamiento de la información	57
3.3.2.1 Creación matriz de servicios críticos.	57
3.3.2.2 Identificación de elementos de recuperación de desastres.....	57
3.3.5 Fase III: Desarrollo del Modelo de gestión Tecnológica	58
3.3.3.1 Análisis de información.	59
3.3.3.2 Inspección.	59
3.3.3.3 Estructuración.	59
3.3.3.4 Resultados.....	59
4. Adaptación del modelo de gestión tecnológica	60
4.1 Comparación modelos de gestión tecnológica.....	60
4.1.1 Selección del modelo de Gestión para el Instituto Nacional de Metrología (INM) ...	60
4.2 Levantamiento de información de los servicios soportados en tecnologías de	
información y su infraestructura tecnológica relacionada.....	62
4.3 Matriz de servicios críticos de información recopilada en el Instituto Nacional de	
Metrología (INM).....	70
4.4 Aplicación del modelo de gestión tecnológica del Instituto Nacional de Metrología	
(INM) 82	
4.4.1 Política de gobierno digital.....	82
4.4.2 Elementos de la política Gobierno Digital	83
4.4.3 Modelo de Gestión y Gobierno de TI.....	84
4.4.4 Evaluación indicadores de cumplimiento del modelo de gestión y gobierno de TI... 86	

4.4.5	Estrategia para cubrir la brecha del modelo de gestión y gobierno de TI	93
4.4.5.1	Recomendaciones dominio Estrategia de TI.....	94
4.4.5.2	Recomendaciones dominio Gobierno de TI.....	94
4.4.5.3	Recomendaciones dominio Información.....	95
4.4.5.4	Recomendaciones dominio Sistemas de Información.....	97
4.4.5.5	Recomendaciones dominio Servicios Tecnológicos	98
4.4.5.6	Recomendaciones dominio Uso y Apropiación de TI	98
4.4.6	Elementos de recuperación de desastre para los servicios críticos de la entidad soportados en tecnologías de información.....	100
	Conclusiones	102
	Referencias bibliográficas.....	106
	Anexos.....	115

Lista de figuras

	Pág.
<i>Figura 1.</i> Fases o etapas de la gestión tecnológica.....	23
<i>Figura 2.</i> Ubicación geográfica Instituto Nacional de Metrología (INM).	24
<i>Figura 3.</i> Modelo nacional de gestión de tecnología.....	31
<i>Figura 4.</i> Gestión tecnológica y modelos de innovación empresarial.....	33
<i>Figura 5.</i> Formas de conversión del conocimiento en la organización.	34
<i>Figura 6.</i> Modelo de gestión del conocimiento.	35
<i>Figura 7.</i> Taxonomía contrastada modelos de la gestión del conocimiento.....	37
<i>Figura 8.</i> Modelo de gestión tecnológica de Nuchera adaptado por Jaimes <i>et al.</i> (2011).....	39
<i>Figura 9.</i> Estructura del Modelo de Gestión y Gobierno de TI.....	40
<i>Figura 10.</i> Cartografía desastres reportados.	42
<i>Figura 11.</i> Enfoques de la investigación	54
<i>Figura 12.</i> Componentes del Plan de Recuperación ante Desastres.....	58
<i>Figura 13.</i> Servicios Ofrecidos por el Instituto Nacional de Metrología (INM).....	62
<i>Figura 14.</i> Diagrama general de activos tecnológicos.....	69
<i>Figura 15.</i> Niveles de clasificación	76
<i>Figura 16.</i> Elementos de la política de gobierno digital.....	84
<i>Figura 17.</i> Estructura de la política de gobierno digital.	85
<i>Figura 18.</i> Escala de cumplimiento del modelo de gestión tecnológica	89

Lista de Tablas

	Pág.
<i>Tabla 1.</i> Definiciones Gestión Tecnológica.....	28
<i>Tabla 2.</i> Reportes de emergencias por departamentos.....	45
<i>Tabla 3.</i> Redes y seguridad.....	65
<i>Tabla 4.</i> Plataformas aplicaciones y software.....	65
<i>Tabla 5.</i> Servidores (Linux y Windows).....	66
<i>Tabla 6.</i> Tipos de activos de información.....	71
<i>Tabla 7.</i> Riesgos identificados.....	72
<i>Tabla 8.</i> Activos de información	74
<i>Tabla 9.</i> Clasificación de criticidad	76
<i>Tabla 10.</i> Criterios de valoración de activos	77
<i>Tabla 11.</i> Valoración de activos de información	77
<i>Tabla 12.</i> Matriz de servicios críticos y su relación con activos de información.....	80
<i>Tabla 13.</i> Cumplimiento dominios modelo de gestión y gobierno de TI.....	90
<i>Tabla 14.</i> Descripción de escenarios	100

Introducción

Actualmente las organizaciones ya sean públicas o privadas, son conscientes que deben ser competitivas a raíz de la globalización de los mercados, por lo cual entienden la importancia que conlleva a la inversión en tecnologías de la información, con el fin de optimizar su operación y ser competitivos, donde es claro que la tecnología, su infraestructura y servicios representan uno de los activos que exige altos índices de inversión de manera continua, lo cual genera interpretaciones desde un punto de vista estratégico, en la búsqueda de aquellas inversiones que sean siempre productivas en el tiempo (Ortiz, 2014)

En Colombia el ministerio de tecnologías de información y las comunicaciones MinTIC, lidera proyectos enfocados a la prestación de servicios tecnológicos con el fin de incentivar el aprovechamiento de las Tecnologías de Información y las comunicaciones (TIC), en la búsqueda de generación de valor hacia el estado y sus ciudadanos, lo cual hace parte de la estrategia de gobierno digital creada por MinTIC, amparada en el decreto 1008 de 2018, cabe aclarar que las entidades públicas en materia de tecnologías de información y las comunicaciones están obligadas a dar cumplimiento a la política de gobierno digital, sin embargo cada entidad de acuerdo a sus capacidades es responsable de adaptar el mapa de ruta y usar el modelo más adecuado que permita el acercamiento a las metas propuestas por el gobierno nacional, basados en la generación de valor, garantizando beneficios a la ciudadanía en la prestación de servicios con la articulación de los lineamientos de MinTIC.

A nivel de entidades públicas, los proyectos de tecnología tienen como soporte principal el Plan Estratégico de Tecnologías de Información (PETI), donde es fundamental definir instrumentos, planes, proyectos y modelos que satisfagan las necesidades de la organización brindando continuidad de operación, basados en el aprovechamiento tecnológico para el cubrimiento de los objetivos misionales de cada entidad.

Con base en el contexto anterior se desarrolló un proyecto que permite la mejora en la operación, continuidad y disponibilidad de servicios críticos soportados en tecnologías de información y las comunicaciones para la entidad pública Instituto Nacional de Metrología (INM), garantizando mediante la adaptación de un modelo de gestión tecnológica, la prestación de servicios ante posibles desastres naturales, o fallas de servicios generadas por errores humanos o alteraciones en la infraestructura tecnológica con la que cuenta actualmente la entidad en su única sede.

A partir de estos conceptos se describió la situación problemática que hace énfasis en las necesidades, no solo tecnológicas con las que cuenta la entidad si no también estratégicas, en donde es evidente la ausencia de mecanismos de gestión tecnológica y gobierno de TI apropiados, que permitan a la entidad prestar sus servicios a la ciudadanía de manera ininterrumpida incluso frente a situaciones de desastres naturales.

En este sentido la adaptación del modelo de gestión tecnológica garantiza que al interior del Instituto Nacional de Metrología (INM), estén plenamente identificadas las fortalezas y también las debilidades a nivel de gobierno de TI, abarcando sus estrategias e infraestructura tecnológica que soporta sus servicios. Con base en lo anterior y teniendo pleno conocimiento de los puntos débiles de la entidad, es posible direccionar esfuerzos mediante una serie de

recomendaciones en concordancia con las directrices de MinTIC, que permitan mejorar los niveles de cumplimiento con la apropiación de una metodología acorde a las características de la organización que permita tener claro el procedimiento a seguir en caso de presentarse un desastre natural o interrupción crítica que afecte la prestación de servicios.

A partir de este contexto surgió la necesidad de adaptar un modelo de gestión tecnológica, para lo cual se comparó diferentes modelos ya existentes, buscando el más apropiado con base en las necesidades y estado actual de la entidad pública intervenida, también se realizó un levantamiento de información al interior de la organización, para determinar los servicios críticos soportados en tecnologías de información y las comunicaciones, con el fin de establecer de manera clara y precisa sus principales características, basados en el portafolio de servicios de la entidad donde se identifica su funcionalidad y objetivos. Posteriormente se efectuó la evaluación del modelo, que a su vez da como aporte a la entidad un diagnóstico con recomendaciones y la inclusión de un plan de recuperación de desastres que busca optimizar la prestación de servicios ofrecidos por la entidad.

Como resultado de esta adaptación a través del modelo de gestión tecnológica y como beneficiado directo que es la entidad pública intervenida, Instituto Nacional de Metrología (INM) ubicada en la ciudad de Bogotá, se incorpora a la misma, una mejora en su capacidad de mantener la prestación de sus servicios incluso en situaciones extremas donde puedan presentarse afectaciones a su infraestructura física o acceso a la misma, cabe recordar que esta entidad cuenta con una única sede a nivel nacional.

Con respecto a sus beneficiados externos, se encuentra la ciudadanía en general que podrá hacer uso de los servicios ofrecidos por el Instituto Nacional de Metrología (INM) y contarán de

manera ininterrumpida con la posibilidad de interactuar en los sitios web, sistemas de radicación, pagos en línea, servicios de calibración, consultas de información y demás trámites disponibles dentro del panorama misional de la organización. .

Por consiguiente, toda organización que decide aplicar modelos de gestión tecnológica con mecanismos de respaldo de información y continuidad de operaciones mediante planes de recuperación de desastres (DRP), obtendrá múltiples beneficios basados en la articulación de procesos internos, toma de decisiones efectivas y la satisfacción de sus clientes.

Finalmente se identifica una alineación con los objetivos y componentes de la maestría en gestión de tecnologías de información de la UNAD, desde el punto de vista de la gestión de proyectos, ya que se caracterizaron activos tecnológicos al interior de la entidad para generar valor a los mismos, se contribuyó a la mejora en la prestación de servicios a la ciudadanía, dando como resultado el fortalecimiento del gobierno, la infraestructura, y la seguridad de TI al interior de la entidad, con soluciones transversales que alinean los objetivos institucionales con las tecnologías de información y las comunicaciones contribuyendo a mejorar la eficiencia administrativa.

1. Planteamiento del problema

1.1 Descripción de la realidad problemática

Actualmente la gestión de tecnologías se considera una de las herramientas de apoyo organizacional más importante para hacer uso eficiente y eficaz de sus recursos, esta tendencia crece de manera acelerada, por lo cual no tener en cuenta los avances tecnológicos, condena a una organización a la obsolescencia lo cual redundará en afectación de la productividad (Ortíz & Nagles, 2014).

Hoy en día, la información en el Instituto Nacional de Metrología (INM) cuenta con un manejo centralizado, en donde existe como único punto de almacenamiento de información el Datacenter de la entidad ubicado en su única sede, bajo el mecanismo de cintas de seguridad en conjunto con un sistema de resguardo de información centralizado tipo Storage Area Network (SAN) o Red de Área de Almacenamiento, con capacidad para almacenar hasta 21 Terabytes (TB) de información donde se resguarda tanto la información de archivos documentales, como la generada en sistemas de bases de datos, aplicaciones y servidores virtuales, los cuales se encuentran en ejecución permanente con diferentes funciones acorde a las necesidades de la entidad. El respaldo se realiza según sea la criticidad de las aplicaciones y la información, bajo un tiempo de retención concertado previamente por los dueños de cada uno de los sistemas de información. Actualmente estos tiempos de retención no supera los dos años, ya que existen limitantes que obligan a sobrescribir las cintas archivando solo aquellas que contienen información crítica. Las cintas catalogadas de esta manera contienen un respaldo de información completo de servidores de archivos, documentos digitales y estructuras de bases de datos y sistemas operativos que permiten una restauración completa en caso de ser necesario. Al final de

cada año se almacenan entre 4 y 5 cintas con este tipo de información tomadas de diferentes trimestres del año para ofrecer un cubrimiento completo de respaldo de información.

Dado lo anterior la entidad cuenta con una capacidad limitada de almacenamiento y respaldo de información, no solo por tener un único Datacenter sino que además al tener concentrada la gran mayoría de servidores virtuales en la unidad SAN existe un posible punto de fallo crítico que pudiese comprometer gran parte de la funcionalidad interna y externa de la organización dejando fuera de servicio múltiples aplicaciones, bases de datos y demás servicios virtualizados.

Como complemento a esta problemática se suma la obsolescencia tecnológica de varios componentes que hacen parte de la infraestructura tecnológica del Datacenter del Instituto Nacional de Metrología (INM).

1.2 Identificación y formulación del problema

El Instituto Nacional de Metrología (INM) no cuenta con los elementos necesarios que permitan la recuperación ante desastres de sus procesos de negocio críticos e infraestructuras tecnológicas que los soportan, lo cual es un mecanismo que genera valor a las organizaciones, ya que se fundamenta en la conformación de estrategias que generan un conjunto de elementos clave para la continuidad de las operaciones ante eventuales catástrofes naturales como lo son inundaciones, terremotos o incendios.

En caso de materializarse un desastre en el Instituto Nacional de Metrología (INM) al no contar con mecanismos de recuperación de desastres y de respaldo de información en sitios alternos a la sede principal, se podría presentar un daño en los activos de infraestructura tecnológica que comprende el Datacenter de la entidad y por consiguiente una interrupción

deliberada de servicios asociados con tecnologías de información, afectando todas sus operaciones desde y hacia el ciudadano, generando graves pérdidas de información, servicios e imagen institucional. Así mismo es importante mencionar que contar con los mecanismos de respaldo adecuados, permite minimizar las pérdidas de información y operación, ya que es claro que la entidad está expuesta a fallas en la prestación de sus servicios alojados en los diferentes servidores físicos y virtuales con los que cuenta, debido a que no existe una solución de respaldo que permita mantener las aplicaciones en un sistema de alta disponibilidad donde se pueda garantizar la continuidad de su operación las 24 horas del día como se requiere para aplicaciones críticas. Es importante aclarar que una de las aplicaciones más importantes y catalogadas como críticas de la entidad es la que contempla la generación y difusión de la hora legal colombiana, de la cual hacen uso otras entidades públicas y privadas a nivel nacional con el fin de tener una sincronización de sus sistemas en su infraestructura tecnológica, también es importante mencionar aplicaciones como la denominada servicios en línea, por medio de la que se reciben y tramitan los servicios de calibración generando a su vez los pagos en línea de este tipo de servicios misionales.

Como se mencionó anteriormente la información susceptible de pérdidas abarca servidores virtuales, físicos, aplicaciones y registros de información relacionados con laboratorios del Instituto Nacional de Metrología (INM), también es susceptible de pérdidas la información relacionada con el histórico de cursos en metrología ofrecidos por la entidad, datos de servicios de calibración prestados a nivel nacional, históricos de pagos, entre otras actividades claves para coordinar la metrología científica e industrial, lo cual es parte fundamental de la misión institucional, donde juegan un papel fundamental las condiciones actuales de infraestructura tecnológica, operación y gestión de TI.

1.2.1 Problema General

¿Mediante qué estrategia de gestión TI se puede contemplar la recuperación ante desastres naturales de información y servicios críticos del Instituto Nacional de Metrología (INM)?

1.2.2 Problemas Específicos

- ¿Qué modelo de gestión tecnológica puede ser pertinente y aplicable a servicios soportados en tecnologías de información ante un posible desastre natural?
- ¿Cuáles son los servicios e infraestructura tecnológica que posee actualmente el Instituto Nacional de Metrología (INM)?
- ¿De qué manera se puede identificar la actual infraestructura tecnológica y de servicios que posee el Instituto Nacional de Metrología (INM)?
- ¿Cómo puede el Instituto Nacional de Metrología (INM) recuperar su operación y ofrecer continuidad en sus servicios críticos en caso de presentarse un desastre natural?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

- Diseñar un modelo de gestión tecnológica que permita su adaptación y contribuya a la mejora de la capacidad, disponibilidad y continuidad de los servicios críticos de tecnologías de información ante posibles desastres naturales en el Instituto Nacional de Metrología (INM).

1.3.2 Objetivos Específicos

- Comparar modelos de gestión tecnológica para determinar la viabilidad de adaptación del más apropiado, que lleve a una adecuada gestión y gobierno de los servicios críticos de tecnologías de información en el Instituto Nacional de Metrología (INM).
- Realizar un levantamiento de información de los servicios soportados en tecnologías de información y su infraestructura tecnológica relacionada, para la identificación de los servicios críticos con los que cuenta el Instituto Nacional de Metrología (INM).
- Aplicar la adaptación del modelo de gestión tecnológica seleccionado donde se establezca un diagnóstico, se generen recomendaciones y se incluya un plan de recuperación de desastres con un enfoque organizado que optimice la operación de los servicios críticos de tecnologías de información en el Instituto Nacional de Metrología (INM).

1.4 Justificación de la investigación

Los desastres naturales pueden afectar cualquier organización sin importar su ubicación geográfica, el impacto generado tiene alcances que van desde pérdidas materiales hasta pérdidas humanas, sin embargo, es posible minimizar estos riesgos mediante procedimientos y elementos tecnológicos que garanticen la operación ininterrumpida de una entidad, haciendo uso de entornos alternos u otros elementos tecnológicos que puedan soportar la operación luego de presentarse un desastre natural.

En este contexto es posible reducir el impacto de las interrupciones en la operación y servicios, provocados por posibles fenómenos naturales que afecten la infraestructura tecnológica de la entidad, esta reducción se logra con la aplicación de modelos de gestión como el que se pretende elaborar, donde diversos mecanismos tecnológicos y estratégicos se combinan para minimizar las posibles fallas ofreciendo disponibilidad y continuidad en sus servicios.

Con base en lo anterior, es preciso afirmar que toda organización que decida aplicar modelos de gestión tecnológica con mecanismos de respaldo de información y continuidad de operaciones mediante Planes de Recuperación de Desastres (DRP), obtendrá múltiples beneficios basados en el fortalecimiento de procesos al interior de la organización y la satisfacción de sus clientes.

Por consiguiente, y dado el análisis realizado a la entidad objeto de intervención, es necesaria la adaptación de un modelo de gestión de tecnología con mecanismos de respaldo de información y continuidad de operación que permita soportar las consecuencias producidas por fenómenos naturales o interrupciones deliberadas de servicio, ya que no existen elementos de control suficientes que permitan administrar adecuadamente la disponibilidad para los servicios de TI, y a su vez garantice que los sistemas de información y operación del Instituto Nacional de

Metrología (INM), se encuentren en un entorno más seguro, organizado y fácilmente gestionable, dado lo anterior es importante tener presente que se pretende aportar a la consecución de los objetivos misionales y estratégicos, para lo cual es necesario tener la posibilidad de actuar de manera adecuada ante una posible situación en la que se materialicen interrupciones de servicios asociados con tecnologías de información, que afecten las operaciones tanto al interior de la organización como de cara al ciudadano.

Adicionalmente se brindó un aporte importante en términos de seguridad de la información, ya que se fortaleció el gobierno de TI al interior de la entidad y se contribuyó al establecimiento de los principios de integridad y disponibilidad de información, para mantener las plataformas de servicios en continua operación, incluso ante eventuales catástrofes naturales, lo cual se logró mediante la aplicación de numerales contemplados en la norma ISO/IEC 27001.

1.5 Limitaciones de la Investigación:

1.5.1. Delimitación Teórica

La conceptualización de la gestión tecnológica se concibe desde varios y diversos puntos de vista o enfoques, que se desarrollan con base en la profundidad de conocimientos sobre el tema. Es por ello que se asumen enfoques que la definen como: procesos, técnicas, estrategias, procedimiento, prácticas, entre otros.

Según Ortiz (2014), se concibe como el proceso de administración, adquisición, implementación y difusión de esta, en diferentes sectores, entre ellos el industrial y de servicios o el público y privado. Implica desde luego, el manejo de los procesos de innovación, investigación y desarrollo (I+D) y se constituye en la mejor forma de introducir y utilizar tecnología para soportar el desarrollo.

Además, Venegas (2015), indica que la gestión tecnológica permite manejar el factor tecnológico como aspecto estratégico en las organizaciones productivas, inicialmente se enfocó en la administración de ciencia y tecnología, por lo cual su definición podría concebirse en la administración de conocimiento para dinamizar procesos a través de la inclusión de enfoques de innovación el cual permite la predicción, la proyección y la prospección tecnológica.

Un ejemplo práctico de lo dicho anteriormente es como se realiza un diagnóstico en un caso real para la gestión estratégica de tecnologías a partir de 6 fases como se muestra en la Figura 1, la primera fase consistió en realizar un reconocimiento tecnológico enfocado a la situación actual, en la segunda fase se identificó el impacto de la evolución tecnológica, en la tercera fase se evaluó el potencial tecnológico y posibles alianzas, en la cuarta fase se realizó el diseño de estrategias tecnológicas en investigación, desarrollo y financiamiento en la quinta fase se identificó la explotación tecnológica y finalmente en la sexta fase se estableció una política de protección intelectual.

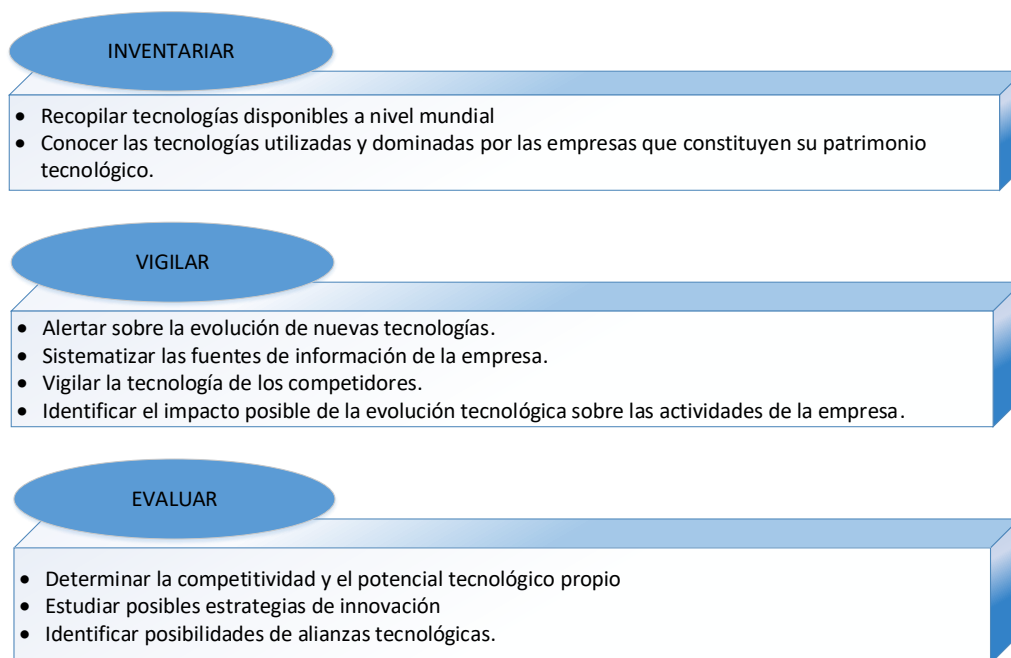




Figura 1. Fases o etapas de la gestión tecnológica.

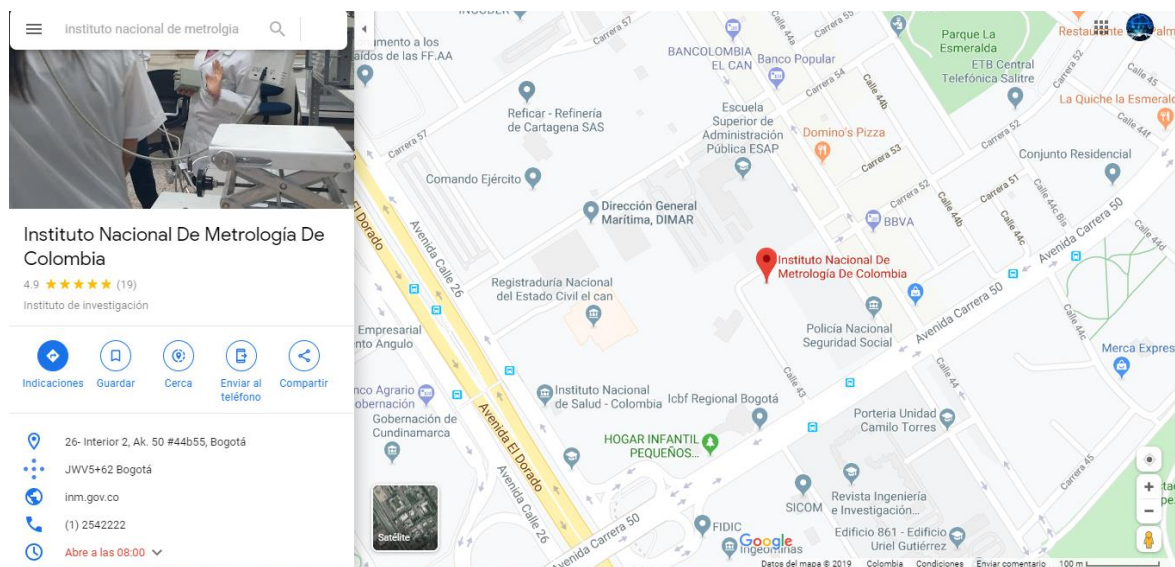
Fuente: (Odremán R., 2014)

Esto demuestra que la gestión tecnológica hace parte de un aspecto clave en cualquier organización, generando un impacto directo e indirecto, sin embargo, para hacer uso de tecnología implica conocer como es el mercado y que tendencias tecnológicas resultan ser las más favorables para posteriormente financiarlas, supervisarlas, evaluar su desarrollo para así garantizar la optimización de los procesos (Solleiro & Castañon, 2016).

Para proceder con la adaptación de un modelo de gestión tecnológica, se consultó el modelo Nacional de gestión de tecnología, el modelo gestión tecnológica COTEC, el modelo de Ray Gehani, el modelo de gestión tecnológica de Hidalgo Nuchera y el modelo de gestión y gobierno de TI, estos serán analizados posteriormente, para seleccionar el más indicado para su evaluación y diagnóstico en el Instituto Nacional de Metrología (INM).

1.5.2 Delimitación Geográfica

La entidad objeto de este proyecto de grado es el Instituto Nacional de Metrología (INM), ubicado en la ciudad de Bogotá en la Av Cra 50 # 26-55 int 2 CAN.



*Figura 2. Ubicación geográfica Instituto Nacional de Metrología (INM).
Fuente: Google Maps (2019)*

2. Marco teórico

2.1 Antecedentes de la investigación

2.1.1 A nivel mundial

A nivel mundial, Cadena (2012), propone la *Construcción De Un Plan De Continuidad De Servicios De Tecnología De Información Para Una Empresa De Seguros*, Concluye el autor que un elemento fundamental en la gestión de tecnologías con miras a la recuperación ante desastres es el catálogo de servicios, el cual genera grandes beneficios al ofrecer un panorama claro y preciso del listado de servicios que el área de sistemas de una organización ofrece a sus usuarios internos y externos. Este elemento se convierte en un insumo clave a la hora de identificar la criticidad de la información, aplicaciones y servicios con los que cuenta la entidad.

Otro punto importante tomado como aporte de este documento es la relación que debe existir entre los modelos de gestión y los principios de seguridad de la información, como son la integridad, disponibilidad y confidencialidad, los cuales deben estar presentes en todo modelo de gestión tecnológica para ofrecer soluciones tecnológicas seguras y aplicables a un entorno corporativo.

Continuando con el ámbito mundial, Manella (2014) propone el, *Diseño de una guía para la implementación del uso de computación en la nube como mecanismo de recuperación ante desastres tecnológicos*, Destaca la continuidad del negocio como la actividad que realizan las empresas para asegurarse de que las funciones críticas estén siempre disponibles para todos sus involucrados, (proveedores, clientes, entes reguladores y demás entidades).

De igual manera concluye la relación e importancia de la computación en la nube y su aplicación con la continuidad de operación en cuanto a sus beneficios, reflejados en el

mejoramiento de infraestructuras corporativos dado que su implementación reduce considerablemente los porcentajes de fallas e interrupciones de servicios.

2.1.2 A nivel nacional

Con relación al ámbito nacional, Fuentes (2019), propone la *Metodología para toma de Decisiones Gerenciales en Infraestructuras IT*, se destacan componentes estratégicos que aportan a una gestión de infraestructura capaz de dar respuesta a las necesidades propias de la organización y sus clientes, para el caso puntual se realiza una intervención en la empresa Claro Colombia donde se destacan la recolección, clasificación y conversión de datos que permiten establecer un resultado basado en información clave, organizada y precisa acerca de la gestión de infraestructura IT, para que esta a su vez facilite la toma de decisiones efectiva dadas las evidencias del comportamiento de una determinada infraestructura tecnológica.

De otra parte, Barragán (2016), destaca la importancia de los planes de recuperación de desastres (DRP) mediante la alineación estratégica de la infraestructura tecnológica organizacional y la gestión de esta, con el objetivo de mantener el cumplimiento de los objetivos misionales.

Este proyecto tiene como objetivo proponer el diseño de un plan de recuperación de desastres en una entidad del estado colombiano que minimice el margen de tiempo de recuperación en la infraestructura tecnológica de la entidad, dando un aporte significativo a la consolidación del modelo propuesto.

Así mismo Hoyos (2016), propone el *Modelo De Gestión De La Innovación Tecnológica Para Aumentar La Competitividad De Las Ladrilleras Del Departamento De Sucre*, Trabajo de grado para obtener el título de Magister en Gestión De La Innovación, como parte de sus

objetivos incorpora la vigilancia tecnológica para determinar que las tecnologías y su aplicación permiten aumentar la competitividad y liderazgo de mercados gracias a su eficiencia en la calidad y prestación de servicios además, se concluye que mediante elementos basados en modelos de gestión tecnológica y de innovación, es posible realizar estudios de características, condiciones y estrategias que permiten un mejor manejo del entorno generando beneficios corporativos y cumplimiento de metas.

2.2 Bases teóricas

2.2.1 *¿Gestión tecnológica o gestión de conocimiento?*

Según Ospina (1993), la gestión tecnológica se define como una orientación agresiva, enfocada a la acción y a la solución creativa de los problemas relacionados con la administración dentro de un contexto de innovación. La gestión tecnológica es el conjunto de actividades que propenden o conllevan a planear, organizar, dirigir, evaluar y controlar el sistema para darle una connotación y un manejo estratégico a la organización.

Así mismo, la tecnología es parte fundamental en toda organización y su fin debe ser generar utilidad y ventaja competitiva, a raíz de esto, existe una necesidad de ligar la tecnología con la estrategia de la organización y es allí donde nace la gestión tecnológica. Algunos teóricos relacionados en la tabla 1 han definido la gestión tecnológica así:

Tabla 1

Definiciones Gestión Tecnológica

Comparación de definiciones y/o aportes al concepto de Gestión tecnológica
Según Khalil (2000) la gestión tecnológica se define como un campo multidisciplinario y multifuncional que une las ciencias y la ingeniería a las disciplinas de negocio
Para Mendoza y Valenzuela (2014) la organización y dirección de recursos humanos y económicos para aumentar la creación de nuevos conocimientos; es también la generación de ideas técnicas que permitan obtener nuevos productos, procesos y servicios o mejorar las ya existentes, el desarrollo de dichas ideas en prototipos de trabajo y su transferencia a las fases de fabricación, distribución y uso
Tapias (2000) define la gestión tecnológica como un conjunto de conocimientos que generan una reconstrucción o reformulación interpretativa de los procesos de generación, transformación y difusión de la tecnología
White and Bruton (2007) la definen como un proceso que incluye todas las fases administrativas: Planeación, organización, dirección y control de las capacidades tecnológicas para formar y lograr objetivos estratégicos y operacionales en una organización.
Robledo, Gómez y Restrepo (2008) indican que todo proceso que conlleva a la innovación de productos y procesos cuya novedad o mejora significativa está asociada a cambios tecnológicos.

Según Barranco (2016) COTEC y la gestión de la tecnología incluye todas aquellas actividades que capacitan a una organización para hacer el mejor uso posible de la ciencia y la tecnología generada tanto de forma externa como interna. Este conocimiento conduce hacia una mejora de sus capacidades de innovación, de forma que ayuda a promocionar la eficacia y eficiencia de la organización para obtener ventajas competitivas

Nota: Elaboración propia, basado en varios autores

Según Farfan y Garzon (2006), la Gestión del Conocimiento hace referencia a la capacidad de aprender y generar conocimiento nuevo o mejorar el existente, por lo que se puede definir como un sistema facilitador de la búsqueda, codificación, sistematización y difusión de las experiencias del talento humano en una organización, para convertirlas en conocimiento globalizado, de común entendimiento y útil en la realización de todas las actividades de la misma, esto permitirá generar ventajas sustentables y competitivas en un entorno dinámico para satisfacer necesidades presentes y futuras, y así identificar recursos de conocimiento tanto nuevos como existentes desarrollar nuevas oportunidades para por ejemplo sistemas de información emergentes o existentes.

Además ConocimientoMinTIC (2018), afirma que a través de la gestión del conocimiento se lleva a cabo en las entidades la construcción, maduración y dinamización del conocimiento, a través de un flujo establecido en dos ciclos; El primer ciclo consiste en generar y producir el conocimiento, luego se recolecta e instrumentaliza para finalmente difundirlo y llevarlo a cabo. Si el conocimiento es aplicado, da origen al segundo ciclo, el cual consiste en evaluar cómo se aplicó, y determinar las acciones de mejora a que haya lugar para nuevamente ser difundidas y de esta forma asegurar que las entidades del estado aprendan y usen las metodologías

implantadas por el mismo MinTIC, para generar estrategias de aprendizaje organizacional, que se adapten a sus necesidades y den cumplimiento a lo establecido a por ejemplo la estrategia de gobierno digital y exista una alineación al Modelo Integrado de Planeación y Gestión (MIPG) en su sexta y tercera dimensión, fortaleciendo de forma transversal las otras dimensiones (Direccionamiento Estratégico y Planeación, Evaluación de resultados, Talento Humano, Control Interno e Información y Comunicación), en cuanto el conocimiento que se genera o produce que es clave para su aprendizaje y su evolución.

Con base a lo investigado en las referencias teóricas acerca de los modelos de gestión del conocimiento y de gestión tecnológica, se identificó que estos modelos incorporan una forma de representación simplificada, simbólica y esquemática que delimitan sus dimensiones, permiten una visión aproximada de la organización, describen procesos y estructuras, orientan estrategias y aportan datos generando una relación, debido a que son instrumentos de dirección estratégica que se caracterizan por la creación de valor y de administración de capital intelectual, que en muchos casos se entrecruzan y relacionan de manera similar.

Cabe destacar, que la gestión de conocimiento permite incorporar aspectos científicos y tecnológicos, ya que estos generan un aporte de tipo individual tácito y son el punto de partida para el estudio o creación de otros modelos como lo puede llegar a ser uno de gestión tecnológica, lo anterior debido a que están relacionados con el uso de información estratégica para conseguir los objetivos de negocio y a nivel de implementación, además la gestión de conocimiento puede contemplar componentes de arquitectura TI y activos de información para ser analizados y al igual que un modelo de gestión tecnológica cuenta con la capacidad de aportar, complementar, soportar y dar cumplimiento a políticas y directrices establecidas por el gobierno nacional colombiano para el mejoramiento en la eficiencia administrativa.

2.2.2 Modelo Nacional de gestión de tecnología

Este modelo citado por Armenteros (2012), comprende una integración entre las actividades que se realizan en una organización junto con el desarrollo y la innovación tecnológica. Así mismo se tiene en cuenta los resultados que genere este tipo de gestión en la empresa.

El modelo es el conjunto de funciones que facilitan la organización y coordinación de las actividades, procesos o tareas cuya agrupación permite hacer más eficiente su gestión.

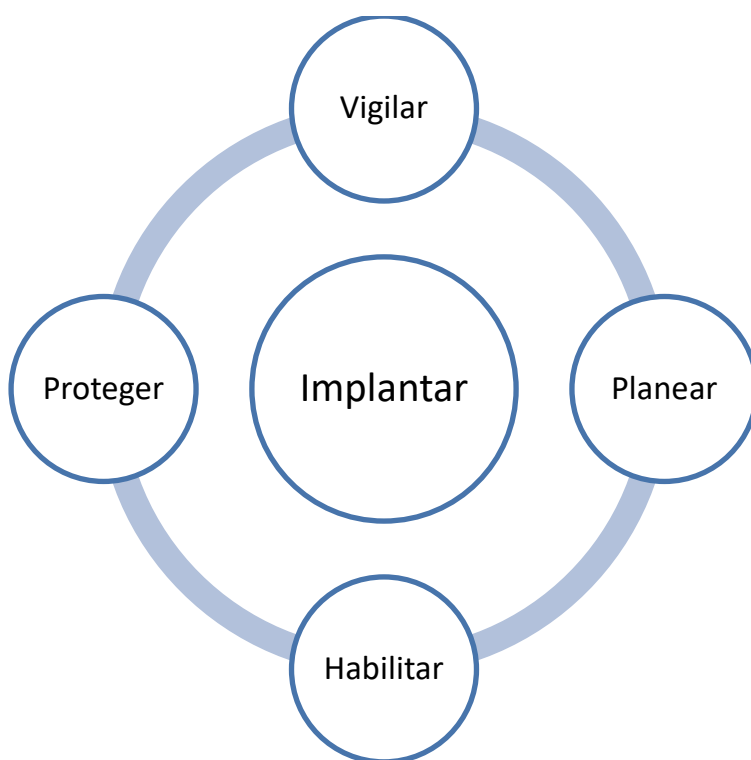


Figura 3. Modelo nacional de gestión de tecnología.
Fuente: (Armenteros, 2012)

Según la Figura 3 el Modelo nacional de gestión de tecnología identifica las siguientes fases:

Vigilar: Es la etapa del modelo que permite a la organización identificar tanto oportunidades como amenazas en el entorno en cuanto al desarrollo e innovación tecnológica que afecten en cierto grado a la organización. Algunos procesos que tienen fundamento en la vigilancia son: Benchmarking, elaboración de estudios de mercados, estudios de competitividad y monitoreo tecnológico.

Planear: Desarrollo de estrategias y planes que le permiten a una organización dirigirse hacia un objetivo específico, líneas de acción que deriven en ventajas competitivas. Por ejemplo, la elaboración y revisión del plan tecnológico.

Habilitar: Es la obtención de recursos tecnológicos dentro y fuera de la organización.

Adquisición de tecnología: compra, licencia, alianzas, otros. Asimilación y desarrollo de la tecnología.

Proteger: Hace referencia a cuidar el patrimonio tecnológico con el que cuenta la organización, a través de contratos de licencia, patentes o títulos de propiedad intelectual.

Implantar: Es la adopción de algún proceso nuevo dentro de la organización o la mejora de uno previamente establecido: Innovación de proceso, innovación de producto, innovación en mercadotecnia, innovación organizacional.

2.2.2 Modelo Gestión tecnológica COTEC

COTEC según Barranco (2016), destaca la importancia de la gestión tecnológica en la organización y su relación cercana con los procesos de innovación, a su vez propone un modelo

que contiene los elementos fundamentales o claves en la gestión exitosa de una estrategia tecnológica o el desarrollo de nuevos productos, a continuación, se presenta el modelo:

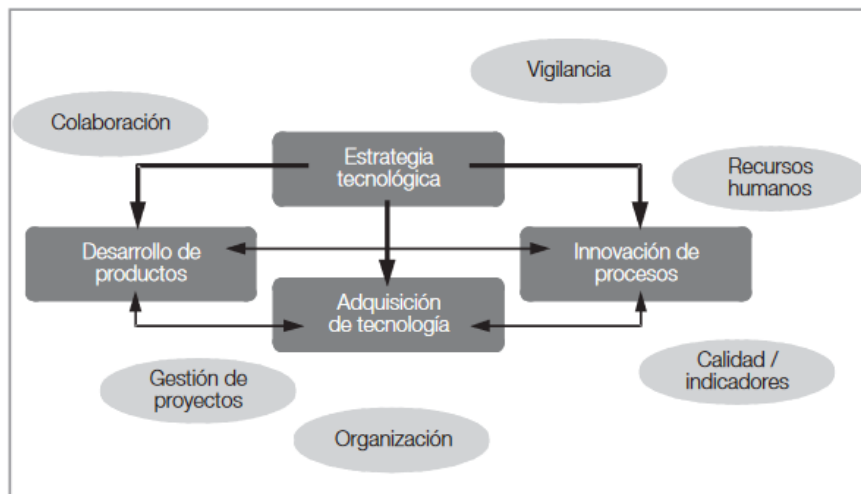


Figura 4. Gestión tecnológica y modelos de innovación empresarial.
Fuente: (Barranco, 2016)

El modelo propuesto por COTEC, se define según la Figura 4 en cuatro procesos fundamentales para la consecución de la eficacia y eficiencia óptima de la actividad empresarial. Estos son: Estrategia tecnológica, adquisición de tecnología, innovación de procesos y desarrollo de nuevos productos; siendo los dos últimos procesos directamente conectados con la innovación y los dos primeros procesos de apoyo (Barranco, 2016).

2.2.3 *Modelo Nonaka y Takeuchi*

El modelo presentado por los japoneses Nonaka y Takeuchi (1995) destaca entre los modelos que describen la construcción del conocimiento en las organizaciones, convirtiéndose así en punto de partida de muchos estudios y otros modelos.

Lo que busca dicho modelo es establecer el proceso por el cual el conocimiento puede ser creado y transformado dentro de cada organización. Así como las condiciones que deben tener

las organizaciones para facilitar dicho proceso. El proceso de creación del conocimiento se da a través de un modelo de generación de conocimiento que se sustenta en dos espirales de contenido epistemológico (conocimiento en sí) y ontológico (en el ser). Es un proceso de interacción entre conocimiento tácito y explícito que tiene naturaleza dinámica y continua. Se constituye en una espiral permanente de transformación interna de conocimiento.

Anclado a este modelo se tiene por un lado al conocimiento explícito que puede ser fácilmente comunicado y compartido, de carácter formal y sistemático, y por otro lado el conocimiento tácito el cual es muy personal y resulta difícil expresarlo formalmente.

De acuerdo con lo anterior, el conocimiento tácito implica una mayor atención y esfuerzo para poder extraerlo de cada individuo y dinamizarlo a los diferentes grupos, sin perder de vista el conocimiento explícito; de modo que la identificación de ambos conocimientos es un primer paso para determinar la mejor forma de expresarlos y compartirlos.

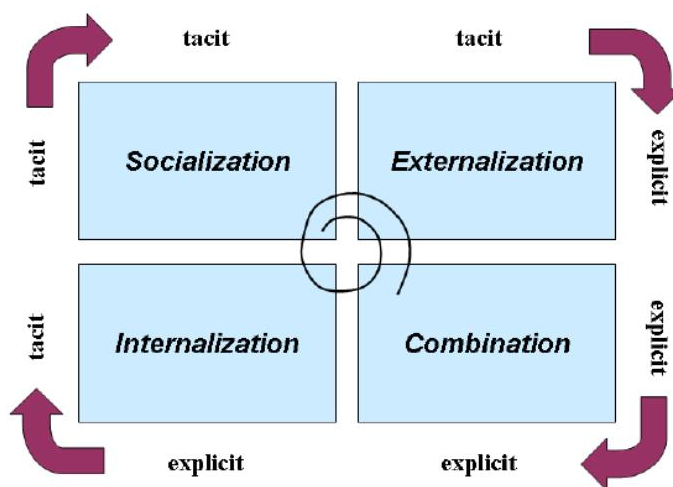


Figura 5. Formas de conversión del conocimiento en la organización.
Fuente: (Nonaka y Takeuchi, 1995)

Las fases de conversión del conocimiento “espiral del conocimiento organizacional” obtenidos en la Figura 5 se describen como:

1. **Socialización (de tácito a tácito):** Proceso donde se comparten experiencias y creencias (cultura organizacional).
2. **Exteriorización (de tácito a explícito):** Proceso de creación de conceptos, generada por el dialogo o la reflexión colectiva.
3. **Combinación (de explícito a explícito):** Consiste en pasar de un conocimiento explícito a otro explícito. Se basa en el intercambio, asociación y estructuración de conocimientos explícitos, procedentes de distintas fuentes, facilitando la creación de nuevos conocimientos del mismo tipo.
4. **Interiorización (de explícito a tácito):** Proceso de conversión de conocimiento explícito en conocimiento tácito. Se facilita a través de la transferencia y aplicación del conocimiento explícito, registrado en manuales de procedimientos, formulas o historias orales.

2.2.4 Modelo de Andersen

El modelo de Andersen (1999) se basa en la transmisión de información valiosa para la organización. La información viajara de los individuos a la organización y luego en proceso inverso hacia los individuos. A través del proceso se busca como objetivo la creación de valor visible y reconocible por los clientes para que estos apuesten más por la empresa.

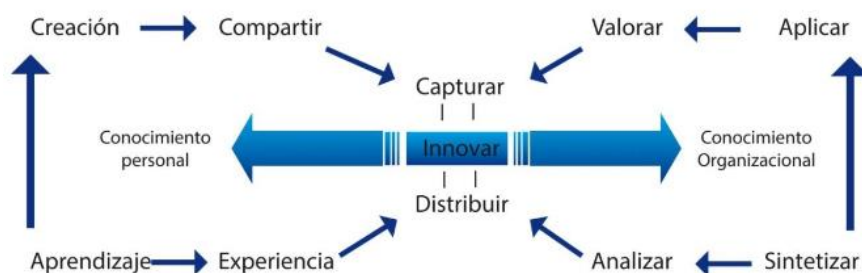


Figura 6. Modelo de gestión del conocimiento.
Fuente: (Andersen, 1999)

En la Figura 6 se presenta dos aspectos novedosos frente a sus antecesores el personal y el organizacional el cual se define como:

Conocimiento individual: El individuo tiene la responsabilidad de compartir y hacer explícito el conocimiento que posee, una obligación ética hacia el resto de sus compañeros de la organización.

Conocimiento organizacional: La dirección de la organización debe apostar y liderar la creación del clima organizacional que fomente el nivel individual anterior.

De otra parte, Jaramillo (2012), establece un listado de modelos de gestión de conocimiento entre los que se puede encontrar:

- La organización creadora del conocimiento
- The 10-Step Road Map
- La gestión del conocimiento desde una visión humanista
- La gestión del conocimiento desde la cultura organizacional
- Un sistema de gestión del conocimiento en una organización escolar
- Knowledge Management Assessment Tool
- Modelo de KPMG Consulting
- Modelo de Gopal & Gagnon
- Un nuevo modelo gestión del conocimiento (López & Castillo, 2002).

Entre la revisión de metodologías específicas se pueden encontrar:

- Diseño de un sistema de gestión del conocimiento para la dirección de servicios y
- Recursos de información de la universidad ICESI (Jaramillo, 2012) .
- Un modelo de gestión del conocimiento basado en procesos e interfaces de conocimiento (Landaeta & Aure, 2002).

- Evaluación de Capacidades de Innovación (Robledo V., López G., Zapata L., & Pérez V., 2010).
- KARAGABI KMMODEL: Modelo de referencia para la introducción de iniciativas de gestión del conocimiento en organizaciones basadas en conocimiento (de J. González, Joaqui, & Collazos, 2009).

Los distintos modelos tanto de gestión de conocimiento como de capital intelectual ponen en evidencia la profunda conexión entre los dos campos, no obstante, una visión más amplia a esta situación puede darse al analizar las tipologías y taxonomías propuestas como lo muestra la Figura 7. Estas aportan en cuanto dan un marco de partida a la revisión de los modelos más reconocidos por los expertos para la gestión de conocimiento y también a los de gestión de capital intelectual; considerados dentro de las tipologías por su innegable relación. Esto da entender entonces que difícilmente estos modelos y tipologías se darán en estado puro en la realidad, tendiendo a mezclarse unas con otras.

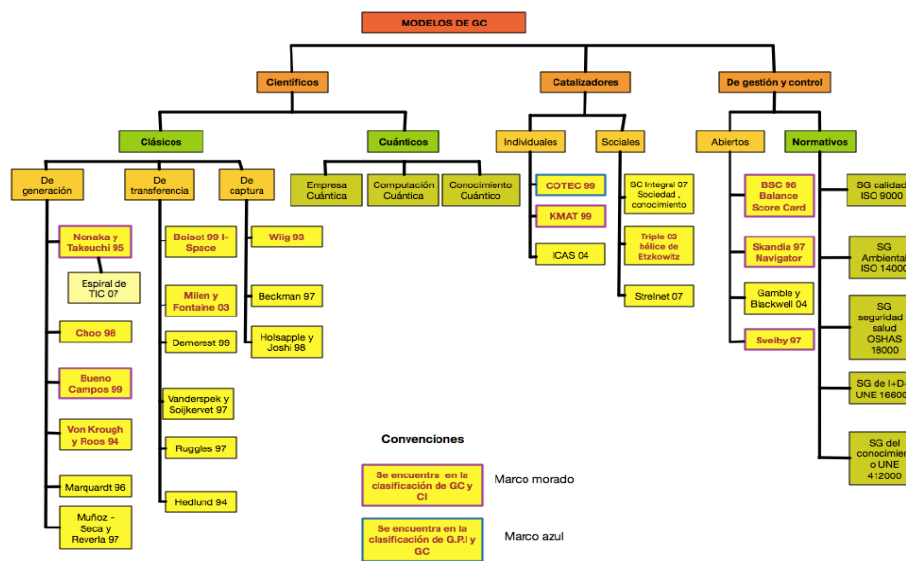


Figura 7. Taxonomía contrastada modelos de la gestión del conocimiento.
Fuente: (Basado en Sáinz *et al.*, 2010)

2.2.5 Modelo de Ray Gehani

Dicho modelo expresa Quintero (2018) que, aunque en los mercados globalizados actuales, la tecnología es uno de los factores críticos para el crecimiento y la supervivencia de las organizaciones, la gestión de esta tecnología requiere de la asignación de recursos, la innovación, el desarrollo de nuevos productos y el talento humano especializado, entre otros.

En este modelo se habla de tres subsistemas:

Subsistema de Transformación: Hace referencia a la gestión de competencias en el núcleo de los procesos operacionales, es decir aquellos que convierten propiedad intelectual en operaciones y desarrollo de nuevos productos.

Subsistema de Recursos: Está relacionado con la gestión de tres recursos importantes:

- Gestión de calidad en los productos y servicios
- Gestión del procesamiento de la información
- Gestión del personal

Subsistema de Integración y Visión: Está orientado hacia la integración entre las competencias de los dos anteriores y comprende:

- La gestión de proyectos tecnológicos
- La gestión del liderazgo

2.2.6 Modelo de gestión tecnológica de Hidalgo Nuchera

Nuchera propone dos tipos de funciones activas y de apoyo, estas dos funciones deben coordinarse para tener una eficiente vigilancia tecnológica y protección de las innovaciones como se ve en la Figura 8. Las funciones activas son definidas como capacidades de adquisición, asimilación y desarrollo de los recursos tecnológicos, por otra parte, las funciones de apoyo son

las capacidades para reconocer e interpretar oportunidades y amenazas del entorno con respecto a su posición tecnológica (Jaimes, Ramírez, Vargas y Carrillo 2011).

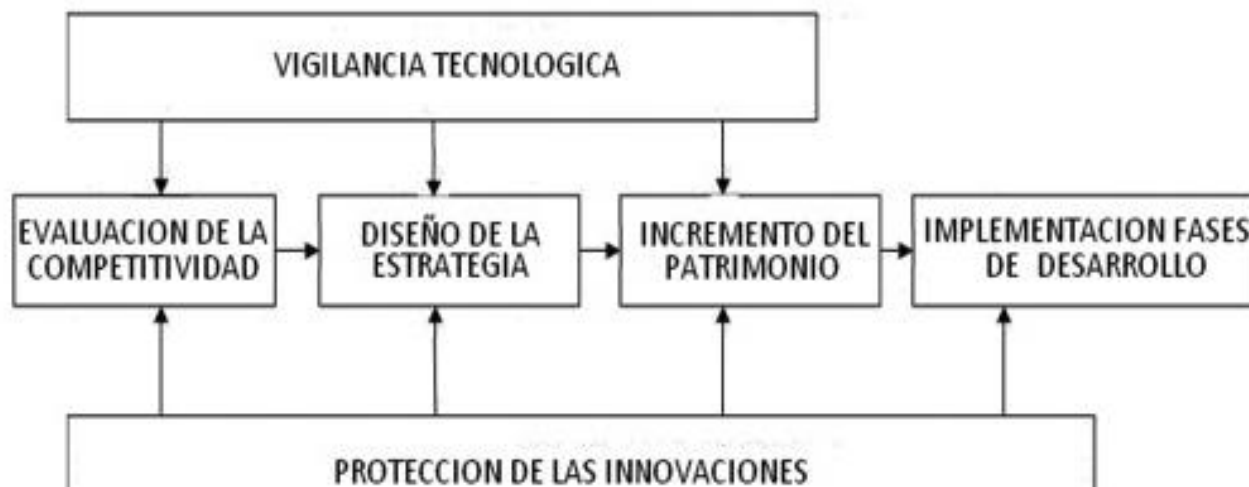


Figura 8. Modelo de gestión tecnológica de Nuchera adaptado por Jaimes *et al.* (2011).
Fuente: Jaimes *et al.*(2011)

2.2.7 Modelo de gestión y gobierno de TI

Según MGGTIG (2019) se define como los principios que deben ser tenidos en cuenta para gestionar y gobernar las tecnologías de la información y las comunicaciones a nivel institucional, territorial y sectorial.

El Modelo de Gestión y Gobierno de TI está estructurado con diferentes elementos que habilitan los propósitos de la política de gobierno digital ,la transformación de las entidades, territorios, sectores y el apoyo adecuado a los procesos de las entidades públicas, en la Figura 9 se muestra como los principios que orientan los dominios agrupan varios lineamientos y estos se implementan mediante guías orientadas a procesos de TI dentro del macroproceso de gestión de TI en las organizaciones (MGGTIG, 2019).

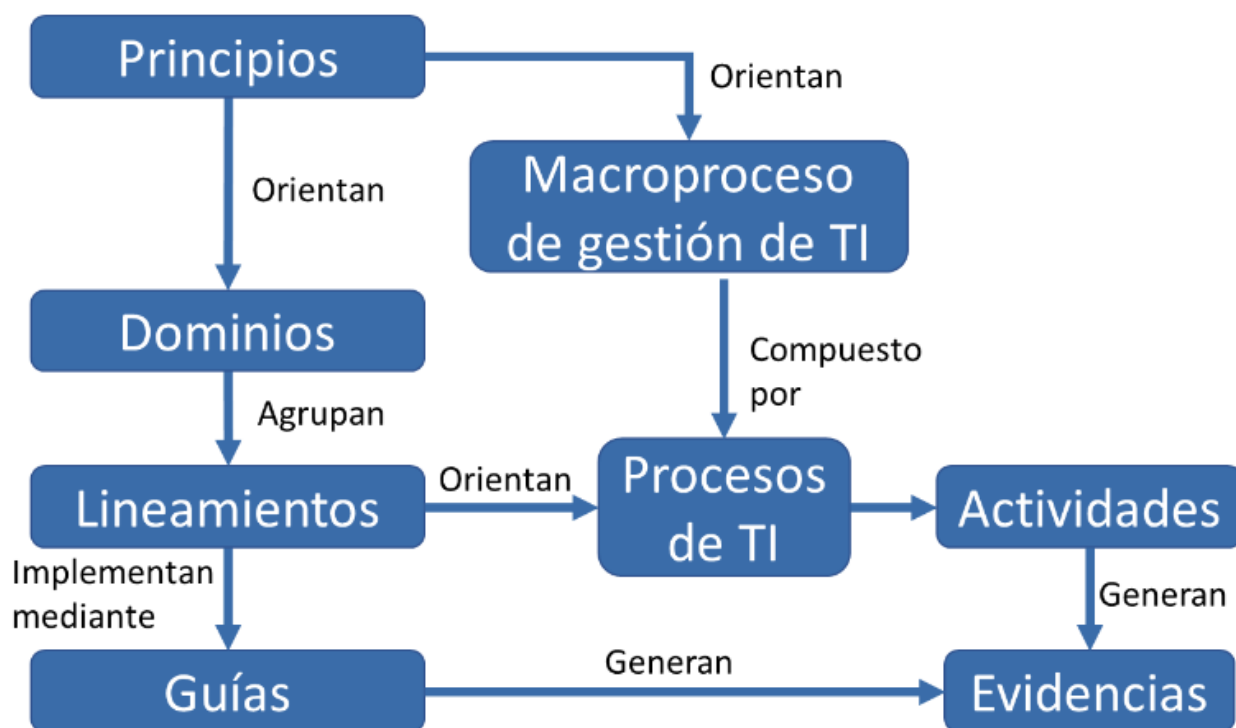


Figura 9. Estructura del Modelo de Gestión y Gobierno de TI
Fuente: (MGGTIG, 2019)

2.2.8 Relación norma ISO/IEC 27001 con un modelo de gestión tecnológica

En el capítulo 4.1 se hace énfasis en el conocimiento de la organización y su contexto, donde se determina los aspectos necesarios para lograr los objetivos a nivel de seguridad de la información con un análisis de índole interno y externo, lo cual es parte fundamental del proceso de adopción de un modelo de gestión tecnológica, así mismo en el capítulo 4.2 se menciona la comprensión de necesidades y expectativas que permiten dar mayor claridad a al entorno organizacional, aspectos como el liderazgo por parte de las directivas también hacen un gran aporte a la consolidación de nuevos proyectos de TI (ISO/IEC 27001, 2013).

El caso específico de tratamiento de riesgos y oportunidades, se incluyen conceptos prevención y reducción de efectos indeseados como pérdidas de información aportando a la

mejora continua de una organización mediante la implementación de acciones y su posterior evaluación. otro aspecto relevante en la norma ISO/IEC 27001 mencionado en el numeral 6.1.2 de la misma, permite hacer una valoración de riesgos incluyendo diferentes criterios que permiten analizar resultados comparables en el tiempo con base en sus probabilidades de ocurrencia (ISO/IEC 27001, 2013).

Otros aspectos clave son los descritos en el numeral 7.5, haciendo referencia a la importancia de la información documentada, su creación, actualización y control de esta con el objetivo de que sea conocida solo por los verdaderamente deben conocerlas dado su rol y responsabilidad (ISO/IEC 27001, 2013).

Así mismo, el numeral 8.1 menciona aspectos importantes en cuanto a la planificación operacional y control, para estar en capacidad de tomar acciones que puedan mitigar aspectos que así lo ameriten (ISO/IEC 27001, 2013).

En cuanto al seguimiento medición y análisis se describen las principales recomendaciones a partir del numeral 9.1, siempre con el objetivo de generar resultados medibles y comparables. Seguido de este aspecto se relaciona la importancia de las auditorías internas y la revisión por la dirección, enfatizando estos aspectos como un deber que asegura la eficacia del camino propuesto para el logro de las metas propuestas. Finalmente se plantea la importancia de la mejora continua en el numeral 10, aplicable para cualquier sistema con el objetivo de mejorar continuamente la conveniencia y eficacia de los procesos al interior de la organización (ISO/IEC 27001, 2013).

2.2.9 Antecedentes desastres naturales

De acuerdo con un informe de la Comisión Económica para América Latina y el Caribe (Cepal) y el Fondo de las Naciones Unidas para la Infancia (Unicef), la frecuencia de desastres en Latinoamérica ha aumentado 3,6 veces en medio siglo, lo cual se evidencia en la Figura 10 en donde se resalta a México, Colombia y Brasil con una tasa de desastres mayor, el informe también señala que mientras en la década de 1960 hubo 19 desastres, en promedio, por año, en la primera década del siglo XXI ese promedio aumentó a 68 fenómenos anuales (Cepal, 2019).

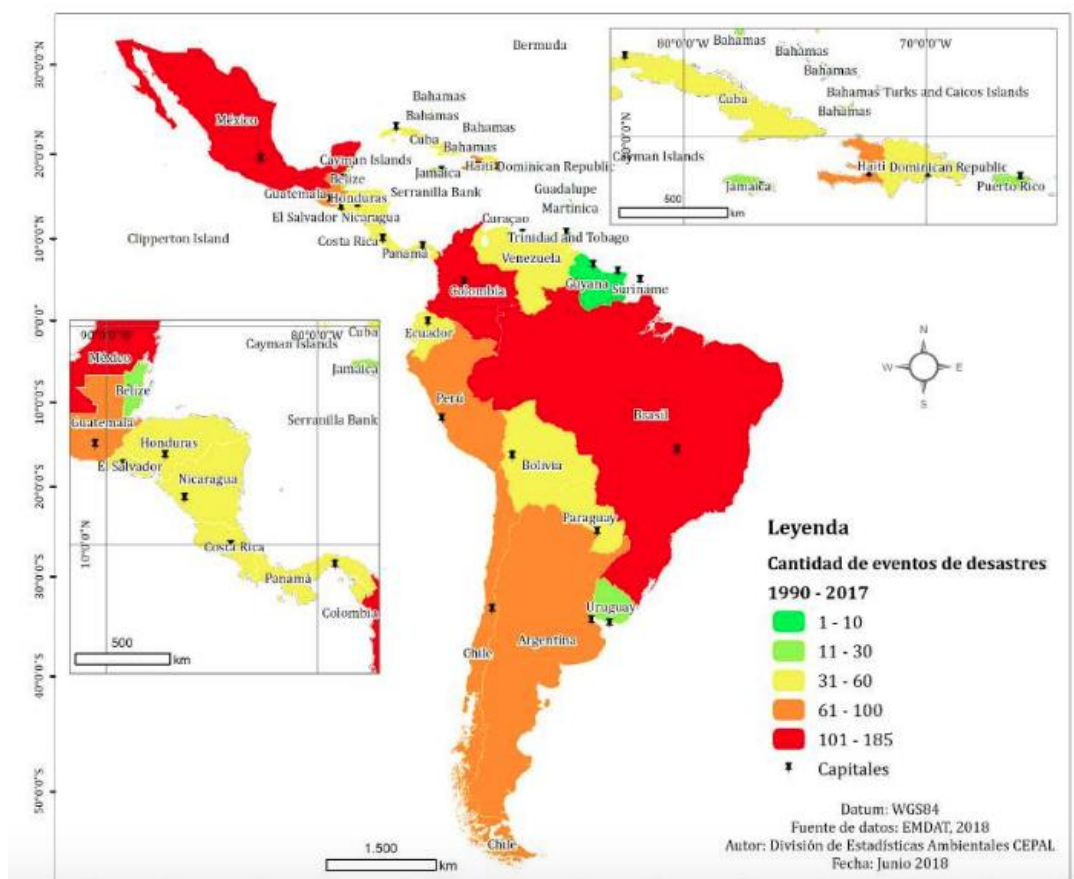


Figura 10. Cartografía desastres reportados.
Fuente: (Cepal, 2019).

La mayoría de los desastres en la región están relacionados con fenómenos de origen meteorológico e hidrológico, que incluye huracanes, tormentas, inundaciones y sequías. No obstante, de acuerdo con el estudio, el desastre con mayor número de víctimas en la región fue el terremoto de Haití en 2010, que dejó 222.570 muertos (Cepal, 2019).

En 2016 se registraron dos eventos que dejaron muchas víctimas, como fue el terremoto en Ecuador, con 677 muertos, y el huracán Matthew, en Haití, con 546 muertes. Este año, Perú y Colombia han sido afectados de manera importante por la ola invernal que ha generado el desbordamiento de ríos, los que a su paso se han llevado poblaciones enteras (Cepal, 2019).

Así mismo, y de acuerdo con el DNP y la base de datos de reporte de Emergencias de la Unidad Nacional para la Gestión del Riesgo de Desastres, para el período 2006-2014 se reportaron en el país 21.594 emergencias generadas por eventos de origen natural, de los cuales 14.853 corresponden a eventos hidrometeorológicos, como se conocen a los generados por la acción violenta de los fenómenos atmosféricos. La principal causa de ellos son las inundaciones y los deslizamientos (DNP, 2015).

Tomando la cifra de 21.594 eventos que generaron emergencias, el promedio de reportes anuales fue de 2.399 eventos. De ellos, 14.641, que corresponden al 67,8%, se concentraron en el período 2011-2014. Los departamentos que reportaron mayor número de personas afectadas han sido Bolívar (1.509.730), Chocó (1.305.965) y Magdalena (1.026.579) (DNP, 2015).

Teniendo en cuenta que una misma persona puede ser afectada varias veces por diferentes eventos, en el caso de Chocó, que proyecta una población de 500.000 habitantes a 2015, esto implicaría que cada habitante se vio afectado en el período cerca de tres veces ante una situación

de emergencia. Esto pone de manifiesto la relación entre los desastres y su contribución a perpetuar las condiciones de pobreza de la población (DNP, 2015).

Así mismo como consecuencia de los eventos ocurridos, se reportaron 3.181 personas fallecidas. Antioquia, con 586 muertos (414 de ellos por inundaciones y deslizamientos), es el departamento con más víctimas en el país a diciembre de 2014 (DNP, 2015).

En el caso particular del municipio de Salgar, las autoridades locales habían reportado 22 eventos de emergencia entre 1999 y 2014. De ellos, 13 fueron inundaciones y tres ocurrieron en un mismo año: 2012 (DNP, 2015).

Los municipios suelen reportar sus emergencias o afectaciones a la UNGRD. El incentivo para hacerlo es quedar registrados entre los subsidios que asigna el Fondo Nacional de Vivienda (Fonvivienda). Entre 2006 y 2014 los subsidios (viviendas) asignados suman 33.052, lo que equivale a casi el doble de los recursos inicialmente calculados (18.190) (DNP, 2015).

Las inundaciones son la primera causa de muertes por fenómenos hidrometeorológicos. De los 12 millones de damnificados entre 2006 y 2014, se vieron afectados por inundaciones 9 millones (DNP, 2015).

De acuerdo con lo descrito por el DNP (2015), y teniendo en cuenta que el Instituto Nacional de Metrología (INM) se encuentra ubicado en la ciudad de Bogotá, las posibles catástrofes naturales que se pueden materializar y tienen un índice de ocurrencia relevante ya que se registran cifras de damnificados muertos y heridos son en inundaciones, terremotos e incendios, por lo que se debe considerar estos fenómenos con una probabilidad de ocurrencia medio, y esto se tendrá en cuenta para el estudio e identificación de activos críticos.

Tabla 2

Reportes de emergencias por departamentos

	Departamento	Población proyectada 2015	Eventos	Muertos	Afectados
1	Antioquia	6.456.299	1.384	586	490.459
2	Cundinamarca	2.680.041	2.206	243	264.539
3	Caldas	987.991	507	223	130.914
4	Tolima	1.408.272	1.576	215	269.395
5	Cauca	1.379.169	1.105	198	784.384
6	Santander	2.061.079	1.581	195	420.405
7	Norte de S.	1.355.787	669	167	176.992
8	Valle	4.613.684	1.262	151	461.840
9	Boyacá	1.276.407	1.252	150	414.286
10	Nariño	1.744.228	1.110	141	586.152
11	Chocó	500.093	666	137	1.305.965
12	Huila	1.154.777	1.164	105	113.873
13	Risaralda	951.953	907	101	219.712
14	Magdalena	1.259.822	493	91	1.026.579
15	Bogotá D.C.	7.878.783	367	68	89.087
16	Meta	961.334	367	57	108.834
17	Atlántico	2.460.863	561	50	457.887
18	Bolívar	2.097.161	604	45	1.509.730
19	La Guajira	957.797	267	44	552.451
20	Cesar	1.028.890	579	35	564.632
21	Caquetá	477.642	298	35	123.430
22	Quindío	565.310	657	33	45.071
23	Córdoba	1.709.644	465	24	848.346
24	Putumayo	345.204	274	22	317.974

25	Casanare	356.479	563	20	116.787
26	Sucre	851.515	358	17	709.138
27	Arauca	262.315	176	11	67.778
28	Guainía	41.482	31	7	29.576
29	San Andrés y Providencia	76.442	32	4	2.641
30	Vichada	71.974	37	2	23.239
31	Amazonas	76.243	21	2	32.482
32	Guaviare	111.060	40	1	33.424
33	Vaupés	43.665	15	1	848
TOTAL		48.203.405	21.594	3.181	12.298.849

Nota. Recuperado de (DNP, 2015).

Por lo anterior el DNP (2015) destaca en la Tabla 2, los reportes de emergencias por departamentos en donde se evidencia la cifra de eventos, muertos y afectados, por lo que se puede concluir lo siguiente:

- Los departamentos con mayor proporción de personas reportadas como afectados han sido Chocó, Putumayo, Sucre y Magdalena.
- Los cuatro departamentos con el mayor número de muertos se localizan en la Región Andina: Antioquia, Cundinamarca, Caldas y Tolima. Su geografía, densidad poblacional y concentración de actividades productivas generan una alta exposición a fenómenos como los deslizamientos e las inundaciones. Otros departamentos que registran un gran número de muertos son Cauca, en el quinto lugar, y Magdalena, que, en el lugar 14, es el que mayores muertes ha registrado en la región Caribe.

- Por el contrario, los cuatro departamentos que cierran el listado con menor mortalidad se localizan en la Región Amazónica: Vichada, Amazonas, Guaviare y Vaupés. Esto podría ser explicado por su menor densidad poblacional y el tipo de inundación (lenta).
- Los departamentos que mayor destrucción de viviendas reportan por concepto de deslizamiento e inundaciones son Nariño, Chocó, Bolívar, Boyacá, Cundinamarca y Santander, que representan el 47% del total de viviendas destruidas.
- Los departamentos con mayores afectaciones sobre la infraestructura vial por deslizamientos han sido Huila, Nariño, Cundinamarca, Santander y Cauca. Estas afectaciones representan el 66% del total de vías impactadas.

2.3 Bases Legales

2.3.1 Normas nacionales

Teniendo en cuenta el contexto de desarrollo del presente trabajo cabe resaltar como uno de los principales elementos de normatividad nacional vigente y aplicable, los contenidos registrados en el Plan Vive Digital, y en general cada uno de los aspectos referenciados en la reciente política de gobierno digital (gdigital, 2019).

También aplican normas de protección de datos basadas en la ley 1581 de 2012 y el decreto 1377 de 2013 de la ley estatutaria de protección de datos personales (Ley1581, 2012).

De igual manera cabe mencionar en este contexto la siguiente normatividad referente al sistema integral de desastres:

- Ley No 46 de 1988 Crea el SNPAD por medio de la cual se genera el Sistema

Nacional para la Prevención y Atención de Desastres, incluyendo la fijación de sus objetivos (SNPAD, 1988).

- Ley 9ª de 1989 – Ley de Reforma Urbana identifica parámetros de planificación y gestión urbana en Colombia. Encargada de incluir en los Planes de Desarrollo temas referentes a la gestión del riesgo para la reubicación en zonas de alto riesgo (EVA, 1989).
- CONPES 2948 de 1997 Formulo actividades para la mitigación y prevención de las consecuencias generadas por el fenómeno del niño (PNPAD, 1997).
- CONPES 3242 de 2003 Define las ventas de servicios ambientales y mitigaciones de cambios climáticos y su adopción (VSAMCC, 2003).
- Ley 1523 de 2012 manifiesta la adopción de la política nacional de gestión del riesgo de desastres, obliga a los municipios del país a tener un plan municipal de gestión de riesgo de desastres aportando a la reducción de sus posibles consecuencias (PNGRD, 2012).
- Decreto 4147 de 2011 –encargado de la Creación de la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD, 2011).

2.3.2 Normas Internacionales

Durante el año 2005 se aprobó a nivel internacional el marco de acción Hyogo, relacionado con la estrategia de Yokohama, que a su vez comprende los acuerdos relacionados con los desastres naturales (HYOGO, 2005).

Desde el punto de vista regional para las américas existe la convención interamericana para generar en casos de desastres.

Así mismo es importante mencionar la siguiente normatividad internacional relacionada

- ISO/IEC 27001:2013 publicada por primera vez en 2005, describe como se debe realizar la gestión a la seguridad de la información en una organización (ISO/IEC 27001, 2013).
- Norma ISO 22301:2012. Este estándar permite a todo tipo de organizaciones ofrecer soluciones al negocio ante posibles contingencias (ISO/IEC 22301, 2012).
- ISO/IEC 24762 Aplicable para los servicios de recuperación de desastres como estándar internacional (ISO/IEC 24762, 2008).
- ISO /IEC 18044, La cual es aplicable a el proceso de respuesta de incidentes (ISO/IEC 18044, 2004).
- ISO /IEC 27031, La cual es aplicable para la gestión de la tecnología de información y Comunicación y obtención de Continuidad de Negocio (ISO/IEC 18044, 2017).

2.4. Definiciones de Términos

Gobierno de TI

El gobierno de TI se enfoca en la alineación que debe existir entre las tecnologías de información y las comunicaciones y su relación directa con las estrategias y objetivos misionales del negocio, buscando la construcción de estándares que favorezcan el crecimiento corporativo mediante el uso y aprovechamiento de las tecnologías existentes como habilitador transversal de procesos misionales (Echeverry, 2017).

Capacidad Tecnológica

Establece que la capacidad tecnológica se refiere al uso eficaz del conocimiento tecnológico con el propósito de mantener la competitividad en precio y en calidad. Dicha capacidad permite a la organización asimilar, emplear, adaptar y modificar las tecnologías

existentes, así como la creación de nuevas tecnologías y el desarrollo de nuevos productos y métodos de fabricación, todo esto para responder a los cambios del entorno, (Velázquez, Dominguez & Andrade, 2018).

Disaster Recovery Plan, DRP

Plan para la recuperación de operación y servicios críticos basados en tecnologías de información y las comunicaciones donde se definen claramente los roles y responsabilidades involucrados, así como las estrategias aplicables y procedimientos a seguir para reactivar la operación y continuidad de servicios (MinTIC, 2010).

Business Continuity Plan, BCP

Es un componente estratégico de planeación para brindar continuidad al negocio, el plan de continuidad de negocio recopila la información suministrada por el DRP, formando un esquema de contingencia global para recuperar operaciones y procesos de la entidad (MinTIC, 2010).

Infraestructura tecnológica crítica

Se refiere a todos aquellos elementos que hacen parte de los sistemas informáticos esenciales para la operación y prestación de servicios de una organización abarcando aspectos de almacenamiento, conexiones de red, sistemas de respaldo, y demás dispositivos tecnológicos que soportan la operación continua (MinTIC, 2017).

Seguridad informática

Es la encargada de asegurar física y lógicamente los datos y la información con que cuenta una organización, la confidencialidad es su característica principal ya garantiza que todos los activos del negocio cuenten con protección permanente ante cualquier riesgo posible (Gil,

2017).

Gestión Tecnológica

La conceptualización de la gestión tecnológica se concibe desde varios y diversos puntos de vista o enfoques, que se desarrollan con base en la profundidad de conocimientos sobre el tema. Es por ello que se asumen enfoques que la definen como: procesos, técnicas, estrategias, procedimiento, prácticas, entre otros.

Según Venegas (2015), la gestión tecnológica permite manejar el factor tecnológico como aspecto estratégico en las organizaciones productivas, inicialmente se enfocó en la administración de ciencia y tecnología, por lo cual su definición podría concebirse en la administración de conocimiento para dinamizar un proceso productivo a través de la inclusión de enfoques de innovación el cual permite la predicción, la proyección y la prospección tecnológica.

Análisis de datos

El análisis de datos e información tiene como objetivo la toma de decisiones acertada y efectiva que permita optimizar las tendencias de uso de información basado en la transformación de registros en información útil mediante técnicas de recolección y procesamiento y análisis cuantitativo o cualitativo de los mismos (Cerillo, 2018).

Data center

Conocido también como centro de procesamiento de datos (CPD), y contiene los

recursos tecnológicos principales encargados de realizar la dispersión de servicios de TI al interior de la organización, así mismo permite la comunicación con el entorno externo.

Normalmente se mantienen en condiciones ambientales específicas, se encuentran aislados de la comunidad de usuarios internos y externos que hacen parte de la organización (Mintic, 2010).

Gestión de riesgos

La probabilidad de ocurrencia y sus consecuencias son los elementos que abarca la gestión del riesgo, sus factores pueden ser motivados por parámetros internos o externos y continuamente aportan seguridad a las empresas al contemplar escenarios futuros de posibles ocurrencias. Una adecuada gestión de riesgos se mantiene continuamente en un ciclo de validación y mejora continua de sus componentes (Almuiñas, 2016).

3. Metodología

La metodología aplicada garantizó el uso de procedimientos, técnicas y elementos de tipo deductivo que dio inicio con la comparación de modelos de gestión tecnológica permitiendo seleccionar el más adecuado y que estuviera enfocado en la optimización y soporte de los servicios de tecnologías de información. Posteriormente se realizó un levantamiento de activos de información, haciendo uso de diferentes mecanismos como revisiones de inventarios, inspección, y observación, con énfasis en la experiencia relacionada de los profesionales del grupo de sistemas de información y redes de la entidad de acuerdo a sus roles y responsabilidades, lo que dio origen al estado actual de componentes tecnológicos y sus servicios soportados, luego se identificaron los servicios críticos como parte del levantamiento de información para determinar sus características y así mismo definir prioridades de intervención teniendo en cuenta el impacto que se puede generar a raíz de fenómenos naturales para una adaptación como parte del proceso de aplicación del modelo de gestión tecnológica seleccionado.

Una vez conocido el contexto de la organización en los aspectos previamente mencionados, se aplicó y evaluó el modelo de gestión tecnológica, de acuerdo con esto se realizó un diagnóstico donde se generó una serie de recomendaciones y se incluyó un plan de recuperación de desastres que contribuye a la mejora en la capacidad, disponibilidad y continuidad en la operación de los servicios soportados por tecnologías de información y las comunicaciones.

La Figura 11 describe con claridad que los aspectos antes mencionados hacen referencia a un enfoque cualitativo, en donde la observación directa y el análisis deductivo de diferentes

elementos con los que cuenta la entidad en torno a la prestación de servicios soportados en TI, permitió el desarrollo de los objetivos propuestos y la aplicación de un modelo de gestión tecnológica que garantice que los sistemas de información, estén en un entorno seguro, organizado y fácilmente gestionable donde sea posible una recuperación de servicios y operación ante posibles desastres naturales o interrupciones de servicio.

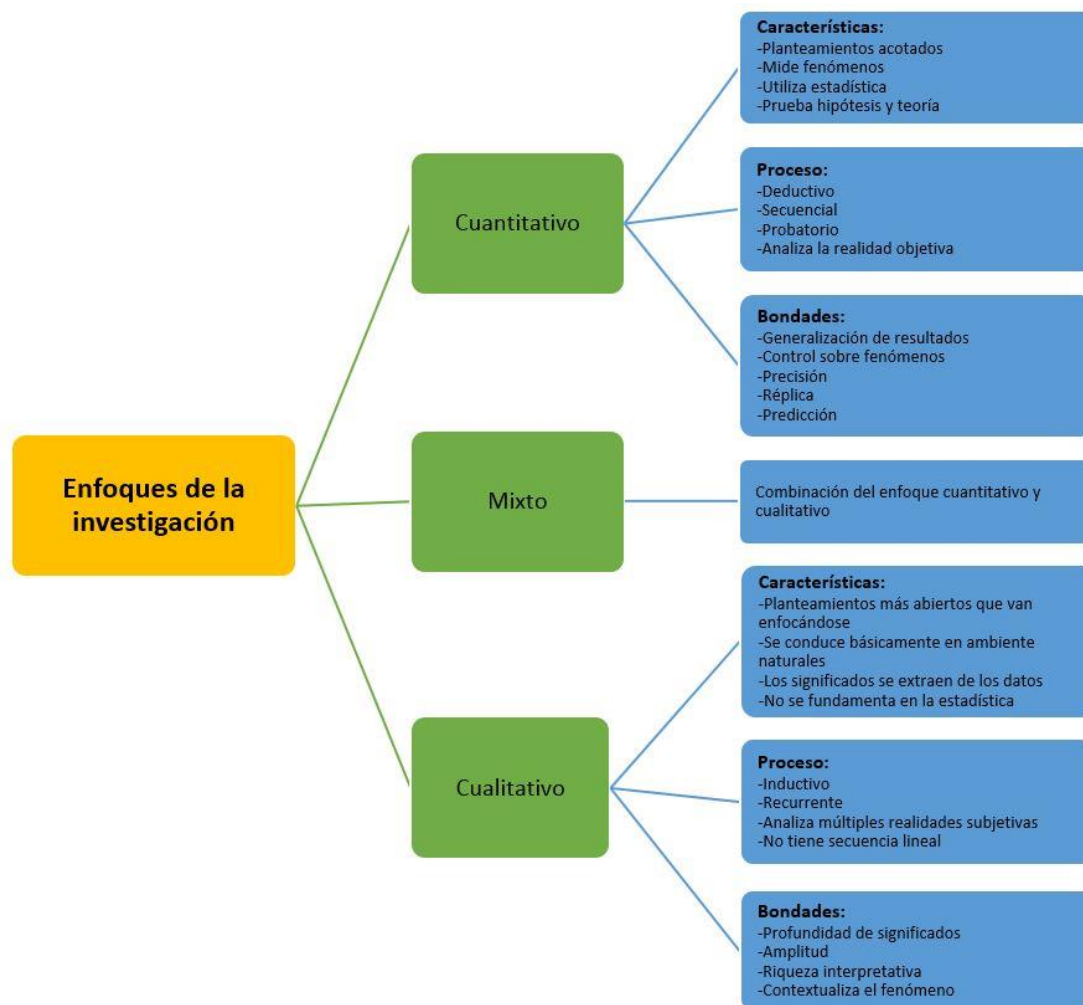


Figura 11. Enfoques de la investigación
Fuente: (Hernández, R., Fernández, C. y Baptista, P. ,2014)

3.1 Tipo y nivel de la Investigación

Debido a que se pretende hacer una descripción de factores, componentes y estrategias de manera estructurada, tomando información de diferentes fuentes y teniendo en cuenta detalles de cifras y/o datos, se definió un tipo de investigación cuantitativa (Hernández, R., Fernández, C. y Baptista, P. ,2014)

3.2. Diseño de la Investigación

Con base en la investigación planteada, la recolección de datos se realizó por medio de observación directa como instrumento de recolección principal, donde dadas las circunstancias en que uno de los proponentes del presente modelo desarrollado hace parte de la entidad, y más específicamente es integrante del grupo de sistemas de información y redes se recurrió a su observación teniendo en cuenta la experiencia en el área de más de 5 años.

De acuerdo con esto se recolectó la información del Instituto Nacional de Metrología (INM) con el fin de estudiar la problemática, identificar los activos críticos, conocer su naturaleza y definir su impacto, para de esta manera darle una solución a la necesidad identificada por medio de la aplicación de un modelo de gestión tecnológica.

Como se ha mencionado anteriormente, la recolección de datos realizada generó un análisis ante los posibles cambios a través del tiempo que pueda llegar a presentar la infraestructura tecnológica y servicios soportados de TI con los que cuenta la entidad. Se enmarcó la investigación en un carácter no experimental, donde la observación del comportamiento y necesidades tecnológicas de la entidad jugaron un papel clave en el desarrollo de la solución propuesta.

3.3 Fases de la Investigación

3.3.3 Fase I: Diagnóstico.

Con el propósito de identificar el estado actual, comportamiento, características, y en general los diferentes componentes que hacen parte de la infraestructura tecnológica de la entidad, así como la descripción detallada de sus servicios ofrecidos de cara al ciudadano y a nivel interno, se realizó una recopilación de información sistemática, que permitió definir un panorama global, donde se identificó aspectos clave para el desarrollo cotidiano de las actividades y servicios soportados en TI así como las diferentes estrategias con las que cuenta el Instituto Nacional de Metrología (INM) para administrar sus recursos tecnológicos, y mecanismos vigentes de respaldo de información.

3.3.1.1 Técnicas de recolección de datos.

La recolección de datos es un proceso fundamental para identificar el contexto de trabajo en el cual se aplicó el modelo de gestión tecnológica propuesto, por esta razón la técnica principal y más utilizada en el contexto de este proyecto es la recolección directa, ya que generó grandes beneficios en el análisis documental, y permitió un levantamiento de información preciso y acorde con las necesidades del proyecto.

Como técnica adicional y dadas las circunstancias en que uno de los proponentes del presente modelo desarrollado hace parte de la entidad, y más específicamente en el grupo de sistemas de información y redes se recurrió a la observación directa teniendo en cuenta la experiencia en el área de más de 5 años.

3.3.1.2 Instrumentos de recolección de datos.

Existen diferentes instrumentos de recolección de datos como listas de chequeo, entrevistas, formularios y demás elementos que permiten indagar, clasificar, almacenar e identificar características y elementos clave para el desarrollo del modelo planteado, sin embargo, para el desarrollo de este proyecto se estableció como soporte principal el análisis de contenido basado en la observación directa, y dado que uno de los integrantes del proyecto hace parte del grupo de sistemas de información y redes, lo cual permitió identificar mediante una serie de componentes registrados en el catálogo de servicios de la entidad, los elementos relacionados con la criticidad de servicios ofrecidos así como el respaldo de información y el entorno en que se desarrollan. Cabe aclarar que la situación de emergencia sanitaria COVID-19 limitó el uso de otros mecanismos de recolección de datos.

3.3.4 Fase II. Procesamiento de la información

3.3.2.1 Creación matriz de servicios críticos.

Para dar cumplimiento a los objetivos planteados en el proyecto, es necesaria la definición de una matriz que permitió el registro, identificación y clasificación de los activos críticos a nivel de software y hardware, que a su vez soportan los servicios misionales y estratégicos de la entidad, lo anterior, con el fin de ofrecer un panorama global acerca de los procesos y elementos que fueron objeto de intervención, para garantizar continuidad en los servicios como parte de la adaptación del modelo de gestión tecnológica seleccionado.

3.3.2.2 Identificación de elementos de recuperación de desastres.

La recuperación de desastres es un factor clave a nivel competitivo, ya que garantiza la continuidad de operación en cualquier circunstancia, así mismo es importante tener presente que todo

evento que cause una interrupción al normal desarrollo de actividades y prestación de servicios del negocio es considerado un desastre (villalobos,2008).

Con base en el contexto anterior, es necesario identificar los elementos descritos en la Figura 12 que minimicen el impacto que puede generar este tipo de interrupciones, por tal motivo dentro de la adaptación del modelo de gestión tecnológica, se identificaron los elementos necesarios para ofrecer continuidad en los servicios ante diferentes factores internos o externos como lo son fenómenos naturales que se puedan presentar. Por medio de la adopción de un plan de recuperación de desastres (DRP), mediante un documento se le indicó a la entidad el procedimiento a seguir en cuanto al restablecimiento de su operación.



Figura 12. Componentes del Plan de Recuperación ante Desastres
Fuente: (Romero, 2013)

3.3.5 Fase III: Desarrollo del Modelo de gestión Tecnológica

A partir de la selección del modelo de gestión tecnológica más adecuado para el Instituto Nacional de Metrología (INM), la recolección de información identificó los activos que posterior a un análisis, permitió establecer cuáles eran críticos, dando paso a la adopción del modelo de

gestión tecnológica basado en componentes de recuperación de desastres, para lo cual fue necesario tener en cuenta los siguientes pasos:

3.3.3.1 Análisis de información.

Se realizó el estudio y análisis de los modelos de gestión tecnológica más reconocidos con el fin de seleccionar el más adecuado para su adopción en el Instituto Nacional de Metrología (INM).

3.3.3.2 Inspección.

Se realizó una caracterización de los servicios de TI objetivo y los instrumentos de recolección de datos, para definir el contexto que permitió conocer e identificar los servicios y activos tecnológicos de la entidad.

3.3.3.3 Estructuración.

Se adaptó el modelo de gestión tecnológica basado en la identificación de elementos que lleve a la mejora en la operación de servicios de TI, en donde el levantamiento de información permitió a la construcción de una matriz de servicios críticos para la entidad.

3.3.3.4 Resultados.

El Instituto Nacional de Metrología (INM) recibió las recomendaciones dadas en el modelo de gestión tecnológica que le permita administrar de manera más eficiente la disponibilidad de los servicios críticos de TI y garantice que los sistemas de información, se preserven un entorno seguro, organizado y gestionable donde sea posible una recuperación de servicios y operación, ante posibles desastres naturales o interrupciones deliberadas de servicio.

4. Adaptación del modelo de gestión tecnológica

4.1 Comparación modelos de gestión tecnológica

En el **Anexo A** se ilustra el cuadro comparativo de los modelos de gestión definidos previamente, en el cual se describió su principio, alcance, ventajas y desventajas. Dicha comparación permitió elegir el modelo para el Instituto Nacional de Metrología (INM) que más se relacionó a las tecnologías y capacidades actuales de la entidad y sea un punto de inicio para su adaptación, el cual propenderá a una respuesta adecuada ante imprevistos y/o desastres naturales y así la tecnología esté debidamente preservada y se garantice un funcionamiento óptimo, balanceado y ajustado a las necesidades institucionales.

4.1.1 Selección del modelo de Gestión para el Instituto Nacional de Metrología (INM)

Posterior a la referencia de los modelos de gestión tecnológica y de conocimiento más relevantes, se concluyó luego del análisis de las bases teóricas, que la selección y adopción debería satisfacer las siguientes necesidades en el Instituto Nacional de Metrología (INM):

- Que el modelo examine el ciclo iterativo de aprendizaje del Instituto Nacional de Metrología (INM) en cuanto a tecnologías de información.
- Que el modelo seleccionado pueda aplicarse a proyectos específicos en el Instituto Nacional de Metrología (INM).
- Que el modelo seleccionado sea de fácil integración con los procesos y metodologías existentes en el Instituto Nacional de Metrología (INM).
- Que el modelo contenga un conjunto consolidado de aspectos relevantes en cuanto a gestión tecnológica se refiere.

- Que el modelo se adopte a las políticas y lineamientos establecidos por el gobierno nacional.
- Que el modelo cuente con la documentación y guías suficientes para su implementación ya sea de manera parcial o completa.

De acuerdo al análisis de cada uno de los alcances, ventajas y desventajas descritas en el **Anexo A**, el que resulta más adecuado y pertinente para el Instituto Nacional de Metrología (INM) es el Modelo de Gestión y Gobierno de TI, ya que es el que reúne todos requisitos en cuanto a flexibilidad, coherencia, versatilidad, se puede aplicar de manera parcial o completa según la disponibilidad con la que se cuente y finalmente el estado colombiano ofrece una gran variedad de información y guías. Todo esto permitirá adaptar el modelo de gestión tecnológica al alcance del proyecto y así entregar un valor agregado que contribuya además con el cumplimiento de las directrices en cuanto a tecnología de información que imparte el Gobierno Nacional por medio de MinTIC a través de la nueva política de Gobierno Digital a las entidades estatales como lo es el Instituto Nacional de Metrología (INM).

4.2 Levantamiento de información de los servicios soportados en tecnologías de información y su infraestructura tecnológica relacionada

El Instituto Nacional de Metrología (INM) es una entidad creada en el año 2011 a través del decreto 4175, y cumple la función de coordinar la metrología científica e industrial, mediante la prestación de servicios metrológicos, la trazabilidad de las mediciones acorde a los estándares internacionales y el desarrollo de actividades de ciencia tecnología e innovación (INM, 2018).

Así las cosas, para contar con los elementos necesarios para adaptar un modelo de gestión tecnológica y basado en la observación, en primera medida se debe realizar una caracterización que permita identificar el estado actual de los servicios y procesos asociados, así como la tecnología que los soporta. El Instituto Nacional de Metrología (INM) como se ilustra en la figura 13, define en su sitio web los servicios para los diferentes usuarios como son las entidades públicas, privadas y ciudadanía en general. Dado lo anterior se relacionan a continuación los servicios actualmente ofrecidos por la entidad y en capacidad de ser prestados:



Figura 13. Servicios Ofrecidos por el Instituto Nacional de Metrología (INM)
Fuente: (INM, 2018).

Descripción de los servicios:

Asistencia técnica: Servicio integral basado en asesorías metrológicas, evaluación de capacidades en metrología, ofrecimiento de cursos de formación específica y evaluación de capacidades en competencia técnica, este último dirigido a organismos nacionales de acreditación (INM, 2018).

Capacitación en Metrología: Este servicio según INM (2018) ofrece cursos en diferentes magnitudes y áreas de medición dictados por personal técnico altamente experimentado. Los cursos se dictan de manera presencial en la sede del Instituto Nacional de Metrología (INM) y algunos de ellos son:

- Metrología Básica
- Estadística Básica
- Incertidumbre de Medición
- Norma ISO/IEC 17025
- Norma ISO/IEC 10012
- Conceptos Básicos en Metrología Química

Calibración: Servicios de calibración de alta calidad y confiabilidad metrológica mediante patrones nacionales en las diferentes magnitudes. Calibración de instrumentos de medición en metrología física y química (INM, 2018).

Ensayos de Aptitud: Con este servicio evalúa la calidad de medición implementadas en los diferentes laboratorios de calibración a nivel nacional, mejorando aspectos de medición mediante el seguimiento continuo a sus operaciones (INM, 2018).

Producción, certificación y comercialización de materiales de referencia: Desarrollo y comercialización de materiales de referencia certificados que ofrecen un patrón de mediciones para entregar resultados más exactos asegurando la calidad y trazabilidad de los procesos relacionados con mediciones químicas y biológicas en el país (INM, 2018).

Hora legal de la república de Colombia: El Instituto Nacional de Metrología (INM) se encarga de generar y difundir la hora legal colombiana a través de su laboratorio de tiempo y frecuencia donde mediante diferentes equipos de medición y relojes de átomos de Cesio se define el segundo que sustenta la hora legal colombiana (INM, 2018).

Guías de calibración: La entidad ofrece diferentes técnicas para asegurar la trazabilidad metrológica, en este caso el servicio es ofrecido en conjunto con el Organismo Nacional de Acreditación (ONAC) ofreciendo guías de calibración para diferentes instrumentos de medición de magnitudes físicas (INM, 2018).

Luego de la anterior descripción de servicios y plataformas ofrecidos por la entidad a continuación en las tablas 3, 4 y 5 se identifican los componentes tecnológicos que soportan parte de estos servicios y que se ubican en el Datacenter de la entidad recordando que únicamente existe una sede, en esta clasificación se tienen en cuenta 3 aspectos para la descripción de infraestructura:

- **Redes y seguridad:** en la siguiente tabla se describen los componentes y sus principales características para este aspecto.

Tabla 3

Redes y seguridad

Componente	Administración Tercerizada	Alta Disponibilidad
Firewall	NO	NO
Solución WAF	NO	SI
Solución Anti DDOS	NO	NO
Switch Core	NO	NO
Switch de distribución	NO	NO

Nota. Elaboración propia

Adicional a los servicios hacia el ciudadano, es importante mencionar las principales plataformas aplicaciones y software con los que cuenta la entidad de acuerdo con lo descrito en la tabla 4:

Tabla 4

Plataformas aplicaciones y software

Nombre	Ubicación	Observación
Kactus - HCM	Datacenter-Servidores INM	Software de nómina
Isolucion	Datacenter-Servidores INM	Software para administración del sistema integrado de gestión
BPmetro	Datacenter-Servidores INM	Software de aplicación BPM (Business process Management)

Open Manager	Datacenter-Servidores INM	Software de monitoreo de infraestructura tecnológica
Software Ofimático	Portal de licenciamiento por volumen - Microsoft	versiones 2013 y 2016
Software de calibración	Laboratorios - INM	Software especializado para atender la demanda de servicios metrológicos
Directorio Activo	Datacenter-Servidores INM	Basado en sistemas operativos Windows server 2012 R2
Página Web	Datacenter-Servidores INM	incluye portal de servicios en línea.
Sitio Web de la hora legal	Laboratorios - INM	Desarrollo propio con difusión desde el laboratorio de tiempo y frecuencia

Nota. Elaboración propia

Tabla 5

Servidores (Linux y Windows)

Servidor	Tipo	Descripción	Sistema operativo	Ubicación
1	FISICO	Servidor Principal Dominio	Windows Server 2012 R2	DATACENTER
2	VIRTUAL	Servidor Archivos	Windows Server 2012 R2	DATACENTER

3	FISICO	Servidor de virtualización Nodo 1 Cluster	Windows Server 2012 R2	DATACENTER
4	FISICO	Servidor de virtualización Nodo 2 Cluster	Windows Server 2012 R2	DATACENTER
5	FISICO	Hora legal 2	Linux –Suse 12.0	LAB-TIEMPO Y FRECUENCIA
6	VIRTUAL	Aplicación Biblioteca digital-INM	Windows Server 2012 R2	DATACENTER
7	FISICO	Servidor Symantec Backup Cintas	Windows Server 2008R2	DATACENTER
8	VIRTUAL	Servidor aplicación-Wsus	Windows Server 2012 R2	DATACENTER
9	VIRTUAL	Servidor Intranet	Windows Server 2012 R2	DATACENTER
10	VIRTUAL	Aplicación Metrored RCM	Linux- Ubuntu Server	DATACENTER
11	VIRTUAL	Metrored-Ambiente de pruebas	Linux – Ubuntu Server	DATACENTER
12	VIRTUAL	Aplicación Help Desk	Windows Server 2012 R2	DATACENTER
13	FISICO	Servicio de Impresión y DHCP	Windows Server 2012 R2	DATACENTER
14	FISICO	Servidor Hora legal	Linux Red Hat 5.0	DATACENTER
15	VIRTUAL	Servidor Open Manager Monitoreo TI	Windows Server 2012 R2	DATACENTER
16	VIRTUAL	Aplicativos Mincit	Linux Red Hat 5.0	DATACENTER
17	VIRTUAL	Aplicaciones Automatización	Windows Server 2012 R2	DATACENTER
18	VIRTUAL	Replica controlador de dominio	Windows Server 2012 R2	DATACENTER
19	FISICO	Host de virtualizacion linux	Linux Red Hat 7.3	DATACENTER
20	VIRTUAL		Linux Red Hat 7.3	DATACENTER

		Servidor Aplicaciones Radicación de documentos		
21	FISICO	Administración MCAFEE	Windows Server 2012 R2	DATACENTER
22	VIRTUAL	Servidor de Archivos 2	Windows Server 2012 R2	DATACENTER
23	FISICO	Almacenamiento SAN	N/A	DATACENTER
24	VIRTUAL	Control de climatización	Windows Server 2012 R2	DATACENTER
25	VIRTUAL	Aplicaciones Elearning	Windows Server 2012 R2	DATACENTER
26	VIRTUAL	Kactus Pruebas	Windows Server 2012 R2	DATACENTER
27	VIRTUAL	Kactus Producción	Windows Server 2012 R2	DATACENTER
28	VIRTUAL	Isolucion Producción	Windows Server 2012 R2	DATACENTER
29	VIRTUAL	Isolucion Pruebas	Windows Server 2012 R2	DATACENTER
30	VIRTUAL	Bases de datos SQL	Windows Server 2012 R2	DATACENTER
31	VIRTUAL	Aplicación BPM Producción	Windows Server 2016	DATACENTER
32	VIRTUAL	Aplicación BPM Pruebas	Windows Server 2012 R2	DATACENTER
33	VIRTUAL	Srv-Telefonia	Windows Server 2016 R2	DATACENTER

Nota. Elaboración propia

De igual manera es importante ilustrar por medio de la figura 14 el panorama global de la distribución de los activos tecnológicos al interior de la entidad, razón por la cual el diagrama de red resulta ser de gran utilidad.

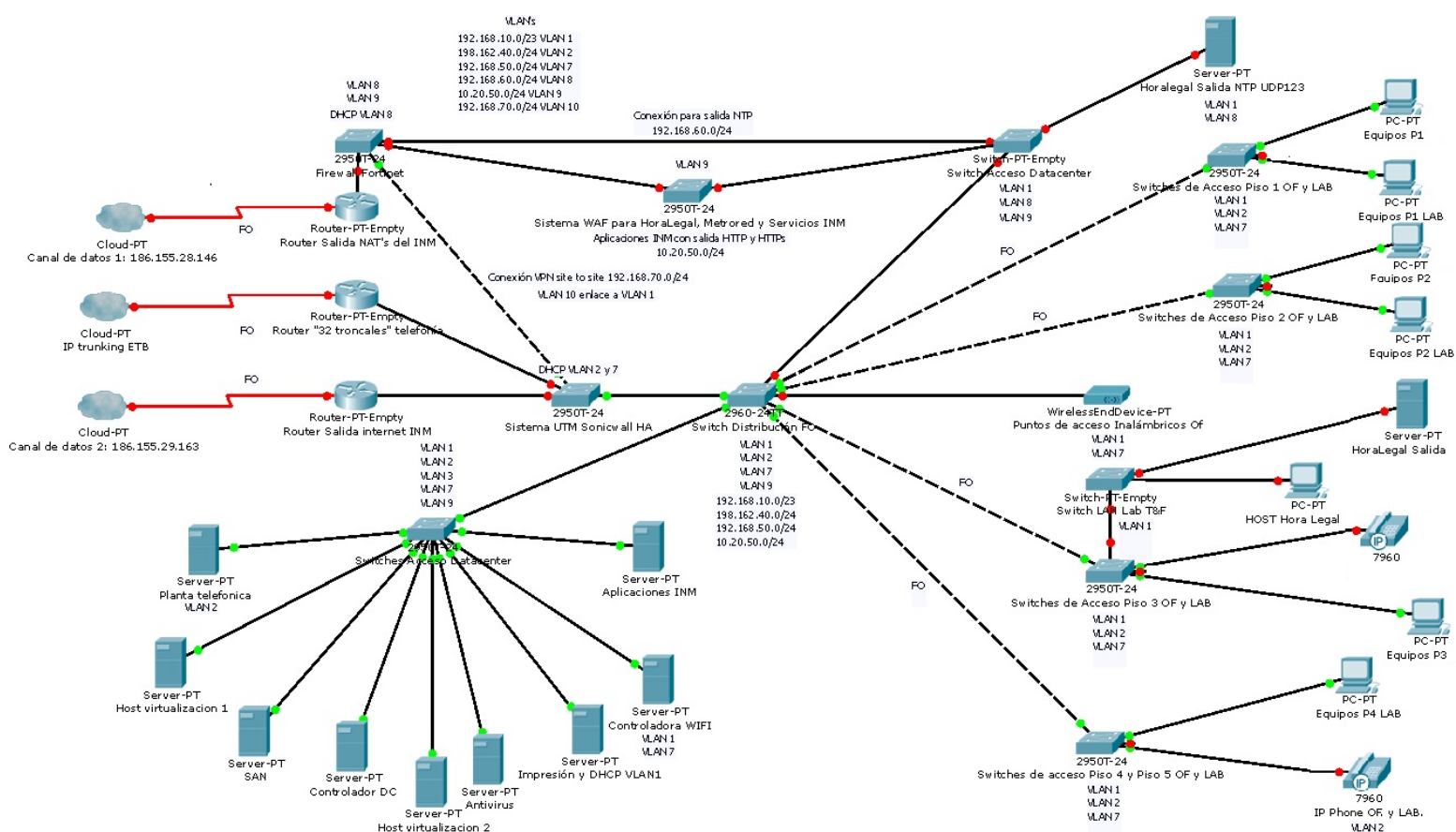


Figura 14. Diagrama general de activos tecnológicos

Fuente: Propia, basado en la información del grupo de sistemas de información y redes de la entidad.

4.3 Matriz de servicios críticos de información recopilada en el Instituto Nacional de Metrología (INM)

Para determinar la criticidad de servicios en el Instituto Nacional de Metrología (INM) es necesario aplicar elementos de la norma ISO/IEC 27001, donde existe una relación directa con el modelo de seguridad y privacidad de la información dado por MinTIC para las entidades públicas, permitiendo identificar de manera clara y precisa algunos elementos clave para esta clasificación entre los que se encuentran:

Activos de Información:

Con base en la norma ISO/IEC 27000 un activo de información representa todo aquello que tiene valor para la organización y que, a su vez, requiere de protección.

De igual manera, Según Dutton (2016) los activos de información representan cualquier pieza o colección de información que se almacena como parte del patrimonio organizacional en donde es posible gestionarla y protegerla de manera adecuada y dada su necesidad no es posible remplazar sin que estos tengan impactos en factores como costo, habilidades, recursos o tiempo.

Sin embargo, cuando estos activos alcanzan cierto nivel de importancia se convierten en activos críticos y a su vez se dice que pueden estar en forma estructurada (bases de datos), semi estructurada (Archivos de diferente tipo) o sin estructura definida, de igual manera estos activos descritos en la Tabla 6 pueden ser clasificados en varios tipos.

Tabla 6

Tipos de activos de información

Tipos de Activos de información	
Hardware y activos físicos	Todo dispositivo físico que pueda manipular información y haga parte de la organización. (Servidores, computadores, dispositivos móviles)
Software	Diferentes herramientas de desarrollo, sistemas operativos, aplicaciones, etc.
Información	Esta puede ser de tipo digital (USB, discos duros bases de datos, audios, video, etc) o física como la que se almacena en papel.
Servicios	Estos activos son todos los que generan dependencia a la organización, energía, backups, suministros de servicios públicos
Personas	Son todos aquellos empleados, gerentes y directivos que conocen la operación y objetividad de la compañía
Intangibles	Hacen parte de estos activos la imagen corporativa, propiedad intelectual, marca, entre otros.

Fuente: (ISO/IEC 27005, 2008).

Complementando los elementos anteriormente descritos y según Dutton (2016) es preciso mencionar que otro elemento importante para definir la criticidad de servicios en la entidad es el **nivel de impacto**, el cual viene dado por 3 factores principales y su nivel de compromiso de los mismos, estos factores son: **Confidencialidad, Integridad y disponibilidad.**

Esta clasificación de información determinará los activos a intervenir dada su criticidad teniendo en cuenta que la misma se enfoca en los servicios críticos y su infraestructura tecnológica utilizada como soporte.

Con base en lo anterior, es preciso definir el método de evaluación de riesgos, el cual como ya se había mencionado esta soportado con la familia de las normas ISO/IEC 27000 donde

de esta manera es posible obtener el valor de los mismos enfocados en la continuidad del negocio aún bajo condiciones de operación o ambientales extremas.

Específicamente la ISO/IEC 27005 ofrece una gestión de riesgos con un enfoque de seguridad de la información en donde surgen elementos como la **Matriz de probabilidad e impacto**, que combina diferentes aspectos, en este contexto es posible observar en la tabla 7 los niveles de riesgo asociados a los activos de información determinando su criticidad. Para dar continuidad a este aspecto se realiza el siguiente levantamiento de riesgos asociados a la prestación de servicios tecnológicos:

Tabla 7

Riesgos identificados

Ítem	Tipo de Riesgo	Riesgo	Descripción	Posibles consecuencias	Origen Natural
1	Externo/Interno	Corte de energía	Falla red eléctrica, que alimenta a los servidores, equipos de comunicaciones.	Inoperatividad de los servidores y equipos de comunicaciones y de acceso. Desconexión de la red.	Si
2	Interno	Falla en la UPS	Falla equipo de respaldo eléctrico	Interrupción del servicio de interconexión momentáneamente.	No
3	Interno	Falla en equipos de ventilación	Temperatura no adecuada	Baja el desempeño de los equipos de comunicaciones a la red	No
4	Externo/Interno	Inundaciones	Agua en las instalaciones	Daño total del equipamiento y desconexión de la red	Si
5	Externos	Terremotos	Eventos naturales	Daño total del equipamiento y Desconexión de la red.	Si
6	Externo/Interno	Incendios	Fuego en las instalaciones	Daño total del equipamiento y Desconexión de la red	No

7	Interno	Desconexiones físicas del Datacenter	Corte de cable accidental, cable desconectado o en mal estado	Desconexión de la red Intermitencia de servicios	No
8	Interno	Corte de servicio en servidores internos	Servicios no disponibles	Usuarios no obtendrán el acceso a servicios	No
9	Externo	Corte de servicio en servidores externos	Servicios Web y DNS no disponibles	Usuarios externos no tendrán acceso web y pérdida de navegación web para usuarios internos.	No
10	Interno	Saturación de carga en el enlace	Por sobrecarga de tráfico el servicio colapsa	Pérdida de desempeño hasta posible desconexión de la red.	No
11	Externo	Interrupción servicio de Internet	Falla en el acceso al servicio de internet	Operaciones que necesiten internet para efectuarse se ven afectadas. Posible desconexión de la red, debido a que el mismo equipo físico provee ambos servicios.	Si
12	Externo/Interno	Interrupción Firewall	Falla en el equipo de filtrado de contenido, no HA	Desconexión hacia servidores y hacia Internet	No
13	Interno	Acceso no autorizado a servidor de aplicaciones	Acceso de usuarios, sin permiso, a la configuración de los servidores	Desconexión de la red Pérdida de información	No

Nota. Elaboración propia

Es importante aclarar que la entidad cuenta con una única sede ubicada en la ciudad de Bogotá y actualmente no hay servicios en nube que respalden la infraestructura actual de la entidad ni sitios alternos, los únicos respaldo con los que cuenta la entidad es a nivel de canal de

internet y sistema eléctrico, con una UPS que soporta toda la carga eléctrica de la entidad cuando se presentan cortes en el suministro de energía, así las cosas la autonomía con la que se cuenta es limitada, de ahí la importancia de adaptar un modelo de gestión tecnológica donde se articulan diversas tecnologías y nuevos procesos que permiten generar un entorno más seguro, organizado y fácilmente gestionable en capacidad de ofrecer continuidad de servicios y operación ante posibles desastres naturales o interrupciones de servicio inesperadas.

Así mismo se elabora en la tabla 8 los activos de información asociados a TI con los que cuenta el Instituto Nacional de Metrología (INM) actualmente, acorde con los tipos de activos mencionados anteriormente:

Tabla 8

Activos de información

Tipo de Activo	Nombre	Código
Información	Documentos Internos	INF_01
	Información compartida en carpetas en Red	INF_02
	Contratos	INF_03
	Material físico (Impreso)	INF_04
	Manuales de Instalación	INF_05
	Manuales de usuario	INF_06
	Manuales Técnicos	INF_07
Servicios	Internet	SER_01
	Red Inalámbrica	SER_02
	Telefonía	SER_03
	Fluido Eléctrico	SER_04
	Almacenamiento de Información	SER_05

	Soporte tecnológico	SER_06
Software	Antivirus	SOF_01
	Desarrollos propios	SOF_02
	Licencias Office	SOF_03
	Portal Web	SOF_04
	Autocad	SOF_05
	Matlab	SOF_06
	Project	SOF_07
	Sistemas Operativos	SOF_08
	Licencias varias	SOF_09
Hardware y activos físicos, Infraestructura TI	Servidores	HAR_01
	Routers	HAR_02
	Equipos de computo	HAR_03
	Terminales Telefónicas	HAR_04
	Impresoras	HAR_05
	Access Point	HAR_06
	Cámaras de seguridad	HAR_07
	Infraestructura física	HAR_08
	Canalización red eléctrica	HAR_09
	Instalación red eléctrica	HAR_010
	Canalización red de datos	HAR_11
	Instalación red de datos	HAR_012
Personal	Usuarios Internos	PER_01
	Expertos Técnicos	PER_02
	Funcionales	PER_03
	Clientes	PER_04
	Proveedores	PER_05

Nota. Elaboración propia

Dada la información anterior, se procede en la Tabla 9 a realizar una clasificación de estos activos con base en los criterios de Confidencialidad [C], Integridad [I] y Disponibilidad [D] como principios fundamentales de la información:

Tabla 9

Clasificación de criticidad

Criterio	Dimensión
Confidencialidad	C
Integridad	I
Disponibilidad	D

Nota. Elaboración propia

Complementando esta clasificación se establecen ciertos criterios de valoración descritos en la figura 15 para facilitar el posterior análisis de criticidad enmarcado por colores:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Figura 15. Niveles de clasificación
Fuente: (MinTIC, 2016)

Complementando lo anterior y con base en la ISO/IEC 27001 es necesario estipular en la Tabla 10 el rango de niveles, que permita totalizar los aspectos de confidencialidad, integridad y disponibilidad para los activos descritos para posteriormente crear los 3 rangos correspondientes para cada caso.

Tabla 10

Crterios de valoración de activos

Criterio	Valor	Nivel
Grave	Alto	9-10
Importante	Medio	5-8
Menor	Bajo	1-5
Irrelevante a efectos prácticos	Despreciable	0

Nota. Elaboración propia

Con base en la información recopilada hasta el momento se procede en la Tabla 11 con la valoración de activos integrando los diferentes elementos mencionados hasta el momento.

Tabla 11

Valoración de activos de información

Activo	C	I	D	Total
Documentos Internos en físico	10	9	10	29
Información compartida de carpetas en Red	10	10	10	30
Contratos	7	8	10	25

Material publicitario físico (Impreso)	5	8	8	21
Manuales de Instalación	8	9	10	27
Manuales de Sistemas de gestión	8	10	9	27
Manuales Técnicos	8	9	10	27
Servicio Internet	7	9	10	26
Red Inalámbrica	7	10	9	26
Telefonía	6	8	8	22
Fluido Eléctrico	7	10	10	27
Servidores de Archivo (File Servers)	10	10	10	30
Soporte tecnológico	8	8	8	24
Antivirus	9	10	10	29
Firewalls	9	10	10	29
Office	7	6	8	20
Portal Web	10	10	10	30
Servidores aplicaciones internas	10	10	10	30
Servidores de aplicaciones externas	10	10	10	30

Periféricos varios	6	8	8	22
Licencias Sistemas Operativos	8	10	10	28
Licencias varias	8	8	8	24
Switchs oficinas	9	9	8	26
Routers	10	10	9	29
Equipos de computo	9	9	10	28
Terminales Telefónicas	8	8	8	24
Impresoras	7	6	8	20
Access Point	10	10	8	28
Cámaras de seguridad	10	10	9	29
Infraestructura física	8	8	10	26
Redes eléctricas	5	7	10	23
redes de datos	6	7	10	23
Usuarios Internos	8	10	8	26
Expertos Técnicos	9	10	8	27
Clientes	5	10	8	23
Proveedores	8	10	9	27

Nota. Elaboración propia

Partiendo del anterior análisis, en la tabla 12 se realiza el cruce de activos críticos con los servicios impactados y que a su vez son ofrecidos por el Instituto Nacional de Metrología (INM), para determinar su criticidad.

Tabla 12.

Matriz de servicios críticos y su relación con activos de información.

Activo	C	I	D	Total	Servicios Críticos Impactados
Información compartida en carpetas en Red (File servers)	10	10	10	30	Manejo de información de recursos compartidos al interior de la entidad
Servicio Internet	7	9	10	26	Aplicaciones de cara al público Servicio Hora legal Capacitaciones y cursos en línea de metrología, contacto en general con la ciudadanía
Antivirus	9	10	10	29	Sincronización con las últimas bases de firmas de antivirus
Firewalls	9	10	10	29	Servicios de red internos y externos
Portal Web	10	10	10	30	Información general de la entidad
Servidores aplicaciones internas	10	10	10	30	Desarrollo de procesos internos soportado en TI
Servidores de aplicaciones externas	10	10	10	30	Servicio de Hora Legal, cursos Virtuales, servicios de solicitud de calibraciones
Routers	10	10	9	29	Intercomunicación interna

Cámaras de seguridad	10	10	9	29	Monitoreo general de la infraestructura física de la entidad
----------------------	----	----	---	----	--

Nota. Elaboración propia

Con base en el desarrollo anterior, es claro que activos de información son claves para la operación de la entidad y como estos impactan en determinados servicios soportados en TI. Con estos insumos se creará el documento “Procedimiento plan de recuperación ante desastres” el cual se presenta como **Anexo B** al presente documento.

4.4 Aplicación del modelo de gestión tecnológica del Instituto Nacional de Metrología (INM)

4.4.1 Política de gobierno digital

Según Gdigital (2019), es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”. Los propósitos para la implementación de la política de Gobierno Digital, están orientados hacia la satisfacción de necesidades y solución de problemáticas tanto en el estado como en los ciudadanos siendo, los propósitos de la política los siguientes:

Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad:

Consiste en poner a disposición de ciudadanos, usuarios y grupos de interés, trámites y servicios del Estado que cuenten con esquemas de manejo seguro de la información, que estén alineados con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI) y que hagan uso de los servicios de autenticación electrónica, interoperabilidad y carpeta ciudadana, a fin de que éstos sean ágiles, sencillos y útiles para los usuarios (Gdigital, 2019).

Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información: Consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información y de la alineación con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI) (Gdigital, 2019).

Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la

información: Consiste en mejorar la toma de decisiones por parte de la entidad, ciudadanos, usuarios y grupos de interés, para impulsar el desarrollo de servicios, políticas, normas, planes, programas, proyectos o asuntos de interés público, a partir del uso y aprovechamiento de datos que incorporan estándares de calidad y seguridad (Gdigital, 2019).

Empoderar a los ciudadanos a través de la consolidación de un estado abierto:

Consiste en lograr una injerencia más efectiva en la gestión del Estado y en asuntos de interés público por parte de ciudadanos, usuarios y grupos de interés, para impulsar la gobernanza en la gestión pública, a través del uso y aprovechamiento de las tecnologías digitales (Gdigital, 2019).

Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de Tecnologías de la Información y las

Comunicaciones: Consiste en promover el diseño y la implementación de iniciativas de tipo social, ambiental, político y económico, por parte de entidades públicas y diferentes actores de la sociedad, para el mejoramiento de la calidad de vida de los ciudadanos e impulsar el desarrollo sostenible, a través del uso y aprovechamiento de las TIC de manera integrada y proactiva (Gdigital, 2019).

4.4.2 Elementos de la política Gobierno Digital

Para Gdigital (2019), la implementación de la Política de Gobierno Digital según lo descrito en la figura 14, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos se desarrollan a través de lineamientos y estándares, que son los requerimientos mínimos

que todos los sujetos obligados deben cumplir para alcanzar los logros de la política, estos elementos se articulan de la siguiente forma:



Figura 16. Elementos de la política de gobierno digital.
Fuente: (Gdigital, 2019)

4.4.3 Modelo de Gestión y Gobierno de TI

Para que sea posible construir el modelo de gestión tecnológica en el Instituto Nacional de Metrología (INM) y se enfatice en la política de Gobierno Digital, es necesario enfocarse en uno de sus tres elementos transversales de la política y es el de Arquitectura Empresarial, este permitirá el fortalecimiento de sus capacidades institucionales y de gestión en tecnologías de información, ya que el habilitador de arquitectura soporta su uso e implementación en el marco de referencia del estado, siendo este el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que la entidad debe realizar para dar cumplimiento a los lineamientos y políticas del Gobierno Nacional (Gdigital, 2019).

Para hacer uso del instrumento de arquitectura empresarial del estado, en (MGGTIG, 2019) se encuentra disponible el documento de referencia denominado “Documento Maestro del

Modelo de Gestión y Gobierno de TI”, el cual contiene los dominios y lineamientos, las guías que componen el modelo de gestión, las evidencias que se deben generar y los procesos que permiten gestionar TI de forma adecuada.

El Modelo de Gestión y Gobierno de TI permite generar capacidades institucionales de TI que se requieren para prestar servicios a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones, el cual es mantenido por MinTIC y orienta a las entidades públicas a generar las capacidades de gestión y gobierno de TI, para ofrecer un mejor contexto, en la figura 15 se observa donde está ubicado el Modelo de Gestión y Gobierno de TI dentro la política de Gobierno Digital y cuál es su alcance como habilitador transversal.

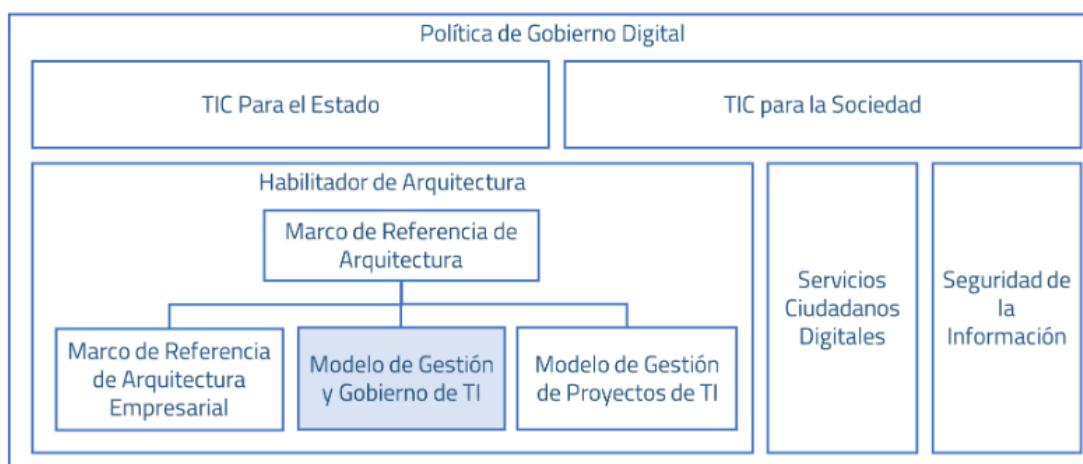


Figura 17. Estructura de la política de gobierno digital.
Fuente: (MGGTIG, 2019)

Dicho documento está compuesto por seis dominios que permitirá alinear las necesidades del Instituto Nacional de Metrología (INM) mediante el uso adecuado de las tecnologías de la información, los dominios del Modelo de gestión y gobierno de TI, según (MGGTIG, 2019) son:

Dominio de Estrategia de TI: El dominio de estrategia de TI contiene los elementos necesarios para orientar a las áreas de TI a realizar una planeación estratégica de TI que habilite los procesos de la entidad mediante el uso adecuado de las TIC.

Dominio de gobierno de TI: Contiene los elementos para orientar a las entidades en la construcción de un esquema de gobierno que le permita direccionar la toma de decisiones para gestionar las tecnologías de la información.

Dominio de sistemas de información: Contiene los elementos para orientar a las entidades en la gestión del ciclo de vida de los sistemas de información.

Dominio de información: Contiene los elementos para orientar a las entidades en la gestión del ciclo de vida de los componentes de información.

Dominio de infraestructura de TI: Contiene los elementos para orientar a las entidades en la correcta gestión del ciclo de vida de la infraestructura de TI.

Dominio de uso y apropiación: Contiene los elementos para orientar a las entidades en asegurar el uso y apropiación de la tecnología y la información por parte de los interesados.

4.4.4 Evaluación indicadores de cumplimiento del modelo de gestión y gobierno de TI

El modelo de gestión y gobierno de TI, entrega las reglas generales que le permitirán al Instituto Nacional de Metrología (INM) planear y organizar las tecnologías de la información

desde una perspectiva integral, por medio del enfoque de arquitectura empresarial como habilitador y alineado a las definiciones de la gestión pública con las mejores prácticas y tendencias aplicables a la gestión de tecnologías.

Una vez se realiza la contextualización del modelo de gestión y gobierno de TI, el siguiente paso en su construcción consiste en la realización de un diagnóstico por medio de un mecanismo de medición de indicadores sugerido en el manual de gobierno digital, como parte de su implementación en las entidades del estado frente al cumplimiento de los dominios y lineamientos que integran modelo de gestión y gobierno de TI, siendo los objetivos de este diagnóstico:

- Determinar el estado actual del Instituto Nacional de Metrología (INM) respecto del cumplimiento de los lineamientos definidos por el modelo de gestión y gobierno de TI.
- Identificar la brecha existente entre la situación actual del Instituto Nacional de Metrología (INM) respecto del cumplimiento de los lineamientos del modelo de gestión y gobierno de TI y el estado futuro deseado, el cual implica la adopción y cumplimiento de la totalidad de los lineamientos del modelo, así como la implementación de procesos mejora continua.

Para la ejecución del ejercicio de diagnóstico se utilizó para el Instituto Nacional de Metrología (INM) un cuestionario de 23 preguntas a través de las cuales se evalúa el cumplimiento o no de las directrices establecidas por cada uno de los dominios del modelo de gestión y gobierno de TI, para cada una de las preguntas evaluadas, en donde había varias opciones de respuesta y una fórmula para determinar el cumplimiento de cada y así realizar la medición de cumplimiento de cada uno de los dominios del modelo. El **Anexo C** presenta el

cuestionario del instrumento de diagnóstico elaborado para la evaluación de cumplimiento en Instituto Nacional de Metrología (INM) respecto modelo de gestión y gobierno de TI, así como las respuestas obtenidas a cada una de las preguntas formuladas en las cuales se indica el cumplimiento de cada una de ellas.

Acorde a la metodología de implementación y medición de la política propuesta en el manual de gobierno digital en cada uno de los habilitadores de arquitectura correspondiente al modelo de Gestión y gobierno de TI, estos se evaluaron acorde al avance actual en el Instituto Nacional de Metrología (INM) por medio de tres grados de clasificación:

Entorno de desarrollo robusto: Corresponde a cuando el dominio objeto de evaluación, ha sido, implementado, medido y apropiado de acuerdo a las directrices adoptadas en el modelo de gestión tecnológica.

Entorno de desarrollo Intermedio: Corresponde a cuando el dominio objeto de evaluación, evidencia avances considerables y/o significativos, además se encuentra en proceso de implementación de acuerdo a las directrices adoptadas en el modelo de gestión tecnológica.

Entorno de desarrollo incipiente: Corresponde a cuando el dominio objeto de evaluación, se encuentra en evaluación y aún no ha contemplado para su proceso de implementación de acuerdo a las directrices adoptadas en el modelo de gestión tecnológica.

De acuerdo con esto, por medio de un cuadro de control se hace uso de un sistema de alerta temprana en este caso de tres colores para los grados de clasificación, donde se representa de forma visual el estado actual del nivel de cumplimiento por dominio del modelo de Gestión y gobierno de TI, la Figura 18 presenta la escala de colores empleada.

Sistema de Alerta Temprana		
0% al 33%	34% al 66%	67% al 100%

Figura 18. Escala de cumplimiento del modelo de gestión tecnológica
Fuente: Propia

Según la escala de color definida, los dominios con un nivel de cumplimiento insipiente igual o inferior al 33% tendrán color rojo, color amarillo para aquellos dominios con un nivel de cumplimiento intermedio entre 34% y 66% y finalmente, verde para aquellos dominios con un nivel de cumplimiento robusto que oscile entre el 67% y 100%.

Por otro lado, con el objetivo de poder medir el grado de cumplimiento del Instituto Nacional de Metrología (INM) respecto del modelo de gestión y gobierno de TI, se diseñó una escala de cumplimiento a través del cual es posible medir el porcentaje de avance de la entidad de cada uno de los seis dominios que lo integran, consolidando a través de este instrumento los resultados individuales de cada una de las 23 preguntas evaluadas para los indicadores de cumplimiento.

La tabla 13 presenta el tablero de control de cumplimiento del del modelo de Gestión y gobierno de TI de Instituto Nacional de Metrología (INM), con los resultados de la medición efectuada como producto de la aplicación del diagnóstico.

En esta medición se destaca que el “*Porcentaje de cumplimiento por dominio*”, el cual consolida los resultados de cumplimiento, permitiendo al Instituto Nacional de Metrología (INM) tener una vista general del avance del modelo a través de cada uno de los dominios que lo integran.

Tabla 13.

Cumplimiento dominios modelo de gestión y gobierno de TI

Tablero de cumplimiento de los dominios del modelo de Gestión y gobierno de TI					
ID	Dominio	Pregunta asociada a la variable medida	Porcentaje cumplimiento o por pregunta	Nivel de desarrollo	Porcentaje cumplimiento dominio
1	ESTRATEGIA DE TI	¿Cuál es el estado del Plan Estratégico de TI (PETI) en la entidad?	70%	Robusto	46%
2		¿El Plan Estratégico de TI (PETI) en el Instituto Nacional de Metrología (INM) incluye?	50%	Intermedio	
3		¿Con respecto al seguimiento del PETI el Instituto Nacional de Metrología (INM)?	20%	Incipiente	
4		Indique el porcentaje de cumplimiento de los objetivos estratégicos del PETI, con respecto a lo planeado para la última vigencia	30%	Incipiente	
5		Con respecto a la Arquitectura Empresarial el Instituto Nacional de Metrología (INM)	50%	Intermedio	
6		Frente a la documentación de la Arquitectura Empresarial en el Instituto Nacional de Metrología (INM)	50%	Intermedio	
7		En relación con el catálogo de servicios de TI, el Instituto Nacional de Metrología (INM)	50%	Intermedio	
8	GOBIERNO DE TI	Señale los aspectos incorporados en el esquema de gobierno de TI del Instituto Nacional de Metrología (INM)	83.3	Robusto	70.8
9		Con respecto a la optimización de las compras de TI, el Instituto Nacional de Metrología (INM)	50%	Intermedio	
10		Frente a la gestión integral de proyectos de TI, el Instituto Nacional de Metrología (INM)	50%	Intermedio	
11		Frente a la gestión de la operación de TI, el Instituto Nacional de Metrología (INM)	100%	Robusto	

12	INFORMACION	Con relación a la gestión y planeación de los componentes de información el Instituto Nacional de Metrología (INM)	16,60%	Incipiente	11.1%
13		Frente a la calidad de los componentes de información, el Instituto Nacional de Metrología (INM) realizó	16,60%	Incipiente	
14		Frente al análisis y aprovechamiento de los Componentes de Información, el Instituto Nacional de Metrología (INM)	0%	Incipiente	
15	SISTEMAS DE INFORMACION	Frente a la planeación y gestión de los sistemas de información, el Instituto Nacional de Metrología (INM)	25%	Incipiente	38.3%
16		Frente al soporte de los Sistemas de Información el Instituto Nacional de Metrología (INM)	50%	Intermedio	
17		Frente al Ciclo de vida de los Sistemas de Información el Instituto Nacional de Metrología (INM)	40%	Intermedio	
18	SERVICIOS TECNOLÓGICOS	Frente al soporte de los servicios tecnológicos en el Instituto Nacional de Metrología (INM)	40%	Intermedio	52.2%
19		Frente a la operación de servicios tecnológicos en el Instituto Nacional de Metrología (INM)	10%	Incipiente	
20		Frente a la Gestión de la calidad de los Servicios Tecnológicos en el Instituto Nacional de Metrología (INM)	33,3%	Incipiente	
21		¿ El Instituto Nacional de Metrología (INM) en qué fases de la adopción de IPV6 se encuentra trabajando?	50%	Intermedio	
22		¿Qué documentación ha adelantado el Instituto Nacional de Metrología (INM) en la adopción de IPV6?	37,5%	Intermedio	
23	USO Y APROPIACION DE TI	Frente a la Estrategia para el Uso y Apropiación de TI en el Instituto Nacional de Metrología (INM)	28,5%	Incipiente	28,5%

Nota. Elaboración propia, basada en el documento “Manual de Gobierno Digital”

Los resultados mostrados previamente para el Instituto Nacional de Metrología (INM) permite evidenciar los dominios y su grado de avance, siendo Gobierno de TI el que presenta un entorno de desarrollo robusto, para Servicios Tecnológicos, Estrategia de TI y Sistemas de Información que presentan un entorno de desarrollo intermedio y aquellos dominios con niveles de avance muy bajos, que corresponden de Información e Uso y Apropiación, los cuales evidencian un entorno de desarrollo incipiente.

Es importante aclarar que el hecho de obtener un porcentaje de avance incipiente en los dominios de información y Uso-Apropiación no necesariamente implica que el Instituto Nacional de Metrología (INM), ejecute gestión alguna sobre dichos dominios sino puede significar que:

- Las acciones ejecutadas no se encuentran dentro de los lineamientos definidos por el modelo de gestión y gobierno de TI para los dominios evaluados.
- Las acciones ejecutadas no son suficientes para cumplir de forma parcial o total en los dominios evaluados.
- Que el Instituto Nacional de Metrología (INM) no tenía conciencia de la necesidad de implementar las acciones para el cumplimiento de lo establecido en los dominios.

En conclusión, los resultados finales de la medición de los indicadores de cumplimiento del modelo de gestión y gobierno de TI, permitieron identificar la situación actual o grado de evolución del Instituto Nacional de Metrología (INM), respecto del cumplimiento de lo que establece cada uno de los dominios, así como, la brecha existente entre dicha situación actual y la situación futura deseada, correspondiente a la implementación de la totalidad de los lineamientos definidos en cada uno de los dominios del modelo de gestión y gobierno de TI.

4.4.5 Estrategia para cubrir la brecha del modelo de gestión y gobierno de TI

Posterior al diagnóstico de los indicadores de cumplimiento del modelo de gestión y gobierno de TI que contribuyen a la implementación de la política de gobierno digital que está alineada con las iniciativas de TI sectoriales, el plan estratégico institucional, el plan estratégico sectorial y el plan nacional de desarrollo, se generará una serie de recomendaciones por cada dominio para el Instituto Nacional de Metrología (INM), como resultado de la ejecución de esta evaluación que contribuya a la implementación del modelo de gestión y gobierno de TI.

Dichas recomendaciones deberían ser incluidas en la programación de la implementación del modelo de gestión y gobierno de TI, la cual debe emplear el documento maestro del modelo de arquitectura empresarial publicado por el MinTIC, Ahora bien, tal como se mencionó anteriormente el Instituto Nacional de Metrología (INM) deberá llevar a cabo la planeación respectiva, con el objetivo de iniciar la implementación del modelo como paso siguiente a su construcción, no obstante eso, y con el objetivo de obtener avances en la adopción del modelo, al Instituto Nacional de Metrología (INM) se le llevará a cabo un análisis orientado a identificar las recomendaciones específicas necesarias a ejecutar para poder cubrir la brecha de cumplimiento identificada como resultado del diagnóstico de indicadores de cumplimiento previamente realizado.

El enfoque empleado para la identificación de recomendaciones en aras del cubrimiento de la brecha, corresponde a listar todos los dominios del modelo y generar las recomendaciones necesarias por cada uno de ellos, para incrementar el porcentaje de cumplimiento.

4.4.5.1 Recomendaciones dominio Estrategia de TI

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de Estrategia para el modelo de gestión y gobierno de TI.

- Actualizar, documentar, oficializar e implementar el Plan Estratégico de Tecnologías de Información (PETI) del Instituto Nacional de Metrología (INM), el cual debe tener una duración de 4 años y estar ajustado a la vigencia del plan nacional de desarrollo y estar alineado con la estrategia de TI de la entidad y con la sectorial.
- Construir la estrategia de TI que esté orientada a generar valor y a contribuir al logro de los objetivos e integrar los proyectos de TI definidos en los planes de funcionamiento e inversión y resulten ser un habilitador de arquitectura empresarial.
- Integrar un plan de comunicación de la estrategia, las políticas, proyectos, resultados y servicios de TI de la entidad.
- Definir indicadores y un tablero de control para medir el avance y resultados en el desarrollo del plan estratégico de TI de la entidad.
- Mantener y actualizar el catálogo de servicios el cual contemple los acuerdos de nivel de servicios ANS y ser socializado por las áreas interesadas en el Instituto Nacional de Metrología (INM).

4.4.5.2 Recomendaciones dominio Gobierno de TI

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de Gobierno para el modelo de gestión y gobierno de TI.

- Identificar las capacidades de TI que actualmente no están siendo gestionadas por el grupo de sistemas de información y redes del Instituto Nacional de Metrología (INM).
- Implementar la gestión de las capacidades de TI que actualmente no están siendo gestionadas por el grupo de sistemas de información y redes del Instituto Nacional de Metrología (INM) y puede ser ejecutada a través del servicio de planes de capacidad.
- Identificar los recursos y talento humano necesarios para gestionar las capacidades de la organización de TI que actualmente no son gestionadas por el grupo de sistemas de información y redes del Instituto Nacional de Metrología (INM).
- Adquirir los recursos y talento humano necesarios para gestionar las capacidades de la organización de TI que actualmente no son gestionadas y priorizadas por el grupo de sistemas de información y redes del Instituto Nacional de Metrología (INM).
- Construir una base de conocimiento que permita registrar y hacer disponible todo el conocimiento que sea susceptible de ser transferido por un tercero al Instituto Nacional de Metrología (INM).
- Crear una política de gestión integral de proyectos de TI que garantice el liderazgo de las partes interesadas y se logre una adecuada transferencia de conocimiento.

4.4.5.3 Recomendaciones dominio Información

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de información para el modelo de gestión y gobierno de TI.

- Identificar en el Instituto Nacional de Metrología (INM) los criterios de calidad de componentes de información que deben ser tenidos en cuenta en cada uno de los procesos misionales y estratégicos de la entidad.
- Generar y divulgar un plan de calidad de componentes de información que permita a los procesos garantizar, que sobre sus componentes de información se agrega valor en las actividades de los procesos.
- Implementar una estrategia de divulgación de los mecanismos que permiten a los consumidores de los componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información.
- Realizar un plan para la implementación del registro de logs en todos los aplicativos del Instituto Nacional de Metrología (INM).
- Realizar una revisión de la capacidad, la operación y los servicios de los principales sistemas de información que soportan la operación del Instituto Nacional de Metrología (INM) con criterios de calidad, seguridad, disponibilidad, continuidad, adaptabilidad, estandarización y eficiencia.
- Crear un comité en la entidad que permita implementar, medir y evaluar controles de calidad en los componentes de información.
- Gestionar que los sistemas de información incorporen aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.

4.4.5.4 Recomendaciones dominio Sistemas de Información

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de Sistemas de Información para el modelo de gestión y gobierno de TI.

- Documentar el proceso de gestión del ciclo de vida de aplicaciones de software en el Instituto Nacional de Metrología (INM), y una vez documentado, hacerlo oficial y ejecutarlo en operación.
- Realizar la definición de características funcionales y no funcionales necesarias para la apertura de sus datos en los sistemas de información del Instituto Nacional de Metrología (INM)
- Implementar ambientes independientes y controlados destinados para desarrollo, pruebas, operación, certificación y capacitación de los sistemas de información y ampliar la capacidad que se tiene en el Instituto Nacional de Metrología (INM).
- Incorporar dentro del plan de pruebas para la aceptación de los sistemas de información de la entidad y su posterior autorización de paso a producción, todos los criterios no funcionales y de calidad de los sistemas actuales y nuevos de la entidad.
- Identificar los faltantes de documentación de usuario, técnica y de operación de la totalidad de los sistemas de información presentes en el catálogo de sistemas de información del Instituto Nacional de Metrología (INM).

4.4.5.5 Recomendaciones dominio Servicios Tecnológicos

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de Servicios Tecnológicos para el modelo de gestión y gobierno de TI.

- Realizar una revisión de la capacidad, la operación y los servicios de los principales sistemas de información que soportan la operación del Instituto Nacional de Metrología (INM) con criterios de calidad, seguridad, disponibilidad, continuidad, adaptabilidad, estandarización y eficiencia.
- Llevar a cabo la actualización del catálogo de servicios de TI del Instituto Nacional de Metrología (INM), incluyendo el inventario de todos los servicios prestados actualmente por la entidad, así como la identificación y definición del nivel de caracterización de los servicios con la información requerida. Este catálogo debe incluir tanto la información, como los sistemas de información y los servicios tecnológicos de la entidad.
- Generar un proyecto para el Instituto Nacional de Metrología (INM) que permita la adopción de IPV6, que contemple capacitación, transición, el direccionamiento, planes de contingencia, diseños detallados acorde a su infraestructura, activación y puesta en marcha de esta tecnología.

4.4.5.6 Recomendaciones dominio Uso y Apropiación de TI

A continuación, se lleva a cabo la definición de un conjunto de recomendaciones dirigidas al Instituto Nacional de Metrología (INM) con el objeto de facilitar la correcta adopción e implementación del dominio de Uso y Apropiación para el modelo de gestión y gobierno de TI.

- Definir, formalizar y documentar un plan de gestión del cambio por medio de un comité donde se consignen las actividades, responsables, objetivos, alcance, recursos, indicadores y demás aspectos del mismo para motivar el uso y apropiación de los sistemas de información en el Instituto Nacional de Metrología (INM).
- Establecer un esquema de incentivos en los funcionarios y contratistas que alineado con la estrategia de uso y apropiación, movilice a grupos de interés en el Instituto Nacional de Metrología (INM) para adoptar satisfactoriamente los nuevos proyectos de TI.

Finalmente, como resultado de este ejercicio para cubrir la brecha existente, se logra una lista de 28 recomendaciones que podrían ser integradas al portafolio de proyectos, a los planes de acción o al plan estratégico de la Entidad, y se espera que estas sean priorizadas e incluidas en el mapa de ruta la entidad para dar cumplimiento a lo establecido en la política de gobierno digital. De igual manera, se planteó un conjunto de acciones concretas que podrán ser ejecutadas con la priorización que disponga el Instituto Nacional de Metrología (INM), y se logre la completa implementación de aquellos dominios del modelo de gestión y gobierno de TI que actualmente se encuentran con cumplimiento incipiente o intermedio.

4.4.6 Elementos de recuperación de desastre para los servicios críticos de la entidad soportados en tecnologías de información

Complementando la adaptación de modelo de gestión tecnológica propuesto, y basados en el análisis de información del estado actual de la entidad, los procesos, procedimientos e infraestructura tecnológica con la que cuenta actualmente el Instituto Nacional de Metrología (INM) se genera un primer acercamiento a los planes de recuperación ante desastres, para lo cual se define el **Anexo C** de este proyecto denominado “**Plan de Recuperación de desastres**”.

Este procedimiento contempla los escenarios descritos en la tabla 14 para los cuales se establece una serie de actividades, roles y responsabilidades que facilitan la recuperación de los servicios ofrecidos por la entidad a la ciudadanía, generando valor para la organización.

Tabla 14.

Descripción de escenarios

Escenario	Descripción	Causas
1	Afectación en Datacenter principal- Indisponibilidad de centro de computo	<ul style="list-style-type: none"> • Terremotos • Inundaciones incendios • Fallas en sistema de aire acondicionado • Fallas en suministro eléctrico
2	Afectación en infraestructura de comunicaciones	Presencia de fallas en: <ul style="list-style-type: none"> • Fibras ópticas de conexión Internas • Firewall Principal • Switch Core • Router Core • Enlace de internet con el ISP

3	Afectación en infraestructura de servidores	Presencia de fallas en: <ul style="list-style-type: none"> • Servidor Hora legal colombiana • Servidor Cursos virtuales Elearning. • Servidor servicios de calibración • Servidores controladores de dominio principal y secundario • Servidor Aplicaciones Kactus • Servidor de Aplicaciones Isolucion • Servidor de aplicaciones BPM
4	Afectación en infraestructura de Almacenamiento.	Presencia de fallas en: <ul style="list-style-type: none"> • Sistema de almacenamiento SAN. • Servidor de Bases de datos • Borrados y/o perdidas de datos masivos • Corrupciones de bases de datos • Servidores de respaldo de información

Fuente: Elaboración Propia

El Plan de Recuperación de desastres, busca orientar al Instituto Nacional de Metrología (INM) en la forma en que debe prepararse y enfrentar posibles desastres naturales y sus consecuencias o fallas extremas en su infraestructura de TI que soporta los servicios críticos para la entidad, el cual es un entregable de alto valor estratégico para la entidad objeto de adaptación del modelo de gestión tecnológica propuesto.

Conclusiones

El Instituto Nacional de Metrología (INM) cuenta ahora con un modelo de gestión tecnológico, adaptado a sus necesidades que le permite identificar claramente sus activos tecnológicos críticos y la relación de estos con los servicios ofrecidos a la ciudadanía, lo que da origen a nuevas estrategias que fortalecerán la disponibilidad y continuidad de operación, aportando al cumplimiento de la misión institucional.

El levantamiento de información y la clasificación de servicios críticos soportados en TI, permitió valorar los activos de información con los que cuenta la entidad en cuanto aspectos de integridad, confidencialidad y disponibilidad, aportando a la toma de decisiones efectiva para garantizar las capacidades de la infraestructura tecnológica con miras al cumplimiento de sus objetivos misionales.

La selección del modelo de gestión y gobierno de TI para el Instituto Nacional de Metrología (INM), permitió una articulación con la política de Gobierno Digital del estado colombiano, que dispuso de mecanismos que contribuyeron a facilitar la identificación y tratamiento de los servicios críticos en los procesos operativos y misionales, contribuyendo a la mejora de la capacidad, disponibilidad y continuidad en la operación de la entidad.

La evaluación del modelo de Gestión y Gobierno de TI por medio del diagnóstico realizado, permitió determinar en qué procesos el Instituto Nacional de Metrología (INM) está realizando una correcta gestión de TI, con un esquema de gobierno definido para la toma de decisiones en el cual se contemple la administración del ciclo de vida en los sistemas de información y en su infraestructura, asegurando una adecuada apropiación de la tecnología, y

con base en los resultados obtenidos, la entidad opte por las recomendaciones sugeridas que contribuirán al mejoramiento y el cumplimiento en los dominios del modelo de gestión.

Por medio del plan de recuperación de desastres entregado, el Instituto Nacional de Metrología (INM) es posible mantener la continuidad en la prestación de sus servicios misionales soportados en TI aun después de condiciones extremas como las derivadas de desastres naturales, ya que identifica los elementos clave tanto a nivel de infraestructura tecnológica como a nivel de procesos, personal y toma de decisiones que deben ser ejecutadas en una situación de crisis para mantener la operación en todo momento beneficiando a la ciudadanía en general y generando valor para la organización.

La metodología aplicada generó información clave para el desarrollo de los objetivos propuestos, ya que permitió a través de elementos como el análisis documental y la observación directa identificar componentes claves para garantizar la correcta selección y adopción de un modelo, que garantice que la entidad esté preparada para afrontar posibles desastres naturales y sus consecuencias en cuanto a la prestación de servicios soportados en TI.

Como aporte a la disciplina es importante mencionar que la gestión adecuada de la tecnología en articulación con los objetivos misionales de una organización, garantiza la generación de valor tanto a nivel interno como externo, como se evidenció en el desarrollo del presente proyecto, donde fue posible establecer mediante la adopción de un modelo de gestión tecnológica, el estado actual de servicios críticos soportados en TI, así como una serie de recomendaciones que permitan soportar una posible situación de pérdida de información o interrupción en la prestación de servicios originada por desastres naturales o alteraciones en la normalidad de operacional de tecnologías de información y las comunicaciones.

En cuanto a las limitaciones de la investigación, se presentaron factores que no fue posible controlar en las diferentes etapas del desarrollo del proyecto, la emergencia sanitaria provocada por el COVID-19 limitó en cierta medida los mecanismos de recolección de información, ya que el aislamiento social y el teletrabajo estuvieron presentes durante la etapa final de este proyecto, lo que generó una reducción significativa en las visitas físicas a la entidad objeto de análisis así como a sus áreas tecnológicas principales, (Datacenter, cuartos de cableado, laboratorios). Sin embargo, esta misma situación desarrolló avances tecnológicos en cuanto a diferentes medios de reunión y plataformas virtuales que permitieron cumplir con los objetivos propuestos y entregar un resultado de gran valor para la organización que cubre aspectos estratégicos y técnicos para el desarrollo y la continuidad de su operación y servicios misionales.

Como recomendaciones a la investigación previo a la adaptación del modelo de gestión tecnológica como mecanismo articulador entre la estrategia y la gestión de tecnologías de información en el Instituto Nacional de Metrología (INM) y partiendo del instrumento de diagnóstico de cumplimiento del modelo de gestión y gobierno de TI, de manera periódica se recomienda en la entidad, registrar el avance obtenido y generar los soportes que sirvan como evidencia del cumplimiento de lineamientos en cada uno de los dominios, adicionalmente se debería llevar a cabo mecanismos que faciliten el entendimiento y contextualización del modelo, de qué se trata, sus objetivos, alcance, beneficios y sinergias con los demás elementos que integran la política de Gobierno Digital para las entidades del estado.

A continuación, se presentan algunos trabajos que pueden desarrollarse posteriormente, como resultado de este proyecto aplicado de adaptación, que por exceder el alcance de los objetivos no fue posible abordarlos, entre los trabajos futuros se destacan:

- Diseñar una metodología de seguimiento, revisión y actualización periódica del grado de evolución del Instituto Nacional de Metrología (INM) para la adopción e implementación de los lineamientos establecidos en el modelo de gestión y gobierno de TI.
- Implementar el modelo de gestión y gobierno de TI en su fase TO-BE, para el desarrollo de capacidades internas en los dominios de estrategia, gobierno, información, sistemas de información, servicios tecnológicos, infraestructura, uso y apropiación.
- Generar un plan de acción del ejercicio del modelo de gestión y gobierno de TI para el Instituto Nacional de Metrología (INM), teniendo en cuenta los lineamientos definidos por el Marco de Referencia de Arquitectura Empresarial para la gestión de TI definido por MinTIC.
- Construir una herramienta de diagnóstico y desempeño del modelo de gestión y gobierno de TI que registre el avance obtenido, se evidencie el cumplimiento y la evolución de los lineamientos implementados en el Instituto Nacional de Metrología (INM).

Referencias bibliográficas

- Almuiñas Rivero, J. L., & Galarza López, J. (2016). Dirección estratégica y gestión de riesgos en las universidades. *Revista Cubana de Educación Superior*, 35(2), 83–92. Recuperado de <http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=123236864&lang=es&site=eds-live>.
- Andersen, A. (1999). *El Management en el Siglo XXI*. Buenos Aires: Granica.
- Armenteros A, M. del C. *et al.* (2012). Las prácticas de gestión de la innovación en las micro, pequeñas y medianas empresas: resultados del estudio de campo en piedras negras coahuila, méxico. *Revista Internacional Administración & Finanzas*, Volumen 5., 29–50. Recuperado de http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954074
- Barranco, J. (2016). *Gestión de la innovación y la tecnología en la empresa*. Madrid: Fundación COTEC. Recuperado de http://informecotec.es/media/B06_Inf_Ges_Inn_Tec_Emp.pdf.
- Cepal, (2019). Comisión Económica para América Latina y el Caribe (Cepal). Cepal.org. Recuperado de https://www.cepal.org/sites/default/files/presentations/2018-06-2areu-expertos-ea-4_2-cepal-pleonard.pdf.
- Cerrillo-Martínez, A. (2018). Datos Masivos Y Datos Abiertos Para Una Gobernanza Inteligente. *El Profesional de La Información*, 27(5), 1128–1135. Recuperado de <https://bibliotecavirtual.unad.edu.co:2444/10.3145/epi.2018.sep.16>.

Chen, 2006; Johnson *et al.*, 2006. Una perspectiva de evaluación basada en la teoría sobre la investigación de métodos mixtos. *Investigación en las escuelas*, 13(1), 75-83 , 33(7), 14-26.

ConocimientoMinTIC. (2018). Gestiondelconocimiento.mintic.gov.co. Recuperado de, https://gestiondelconocimiento.mintic.gov.co/714/articles-100726_recurso_1.pdf.

DNP. (2015). Cifras de desastres naturales entre 2006 y 2014. Dnp.gov.co. Recuperado de <https://www.dnp.gov.co/Paginas/3-181-muertos,-21-594-emergencias-y-12,3-millones-de-afectados-las-cifras-de-los-desastres-naturales-entre-2006-y-2014-.aspx>.

Dutton, J. (2016). Identifying assets for conducting an asset-based information security risk assessment. Londres, Reino Unido. Portal Vigilant Software

Echeverry, c. E. M., trujillo, m. L., & duque, f. J. V. (2017). Gobierno y gestión de ti en las entidades públicas. (spanish). *Ad-minister*, (31), 75. Recuperado de <http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=128066255&lang=es&site=eds-live>.

EVA. (1989). Ley 9 de 1989 - EVA - Función Pública. Funcionpublica.gov.co. Recuperado de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1175>.

Farfán Buitrago, D. Y., Garzón Castrillón, M. A. (2006). La gestión del conocimiento.

Documentos de investigación, 29. Recuperado de:

<http://repository.urosario.edu.co/bitstream/handle/10336/1207/BI%2029.pdf?sequence=1>

Fuentes (2019). Metodología para toma de decisiones gerenciales en infraestructuras IT.

Universidad EAN. Recuperado de

<https://repository.ean.edu.co/bitstream/handle/10882/9552/FuentesWilber2019.pdf?sequence=1>.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et Technica*, 22(2), 193–197.

Recuperado de

<http://ez.urosario.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129781870&lang=es&site=eds-live&scope=site>.

Gdigital (2019). Estrategia.gobiernoenlinea.gov.co. Recuperado de

https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

Google Maps (2019). Instituto Nacional de Metrología, recuperado de:

<https://www.google.com/maps/place/Instituto+Nacional+De+Metrolog%C3%ADa+De+Colombia/@4.6431178,-74.0945688,17z/data=!3m1!4b1!4m5!3m4!1s0x8e3f9bc68e0a0c67:0xdbf6f58ef91d094c!8m2!3d4.6431178!4d-74.0923801?hl=es>

Hernández, R., Fernández, C. y Baptista, P. (2014). Metodología de la investigación (6ª ed.).

México: McGraw Hill Education.

- HYOGO. (2005). Marco de Acción de Hyogo 2005-2015 - Dirección General de Protección Civil y Emergencias. Proteccioncivil.es. Recuperado de http://www.proteccioncivil.es/busqueda?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=319016&_101_type=content&_101_urlTitle=marco-de-accion-de-hyogo-2005-2015&inheritRedirect=true.
- INM. (2018). Portafolio de servicios - Instituto Nacional de Metrología - INM. Instituto Nacional de Metrología - INM. Recuperado de <http://www.inm.gov.co/servicios/portafolio-de-servicios/>
- ISO/IEC 27001. (2013). Norma Internacional ISO/IEC 27001. ISO. Recuperado de <https://www.iso.org/standards.html>.
- ISO/IEC 27005. (2008). Norma Internacional ISO/IEC 27005. ISO. Recuperado de <https://www.iso.org/standards.html>.
- ISO/IEC 22301. (2012). Norma Internacional ISO/IEC 22301. ISO. Recuperado de <https://www.iso.org/standards.html>.
- ISO/IEC 24762. (2008). Norma Internacional ISO/IEC 24762. ISO. Recuperado de <https://www.iso.org/standards.html>.

ISO/IEC 18044. (2004). Norma Internacional ISO/IEC 18044. ISO. Recuperado de <https://www.iso.org/standards.html>.

ISO/IEC 27031. (2017). Norma Internacional ISO/IEC 27031. ISO. Recuperado de <https://www.iso.org/standards.html>.

Jaimes, Ramírez, Vargas y Carrillo (2011). Estado del arte vigilancia tecnológica: una aplicación para la innovación. Volumen 10. Número 27. Mayo – Agosto.

Jaramillo, R. (2012). Diseño de un sistema de gestión del conocimiento para la Dirección de Servicios y Recursos de Información de la Universidad Icesi. Recuperado de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/handle/10906/66936.

J. González, Joaquín, & Collazos. (2009). KARAGABI KMMODEL: Modelo de referencia para la introducción de iniciativas de gestión del conocimiento en organizaciones basadas en conocimiento KARAGABI KM

Khalil, T. M. (2000). Management of Technology: The Key to Competitiveness and Wealth Creation.

Landaeta, R. P., & Aure, N. G. (2002). La gestión del conocimiento organizativo.

Ley1581. (2012). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. Secretariassenado.gov.co. Recuperado de http://www.secretariassenado.gov.co/senado/basedoc/ley_1581_2012.html.

López, J. D. O., & Castillo, J. N. P. (2002, noviembre 30). Un Modelo para Aplicar Gestión del Conocimiento en las Organizaciones. Ingeniería. Recuperado de

<http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/2689/3871>.

Mendoza, J., & Valenzuela, A. (2014). Aprendizaje, innovación y gestión tecnológica en la pequeña empresa: Un estudio de las industrias metalmecánica y de tecnologías de información en Sonora. *Contaduría Y Administración*, 59(4), 253–284.

[https://doi.org/10.1016/S0186-1042\(14\)70162-7](https://doi.org/10.1016/S0186-1042(14)70162-7)

MGGTIG, (2019). Documento Maestro del Modelo de Gestión y Gobierno de TI. Recuperado de

https://www.mintic.gov.co/arquiturati/630/articles-144767_recurso_pdf.pdf

MinTIC. (2010). Guía para la preparación de las TIC para la continuidad del negocio.

Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

MinTIC. (2016). Guía de gestión de riesgos. Mintic.gov.co. Recuperado de

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

MinTIC. (2017). Guía de Arquitectura empresarial. Recuperado de

https://www.mintic.gov.co/arquiturati/630/propertyvalues-8158_descargable_1.pdf.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge creating company*. New York: Oxford

Artículo universitario.

Ortiz & Nagles. (2014). Las unidades de la inteligencia: Conocimiento en el Diseño de Políticas Científicas y Tecnológicas. *Memorias del IX Seminario Latino- Iberoamericano de*

Gestión Tecnológica.

- Odremán R., J. (Diciembre de 2014). GESTIÓN TECNOLÓGICA: ESTRATEGIAS DE INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA EN LA INDUSTRIA . Recuperado de <http://www.scielo.org.ve/pdf/uct/v18n73/art04.pdf>.
- Ospina, S. (1993). Gestión, política pública y desarrollo social: hacia la profesionalización de la gestión pública. Gestión Y Política Pública, II.
- PNPAD. (1997). CONPES 2948 de 1997. Colaboracion.dnp.gov.co. Recuperado de <https://colaboracion.dnp.gov.co/CDT/CONPES/Econ%C3%B3micos/2985.pdf>.
- PNGRD. (2012). Política nacional de gestión del riesgo de desastres. Secretariassenado.gov.co. Recuperado de http://www.secretariassenado.gov.co/senado/basedoc/ley_1523_2012.html.
- Quintero Marín, E. (2018). Modelo de gestión tecnológica para apoyar y fortalecer los procesos de enseñanza - aprendizaje en el Instituto Técnico La Cumbre de Floridablanca - Santander. Colombia: Recuperado de: <http://hdl.handle.net/10596/20819>.
- Robledo, J., Gómez, F., & Restrepo, J. F. (2008). Relación entre capacidades de innovación tecnológica y desempeño empresarial en Colombia. Memorias I Congreso Internacional De Gestión Tecnológica E Innovación, 1.
- Romero Jairo A, (2013). Propuesta para el Diseño del Plan de recuperación de desastres DRP. Recuperado de: <http://repository.ucatolica.edu.co/jspui/bitstream/10983/1322/1/DISE%C3%91O%20E>
- Sampieri, r; Collado, C & Lucio, M. (2014). Metodología De la investigación. Sexta Edición. McGraw-Hill. ISBN: 978-607-15-0291-9 (de la edición anterior). México. Recuperado

de: <http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf>.

Sánchez, D., Gutiérrez, J., Robledo, J., & Rueda, J. (2014). Estudios económicos sectoriales[Ebook] (1st ed., p. SIC). Bogotá. Recuperado de:

http://www.sic.gov.co/recursos_user/documentos/estudio_metrologia_2014.pdf.

Solleiro, J., & Castañon, R. (2016). Gestión tecnológica, Modelos y Prácticas. Recuperado de

<http://cambiotec.org.mx/site/wp-content/uploads/2017/09/E-Libro-Gestio%CC%81n-2.pdf>.

SNPAD. (1988). Idea.manizales.unal.edu.co. Recuperado de

http://idea.manizales.unal.edu.co/sitios/gestion_riesgos/descargas/legislacion/ley_46_88.pdf.

Tapias García, H. (2000). Gestión tecnológica y desarrollo tecnológico. Revista Facultad de Ingeniería.

UAECD. (2016). Propuesta para el diseño del plan de recuperación de desastres DRP.

Repository.ucatolica.edu.co. Recuperado de

<https://repository.ucatolica.edu.co/bitstream/10983/14044/4/Proyecto%20Final.pdf>

Ucatolica. (2016). Diseño del plan de recuperación de desastres (D.R.P) para la compañía agencia de aduanas profesional siap nivel 1 sede Bogotá. Repository.ucatolica.edu.co.

Recuperado de

<https://repository.ucatolica.edu.co/bitstream/10983/13914/4/TRABAJO%20DE%20GRADO.pdf>.

UNGRD. (2011). Creación de la Unidad Nacional para la Gestión del Riesgo de Desastres.

Wp.presidencia.gov.co. Recuperado de

<http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/DECRETO%20147%20DEL%203%20DE%20NOVIEMBRE%20DE%202011.pdf>.

UPC. (2019). Diseño de un plan de recuperación de desastres DRP para el Centro de Cómputo de

la sede principal de una entidad educativa superior del sector privado basado en la norma

NISTSP 800-34 Recuperado de

https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625709/yarleque_ga.pdf?sequence=1&isAllowed=y

Venegas, R. (2015). Enfoques de innovación en las organizaciones [Ebook]. San Jerónimo:

Universidad Internacional. Recuperado de

<https://www.uandina.edu.pe/descargas/investigacion/ayuda/eoi-gestion-tecnologia-2012.pdf>.

Velázquez, A., Dominguez, D., & Andrade, M. (2018). Las capacidades tecnológicas para la

innovación en empresas de manufactura. Recuperado de

<https://revistas.urosario.edu.co/xml/1872/187243745011/index.html>.

VSAMCC. (2003). CONPES 3242 de 2003. Minambiente.gov.co. Recuperado de

http://www.minambiente.gov.co/images/normativa/conpes/2003/Conpes_3242_2003.pdf

Villalobos, J. S (Enero de 2008). <http://www.uci.ac.ar/> Recuperado de

<http://www.uci.ac.cr/Biblioteca/Tesis/PFGMAP505.pdf>

Anexos

Anexo A

(Modelos de Gestión Tecnológicas aplicables a la entidad)

Modelos de Gestión tecnológica aplicables al Instituto Nacional de Metrología (INM)

Nombre	Definición y alcance	Ventajas	Desventajas
Modelo Nacional de gestión de tecnología	Armenteros (2012), define como una integración entre las actividades que se realizan en una organización junto con el desarrollo y la innovación tecnológica. Así mismo se tiene en cuenta los resultados que genere este tipo de gestión en la empresa.	Permite identificar amenazas y oportunidades de desarrollo e innovación tecnológica. Permite desarrollar un marco estratégico tecnológico. Vigila habilita, planea y protege el patrimonio tecnológico.	No evidencia enfoques de integración de tecnología con los objetivos organizacionales. Posee un componente de obtención de recursos lo cual no aplica por el alcance del proyecto. El plan tecnológico no está integrado a políticas gubernamentales.

<p>Modelo gestión tecnológica COTEC</p>	<p>De acuerdo con Barranco (2016), se destaca la importancia de la gestión tecnológica en la organización y su relación cercana con los procesos de innovación y propone elementos claves en la gestión exitosa de una estrategia tecnológica o el desarrollo de nuevos productos.</p>	<p>Corresponde a un modelo cíclico, secuencial y estructurado.</p> <p>Está enfocado a la generación de valor por medio de la innovación y TI.</p> <p>Se enfoca en el desarrollo de nuevos productos y la estrategia tecnológica.</p>	<p>El estado no utiliza este modelo en sus organizaciones.</p> <p>Es un modelo relativamente antiguo.</p> <p>No es posible aplicar el ciclo completo, por el alcance del proyecto aplicado al Instituto Nacional de Metrología (INM).</p>
<p>Modelo de Ray Gehani</p>	<p>En Quintero (2018) se menciona que, aunque en los mercados globalizados actuales, la tecnología es uno de los factores críticos para el crecimiento y la supervivencia de las organizaciones, la gestión de esta tecnología requiere de la asignación de recursos, la innovación, el desarrollo de nuevos productos y el talento humano especializado.</p>	<p>Es un modelo enfocado a la innovación y valor en las TI.</p> <p>Considera el talento humano indispensable para el crecimiento en TI.</p> <p>Tiene en cuenta el desarrollo de proyectos tecnológicos.</p>	<p>La documentación del modelo es escasa.</p> <p>Es un modelo genérico que no se usa en las entidades del estado.</p> <p>Las actividades descritas en los subsistemas no son explícitas.</p>

<p>Modelo de gestión tecnológica de Hidalgo Nuchera</p>	<p>Hidalgo propone funciones activas y de apoyo las cuales deben coordinarse para tener una eficiente gestión de la tecnología en donde las funciones activas son definidas como capacidades de adquisición, asimilación y desarrollo de los recursos tecnológicos y las funciones de apoyo son las capacidades para reconocer e interpretar oportunidades y amenazas del entorno con respecto a su posición tecnológica</p>	<p>Es un modelo enfocado a la innovación y valor en las TI.</p> <p>Propone dos funciones para la gestión eficiente de las tecnologías.</p> <p>Identifica con base en la tecnología existente, las ventajas competitivas en una organización.</p>	<p>El modelo propuesto carece de información para su implementación.</p> <p>El estado no utiliza este modelo en sus organizaciones.</p> <p>No son claras las actividades activas y de apoyo para su implementación.</p>
<p>Modelo de Gestión y gobierno de TI</p>	<p>El modelo según MGGTIG (2019), busca que los dominios, lineamientos, guías, evidencias que se deben generar permitan gestionar TI de forma adecuada. Este está dirigido a los líderes estratégicos de TI, a los profesionales de las áreas</p>	<p>Se puede implementar por fases y de acuerdo a la disponibilidad de recursos.</p>	<p>No contar con el apoyo del grupo directivo en una organización.</p> <p>Las fases de implementación no se ajustan a todas las entidades del estado.</p>

	<p>de TI y a los profesionales encargados de la implementación de la política de gobierno digital en las entidades públicas en Colombia.</p>	<p>Es un modelo diseñado para las necesidades del país.</p> <p>Posee información abundante de cómo implementarlo.</p> <p>El modelo está articulado con las políticas de tecnologías de información vigentes.</p> <p>Permite conocer el estado actual de una organización en distintos ámbitos del conocimiento.</p>	<p>Requiere en ocasiones recursos los cuales no son otorgados.</p> <p>No cuenta con mecanismos de seguimiento y control unificados.</p>
--	--	---	---

Nota: Elaboración Propia basado en los autores de los modelos

Anexo B
(Plan de recuperación de desastres DRP)

PLAN DE RECUPERACION DE DESASTRES

GESTION DE TECNOLOGIAS DE INFORMACION Y LAS COMUNICACIONES

INSTITUTO NACIONAL DE METROLOGIA DE COLOMBIA-INM

BOGOTA

2020

1. Contexto General

Objetivo

Establecer y definir las actividades necesarias para mantener la continuidad de operación y servicios soportados en TI, así como los roles y responsabilidades requeridos para su ejecución en caso de presentarse un desastre natural o interrupción mayor de servicios

Responsables

- Coordinador de grupo sistemas de Información y Redes
- Oficial de seguridad de la información.

Alcance

Inicia con la identificación de servicios interrumpidos por fallas producto de desastres naturales abarcando la protección de los servicios críticos ofrecidos por la entidad y soportados en las tecnologías de información y las comunicaciones TIC, los cuales se activan en el sitio alternativo (Nube) y finaliza con la reanudación de servicios en su operación y condiciones normales.

Definiciones

Disaster Recovery Plan, DRP

Plan para la recuperación de operación y servicios críticos basados en tecnologías de información y las comunicaciones donde se definen claramente los roles y responsabilidades involucrados, así como las estrategias aplicables y procedimientos a seguir para reactivar la operación y continuidad de servicios (Mintic, 2010).

Business Continuity Plan, BCP

Es un componente estratégico de planeación para brindar continuidad al negocio, el plan de continuidad de negocio, recopila la información suministrada por el DRP, formando un esquema de contingencia global para recuperar operaciones y procesos de la entidad (Mintic, 2010).

Infraestructura tecnológica crítica

Se refiere a todos aquellos elementos que hacen parte de los sistemas informáticos esenciales para la operación y prestación de servicios de una organización abarcando aspectos de almacenamiento, conexiones de red, sistemas de respaldo, y demás dispositivos tecnológicos que soportan la operación continua (Mintic, 2017).

Seguridad informática

Es la encargada de asegurar física y lógicamente los datos y la información con que cuenta una organización, la confidencialidad es su característica principal ya garantiza que todos los activos del negocio cuenten con protección permanente ante cualquier riesgo posible (Gil, 2017).

Gobierno de TI

El gobierno de TI se enfoca en la alineación que debe existir entre las tecnologías de información y las comunicaciones y su relación directa con las estrategias y objetivos misionales del negocio, buscando la construcción de estándares que favorezcan el crecimiento corporativo mediante el uso y aprovechamiento de las tecnologías existentes como habilitador transversal de procesos misionales (Echeverry, 2017).

RPO: Recovery Point Objective, Tiempo transcurrido desde que ocurre el desastre con el último punto de restauración que se tiene de los datos de la organización

RTO: Recovery Time Objective, Tiempo máximo de interrupción que puede soportar un proceso, sistema de información o servicio soportado en TI

Capacidad Tecnológica

Establece que la capacidad tecnológica se refiere al uso eficaz del conocimiento tecnológico con el propósito de mantener la competitividad en precio y en calidad. Dicha capacidad permite a la organización asimilar, emplear, adaptar y modificar las tecnologías existentes, así como la creación de nuevas tecnologías y el desarrollo de nuevos productos y métodos de fabricación, todo esto para responder a los cambios del entorno, (Velázquez, Domínguez & Andrade, 2018).

Gestión Tecnológica

La conceptualización de la gestión tecnológica se concibe desde varios y diversos puntos de vista o enfoques, que se desarrollan con base en la profundidad de conocimientos sobre el tema. Es por ello que se asumen enfoques que la definen como: procesos, técnicas, estrategias, procedimiento, prácticas, entre otros.

Según (Venegas, 2015), la gestión tecnológica permite manejar el factor tecnológico como aspecto estratégico en las organizaciones productivas, inicialmente se enfocó en la administración de ciencia y tecnología, por lo cual su definición podría concebirse en la administración de conocimiento para dinamizar un proceso productivo a través de la inclusión de enfoques de innovación el cual permite la predicción, la proyección y la prospección tecnológica.

Análisis de datos

El análisis de datos e información tiene como objetivo la toma de decisiones acertada y efectiva que permita optimizar las tendencias de uso de información basado en la transformación de de registros en información útil mediante técnicas de recolección y procesamiento y análisis cuantitativo o cualitativo de los mismos (Cerillo, 2018).

Data center

Conocido también como centro de procesamiento de datos (CPD), y contiene los recursos tecnológicos principales encargados de realizar la dispersión de servicios de TI al interior de la organización, así mismo permite la comunicación con el entorno externo. Normalmente se mantienen en condiciones ambientales específicas, se encuentran aislados de la comunidad de usuarios internos y externos que hacen parte de la organización (Mintic, 2010).

Gestión de riesgos

La probabilidad de ocurrencia y sus consecuencias son los elementos que abarca la gestión del riesgo, sus factores pueden ser motivados por parámetros internos o externos y continuamente aportan seguridad a las empresas al contemplar escenarios futuros de posibles ocurrencias. Una adecuada gestión de riesgos se mantiene continuamente en un ciclo de validación y mejora continua de sus componentes (Almuniñas, 2016).

2. Condiciones Generales

El DRP se enfoca en la protección de la plataforma tecnológica que soporta los servicios misionales principales de la entidad y aquellos que son críticos para la operación interna de la organización los cuales son:

Servicio	Ambito
Servicio de hora legal colombiana	Externo
Sitio Web principal	Externo
Plataforma de Servicio en línea para calibraciones.	Externo
Controlador de dominio principal	Interno
Servicios Financieros, nomina Y TH (Kactus)	Interno
Consulta de información de procesos internos (File servers)	Interno
Sistema de radicación de documentos	Interno

Supuestos

El resultado de la aplicación de esta guía, frente a los posibles desastre naturales que se puedan presentar o interrupciones deliberadas de servicio se basa en los siguientes supuestos:

- El personal del grupo de información y redes con acceso a este documento cuenta con la capacidad de interpretar las instrucciones dadas en el mismo. De igual

manera hacen parte del personal que no ha sido afectado durante el desastre presentado.

- Se mantiene un proveedor permanente con servicios de nube a disposición para la entidad habilitado en una franja de horario de 24/7
- Se han efectuado las correspondientes pruebas con una periodicidad mínima de 6 meses.
- Se han realizado capacitaciones técnicas y estratégicas al personal encargado de la ejecución de esta guía.
- La entidad mantiene de manera complementaria e independiente a esta guía un procedimiento de Backups de sus sistemas de información.

3. Escenarios de Desastre

Como escenarios de desastre se contemplan dentro de este documento los siguientes:

Escenario	Descripción	Causas
1	Afectación en Datacenter principal- Indisponibilidad de centro de computo	<ul style="list-style-type: none"> ▪ Terremotos ▪ Inundaciones ▪ incendios ▪ Fallas en sistema de aire acondicionado ▪ Fallas en suministro eléctrico
2	Afectación en infraestructura de comunicaciones	Presencia de fallas en: <ul style="list-style-type: none"> ▪ Fibras ópticas de conexión Internas ▪ Firewall Principal ▪ Switch Core ▪ Router Core ▪ Enlace de internet con el ISP
		Presencia de fallas en:

3	Afectación en infraestructura de servidores	<ul style="list-style-type: none"> ▪ Servidor Hora legal colombiana ▪ Servidor Cursos virtuales Elearning. ▪ Servidor servicios de calibración ▪ Servidores controladores de dominio principal y secundario ▪ Servidor Aplicaciones Kactus ▪ Servidor de Aplicaciones Isolucion ▪ Servidor de aplicaciones BPM
4	Afectación en infraestructura de Almacenamiento.	<p>Presencia de fallas en:</p> <p>Sistema de almacenamiento SAN.</p> <p>Servidor de Bases de datos Borrados y/o pérdidas de datos masivos</p> <p>Corrupciones de bases de datos</p> <p>Servidores de respaldo de información</p>

Fuente: Elaboración propia.

NOTA: Los escenarios no descritos anteriormente no se consideran en el desarrollo de la presente guía y su aplicación estará sujeta a las condiciones del contexto y los Roles y Responsabilidades descritos más adelante.

Roles y responsabilidades:

- **Alta Dirección:** fijar las políticas asociadas a la gestión integral de los servicios relacionados con los planes de recuperación de desastres y asociados a la infraestructura de TI.
- **Lider del DRP: Coordinador de grupo sistemas de información y redes,** Orientar y coordinar las actividades que deba desarrollar el grupo de Sistemas de Información y Redes, y suministrar los recursos necesarios para el buen desempeño del DRP. Velar por su actualización permanente y suministro de recursos necesarios para su ejecución. Informar de las situaciones de contingencia que se puedan presentar.
- **Grupo de Sistemas de Información y Redes,** es el encargado de monitoreo, gestión y administración de la infraestructura tecnológica así como de la ejecución operativa del DRP.

Evaluar la magnitud del desastre, comunicar el desastre al líder, verificar disponibilidad de servicios, reportar avances o nuevas situaciones.

Los funcionarios y contratistas: tienen la responsabilidad de informar o solicitar apoyo ante cualquier evento sospechoso o incidente que afecte la seguridad de la información, continuidad de operación o el buen funcionamiento de los servicios de TI.

- **Responsable de seguridad de la Información.**

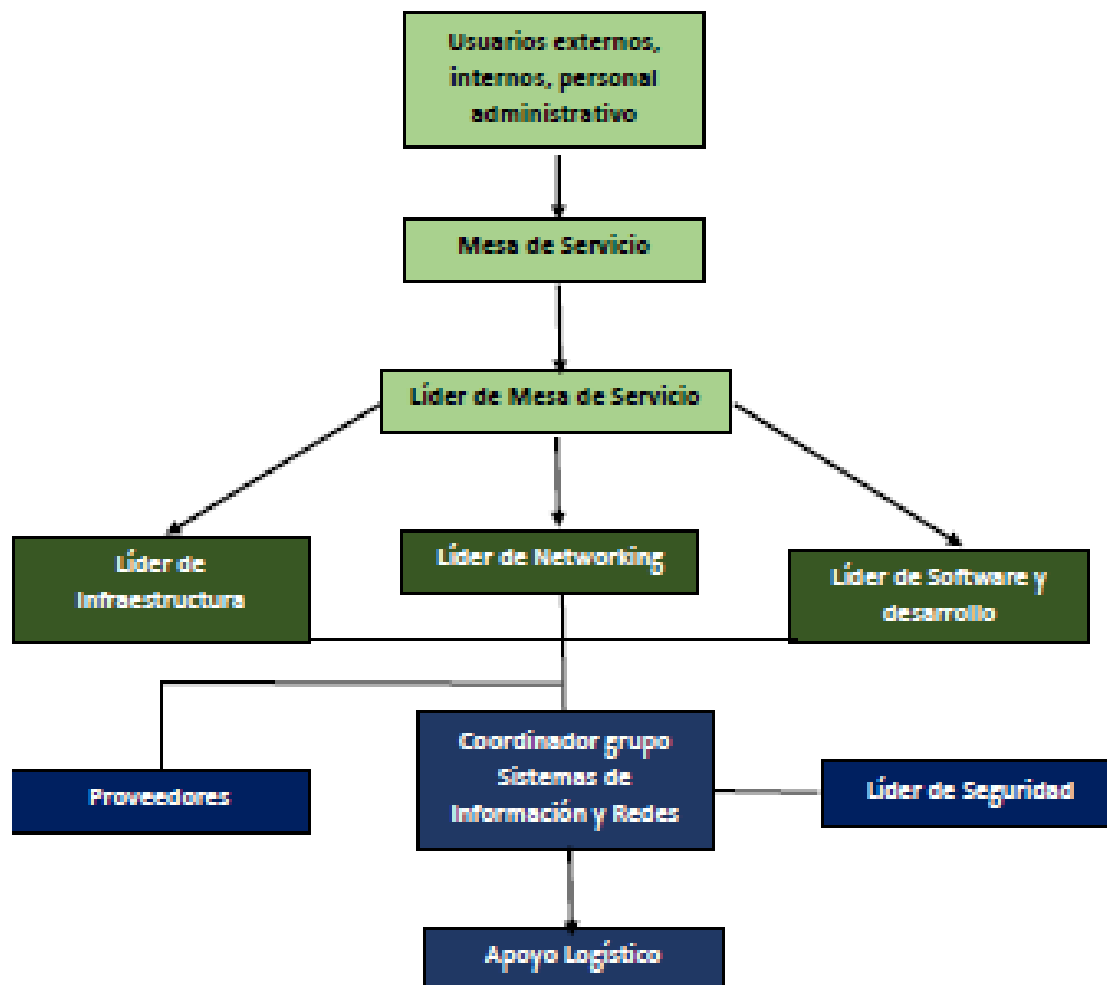
Identificar la brecha entre el Estado de alarma y la situación de operación de la entidad.

Coordinar jornadas de capacitación y entrenamiento, pruebas y análisis de recursos para el DRP

Trabajar de manera integrada con el grupo o áreas (internas y Externas) dispuestas para la gestión de eventos de seguridad de la información y planes de recuperación de desastres.

Liderar la gestión de riesgos sobre criticidad de servicios soportados en TI y de información de la institución.

Árbol de llamadas:



Fuente: Elaboración Propia

4. Notificación DRP

- Se debe registrar el evento a la mesa de servicio en los siguientes casos:

ITEM	INCIDENTE	PERSONAL QUE NOTIFICA	
		Usuarios, Funcionarios, Contratistas colaboradores	Personal administrativo, servicios generales, vigilancia
1	Sistemas de información inutilizables	X	
2	Falla masiva en red de comunicaciones	X	
3	Sin acceso a servidores de archivo e información digital centralizada	X	
4	Activación de alarmas de incendio	X	X
5	Todo evento que afecte de manera masiva la continuidad de servicios y operación de TI	X	
6	Se presenta una inundación en el centro de Datacenter principal.	X	X
7	Falla masiva de Acceso al correo electrónico	X	

Fuente: Elaboración propia

5. Evaluación de situación DRP

Una vez el incidente es recibido por la mesa de servicio debe realizarse la atención del mismo según el procedimiento interno de atención de incidentes, luego se evalúan los siguientes aspectos:

- Validación de afectación de acceso y disponibilidad masiva de los sistemas de información (Aplicaciones principales y secundarias)
- Validación de afectación en disponibilidad masiva de red de comunicaciones
- Validación de afectación en disponibilidad masiva de correo electrónico
- Validación de afectación en disponibilidad masiva de servicios de archivo de información digital centralizada.

La validación se realiza con el apoyo de los líderes de Infraestructura, Networking o con el líder de software desarrollo según corresponda.

Los Líderes antes mencionados deben ejecutar la siguiente lista de chequeo:

- El tiempo aproximado que podría durar el incidente
- Impacto y naturaleza del evento
- Aplicación de soluciones generales posibles
- Aplicaciones de soluciones mediante la activación del DRP

El paso final por parte de los líderes es informar de inmediato el resultado obtenido del diagnóstico al coordinador de grupo de sistemas de información y redes.

6. Activación del DRP

Con base en el resultado de los pasos realizados hasta el momento, el Coordinador de grupo de sistemas de información y redes en conjunto con el líder de seguridad de la información, toman la decisión de activar o no el plan de recuperación de desastres. Lo anterior basado en los siguientes aspectos:

- El incidente presentado toma mas de 24 horas en ser solucionado y devolver la normalidad de operación.
- El incidente genera un impacto que no permite la operación normal del Datacenter principal de la entidad

Se informa a la alta dirección el estado actual del proceso de activación DRP.

7. Sitio Alterno (Nube, colocation)

Para la activación del sitio alerno se consideran necesarias las siguientes actividades:

- Comunicación inmediata con el proveedor de servicio de sitio alerno, (Nube, colocation)
- Detención de proceso de replicación
- Registrar fecha y hora de inicio de actividades en sitio alerno
- Trabajo conjunto de líderes Networking e infraestructura del grupo de TI con proveedores de sitio alerno para enrutar:
 - Controladores de dominio secundarios

- Servicios ofrecidos por la entidad a los servidores virtuales del centro de cómputo alterno.
- El líder de infraestructura valida la operación de plataforma base (Servidores físicos o virtuales) para el funcionamiento de los servicios a publicar.
- El líder de infraestructura valida la disponibilidad de bases de datos.
- El líder de desarrollo de software valida acceso a los sistemas de información.
- El personal de mesa de servicio apoya la validación de la disponibilidad de recursos compartidos y aplicaciones internas y externas.

Se informa a la alta dirección el estado actual del proceso de activación DRP.

8. Recuperación de contingencia

Solucionada la contingencia en apoyo con los proveedores de servicio o fabricantes de las soluciones tecnológicas con las que cuenta la entidad se deben tener en cuenta las siguientes actividades para el retorno de la normalidad en la operación de TI y sus servicios soportados:

El coordinador de grupo mantiene comunicación con los líderes de TI define la estrategia de retorno a la normalidad bajo las siguientes acciones.

- El líder de infraestructura valida la operación de plataforma base en la sede de la entidad
(Servidores físicos o virtuales con reinicio total) para el funcionamiento de los servicios a publicar.

- El líder de infraestructura valida la disponibilidad de bases de datos en la sede de la entidad.
- El líder de desarrollo de software valida acceso a los sistemas de información en la sede de la entidad.
- Se fija fecha y hora de retorno a operación normal
- Una vez recuperada la operación normal de TI se sincroniza la información con el sitio alterno teniendo en cuenta los tiempos en que este estuvo activo.

El líder de seguridad de la información recopila la información general del incidente y su proceso para realizar la documentación respectiva identificando el análisis del paso a paso realizado.

Finalmente se cierra el incidente presentado y se generan las lecciones aprendidas.

Se informa a la alta dirección el estado actual de operación normal de TI.

9. Actualización y mantenimiento DRP

Los líderes de TI con el acompañamiento del líder de seguridad de la información articulan los cambios en infraestructura tecnológica con el posible impacto que estos puedan tener con el plan de recuperación de desastres -DRP descrito anteriormente.

Se debe realizar la actualización de este procedimiento mínimo una vez por año.

Se deben incluir los cambios de estructura organizacional presentadas en el grupo de sistemas de información y redes.

Se deben sugerir y hacer auditorias periódicas al procedimiento de plan de recuperación de desastres

Se deben hacer pruebas del funcionamiento del mismo y sincronización con el sitio alternativo mínimo cada 6 meses.

Nota: Elaboración propia

Anexo C

(Evaluación Modelo de Gestión y Gobierno de TI)

Dominio	Fórmula cumplimiento dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento dominio
Estrategia de TI	$ID01=(\text{Planeación Estratégica de TI} + \text{Seguimiento} + \text{Cumplimiento de la implementación de la Estrategia de TI} + \text{Arquitectura Empresarial} + \text{Documentación de la Arquitectura Empresarial} + \text{Servicios de TI})/7$	Planeación Estratégica de TI	$(PR01+PR02)/2$	PR01	¿Cuál es el estado del Plan Estratégico de TI (PETI) en la entidad?	A. No lo tiene o está en proceso de construcción B. Lo formuló, pero no está actualizado C. Lo formuló y está actualizado	SI A = 0 SI B=70 SI C =100	B,70	60	46%
				PR02	¿El Plan Estratégico de TI (PETI) en el Instituto Nacional de Metrología (INM) incluye?	A. El portafolio o mapa de ruta de los proyectos B. La proyección del presupuesto, C. El entendimiento estratégico, D. El análisis de la situación actual, E. El plan de comunicaciones del PETI F. Todos los dominios del Marco de Referencia. G. Diagnostico Interoperabilidad H. Diagnostico Autenticación Electrónica I. Diagnostico Carpeta ciudadana. J Ninguna de las anteriores	SI A = +100/6 SI B = +100/6 SI C = +100/6 SI D = +100/6 SI E = +100/6 SI F= +100/6	A,C,D 50		

<p>Seguimiento</p>	<p>PR03</p>	<p>PR03</p>	<p>¿Con respecto al seguimiento del PETI el Instituto Nacional de Metrología (INM)?:</p>	<p>A. Definió indicadores de monitoreo y evaluación del PETI. B. Realizó la medición de indicadores de monitoreo y evaluación del PETI. C. Formuló en caso de ser necesario, acciones de mejora a partir de la medición de indicadores de monitoreo y evaluación del PETI. D. Difundió, comunicó y trabajó en la apropiación del PETI en todos los niveles de la entidad. E. La entidad utilizó tableros de control de indicadores para la gestión de la implementación del PETI. F Ninguna de las anteriores</p>	<p>SI A = +100/5 SI B = +100/5 SI C = +100/5 SI D = +100/5 SI E = +100/5 SI F= 0</p>	<p>D,20</p>	<p>20</p>	
---------------------------	--------------------	--------------------	--	--	---	--------------------	------------------	--

<p>Cumplimiento de la implementación de la Estrategia de TI</p>	<p>PR04</p>	<p>PR04</p>	<p>Indique el porcentaje de cumplimiento de los objetivos estratégicos del PETI, con respecto a lo planeado para la última vigencia</p>	<p>A. Porcentaje</p>	<p>Porcentaje</p>	<p>A, 30</p>	<p>30</p>	
<p>Arquitectura Empresarial</p>	<p>PR05</p>	<p>PR05</p>	<p>Con respecto a la Arquitectura Empresarial el Instituto Nacional de Metrología (INM):</p>	<p>A. Cuenta con las capacidades para realizar ejercicios de Arquitectura Empresarial (Personas, Procesos, Herramientas). B. Hace uso de una metodología de Arquitectura Empresarial para el diseño y planeación de las iniciativas de Tecnologías de Información (TI). C. Desarrollo uno o más ejercicios de Arquitectura Empresarial D. Cuenta con un grupo de Arquitectura empresarial que gobierna y toma decisiones frente al impacto o evolución de la arquitectura empresarial E. Ninguna de las anteriores</p>	<p>SI A =+ 100/4 SI B =+ 100/4 SI C =+ 100/4 SI D=+100/4 SI E=0</p>	<p>50</p>	<p>50</p>	

	Documentación de la Arquitectura Empresarial	PR06	PR06	Frente a la documentación de la Arquitectura Empresarial en el Instituto Nacional de Metrología (INM)	A. Documentó la Arquitectura misional o de Negocio B. Documentó la Arquitectura de Información C. Documentó la Arquitectura de Sistemas de Información D. Documentó la Arquitectura de Servicios tecnológicos E: Ninguna de las anteriores	SI A =+ 25 SI B =+ 25 SI C =+ 25 SI D=+ 25 SI E= 0	50	50	
	Servicios de TI	PR07	PR07	En relación con el catálogo de servicios de TI, el Instituto Nacional de Metrología (INM):	A. No lo tiene o está en proceso de construcción. B. Lo tiene y esta actualizado sin los Acuerdos de Nivel de Servicio (ANS) C. Lo tiene y está actualizado con los Acuerdos de Nivel de Servicio (ANS)	SI A = 0 SI B =50 SI C =100	50	50	

Dominio	Fórmula cumplimiento o dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento o dominio
Gobierno de TI	(Esquema de gobierno de TI+ Inversiones/Compras de TI+ Gestión de proyectos +Operación de TI)/4	Esquema de gobierno de TI	PR08	PR08	Señale los aspectos incorporados en el esquema de gobierno de TI del Instituto Nacional de Metrología (INM):	A. No cuenta con un esquema de gobierno de TI B. Políticas de TI. C. Proceso de Gestión de TI D. Indicadores de desempeño de TI. E. Instancias de decisión de TI definidas. F. Roles y responsabilidades de TI. G. Estructura organizacional del área de TI.	SI A = 0 SI B = 100/6 SI C = 100/6 SI D = 100/6 SI E = 100/6 SI F = 100/6 SI G = 100/6	A,B,C, D,F,G 83.3	83.3	70.8%
		Inversiones / Compras de TI	PR09	PR09	Con respecto a la optimización de las compras de TI, el Instituto Nacional de Metrología (INM):	A. Utilizó Acuerdos Marco de Precios para bienes y servicios de TI (Aplica Entidades Nacionales) B. Utilizó contratos de agregación de demanda para bienes y servicios de TI, C. Aplicó metodologías o casos de negocio y criterios para la selección y/o evaluación de soluciones de TI,	Si A ó B ó C = 50. Si selecciona A y B = 70. Si selecciona (A ó B) y c = 100. Si selecciona	A,50	50	



				D. Ninguna de las anteriores	D=0			
Gestión de proyectos	PR10	PR10	Frente a la gestión integral de proyectos de TI, el Instituto Nacional de Metrología (INM):	A. Aplicó una metodología para la Gestión integral de Proyectos de TI. B. Garantizó que cualquier iniciativa, proyecto o plan de la entidad que incorpora TI, es liderado en conjunto entre las áreas misionales y el área de TI de la entidad. C incorpora desde el inicio de la visión del usuario D. Realizó transferencia de conocimiento de los proveedores y/o contratistas de TI E. Ninguna de las anteriores	SI A =+ 100/4 SI B =+ 100/4 SI C =+ 100/4 SI D= +100/4	B,C, 50	50	

	Operación de TI	PR11	PR11	Frente a la gestión de la operación de TI, el Instituto Nacional de Metrología (INM):	<p>A. Define indicadores y mide el desempeño de la Gestión de TI sin usar tableros de control</p> <p>B. Define indicadores y mide el desempeño de la Gestión de TI a través de tableros de control.</p> <p>C. Formula acciones de mejora a partir de la medición de indicadores de desempeño de la Gestión de TI si le aplica</p> <p>D. Ninguna de las anteriores</p>	<p>SI B =+ 100/2 SI C =+ 100/2</p>	B,C, 100	100	
--	-----------------	------	------	---	---	--	-------------	-----	--

Dominio	Fórmula cumplimiento dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento dominio
Información	(Gobierno de Información+ Calidad de la información+ Análisis y aprovechamiento de los Componentes de Información) /3	Gobierno de Información	PR12	PR12	Con relación a la gestión y planeación de los componentes de información el Instituto Nacional de Metrología (INM):	A. Documentó el catálogo de componentes de información B. Definió un esquema de gobierno de los componentes de información. C. Implementó un esquema para el gobierno de los componentes de información. D. Definió las fuentes únicas de información en la Entidad. E. Definió un esquema de roles y responsabilidades sobre los componentes de información F. Estableció indicadores de seguimiento de los componentes de información G. Ninguna de las anteriores	SI A =+ 100/6 SI B =+ 100/6 SI C =+ 100/6 SI D =+ 100/6 SI E =+ 100/6 SI F =+ 100/6 SI G =0	E, 16,6	16,6	11.11%

<p>Calidad de la información</p>	<p>PR13</p>	<p>PR13</p>	<p>Frente a la calidad de los componentes de información, el Instituto Nacional de Metrología (INM) realizó:</p>	<p>A. Definió un plan de gestión de la calidad de los componentes de información. B. Hizo la medición de la calidad de los componentes de información utilizando indicadores y métricas. C. Hizo seguimiento al plan de gestión de la calidad de los componentes de información. D. Implementó los controles de calidad y acciones de mejora sobre los componentes de información. E. Ninguna de las anteriores</p>	<p>SI A = 100/4 SI B = 100/4 SI C = 100/4 SI D = 100/4 SI E = 0</p>	<p>E, 16,6</p>	<p>16,6</p>	
<p>Análisis y aprovechamiento de los Componentes de Información</p>	<p>PR14</p>	<p>PR14</p>	<p>Frente al análisis y aprovechamiento de los Componentes de Información, el Instituto Nacional de Metrología (INM):</p>	<p>A. Utilizó mecanismos/canales para el uso y aprovechamiento de los componentes de información B. Fomentó el uso y aprovechamiento de los componentes de información por parte de los grupos de interés. C. Ninguna de las anteriores</p>	<p>SI A =+ 50 SI B =+ 50 SI C = 0</p>	<p>0</p>	<p>0</p>	

Dominio	Fórmula cumplimiento dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento dominio
Sistemas de información	(Planeación y gestión de los Sistemas de Información + Soporte de los sistemas de información + Ciclo de vida)/3	Planeación y gestión de los Sistemas de Información	PR15	PR15	Frente a la planeación y gestión de los sistemas de información, el Instituto Nacional de Metrología (INM):	<p>A. Tiene actualizado el catálogo de sistemas de información.</p> <p>B. Definió e implementó una metodología de referencia para el desarrollo de sistemas de información.</p> <p>C. Incluyo características que permitan la apertura de sus datos de forma automática</p> <p>D. Documentó la arquitectura de solución y de solución para sus sistemas de información.</p> <p>E. incorporó dentro de los contratos de desarrollo de sus sistemas de información, cláusulas que obliguen a realizar transferencia de derechos de autor a su favor</p> <p>F. Implemento funcionalidades de trazabilidad y auditoría de transacciones o acciones de creación, actualización, modificación o borrado de información.</p> <p>G .Cuenta con la documentación técnica y funcional debidamente actualizada.</p> <p>H. Cabeza de sector posee consolidado y mantiene actualizado el catálogo de sistemas de información sectorial (entidades orden nacional)</p> <p>I. Ninguna de las anteriores</p>	SI A =+ 100/8 SI B =+ 100/8 SI C =+ 100/8 SI D =+ 100/8 SI E =+ 100/8 SI F =+100/8 SI G=+100/8 SI H =+100/8	E,F 25	25	38,3%

		Soporte de los sistemas de información	PR16	PR16	<p>Frente al soporte de los Sistemas de Información el Instituto Nacional de Metrología (INM):</p> <p>A. Definió un esquema de mantenimiento/soporte a los sistemas de información incluyendo si estos son mantenidos por terceros.</p> <p>B. Implementó un esquema de mantenimiento/soporte a los sistemas de información incluyendo si estos son mantenidos por terceros.</p> <p>C. Estableció criterios de aceptación y definió Acuerdos de Nivel de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información.</p> <p>D. Tiene establecido y aplica un procedimiento para el mantenimiento preventivo de los sistemas de información.</p> <p>E. Ninguna de las anteriores</p>	<p>SI A =+ 25</p> <p>SI B =+ 25</p> <p>SI C =+ 25</p> <p>SI D =+ 25</p> <p>SI E= 0</p>	C, 50	50	
--	--	--	------	------	--	--	-------	----	--

					<p>Frente al Ciclo de vida de los Sistemas de Información el Instituto Nacional de Metrología (INM):</p> <p>A. Implementó un esquema para el gobierno que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento.</p> <p>B. Definió un proceso para el gobierno que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento.</p> <p>C. Implementó un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales</p> <p>D. Definió y aplicó una guía de estilo en el desarrollo de sus sistemas de información e incorpora especificaciones y lineamientos de usabilidad definidos por el MinTIC.</p> <p>E. Tienen las funcionalidades de accesibilidad que indica la Política de gobierno Digital, en los sistemas de información de acuerdo con la caracterización de usuarios.</p> <p>F. Ninguna de las anteriores</p>	<p>SIA=+ 20 SIB=+ 20 SIC =+ 20 SID=+20 SIE=+ 20 SIF =0</p>	<p>A, E 40</p>	<p>40</p>	
--	--	--	--	--	---	---	----------------	-----------	--

Dominio	Fórmula cumplimiento dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento dominio
Servicios tecnológicos	(Soporte a los servicios de TI+ Operación de servicios tecnológicos + Calidad de servicios tecnológicos + Avance en la adopción de IPV6)/4	Soporte a los servicios de TI	PR18	PR18	Frente al soporte de los servicios tecnológicos en el Instituto Nacional de Metrología (INM)	<p>A. Definió un proceso para atender los requerimientos de soporte de los servicios de TI.</p> <p>B. Definió un esquema de soporte con niveles de atención (primer, segundo y tercer nivel) a través de un punto único de contacto y soportado por una herramienta tecnológica.</p> <p>C. Implementó un plan de mantenimiento preventivo y evolutivo sobre los Servicios Tecnológicos.</p> <p>D. Definió el cumplimiento de los ANS para los servicios tecnológicos que presta la Entidad.</p> <p>E. Evaluó el cumplimiento de los ANS para los servicios tecnológicos que presta la Entidad.</p> <p>F. Implementó un programa de correcta disposición final de los residuos tecnológicos de acuerdo con la normatividad del gobierno nacional.</p> <p>G. Ninguna de las anteriores</p>	<p>SI A =+ 100/6</p> <p>SI B =+ 100/6</p> <p>SI C =+ 100/6</p> <p>SI D=+ 100/6</p> <p>SI E = +100/6</p> <p>SI F =+ 100/6</p> <p>SI G =0</p>	A, B, C,D,E 100	100	55.2%

		Calidad de servicios tecnológicos	PR20	PR20	<p>Frente a la Gestión de la calidad de los Servicios Tecnológicos en el Instituto Nacional de Metrología (INM)</p> <p>A Implementó controles de seguridad para los servicios tecnológicos</p> <p>B Hizo la gestión de los riesgos asociados a su infraestructura tecnológica y servicios tecnológicos</p> <p>C Ninguna de las anteriores</p>	<p>SI A =+ 100/2</p> <p>SI B =+ 100/2</p> <p>SI C=0</p>	A, 50	50	
--	--	--	-------------	-------------	---	---	--------------	-----------	--

				PR21	<p>¿ El Instituto Nacional de Metrología (INM) en qué fases de la adopción de IPv6 se encuentra trabajando?</p> <p>A. Fase de Planeación B. Fase de Implementación C. Fase de pruebas de funcionalidad D. No ha iniciado ninguna fase</p>	<p>SI A =+60 SI B =+30 SI C =+10</p>		A, 60	37,5	
--	--	--	--	-------------	--	---	--	--------------	-------------	--

Avance en la adopción de IPV6

$$\frac{(PR21+PR22)}{2}$$

PR21

SI A
=+60
SI B
=+30
SI C
=+10

A, 60

37,5

				PR22	<p>¿Qué documentación ha adelantado el Instituto Nacional de Metrología (INM) en la adopción de IPV6?</p> <p>A. Plan de Diagnóstico (Fase planeación) B. Plan detallado del proceso de transición (Fase planeación) C. Plan de direccionamiento IPv6 (Fase planeación) D. Plan de contingencias para IPv6 (Fase planeación) E. Diseño detallado de la implementación de IPv6 (Fase implementación) F. Informe de pruebas piloto realizadas (Fase implementación) G. Informe de activación de políticas de seguridad en IPv6 (Fase implementación) H. Documento de pruebas de funcionalidad en IPv6 (Pruebas de funcionalidad) I. Acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos intervenidos en la fase de implementación. (Pruebas de funcionalidad)</p>	<p>SI A =+ 15 SI B =+ 15 SI C=+ 15 SI D=+ 15 SI E=+ 10 SI F =+ 10 SI G =+ 10 SI H =+ 5 SI I =+ 5</p>	A, 15		
--	--	--	--	------	---	---	-------	--	--

Dominio	Fórmula cumplimiento dominio	Variable	Fórmula	ID pregunta	Pregunta asociada a la variable a medir	Opciones de respuesta	Formula	Respuesta	Resultado fórmula	% Cumplimiento dominio
Uso y apropiación de TI	Estrategia de uso y apropiación de TI	Estrategia de uso y apropiación de TI	PR23	PR23	Frente a la Estrategia para el Uso y Apropiación de TI en el Instituto Nacional de Metrología (INM)	<p>A. Definió y ejecutó una estrategia de uso y apropiación para todos los proyectos de TI que se realizan en la institución de acuerdo con la caracterización de grupos de interés.</p> <p>B. Realizó la caracterización de los grupos de interés internos y externos. C Definió un plan de formación para el desarrollo de competencias requeridas para el desarrollo de sus funciones y hacer un uso adecuado de los servicios de TI.</p> <p>D. Realizo divulgación y comunicación interna de los proyectos de TI</p> <p>E Implementó estrategias de gestión del cambio para los proyectos de TI F. Definió indicadores para la medición del impacto del uso y apropiación de TI en la entidad.</p> <p>G Ejecutó acciones de mejora y transformación a partir de los resultados obtenidos.(si aplica)</p> <p>H. Ninguna de las anteriores</p>	<p>SI A =+ 100/7</p> <p>SI B =+ 100/7</p> <p>SI C=+ 100/7</p> <p>SI D= + 100/7</p> <p>SI E =+ 100/7</p> <p>SI F =+ 100/7</p> <p>SI G =+ 100/7</p> <p>SI H = 0</p>	C, D 28,5	28,5	28,5%

Nota: Elaboración propia, basada en el documento “Implementación de la Política de Gobierno Digital, Anexo 5”