

**Integración Documental ISO 9001, ISO 19770-1, ITIL e IAITAM en la
Gestión de Activos de Tecnología Informática del Área de Dirección
General de Tecnología Banco de la República**

Diana Marcela Mantilla Parra

ID: 000351098

Universidad Pontificia Bolivariana – Seccional Bucaramanga

Escuela de Ingeniería

Facultad de Ingeniería Industrial

Bucaramanga

2021

**Integración Documental ISO 9001, ISO 19770-1, ITIL e IAITAM en la
Gestión de Activos de Tecnología Informática del Área de Dirección
General de Tecnología Banco de la República**

Diana Marcela Mantilla Parra

ID: 000351098

Trabajo de Grado presentado como requisito para optar al título de:
INGENIERA INDUSTRIAL

Supervisor Empresa

Carlos Alberto Balcázar Navarrete

Supervisor Universidad

MSc. Lupita Serrano Gómez

Universidad Pontificia Bolivariana – Seccional Bucaramanga

Escuela de Ingeniería

Facultad de Ingeniería Industrial

Bucaramanga

2021

Agradecimientos

En primer lugar, quiero agradecer a Dios, Él que ha permitido que este proyecto se lleve de la mejor manera llenándome siempre con sus bendiciones.

A la Universidad Pontificia Bolivariana Seccional Bucaramanga y a sus docentes que me brindaron apoyo durante mi proceso de formación académica.

Al Banco de la República de Colombia que me permitió afianzar y ganar nuevos conocimientos durante el proceso de la práctica empresarial, y en especial a mis jefes Camilo Andrés Cañón Correa y Carlos Alberto Balcázar Navarrete.

Gracias a mi Supervisora Académica MSc. Lupita Serrano Gómez por sus observaciones y consejos para sacar adelante este Trabajo de grado.

Finalmente, agradecer a mi familia, que siempre han estado para mí cuando los he necesitado; en especial a mi madre que creyó en mí, incluso cuando yo no lo hacía, sin ella esto no sería posible, infinitas gracias, madre.

Tabla de Contenido

Introducción	10
Capítulo 1 Generalidades de la Empresa	13
Capítulo 2 Diagnóstico de la Empresa	19
Capítulo 3 Delimitación del Problema	24
Capítulo 4 Antecedentes	26
Capítulo 5 Justificación	31
Capítulo 6 Objetivos	33
Capítulo 7 Marco Teórico	34
Capítulo 8 Metodología	52
Capítulo 9 Resultados y Discusión	55
9.1 Marco de referencia y requisitos ISO 9001, ISO 19770-1, ITIL e IAITAM a la gestión de activos de tecnología de información para el Banco de la República	55
9.1.1. Norma ISO 9001:2015	55
9.1.2. Norma ISO/IEC 19770-1	64
9.1.3. Guía ITIL	71
9.1.4. Guía IAITAM	88
9.2 Integración documental normas, guías y procedimientos para el área de Dirección General de Tecnología Banco de la República	96
9.3 Documentación de procedimientos área de Dirección General de Tecnología Banco de la República	110

9.4 Sensibilización y socialización en el área de Dirección General de Tecnología de la integración documental ISO 9001, ISO 19770-1, ITIL e IAITAM	127
Capítulo 10 Conclusiones y Recomendaciones	128
Referencias	130

Lista de Tablas

Tabla 1. Tabla resumen norma ISO 9001:2015	56
Tabla 2. Tabla resumen Norma ISO/IEC 19770-1	64
Tabla 3. Tabla resumen Guía ITIL.	72
Tabla 4. Tabla resumen Guía NIST	90
Tabla 5. Resumen de la integración documental normas y guías.	97

Lista de Ilustraciones

Ilustración 1. Organigrama Banco de la República	17
Ilustración 2 Dirección General de Tecnología	18
Ilustración 3 <i>Ciclo de Vida de un Activo TI</i>	37
Ilustración 4 Ciclo PHVA, ISO 9001	40
Ilustración 5 Principales tipos de activos TI	43
Ilustración 6 Ciclo de vida del servicio TI, ITIL V3	46
Ilustración 7 Sistema de valor de servicio, ITIL V4	47
Ilustración 8 Interacción requisitos IAITAM	49
Ilustración 9 Objetos ARIS CLOUD	113
Ilustración 10 Estructura procedimiento ARIS	115
Ilustración 11 Gestión de datos básicos	117
Ilustración 12 Menú inicio- Ficha técnica.	120
Ilustración 13 Ficha técnica.	121
Ilustración 14 Formulario datos	122
Ilustración 15 Campos ficha técnica	123
Ilustración 16 Gestión de licencias en uso	124

RESUMEN GENERAL DE TRABAJO DE GRADO

TÍTULO:	Integración documental ISO 9001, ISO 19770-1, ITIL e IAITAM en la Gestión de Activos de Tecnología Informática del área de Dirección General de Tecnología Banco de la República
AUTOR(ES):	Diana Marcela Mantilla Parra
PROGRAMA:	Facultad de Ingeniería Industrial
DIRECTOR(A):	Lupita Serrano Gómez

RESUMEN

El Banco de la República de Colombia es un órgano del Estado de naturaleza única, con autonomía administrativa, patrimonial y técnica. Una de las funciones desarrolladas por el Banco es la de coordinar y dirigir la implementación de políticas y estándares de uso de tecnologías de información, telecomunicaciones, multimedia, seguridad informática y la seguridad electrónica asumida por la Subgerencia General de Servicios Corporativos que tiene como una de las áreas la dirección general de tecnología. El objetivo principal del presente trabajo es realizar la integración documental de la ISO 9001, ISO 19770-1, ITIL y NIST, en la gestión de activos de tecnología informática (TI) con el propósito de mejorar las prácticas del área de Dirección General de Tecnología en el Banco de la República. Para lograr este propósito en primer lugar, se identifican los requisitos y marcos de referencia de las normas y guías objeto de integración como base fundamental; luego, con los resultados encontrados se logra una integración en cuanto a las mejores prácticas ofrecidas para la gestión de activos TI, posteriormente se documentan los procedimientos recirculación de software, gestión de datos básicos TI, inventario de licencias y se realizó una plantilla para ficha técnica del software que dan respuesta a la integración en la gestión de activos; y finalmente, se socializa el trabajo realizado. Como resultado se obtuvo un documento guía que busca garantizar un uso eficiente de los recursos, una reducción en costos, una mejora en la gestión de los mismos y garantizar las políticas corporativas trazadas por el Banco.

PALABRAS

CLAVE:

Gestión de activos TI, Documentación, Tecnología, Procedimientos.

V° B° DIRECTOR DE TRABAJO DE GRADO

GENERAL SUMMARY OF WORK OF GRADE

TITLE: Document integration ISO 9001, ISO 19770-1, ITIL and IAITAM in the Management of it Technology Assets of the general management area of Technology Banco de la República

AUTHOR(S): Diana Marcela Mantilla Parra

FACULTY: Facultad de Ingeniería Industrial

DIRECTOR: Lupita Serrano Gómez

ABSTRACT

El Banco de la República de Colombia is a state body of a unique nature, with administrative, patrimonial and technical autonomy. One of the functions developed by the Bank is to coordinate and direct the implementation of policies and standards for the use of information technologies, telecommunications, multimedia, computer security and electronic security assumed by the Deputy General Manager of Corporate Services that has as one of the areas the general direction of technology. The main objective of this work is to carry out the documentary integration of ISO 9001, ISO 19770-1, ITIL and NIST, in the management of information technology (IT) assets with the purpose of improving the practices of the General Direction of Technology area in El Banco de la República. To achieve this purpose in the first place, the requirements and frameworks of the standards and guides subject to integration as a fundamental basis are identified; then, with the results found, an integration is achieved in terms of the best practices offered for it asset management, software recirculation procedures, basic IT data management, license inventory are subsequently documented and a template was made for the software data sheet that responds to the integration in asset management; and finally, the work done is socialized. As a result, a guiding document was obtained that seeks to ensure an efficient use of resources, a reduction in costs, an improvement in their management and guarantee the corporate policies drawn up by the Bank

KEYWORDS:

IT asset management, Documentation, Technology, Procedures.

V° B° DIRECTOR OF GRADUATE WORK

Introducción

En las últimas décadas la tecnología ha empezado a cambiar la forma en la que se percibe el mundo, según un reporte sobre las tendencias de la tecnología realizado por Deloitte.insights (2019), concluye que estos cambios en algunos casos han facilitado las operaciones diarias, mejorando la comunicación y siendo parte vital de la evolución de las industrias. En el ámbito laboral ha sido fundamental para incrementar su producción, agilizar procesos, mejorar la toma de decisiones, en pocas palabras para hacer a las empresas más competentes. Ahora bien, según (DELOITTE, 2016) si una empresa no está constantemente renovando su tecnología queda en gran desventaja y queda apartada de la competencia y los clientes.

Más aún, en estos tiempos que atraviesa actualmente el mundo entero por la situación de pandemia, el impacto de las tecnologías ha sido vital, pues ha obligado a las empresas y a las personas a hacer uso de ellas al reducirse drásticamente su contacto como sociedad y reinventarse (Caillaux, 2020). Aunque, no fue sólo hasta hace unos meses donde las compañías vieron como fundamental implementar herramientas tecnológicas que pudieran mejorar los servicios, conectarse con sus clientes y sus colaboradores; sí se ha visto un incremento marcado en el uso de la tecnología en estos tiempos, la cual ha incidido de manera positiva y ha ayudado a prevenir la propagación, así como a adaptar a las personas y empresas a la nueva normalidad.

Debido a la evolución que ha tenido la tecnología, además del impacto generado por la pandemia, donde se han integrado mayores herramientas tecnológicas para las operaciones, en el Banco de la República de Colombia, más específicamente en el área de Dirección General de Tecnología se vio la necesidad de responder de manera ágil y oportuna a toda esta situación que se ha venido presentando buscando las mejores prácticas para gestionar los activos de tecnología de información que apoyen los procesos misionales y corporativos de la empresa; por tanto, el objetivo principal de este Trabajo de Grado es el de realizar una integración documental de las buenas prácticas que ofrecen las normas y guías ISO 9001, ISO 19770-1, ITIL e IAITAM en cuanto a la gestión de activos de tecnología informática para el área.

Para lograr los objetivos planteados se utiliza como metodología la recolección de datos e información preliminar sobre el tema y el conocimiento que poseen los integrantes de la DG-T para identificar los marcos de referencia y requisitos en las Normas ISO 9001, ISO 19770-1 y Guías ITIL e IAITAM que apliquen a la gestión de activos de tecnología de información para el Banco. Seguido, se realiza el estado del arte donde se identifican las mejores prácticas según las normas y guías en el mercado, buscando así documentar la propuesta de integración. Y, por último, se documentan los procedimientos: Circularización de software, Gestión de datos básicos, Inventario de licencias y una ficha técnica de Excel para dar cumplimiento a alguna de estas prácticas.

Los resultados obtenidos de la integración documental de la ISO 9001, ISO 19770-1, ITIL e IAITAM en la gestión de activos de tecnología informática (TI) para mejorar las

prácticas del área de Dirección General de Tecnología en el Banco de la República se plasman en un documento en el cuál se encuentran los más altos estándares internacionales y las mejores guías del mercado referentes al tema; y se socializan dichos resultados al personal ayudando así según la perspectiva del autor, al área de Dirección General de Tecnología a mejorar su gestión, e impulsando de esta manera su factor competitivo a nivel mundial.

Capítulo 1

Generalidades de la Empresa

El Banco de la República de Colombia es un órgano del estado que posee una naturaleza única puesto que, tiene autonomía tanto administrativa, técnica, como también patrimonial; por lo cual, se le es considerado como un ente independiente del gobierno colombiano. Todas estas atribuciones le fueron concedidas en 1923 mediante la Ley 25, donde se le denominó con el nombre del Banco Central de Colombia.

Sin embargo, la historia del Banco de la República se remonta a muchos años atrás, más específicamente al año 1880; en el cual, bajo la Ley 39 del 16 de Julio del mismo año, es fundado el Banco Nacional, entidad de naturaleza mixta a la que el Gobierno nacional destinó las funciones de promover el crédito público, tesorería, préstamos internos, externos, administración de títulos de deuda pública, fabricación y distribución de la moneda oficial del país. No obstante, este ente fue liquidado en 1894 debido a incidencias en las capacidades de emisión (Banco de la República, 2020).

Después de varios intentos de consolidar la Banca Central de Colombia se estableció finalmente el Banco de la República de Colombia, por medio de la figura jurídica de sociedad anónima, donde el Gobierno colombiano aportó el 50% del capital y el 50% del capital restante fue aportado por diferentes bancos nacionales, extranjeros y personas particulares (Banco de la República, 2020).

Como principales funciones destinadas por la constitución política y Ley 31 de 1992, se encuentran:

- Preservar la capacidad adquisitiva de la moneda, por medio de las políticas monetaria, de intervención cambiaria y crediticia
- Emitir la moneda legal colombiana
- Administrar las reservas internacionales
- Ser prestamista de última instancia y banquero de establecimientos de crédito
- Ser agente fiscal del Gobierno
- Contribuir a la actividad cultural
- Contribuir a la generación de conocimiento.

En cuanto a la estructura jerárquica del Banco está en cabeza de la Junta Directiva, está conformada por siete miembros, de los cuales cinco de ellos son elegidos de dedicación exclusiva, el ministro de Hacienda y Crédito Público y el Gerente General del Banco nombrado por los anteriores. Este último es el señor Leonardo Villar, quien tiene a su cargo las dos grandes áreas: Gerencia Técnica, la cual cumple funciones de brindar soporte de las políticas monetarias y administración de reservas; y la Gerencia Ejecutiva, la cual es la encargada de la generación de la moneda y actividades culturales. Asimismo, se encuentra la Subgerencia General de Servicios Corporativos, las cuales brindan el apoyo a los procesos misionales de la compañía (Banco de la República, 2020).

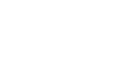
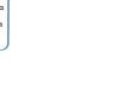
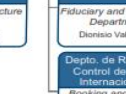
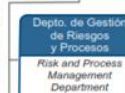
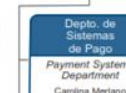
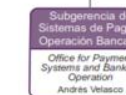
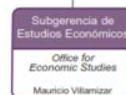
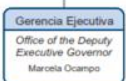
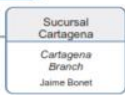
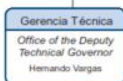
Además de esto, existen rganismos que regulan el buen funcionamiento de las actividades del Banco, los cuales son: el Congreso de la República, actuando de forma política, en donde se debe rendir cuentas dos veces al año sobre la ejecución de las políticas

monetarias, crediticias y gestión de las reservas internacionales; la Superintendencia Financiera de Colombia y la Auditoría General que realizan la inspección, vigilancia y control; Contraloría General de la República, que realiza las función de control en las actividades que el Banco es agente fiscal del Gobierno (Banco de la República, 2020). En la ilustración 1, se observa el organigrama del Banco de la República, y en donde se señala el área de trabajo donde se desarrolla la presente práctica empresarial.

En cuanto al personal, el Banco de la República emplea a más de mil personas, distribuidas en 17 sucursales y 15 centros culturales ubicados en las ciudades de: Armenia, Barranquilla, Bogotá, Bucaramanga, Buenaventura, Cali, Cartagena, Cúcuta, Florencia, Girardot, Honda, Ibagué, Ipiales, Leticia, Manizales, Medellín, Montería, Neiva, Pasto, Pereira, Popayán, Quibdó, Riohacha, San Andrés, Santa Marta, Sincelejo, Tunja, Valledupar y Villavicencio.

Además, posee 2 plantas industriales de fabricación de la moneda ubicadas en Bogotá D, C, donde también se encuentra su sede principal, la cual es la ubicación donde se realizan estas prácticas empresariales:

- Dirección: Carrera. 7 #14-78, Esquina de la Avenida Jiménez. Bogotá, D.C.
- Teléfono: +571 343 1111.
- Correo electrónico: atencionalciudadano@banrep.gov.co.



Fecha de actualización, ene

Ilustración 1. Organigrama Banco de la República

Fuente: Banco de la República, 2021. Tomado de <https://www.banrep.gov.co/es/organigrama>

Como se puede observar en el organigrama, se señala en un rectángulo naranja la Subgerencia General de Servicios Corporativos, en donde se encuentra ubicado el departamento en el cual se realizará esta práctica empresarial. Además, esta subgerencia es la encargada de orientar las funciones corporativas de apoyo relacionadas con Gestión Humana, Tecnología, Logística, Servicios Financieros, Protección y Seguridad, Infraestructura y Gestión de Salud (Banco de la República, 2020).

Ahora bien, señalado con un círculo rojo, se encuentra el área a estudiar en este proyecto, la Dirección General de Tecnología (DG-T) en la cual se cuenta con cuatro departamentos y una unidad: Departamento de Tecnología Informática, Departamento de Sistemas de Información, Departamento de Seguridad Informática, Departamento de Servicios de Tecnología Informática y la Unidad de Seguridad Electrónica.

En la ilustración 2, es posible observar a mayor detalle la Dirección General de Tecnología con el fin de interrelacionar las áreas bajo estudio.

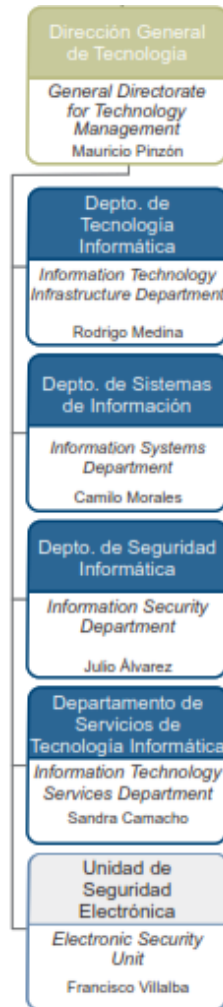


Ilustración 2 Dirección General de Tecnología

Fuente: Banco de la República, 2021. Tomado de <https://www.banrep.gov.co/es/organigrama>

Capítulo 2

Diagnóstico de la Empresa

La Dirección General de Tecnología o en sus siglas (DG-T), es una organización matricial que mejora los procesos corporativos y misionales del Banco de la República, con tecnología desplegada mediante un enfoque basado en los clientes y apropiándose de las mejores prácticas del mercado, cuenta con un talento humano en su interior con alrededor de 200 empleados (DG-T, 2021). La función de esta área es coordinar y dirigir la implementación de políticas y estándares de uso de tecnologías de información, telecomunicaciones, multimedia, seguridad informática y la seguridad electrónica del Banco. Es decir, esta área adquiere y crea activos TI, realiza mantenimientos, presta soporte técnico, ayuda en la operación y brinda seguridad informática. Estos servicios son para todos los usuarios internos del Banco de la República y algunos externos a la compañía.

Ahora bien, la DG-T ofrece dos tipos de servicios, dependiendo del tipo de usuario, el cuál puede ser un usuarios de área interna o de área corporativa; es decir, ofrece un portafolio de servicios básicos donde se encuentra la administración de recursos tecnológicos, como los servicios de navegación y permisos; administración de usuarios en aplicaciones corporativos, es el encargado de asignar acceso a estas aplicaciones; computación personal, provee a los usuarios de estos productos; Soluciones de comunicación tecnológica, en donde se revisa los puntos e instala servicios de red; soporte tecnológico y asesoría, en donde presta soporte a los usuarios internos y externos.

El otro tipo de servicio ofrecido son los corporativos en el cual se realiza aseguramiento y automatización de áreas físicas, por medio de diferentes mecanismos para

garantizar la seguridad del banco; Infraestructura tecnológica y de comunicaciones, puesto que es el encargado de proveer y administrar plataformas tecnológicas, bases de datos y software; Operación y continuidad de los servicios de tecnología; Seguridad informática y electrónica, asesora y atiende incidentes de seguridad; sistemas de información, desarrollando, asesorando y manteniendo en buen funcionamiento estos sistemas.

Para el periodo 2021-2024 según la DG-T (2021) se prevé realizar una serie de cambios tecnológicos, ajustes en los procesos y un cambio en la cultura del trabajo diario, donde se deben concluir proyectos y actualizar sistemas para modernizar algunos procesos misionales de la compañía; además, de migrar a la nube más de 100 sistemas que funcionan actualmente gracias a los centros de cómputo. Otro tema fundamental, es la innovación, donde se pretende generar una cultura en sus empleados de aprendizaje basado en la experiencia y realizar un mejoramiento continuo donde ellos realicen ajustes a los sistemas, con el fin de optimizar los procesos misionales y corporativos de la compañía.

En consecuencia, con lo mencionado anteriormente, la Dirección General de Tecnología con ayuda de sus colaboradores y practicantes plantea para el año en curso, realizar cambios que mejoren las prácticas realizadas, identificando las principales necesidades de los departamentos y priorizando una solución conjunta que permita mejorar los sistemas de la compañía.

Ahora bien, la práctica profesional se realiza en esta área descrita bajo la supervisión de la organización de calidad adscrita al departamento; es decir, para este proyecto, se debe identificar una solución que integre las diferentes necesidades de toda la DG-T y además que esté encaminado a responder a los lineamientos del sistema de gestión

de calidad de la compañía, cumpliendo con los requisitos establecidos en la ISO 9001 para la cual el Banco se encuentra certificado.

En cuanto al Sistema de Gestión de Calidad – SGC-, aplica para el área todos los requisitos de la Norma a excepción del numeral 8.5.4 denominado preservación, puesto que no es necesario conservar las salidas durante la producción y prestación del servicio. Ahora bien, dentro de las generalidades del sistema, el contexto de la organización se encuentra definido y documentado en un manual en donde detalla la planeación estratégica comprende las necesidades y expectativas de sus partes interesadas, como es la planificación y el alcance del sistema de calidad, como también identifica los procesos en los cuales se ejecuta dicho sistema.

Dentro del liderazgo se promueve a sus colaboradores el adecuado manejo del SGC, se sensibiliza sobre la importancia del cumplimiento de éste, definiendo las responsabilidades de cada uno de ellos para con el área y el sistema de calidad; además se encuentra la definición de las políticas y la comunicación también de forma accesible por medio de la intranet del Banco para que sea posible visualizar.

En cuanto, a la planificación el grupo de la organización de calidad con sus directivos del área, determinan los objetivos de calidad de acuerdo con los planes estratégicos de la compañía, se definen los lineamientos a seguir por medio de acciones y además identifica las metas, recursos, responsables y tiempos para que estos puedan ser cumplidos a cabalidad. Dentro de esta planificación también se determina cuáles riesgos y oportunidades existen en el mercado, de forma que no atente al buen funcionamiento del SGC y se aprovechen dichas oportunidades para mejorar.

Como área de TI del Banco, posee recursos, personas e infraestructura limitada, la cual es aprobada dependiendo del presupuesto anual de la organización; por consiguiente, se deben velar a que este tipo de apoyo sea utilizado de la manera eficiente y eficaz, con el fin de preservar el buen funcionamiento de las operaciones y prestar el soporte adecuado a los usuarios. Asimismo, se vela para que su personal tenga los conocimientos adecuados, promoviendo el entrenamiento permanente y necesario para el desarrollo de sus funciones.

El Banco de la República cuenta con una gestión basada en procesos, donde por medio de diferentes herramientas de diagramación como ARIS, es posible definir los procesos, procedimientos, guías e instructivos que cada área realiza como fuente de documentación y estandarización de sus funciones, además esta herramienta permite verificar el organigrama general, como también las descripciones de roles y funciones de los diferentes cargos de la compañía y define las responsabilidades que estos realizan en sus labores diarias.

Los productos y servicios que ofrece el área a sus partes interesadas se planifican y diseñan según las necesidades existentes de estos, estas propuestas son evaluadas por un grupo de profesionales que trabajan en áreas transversales o también denominados BRM. Además, las soluciones tecnológicas que ofrecen pueden ser herramientas elaboradas internamente por los profesionales de la DG-T, por consiguiente, aplica los numerales de diseño y elaboración de productos del sistema de gestión de calidad; adicional a esto, es primordial que aquellas soluciones que sean contratadas por los proveedores sean preservadas y cumplan con los contratados establecidos.

Por último, se realizan constantes seguimientos y evaluaciones de desempeño por medio de un tablero de indicadores que identifica el nivel de cumplimiento de los servicios y productos, como también el nivel de cumplimiento de los objetivos de calidad; todo esto va de la mano con revisiones periódicas por parte de los auditores externos e internos que verifican el adecuado funcionamiento del SGC y documentan las acciones correctivas y de mejora que se deben ejecutar periodo a periodo.

Capítulo 3

Delimitación del Problema

El área de la Dirección General de Tecnología en el Banco de la República ejecuta los procesos corporativos que apoyan las actividades misionales de la compañía para mantener seguros los datos informáticos y documentos relacionados con las actividades de la empresa; asimismo, protege de amenazas externas que deseen sustraer información, realiza mantenimiento tanto en hardware como software, mantiene eficientes los canales de comunicación tanto internos como externos, gestiona licencias software y administra toda la infraestructura de las tecnologías de información.

Una de las principales dificultades evidenciadas en el área es la relacionada con las prácticas realizadas para gestionar los activos de tecnología de información, puesto que la compañía posee una gran cantidad de estos y en su gran mayoría son intangibles; por consiguiente, no se pueden administrar de la misma forma en la que se gestionan los activos tangibles. Todo esto ha generado diferentes repercusiones como lo son: la dificultad con la actualización del inventario real sobre los softwares instalados en el Banco, la falta de documentación requerida para realizar seguimiento de las licencias con el fin de identificar cuáles son sobre utilizadas y subutilizadas, y el realizar un adecuado seguimiento al ciclo de vida de los diferentes productos, entre otras.

Además de esto, al estar integrada el área por cuatro departamentos y una unidad encargada de la seguridad, es posible que existan algunos casos de interdependencias entre las distintas áreas en cuanto a algunos procedimientos que se ejecutan y son transversales a los diferentes departamentos, siendo este un problema, ya que pueden darse casos de falta

de comunicación entre sus empleados para la documentación de los procesos y procedimientos en conjunto en toda el área.

Asimismo, es importante realizar una integración de todas las buenas prácticas que puedan ofrecerse para la gestión de activos de TI con la normatividad que rige actualmente en el Banco, esto con el fin de evitar problemas en cuanto a no contar con una información confiable, ágil, útil y oportuna para la toma de decisiones y la gestión de los activos; además de sobre costos por realizar duplicidad de actividades, reprocesos, pérdidas de tiempo en realizar búsquedas de información y realizar auditorías para identificar los hallazgos y las no conformidades en los procesos. Por consiguiente, se hace fundamental conocer los cambios provenientes en los últimos años sobre el adecuado manejo para la administración de activos TI, identificando las principales guías y normas que aplican, y con estos resultados poder integrar la documentación de los requisitos exigidos por ellas y agilizar la gestión de los activos para el caso.

Ahora bien, los criterios más importantes a tener en cuenta en el desarrollo de esta práctica empresarial son los establecidos en la normativa y las buenas prácticas asociadas a la gestión de activos de tecnología informática, tales como: ISO 19770, Information Technology Infrastructure Library (ITIL), International Association of Technology Asset Management (IAITAM); como también los ciclos de vida de las TI, los inventarios, la gestión de cambios, entre otros; para lograr garantizar un uso eficiente de los recursos, como también reducir costos, mejorar la gestión, y garantizar las políticas corporativas.

Capítulo 4

Antecedentes

Por medio de un caso de estudio “Diseño, análisis, implementación y medida de procesos de gestión de activos software (SAM) basados en la norma ISO 19770-1 y las recomendaciones SAM de ITIL y COBIT 5 para entornos empresariales”, elaborado en una empresa del sector de construcción en Valladolid, España (González, 2018), y cuyo objetivo principal era brindar una perspectiva global de las prácticas SAM que existen y que sirviera de diseño para un modelo que optimizará dichos activos software en la empresa; se puede evidenciar una integración teórica de las buenas prácticas para la gestión de activos TI por medio de esas normas; como también, una propuesta metodológica para la implementación con la puesta en marcha de actividades para analizar los ciclos de vida TI, identificación de inventarios software y hardware, verificación y optimización de licencias, Assement Cloud, soporte a auditorías, medición de uso de software y repositorio de licencias, lo cual orienta el propósito del presente trabajo de grado.

Asimismo, en el estudio “Propuesta de un modelo para mejorar el control de los activos de software en la SUNAT basado en la ISO/IEC 19770”, realizado en una entidad pública peruana, por Alcántara, Palacios, & Vigo (2018), se puede evidenciar que por medio de la metodología “Top-Down” se evalúan los objetivos del negocio, procesos, servicios TI e infraestructura TI, para con estos poder identificar los activos software que debían ser controlados; además del nivel de cumplimiento de estos según la norma ISO/IEC 19770-1. Como resultado se pudo determinar por medio de un diagnóstico situacional las carencias que poseía la compañía en cuanto a los macroprocesos de gobierno y gestión,

donde se elaboraron políticas de gestión de activos y se definieron los roles y responsabilidades, se identificaron falencias en las operaciones, se documentaron procedimientos, herramientas y controles para identificar activos software, gestionar inventario, realizar un adecuado cumplimiento de licencias, adquisición y retiro.

Por otra parte, un estudio realizado por Taslaviña & Miguel (2018) con el nombre de “Lineamientos para la gestión de inventario de servidores para el Banco Caja Social” se buscaba generar un conjunto de buenas prácticas según las diferentes normas para la administración, e inventario de los activos hardware. En este estudio se pudo determinar un marco de referencia en común basado en las normas ISO 19770-1 e ITIL, donde con ellas, se recomendaron posibles acciones para obtener un adecuado manejo de inventarios de elementos hardware, se documentaron procedimientos de actualización y planes de mejora de las prácticas realizadas por la compañía en cuanto a los ciclos de vida, gestión de riesgo, definición de políticas, responsables y equipos, para dar un adecuado seguimiento a la gestión de activos TI.

En la propuesta de “Sistema automatizado de gestión de activos de tecnología de información basado en la norma ISO/IEC 19770-3:2017 en Alfredo Pimentel Sevilla S.A., Lima, 2018”, elaborada por Gonzales (2018) se plantea elaborar un sistema automatizado para la gestión de activos; en donde, además de verificar las políticas, lineamientos, funcionamiento de procesos y responsables según los estándares de la norma para su elaboración, se realizaron entrevistas con los diferentes empleados de la compañía para determinar el nivel de conocimiento y de planificación sobre la gestión de activos. Según los resultados demostraron que existía una mala gestión, puesto que no existía una

estandarización de procesos interdepartamentales, no se hacía el seguimiento del ciclo de vida de los activos, y había falta de exigencia sobre el proceso. Para solucionar estos problemas se utilizaron diferentes actividades las cuales fueron medidas por indicadores, se elaboraron diagramas de flujo para la documentación, diagramas de Gantt para determinar el alcance en tiempo de la implementación de cada objetivo propuesto, diagramas de arquitectura, elaboración de un modelo ER que contiene las interacciones de los servicios; y, por último, se definieron las políticas y las responsabilidades.

En otra investigación titulada: “Beneficios de implementación de las mejores prácticas de ITIL en grandes empresas de la zona metropolitana de Monterrey” realizada por Maisterra (2008), se ejecutaron encuestas a diferentes empresas que implementan estos sistemas, donde el 77% de las empresas experimentó grandes beneficios, se identificaron los factores clave de éxito como: una alta dirección comprometida, cultura de calidad y mejora continua, herramientas certificadas, entre otras. Todo esto pudo concluir el impacto que genera un capital humano capacitado y dispuesto al cambio en las tecnologías de información para generar mejoras significativas, en cómo se percibe tanto los servicios como productos ofrecidos a los clientes.

Por último, en el “Proyecto de implementación de procesos para la gestión de servicios informáticos alineados a las mejores prácticas ITIL en la gerencia de servicios informáticos (GSI) del grupo monómeros S.A” se documentaron procesos en la gestión de incidentes, requerimientos, niveles de servicio, problemas, cambios y de activos. Esto se realizó por medio de diagramas de flujo, donde se identifican las entradas, funciones, salidas, y el personal que ejecutaba los roles con el fin de mejorar los servicios prestados y

generar una directriz base para realizar seguimiento y futuras mejoras de los procesos (Quintero, 2009).

Ahora bien, el Banco de la República cuenta con el sistema de gestión de calidad certificado en sus servicios de TI y procesos que los soportan con la norma ISO 9001:2015, el cual sigue una estructura basada en el ciclo PHVA, se encuentra documentado y se recertifica cada 3 años; también se realizan auditorías periódicas para revisar los planes de mejoramiento. Debido a que presenta una estructura de alto nivel, permite la integralidad de otras normas de la familia ISO, como la 27000 y la 19770, puesto que permite la unidad entre vocabularios y algunos requisitos. Sin embargo, actualmente el Banco no cuenta con ninguna certificación sobre la gestión de activos TI, ni con la ISO/IEC 19770-1 ni con IAITAM; sin embargo, al interior de la compañía, en especial el área de la DG-T se realizan algunas prácticas encontradas en la guía de ITIL, en cuanto a la forma en que se deben gestionar incidentes y eventos; además, existe gran conocimiento en general sobre la funcionalidad que ofrece esta guía, como también la importancia de realizar una implementación de buenas prácticas para la IT Asset Management o ITAM para optimizar la funcionalidad de todo el área en general.

Como conclusión, las investigaciones mencionadas anteriormente, reflejan la importancia de la implementación de buenas prácticas en los sistemas de tecnología informática basándose en diferentes normativas, como lo son la ISO 19770-1, ITIL, y COBIT 5, las cuales son guías para mejorar la administración de la gestión de activos TI, que no han sido implementadas por la compañía. Donde, por medio de seguimientos a los ciclos de vida de los inventarios de software y hardware, y con la aplicación de

herramientas de gestión y la identificación de los requerimientos en los servicios es posible evaluar los costos, mejorar la eficiencia de los productos, y gestionar mejor los activos.

Es decir, estas guías ayudan al mejoramiento de las operaciones del área que al integrarse con los requisitos exigidos en la norma ISO/IEC 19770-1, complementan las buenas prácticas del ITAM. A su vez, al ser de la familia ISO, es posible integrarse con el sistema de gestión de calidad ISO 9001 generando una única documentación, la cual busca ser confiable, ágil, útil y oportuna.

Capítulo 5

Justificación

Esta integración documental llevada a cabo en el área de la Dirección General de Tecnología del Banco de la República nace gracias a la identificación de necesidades de mejoramiento de algunos procedimientos relacionados con la gestión de activos TI como lo son: el adecuado seguimiento a los activos, la determinación del ciclo de vida de los mismos, los inventarios de software, las solicitudes de los usuarios para adquisiciones, entre otros.

Asimismo, el Banco de la República es un órgano emblemático para el Estado Colombiano, por lo que la imagen institucional es un aspecto fundamental con relación al cumplimiento que deben tener los contratistas y operadores, y el desempeño que debe tener la Entidad para con otras entidades nacionales y privadas; y donde se refiere como cumplimiento, el contar con un sistema estandarizado internacional para la administración, control, uso y asignación de los recursos TI.

Bajo este contexto, es de gran importancia que se establezcan diferentes estrategias que garanticen la integridad y disponibilidad de la información en la organización basada en la norma ISO 9001, ISO/IEC 19770-1, en los estándares ITIL y en las certificaciones IAITAM, definidas por organismos internacionales especializados en la estandarización de procesos que se aplican a productos y servicios. Esto ya que las normas ISO permiten el alineamiento de TI con la estrategia de negocio de las organizaciones, el logro de beneficios, la reducción de costos, el control de riesgos y en general mejorar las operaciones de TI en las organizaciones. Paralelamente, los estándares ITIL junto con las

certificaciones IAITAM, permiten gestionar recurso humano competente para el desarrollo de las actividades propias de TI.

Ahora bien, desde hace unos años atrás el Banco de la República ha venido implementado un sistema de gestión basado en procesos, donde por medio de diferentes herramientas, es posible determinar los procesos, procedimientos, roles, aplicativos, salidas y entradas de cada área, para así poder encaminar los resultados esperados a los requerimientos de los clientes, según las mejores prácticas. A esto se le suma, la certificación de calidad que posee el Banco en la Norma ISO 9001, en el que según este se entiende como calidad a (ISO 9001, 2015) “el grado en el que un conjunto de características inherentes cumple con los requisitos”, dentro de estos estándares se encuentra la documentación de procesos y procedimientos para establecer, implementar, mantener y mejorar continuamente los procesos de la compañía y de sus interacciones.

De esta manera, es necesario para lograr esta integración en los requisitos de las normas y parámetros de las guías, el ejercicio de un ingeniero industrial para realizar una integración documental de la gestión de activos TI, con el sistema de calidad que posee la compañía, para unificar los requisitos y obtener un sistema integrado de gestión que facilite la administración de los procesos orientados a los objetivos, reduzca costos por documentación, optimice el tiempo de los procesos, apoye el desarrollo de una cultura organizacional, mejore la comunicación interna, optimice la planeación, auditoría y revisión del sistema de gestión; con un enfoque holístico ayudando con las necesidades de la empresa, y del área en general donde se desarrolla la práctica empresarial.

Capítulo 6

Objetivos

Objetivo General

Realizar la integración documental de la ISO 9001, ISO 19770-1, ITIL e IAITAM, en la gestión de activos de tecnología informática (TI) para mejorar las prácticas del área de Dirección General de Tecnología en el Banco de la República.

Objetivos Específicos

Identificar los marcos de referencia y requisitos en la ISO 9001, ISO 19770-1, ITIL e IAITAM que apliquen a la gestión de activos de tecnología de información propios para el Banco de la República.

Realizar la integración documental de los diferentes estándares de las normas y guías con los procedimientos ya establecidos por el área de Dirección General de Tecnología en el Banco de la República.

Documentar los nuevos procedimientos para dar cumplimiento a la integración de las normas y guías, sujeto al alcance en el tiempo establecido por la práctica empresarial.

Sensibilizar y socializar el trabajo realizado de la integración documental de la ISO 9001, ISO 19770-1, ITIL e IAITAM, en la gestión de activos de tecnología informática (TI) para mejorar las prácticas del área de Dirección General de Tecnología en el Banco de la República.

Capítulo 7

Marco Teórico

Gestión de Activos Tecnología Informática (TI)

El propósito principal de la gestión de activos TI es planificar el ciclo de vida completo de todos los activos TI, para ayudar a la organización a: maximizar el valor, controlar los costos, gestionar riesgos, apoyar la toma de decisiones sobre la compra de activos, reutilizar, jubilar y eliminar activos TI (ITIL FOUNDATION, 2019).

Para asegurar la efectividad de un sistema de gestión de activos TI, es necesario documentar todas las políticas, procedimientos y normas necesarias para su puesta en marcha. Existen instituciones internacionales dedicadas al desarrollo y publicación de normativas, prácticas y pautas para la implementación de los diferentes tipos de sistemas de gestión de activos TI.

Tipos de Gestión de Activos TI

Esta gestión puede basarse dependiendo de los enfoques y objetivos deseados por las organizaciones, algunos de los tipos más comunes de gestión de activos son:

Gestión de activos de TI: también se le conoce como ITAM, que sus siglas en inglés significan IT Asset Management, las cuales según IAITAM (2019) significan "conjunto de prácticas de negocios que incorpora los activos de TI a las unidades de negocios dentro de la organización". Específicamente están dirigidas a los ciclos de vida y costos de todos los activos TI, que ayudan a apoyar la gestión

y toma de decisiones. Es decir, esta gestión incluye todos los elementos de software y de hardware que se encuentran en el entorno del negocio.

Gestión de activos digitales: Freshservice (2018) la define como el conjunto de funciones que contienen la propiedad intelectual de la empresa, y medios electrónicos que se encarga de la gestión de activos digitales, tales como: fotos, videos y datos digitales, que la compañía produce o para los cuales otorga licencias a terceros.

Gestión de activos de software y gestión de licencias: también conocida como SAM, que sus siglas en inglés significan Software Asset Management, la cual tiene como objetivo mantener actualizada la información mediante el uso de inventarios que llevan registros específicos de cada licencia o programa software, como sus características, versión, funcionario asignado, histórico de usos, entre otros. En otras palabras, esta es la gestión de adquisición, desarrollo, implementación, mantenimiento y eventual retirada, que específicamente va dirigida a los activos software (DELOITTE, 2016).

Beneficios de implementar la gestión de activos TI

Así mismo, después de definir los diferentes enfoques se determina que la gestión de activos TI genera impactos positivos en la organización de las empresas, siempre y cuando ésta sea aplicada de manera correcta. Llevando a las empresas a poseer una mejor

gestión administrativa de sus sistemas tecnológicos, aportando importantes ventajas según lo afirma ITIL FUNDATION (2019), como:

- Control: conocimiento acerca de las capacidades de cada activo, existencias, periodo de vida útil, activos en uso, activos disponibles, activos obsoletos.
- Reducción de costos: al tener toda la información acerca de los activos se evita la sobre adquisición de licencias y software. Adicionalmente, se evita los sobrecostos de pagos extemporáneos en el caso de licencias y software bajo suscripción.
- Seguridad: previsión y control de riesgos debido al uso de software ilegal, corrupto o viciado. Así mismo, seguimiento a los roles y/o permisos concedidos a cada usuario, para evitar fugas de información o explotación de permisos.
- Eficiencia: los procesos tanto en adquisición como en asignación de activos, ya no se diversifican hacia otros departamentos permitiendo la reducción de tiempos en ambos casos, impactando en mayores niveles de productividad.

Activos de Tecnología Informática (TI)

Con el continuo avance de la tecnología y la diversificación de los entornos TI cada día se generan nuevos desarrollos que van ampliando la definición de un activo TI. A través del tiempo, muchas organizaciones se han ido separando de la definición exacta del término y han ampliado su librería en torno a la naturaleza de la industria a la que pertenecen (Freshservice, 2018). Algunos de los activos más comunes son:

- Hardware de Infraestructura
- Acuerdos y contratos de instalaciones e infraestructuras

- Software de desarrollo interno
- Licencias de software
- Hardware propio, creado para usuarios finales
- Datos digitales de operaciones

Ciclo de Vida de un Activo TI

Al igual que un activo físico, los activos TI también poseen un periodo de vida útil, ya sea por el lanzamiento de una nueva versión de un software para prestar mejor calidad de uso, o por la limitación de tiempo y destino que pueda tener una licencia, la obsolescencia de un software o hardware, entre otros. Por consiguiente, existen fases que determinan el ciclo de vida, en la ilustración 3 se evidencia el ciclo de vida de los activos TI.



Ilustración 3 *Ciclo de Vida de un Activo TI*

Fuente: Freshservice, 2021, <https://freshservice.com/latam/it-asset-management-software/>

Cada organización, dentro de su gestión de activos TI, puede definir las etapas y duración del ciclo de vida de su hardware, software y derivados. Sin embargo, sin importar la naturaleza del activo, el ciclo inherente siempre es el mismo (Freshservice, 2018), el cual se relaciona a continuación:

- **Planificación:** son todas aquellas decisiones tomadas por los altos directivos para determinar el ¿Qué activo?,¿Para qué se empleará?,¿Cómo se implementará? y, ¿Cuánto Costará a la compañía?, ¿Dónde es frecuente utilizar analistas, expertos en tecnologías, para apoyar este tipo de decisiones que presenten un costo/beneficio sostenible?
- **Adquisición:** son las actividades realizadas para la construcción, compra de software o hardware o arrendamiento de licencias con contratistas o terceros de la compañía.
- **Asignación:** después de la adquisición de los activos TI es necesario integrar el nuevo sistema, donde se realiza la asignación del personal, las actividades de instalación, el establecimiento de políticas de uso/soporte y suministro de acceso para los usuarios.
- **Mantenimiento:** es necesario que se implementen mejoras en los activos, puesto que después de un uso prolongado se generan fallas y actualizaciones, por las que es primordial ejercer planes de mantenimiento preventivo para perdurar el uso de los activos.
- **Retiro:** todos los activos tienen un ciclo de vida útil, cuando estos llegan a su fin, es necesario realizar el retiro, para el caso de activos hardware debe

ser desechado o eliminado, en caso de elementos software se deben cancelar las licencias o los acuerdos de soporte realizados con los terceros.

Norma Técnica ISO 9001:2015

La organización internacional de normalización ISO estableció por medio de diferentes comités en el año 2015 la quinta edición de la norma ISO 9001 denominada sistema de gestión de calidad. La cual pauta una base de requisitos que una organización puede decidir adoptar para certificar que sus productos o servicios cumplen con unos estándares de calidad, además que al implementar dicha norma se obtienen beneficios en la percepción hacia el cliente, mejorando la imagen corporativa y la satisfacción del cliente.

Esta norma, además maneja un enfoque basado en los procesos, el cual permite controlar las interrelaciones e interdependencia entre los procesos del sistema, de modo que se pueda mejorar el desempeño global de la organización (ISO 9001, 2015). Asimismo, al ser una norma de alto nivel, utiliza como metodología el ciclo Planear- Hacer-Verificar-Actuar (PHVA), el cual puede aplicarse a todos los procesos. En la ilustración 4 se puede observar los requisitos de la norma según el ciclo PHVA.

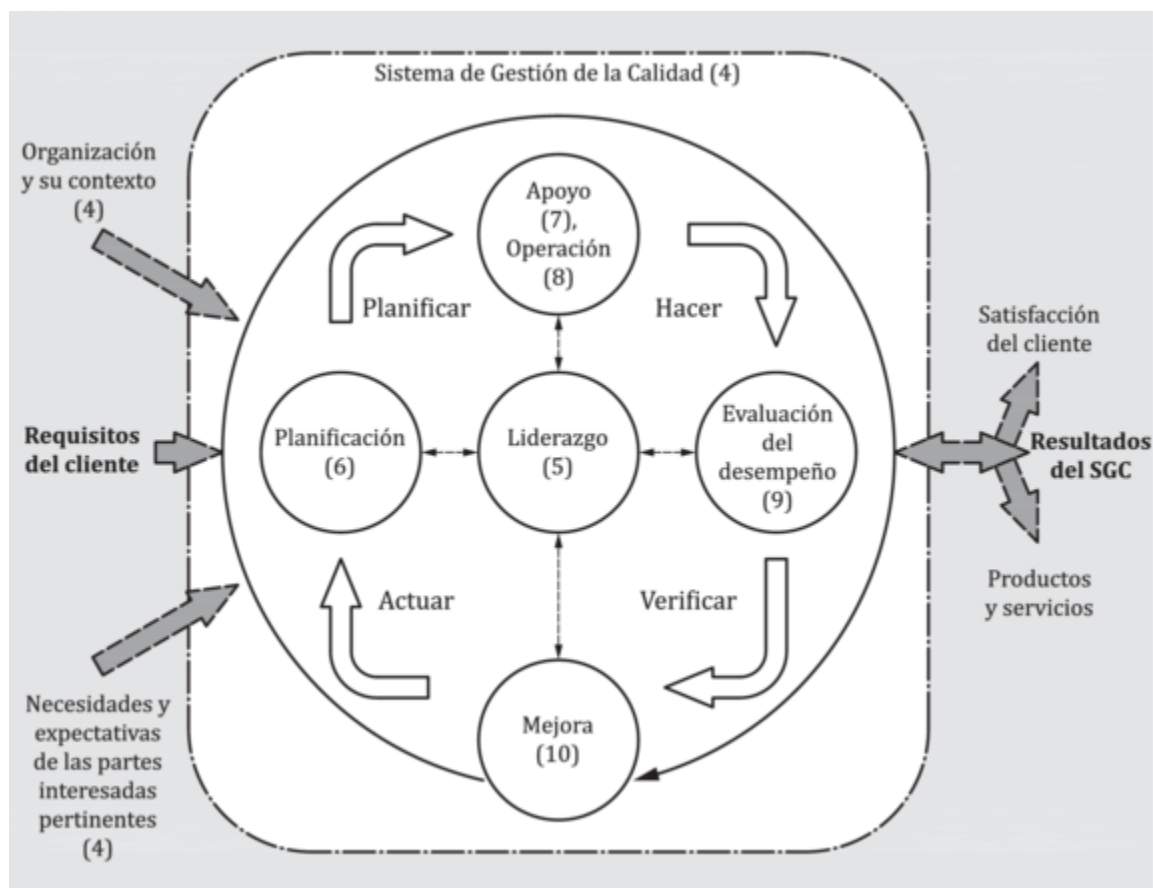


Ilustración 4 Ciclo PHVA, ISO 9001

Fuente: (ISO 9001, 2015), <https://www.iso.org/obp/ui/es/#iso:std:iso:9001:ed-5:v1:es>.

Esta norma (ISO 9001, 2015), los siguientes requisitos que deben ser cumplidos:

1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Apoyo o soporte

8. Operación
9. Evaluación de desempeños
10. Mejora continua

Norma Técnica ISO/IEC 19770

Por medio de la norma ISO 55001: 2014 existían requisitos en común para administrar los activos totales de una compañía (tangibles e intangibles) especificando los requisitos para el establecimiento, implementación, mantenimiento y mejora de un sistema de gestión para la gestión de activos, denominado "sistema de gestión de activos". Pero, se vio necesario crear una norma para realizar una adecuada administración de los diferentes activos de tecnología, que por su naturaleza presentan otros criterios, a los activos físicos.

En el año 1987, la ISO y la IEC conformaron la agrupación de comités especializados en la estandarización de tecnologías de la información TI a nivel mundial. Esta unión nació como un esfuerzo entre las dos organizaciones para evitar duplicados o la posibilidad de crear estándares que sean incompatibles. En el campo específico de tecnologías de la información, la ISO y la IEC establecieron el comité técnico ISO/IEC JTC 1 (ISO, s.f.), y desde su creación el comité ha sido responsable de la creación y publicación de 3.252 estándares, dentro de los cuales se encuentran la ISO/IEC 19770, la cual es el estándar internacional relacionado con la gestión de activos de software (SAM por sus siglas en inglés). El comité responsable de este documento es ISO / IEC JTC 1 Tecnologías de la información Subcomité SC 7, Software e ingeniería de sistema (ISO, s.f.).

La norma ISO/IEC 19770 consta de las siguientes partes, bajo el título general Tecnología de la información - Gestión de activos de software:

ISO/IEC 19770-1: Procesos y evaluación por niveles de la conformidad

ISO/IEC 19770-2: Etiqueta de la identificación del software

ISO/IEC 19770-3: Esquema de derechos de software

ISO/IEC 19770-4: Medición de la Utilización de Recursos (RUM)

ISO/IEC 19770-5: Visión general y vocabulario

ISO/IEC 19770-8: Directrices para mapear las prácticas de la industria hacia y desde los estándares 19770.

Las siguientes subdivisiones aún se encuentran en desarrollo:

ISO/IEC 19770-6: Esquema de Hardware

ISO/IEC 19770-7: Orquestación de elementos de estructura de datos de ITAM

ISO/IEC 19770-10: Sistema de gestión de activos de TI: plan de implementación
ejemplar para ISO/IEC 19770-1

ISO/IEC 19770-11: Requisitos para la auditoría de sistemas de gestión de activos de TI.

La familia de estándares ISO/IEC 19770 está diseñada para ayudar a las organizaciones de todo tipo a implementar y operar un sistema de gestión de activos de software utilizando los avances tecnológicos.

Ahora bien, la norma (ISO/IEC 19770-1, 2017) define como activos TI a todos aquellos artículos adquiridos por una organización para procesar, almacenar y distribuir información digital. Dentro de estos se encuentran: software, medios (físicos y digitales),

equipos de TI (físicos y virtuales), licencias y activos de gestión del sistema ITAM (incluidos los sistemas y herramientas de ITAM, y los metadatos necesarios para gestionar todos los activos de TI). En la ilustración 5 se pueden observar los principales tipos de activos TI.

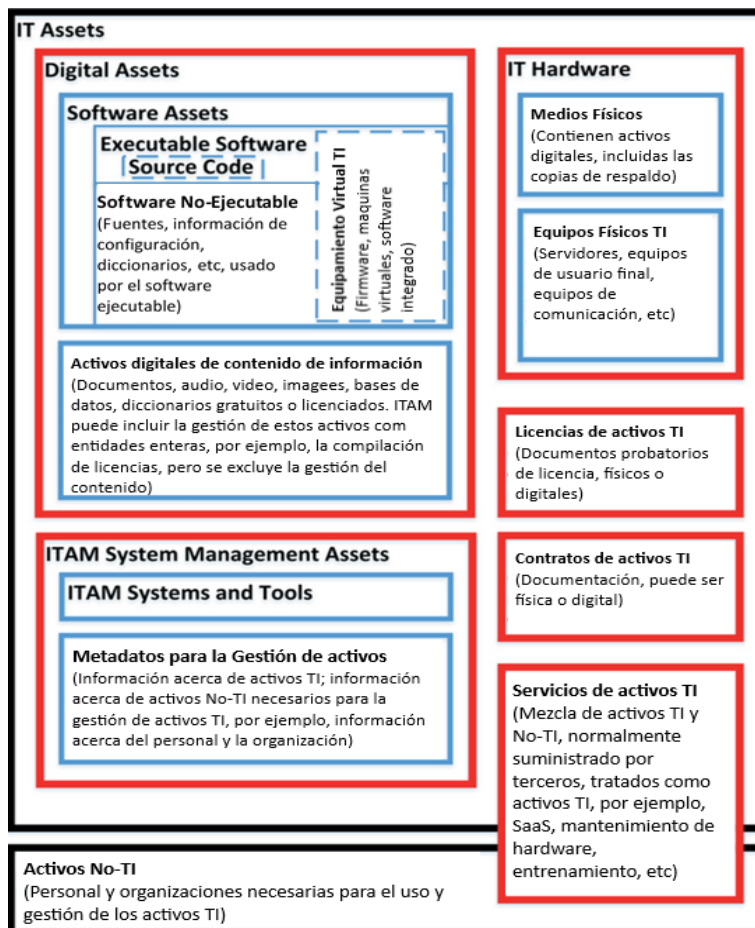


Ilustración 5 Principales tipos de activos TI

Fuente: (ISO/IEC 19770-1, 2017), <https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en>.

Ahora bien, existen 10 requisitos que exige la norma (ISO/IEC 19770-1, 2017):

1. Objeto y campo de aplicación

2. Referencias normativas
3. Términos y definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Apoyo o soporte
8. Operación
9. Evaluación de desempeños
10. Mejora continua

Information Technology Infrastructure Library -ITIL-

La Biblioteca de Infraestructura de Tecnologías de la Información o en sus siglas en inglés ITIL nació en 1989, como una guía de buenas prácticas sobre el uso de las tecnologías de información, el cual va dirigido a organizaciones e individuos que deseen transformar sus negocios alineando los servicios digitales con las necesidades tanto de los clientes como los objetivos de negocio.

El marco ITIL, cuenta con diferentes versiones de sus documentos publicados, donde a medida que han avanzado los años, las tecnologías y las organizaciones han cambiado, generando que sus prácticas estén en constante evolución, por consiguiente, se han ido actualizando dependiendo de los enfoques que se deseen estudiar y se consideren más relevante para la época e industrias. Para el caso de este proyecto se realizará la revisión bibliográfica para las versiones 3 del año 2011 y versión 4 del año 2019.

La versión 3 de ITIL desarrollada por AXELOS presenta un enfoque hacia la gestión de los servicios de tecnología de información, por medio del ciclo de vida de los servicios, el cuál consta de cinco etapas, las cuales se describen en cinco diferentes publicaciones. El conjunto de todos estos documentos incluye las mejores prácticas en cuanto, principios clave, procesos y actividades requeridos, organización y roles, tecnología, desafíos, factores críticos de éxito y riesgos de los servicios de TI.

Dentro de sus publicaciones se definen 26 procesos que complementan el ciclo de vida del servicio, dicho ciclo está compuesto por: la estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejoramiento continuo. Ahora bien, el ciclo de vida del servicio definido por AXELOS (2011), emplea un diseño de centro y distribución o como es conocido en inglés “hub-and spoke”. En el centro se encuentra la estrategia del servicio y alrededor de esta se encuentran los procesos de diseño, transición y operación, que son rodeados a su vez por la mejora continua que apoya en la retroalimentación de todas las etapas. Este modelo permite que se vea la organización de manera holística y que el sistema permita realizar cambios de acuerdo con las necesidades, lo cual genera que los servicios pueden adaptarse y responder efectivamente. En la ilustración 6 se puede observar el ciclo de vida del servicio.

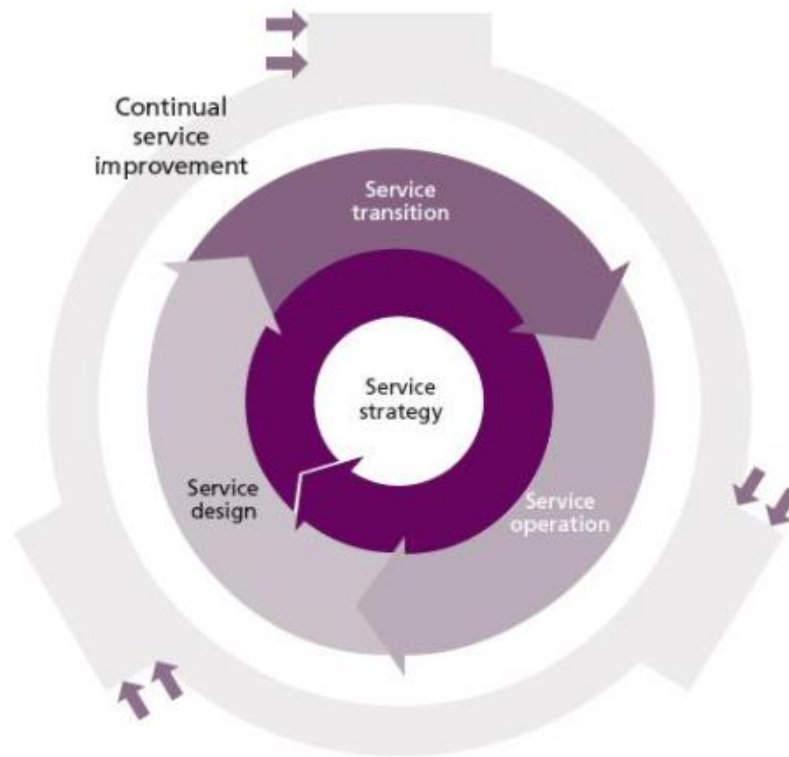


Ilustración 6 Ciclo de vida del servicio TI, ITIL V3

Fuente: (AXELOS, 2011)

Cada publicación ofrece grandes recomendaciones para la administración de los servicios de TI; sin embargo, para administrar la gestión de activos TI estos son los hallazgos encontrados sobre este tema según esta versión.

ITIL versión número cuatro, fue oficializada en el 2019 por AXELOS, este nuevo documento ofrece un enfoque diferente, puesto que cambia el modelo del ciclo de vida del activo por un sistema de valor de servicios (SVS) como todos aquellos componentes que trabajan en conjunto para permitir crear un valor. En esta versión se ofrece un modelo de cuatro dimensiones, las cuales son: Organizaciones y personas; Información y tecnología; Socios y proveedores; Flujos y procesos de valor. En donde estas dimensiones sumadas al

SVS generan un enfoque más holístico y flexible Además en diferencia de los 26 procesos que ofrecía ITIL V3, este presenta 34 prácticas como el conjunto de recursos organizacionales diseñados para realizar un trabajo o lograr un objetivo en común.

Este documento está dividido en 5 capítulos, los cuales son la integración del sistema de valor de servicio se incluyen cinco componentes: Principios rectores, gobernanza, cadena de valor de servicio, prácticas y mejora continua. En la ilustración 7 es posible evidenciar el sistema de valor de servicio donde interactúan los diferentes componentes.

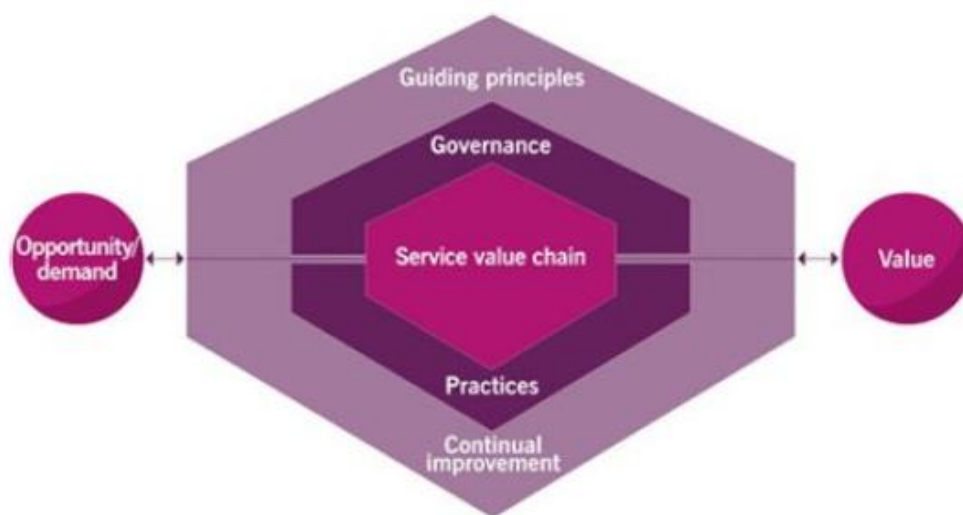


Ilustración 7 Sistema de valor de servicio, ITIL V4.

Fuente: (AXELOS, 2019)

International Association of IT Asset Managers – IAITAM-

La Asociación Internacional de Administradores de Activos de Tecnología de la Información, IAITAM por sus siglas en inglés, es la asociación profesional de personas y organizaciones involucradas en cualquier aspecto de la gestión de activos de TI, la gestión

de activos de software "SAM", la gestión de activos de hardware y los procesos del ciclo de vida que respaldan la gestión de activos de TI en organizaciones de todos los tamaños e industrias en todo el globo (IAITAM, 2020).

Los requisitos que posee una certificación ITAM no son lineales y se trata de un entramado de diferentes departamentos y directrices que funcionan entre sí, como son:

- Adquisiciones
- Identificación de activos
- Disposición
- Certificación
- Legislación
- Financiera
- Políticas
- Proveedores

Esto se observa de una mejor forma en la Ilustración 8, y están siempre dirigidos por un profesional CITAM -Gerente de activos TI certificado.

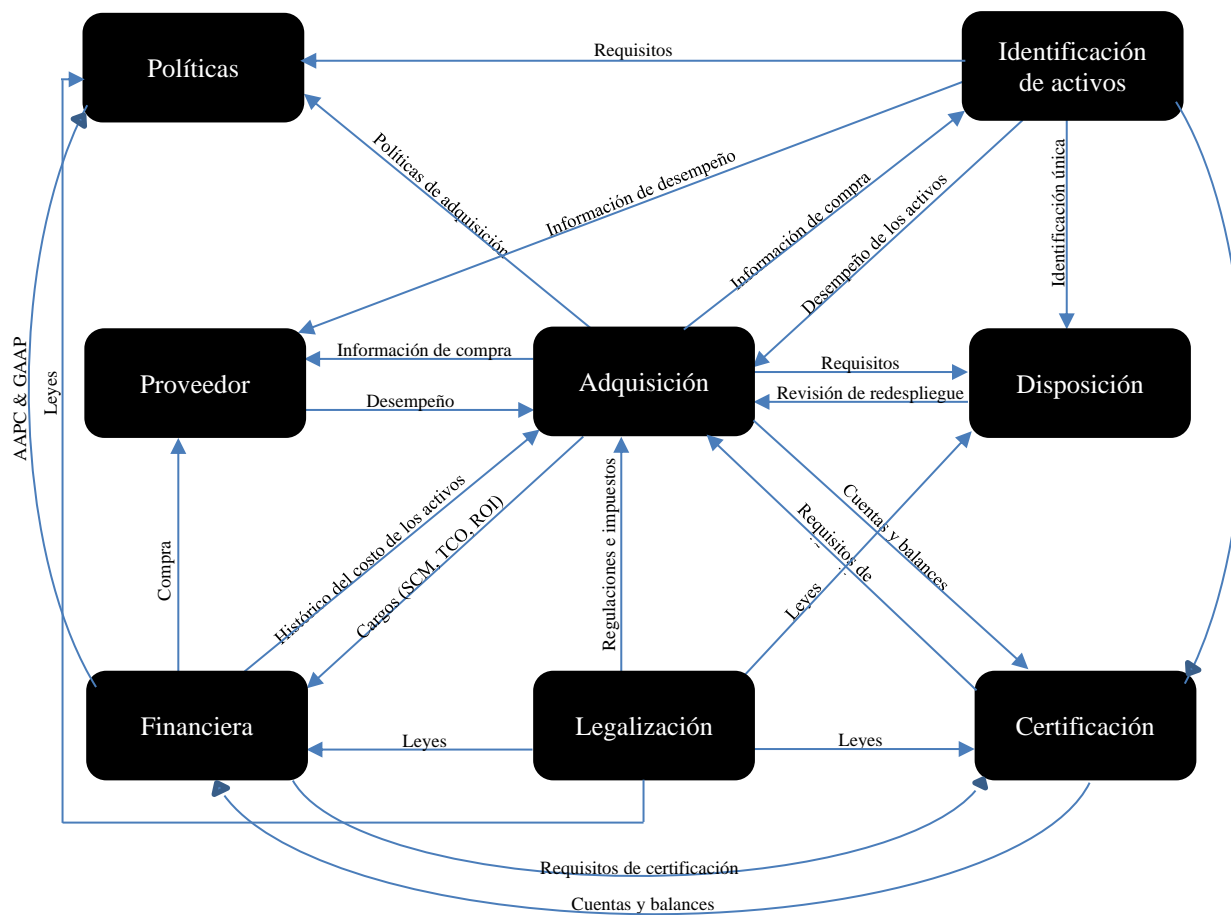


Ilustración 8 Interacción requisitos IAITAM

Fuente: Elaboración propia

NIST 1800-5

El National Institute of Standards and Technology (NIST) es un laboratorio de Estados Unidos que fue establecido con el objetivo de Promover la innovación y la competitividad industrial de este país. Mediante el avance de la ciencia, los estándares y la tecnología de medición (NIST, 2012).

El estándar NIST SP 1800-5 sobre la Gestión de Activos TI, que fue realizada con colaboración del National Cybersecurity Center of Excellence (NCCoE), publicado en el

año 2018, esta guía se desarrolló con el fin de monitorear y administrar las tecnologías de información como activos software y hardware, por medio de ejemplos de empresas del sector financiero. cuenta con 3 volúmenes, donde el primero realiza un resumen ejecutivo sobre el documento en cuestión, el segundo, describe los enfoques, arquitectura y características de seguridad y, por último, una guía de prácticas propuestas.

Sistemas Integrados De Gestión

Es un conjunto de elementos que se interrelacionan sea de una sola disciplina o varias y busca requisitos comunes entre las diferentes normas (ISO), donde se planea de forma en que tiene en cuenta integralmente los objetivos de las diferentes partes interesadas, políticas, procesos, los requisitos. La estructura organizacional, responsabilidades, roles y lineamientos de los distintos referenciales. Este tipo de sistema sigue el ciclo DEMING o comúnmente denominado PHVA. (ISO 9001, 2015)

Marco Legal

En la República de Colombia no existe una estandarización para la gestión de activos TI; aun así, existen legislaciones y normativas relacionadas con software y licenciamiento, que obligan a las empresas a poseer un sistema de gestión de activo TI competente para poder cumplir con la reglamentación nacional. A continuación, se contextualizan algunas de ellas.

Ley 603 del 2000. En la presente Ley se obliga a las empresas a presentar un detallado informe de gestión sobre la evolución de los negocios y la situación económica,

administrativa y jurídica de la sociedad. En donde se resalta además el tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería en Colombia (Manga, 2016).

Ley 1581 de 2012. En el año 2012 se estandarizó la manera en que las empresas recolectaban datos de sus usuarios, impulsando a todas las empresas a integrar dicha información en una plataforma nacional (RNBD) (SIC, 2016). Este movimiento, impulsó a grandes y pequeñas organizaciones a normalizar los procesos en que se recolectaba y entregaba la información de manera digital.

Capítulo 8

Metodología

Dentro de este capítulo se describe la metodología utilizada para el logro de los objetivos planteados en el desarrollo completo de este proyecto. Para esto, se plantea detalladamente las fases y los métodos utilizados y los cuales se encuentran divididos así:

Fase 1: Documentación

En esta fase están descritos los métodos realizados para el desarrollo de los objetivos específicos 1 y 2. La metodología a realizar en esta fase es una investigación Descriptiva Cualitativa, donde según (Mejía, 2020) “es la que describe un fenómeno o situación actual”; es decir, brinda información relativa sobre el problema a investigar.

Principalmente se realiza una recolección de datos e información preliminar por medio de entrevistas diagnósticas para determinar el grado de conocimiento que poseen las personas dentro de la compañía sobre el tema en cuestión, además de identificar si se tiene algún antecedente sobre alguna de estas prácticas documentadas en el interior del departamento. La Población objeto de estudio es la Dirección General de Tecnología del Banco de la República, y la unidad de observación son especialmente los Directivos de cada departamento de la DG-T.

Para esta Fase de documentación se identifican como instructivos los siguientes:

- Narrativa por base de los jefes de los departamentos sobre el tema en cuestión, para el conocimiento de los procesos y procedimientos actuales de la compañía.

- Base de datos en SharePoint, ofimática y Biblioteca Luis Ángel Arango, sobre documentos referentes a la gestión de activos.

Seguidamente con los datos obtenidos de esta información se pretende realizar un estado del arte, sobre las diferentes prácticas que ofrece el mercado; cuáles son los principales exponentes en estos temas e identificar los requisitos y lineamientos de las principales normas y guías que rige la estandarización de estos procesos y procedimientos, con el fin de obtener un marco conceptual detallado.

Después de identificar los marcos de referencia, las normas y guías que existen en el estado del arte sobre la gestión de activos, es necesario adquirir las más relevantes, y con estas realizar un estudio detallado sobre las soluciones que proponen al problema propio del área TI del Banco de la República. Con estos resultados, es posible realizar una asociación de las diferentes normativas y guías en cuanto a la gestión de activos (TI ITIL, IAITAM, ISO 19770 e ISO 9001) y una aproximación a la integración documental con el sistema de gestión de la compañía.

Para esta parte se identifican como instructivos los siguientes:

- Base de datos en la Biblioteca Luis Ángel Arango, sobre normas adquiridas con ICONTEC de la ISO, además de SharePoint y One Drive donde se encuentran las guías adquiridas por IAITAM e ITIL.

Fase 2: Implementación

En esta fase están detallados los métodos para el desarrollo de los objetivos específicos 3 y 4. La metodología a realizar en esta fase es una investigación Descriptiva

Aplicada, debido a que la información recolectada sobre las diferentes normas y buenas prácticas sirven de soporte para la descripción y documentación de procedimientos y actividades, que ayudarán a mejorar la gestión de activos TI del Banco.

Es decir, con base en la documentación de las mejores prácticas sobre la gestión de activos, se realiza una priorización con los directivos encargados del tema, para realizar una propuesta de procedimientos en los cuales se apliquen dichas prácticas y que puedan ser homologados con algunos procedimientos existentes ya en el sistema de gestión de Calidad, o por el contrario sean nuevos para el departamento.

Asimismo, con la integración documental de procesos del área de Dirección General de Tecnología, donde se unifiquen todos los resultados de la investigación, y junto con los procedimientos documentados, se realiza una socialización con el grupo de interés del proyecto para discutir los resultados encontrados, y dar soporte para una futura implementación de otros procedimientos con el fin de capacitar al personal para seguir efectuando dichas prácticas.

Para esta parte se identifican como instructivos los siguientes:

- Base de datos de todos los softwares instalados en el Banco.
- Narrativa por base del autor sobre los resultados encontrados.
- Software como ARIS CLOUD para realizar los respectivos flujogramas y herramientas de Office 365 para documentar los resultados.

Capítulo 9

Resultados y Discusión

En este capítulo se detalla el compendio de los resultados plasmando el alcance de cada uno de los objetivos específicos logrando la integración documental de la ISO 9001, ISO 19770-1, ITIL e IAITAM en la gestión de activos de tecnología informática (TI) para mejorar las prácticas del área de Dirección General de Tecnología en el Banco de la República, el cual es el propósito general del presente Trabajo de grado.

9.1 Marco de referencia y requisitos ISO 9001, ISO 19770-1, ITIL e IAITAM a la gestión de activos de tecnología de información para el Banco de la República

Como primer objetivo específico se tiene la identificación de los diferentes marcos de referencias y guías que aplican a la gestión de activos TI; las cuales, por medio de una priorización realizada con base a la socialización preliminar con los directivos de cada departamento, además de una investigación preliminar en las diferentes bases de datos y fuentes de internet, se identificaron los siguientes normas y guías ISO 9001, ISO 19770-1, ITIL e IAITAM, que son el objeto de estudio para esta práctica empresarial.

9.1.1. Norma ISO 9001:2015

A continuación, en la tabla 1, se evidencia un resumen sobre los numerales de la norma, descritos con el título, casillas donde se identifica si es aplicable para el área de la Dirección General de Tecnología o no y como se cumple el requisito expuesto por la norma en el área.

Tabla 1. Tabla resumen norma ISO 9001:2015

Numeral	Título	Aplica	No aplica	Cumplimiento por el área
4	Contexto de la organización			
4.1	Comprensión de la organización	X		Se encuentra documentado en un manual de sistema de gestión
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	X		Se encuentra documentado en un manual de sistema de gestión, en donde se definen los siguientes: Clientes (personas externas o entidades), Áreas usuarias (áreas internas del banco), Áreas de apoyo (áreas transversales a la DG-T) y proveedores.
4.3	Determinación del alcance del sistema de gestión de la calidad	X		“La prestación de servicios de desarrollo e implantación de sistemas de información, servicios de implementación y operación de infraestructura informática y comunicaciones; servicio de seguridad informática, electrónica y mecánica; así como, los servicios y procesos de soporte, continuidad tecnológica, asesoría y apoyo complementarios que gestiona la Dirección General de Tecnología del Banco de la República”
4.4	Sistema de gestión de la calidad y sus procesos	X		Se encuentra documentado en un manual de sistema de gestión
5	Liderazgo			
5.1	Liderazgo y compromiso			
5.1.1	Generalidades	X		El liderazgo de la compañía se encuentra descentralizada según las actividades de operación, para el caso del área de tecnología, el principal líder es el director general, que responde al subgerente general de los servicios corporativos.
5.1.2	Enfoque al cliente	X		El área comprende las necesidades los clientes, donde por medio de diferentes reuniones, se identifican posibles iniciativas para ser llevadas a cabo, además ofrece por medio de una línea telefónica, comunicación constante para resolver problemas de conectividad en las diferentes plataformas, las cuales son evaluadas por los niveles de cumplimiento de satisfacción de los clientes.

5.2 Política				
5.2.1	Establecimiento de la política de la calidad	X		Se encuentra documentado en un manual de sistema de gestión
5.2.2	Comunicación de la política de la calidad	X		Se realiza por medio de capacitaciones y la intranet del banco, donde se deja a disposición de los usuarios en el portal de SharePoint.
5.3	Roles, responsabilidades y autoridades en la organización	X		Para el sistema en cuestión, el área cuenta con un grupo de personas que verifican el cumplimiento del sistema, además son los encargados de presentar informes, realizar seguimientos y ser intermediarios con los entes externos de ICONTEC y la organización. Este grupo se encuentra descrito en el organigrama, manual corporativo, manual de procesos y procedimientos, descripciones de cargos y reglamento interno.
6 Planificación				
6.1	Acciones para abordar riesgos y oportunidades	X		El grupo organizacional de calidad realiza diferentes reuniones con todos los miembros del área para evaluar los riesgos existentes y prevenirlos según sea el caso, además por medio de reuniones entre los principales integrantes de la compañía, se evalúan oportunidades en el mercado que ofrezcan soluciones a problemas existentes.
6.2	Objetivos de la calidad y planificación para lograrlos	X		Se encuentran documentados en un manual de sistema de gestión.
6.3	Planificación de los cambios	X		Por medio del SharePoint, se publica el plan anual, donde solicita a todas las áreas cumplir con las fechas estimadas y además se realizan acciones de seguimiento para verificar que los cambios sean realizados acorde con lo propuesto.
7 Apoyo				
7.1 Recursos				
7.1.1	Generalidades	X		Los recursos del área son asignados según el presupuesto anual de la compañía.
7.1.2	Personas	X		Estos recursos son proporcionados según las necesidades emergente del área por la transversal de apoyo Recursos humanos, por lo general este personal no rota en gran medida.
7.1.3	Infraestructura	X		Como parte primordial de este numeral, se encuentra la infraestructura de hardware y software, la cual maneja el área de la DG-T, donde provee a las distintas áreas el soporte y computación personal, como también es la encargada de realizar la adquisición y administración de software

				de la compañía. Estas necesidades son evaluadas según los diferentes comités donde se evalúan las necesidades y el presupuesto para la adquisición de nuevos productos. Por otra parte, las edificaciones del Banco en donde se realizan las actividades principales del área son la sede principal en Bogotá, pero sus productos y servicios están ubicados en las distintas sedes alrededor del país, como también en la nube.
7.1.4	Ambiente para la operación de los procesos	X		La organización provee a cada una de sus áreas un ambiente adecuado tanto en infraestructura, como en dispositivos necesarios para la ejecución de sus actividades, estos espacios se encuentran dotados en la sede principal.
7.1.5	Recursos de seguimiento y medición			
7.1.5.1	Generalidades	X		La organización realiza un seguimiento frecuente sobre el alcance de los objetivos, el cumplimiento de sus indicadores, en el cual ha tenido éxito para medir la eficacia del sistema desde hace años atrás, además mantiene la información documentada en las sedes de intranet y SharePoint.
7.1.5.2	Trazabilidad de las mediciones		X	No es aplicable al área
7.1.6	Conocimientos de la organización	X		Se realizan capacitaciones frecuentes sobre los diferentes temas emergentes en el mercado de los productos o servicios, además se promueve a los empleados la realización de estudios sobre cursos, especializaciones, maestrías o doctorados.
7.2	Competencia	X		El nivel de conocimiento de los empleados del área es muy elevado, puesto que la gran mayoría cuanta con mucha experiencia laboral y poseen grandes especializaciones.
7.3	Toma de conciencia	X		Los colaboradores responsables de la implementación del sistema, como aquellos que realizan tareas diferentes a esta, necesarias para las operaciones diarias, conocen las implicaciones de la implementación de este requisito, como logran los objetivos y los beneficios que conllevan esta estandarización, además de que conocen las implicaciones del incumplimiento que generarían riesgos tanto con la seguridad de la información, como el funcionamiento de las actividades que realiza toda la organización.
7.4	Comunicación	X		La comunicación se maneja según fuentes oficiales de intranet, o por aplicaciones de comunicación disponibles solo internamente en los computadores del Banco.
7.5	Información documentada			
7.5.1	Generalidades	X		Todos los documentos relacionados con las operaciones diarias y el sistema de gestión de calidad se encuentran ubicados en la nube de los servidores web del intranet, donde solo se tiene acceso si se ingresa de manera remota a los computadores de la organización. Dentro de estos documentos se encuentran un repositorio de años anteriores.

7.5.2	Creación y actualización	X	Al momento de crearse y/o actualizar los documentos se deben tener en cuenta varios factores, principalmente el nombre, área encargada, fecha, responsable, fuente de información, versión. En los casos de documentación de software o hardware se documenta datos de proveedores, licencias, acuerdos firmados, manual de uso, entre otros.
7.5.3	Control de la información documentada	X	Esta información está disponible solo para usuarios internos de la DG-T, además solo es posible visualizarse por medio de computadores que tenga acceso a la red del banco o por acceso remoto donde se conecten a alguno de estos. Esta información se encuentra dentro de los servidores internos y la nube de la intranet del banco.
8 Operación			
8.1	Planificación y control operacional	X	Por medio de herramientas tecnológicas como ARIS, se realiza la documentación procesos y procedimientos que ayudan al cumplimiento de los requisitos de la prestación de servicio, como también de la creación de productos de software. Donde por medio de reuniones con los directivos del área se determinan los recursos necesarios para la planificación y control operaciones, como también se establecen los criterios con los que estos deben ser aceptados.
8.2	Requisitos para los productos y servicios		
8.2.1	Comunicación con el cliente	X	Esta comunicación puede ser realizada por medio físico, telefónico y electrónico, donde se proporciona una línea de ayuda para resolver dudas, reparar o realizar mantenimientos de los servicios y productos ofrecidos, además por estos mismos medios se realizan retroalimentaciones para verificar que se resuelven las inquietudes y se satisface las necesidades existentes por los clientes.
8.2.2	Determinación de los requisitos para los productos y servicios	X	La organización cuenta con un grupo especial denominado BRM, conformado por diferentes personas de áreas estratégicas, las cuáles ayudan a consolidar las necesidades, requisitos y determinan algunos tipos de productos y servicios que puedan ser transversales o priorizados según la relevancia, por medio de los casos de negocio. Adicional a esto, el área cuenta con un portafolio de servicios definido, estructurado de manera que pueda ayudar a los usuarios internos a cumplir sus tareas diarias y a cumplir las tareas de la DG-T. Este portafolio, posee especificaciones mínimas, para su uso, como manuales de funcionamiento, identificando posibles usuarios autorizados y además disponiendo de personal de soporte.
8.2.3	Revisión de los requisitos para los productos y servicios	X	La organización realiza revisiones de sus diferentes productos y servicios donde se identifican principalmente que los productos y servicios ofrecidos a los clientes cumplan con las expectativas de estos, además cuando se realiza actualizaciones de software o cambios en algún producto por parte del proveedor se evalúan de nuevo los requisitos de estos para verificar que no se incumpla con los contratos de licenciamiento.

8.2.4	Cambios en los requisitos para los productos y servicios	X		Al momento de identificar algún cambio de requisito, se informa a los usuarios sobre las nuevas políticas de uso de los productos y servicios para que estos estén al tanto de los nuevos cambios, además se envía un correo con una carta circular donde especifique y quede guardado en la nube las modificaciones.
8.3	Diseño y desarrollo de los productos y servicios			
8.3.1	Generalidades	X		Este diseño y desarrollo se realiza basándose en una planeación y verificación de requisitos, donde se realizan diferentes actividades para que esta etapa cumpla con la adecuada funcionalidad de los productos.
8.3.2	Planificación del diseño y desarrollo	X		En el caso de alguna creación de software a la medida para dar una solución a una necesidad de los clientes, se planifica primeramente el caso de negocio y se identifica que recursos tanto financieros como de talento humano se utilizarán, los objetivos, beneficios y alcance de la iniciativa en cuestión
8.3.3	Entradas para el diseño y desarrollo	X		La organización determina los requisitos necesarios para diseñar y elaborar un producto o servicio, con base a la funcionabilidad que este desee cumplir, como también se asesora de que estos cumplan con los requisitos legales según las políticas internas, como también políticas del país.
8.3.4	Controles del diseño y desarrollo	X		Se determinan actividades, personal y métodos para que realicen control en el diseño y desarrollo, además se documentan los hallazgos encontrados y como estos cumplen los objetivos planteados.
8.3.5	Salidas del diseño y desarrollo	X		Se verifican que las salidas sean acordes a los requisitos estimados en las entradas, que cumplan con la funcionalidad estimada y que su funcionamiento sea seguro y efectivo.
8.3.6	Cambios del diseño y desarrollo	X		Todos los cambios que se realicen en el diseño y desarrollo, como también los solicitantes de dichos cambios son documentados y se encuentran en la base documental internamente.
8.4	Control de los procesos, productos y servicios suministrados externamente			
8.4.1	Generalidades	X		Las decisiones sobre la realización de procesos, productos y servicios por terceros, se toman por la alta dirección, donde se evalúan a los contratistas, verificando que principalmente cumpla con las legalidades exigidas por el país para la prestación de servicios, como también que ofrezcan servicios y productos certificados o acreditados con alta calidad.
8.4.2	Tipo y alcance del control	X		La prestación de servicios por externos se realiza en actividades que no son propias del desarrollo del área, donde se ejerce un control sobre las salidas de estos, para verificar que cumplan con los requisitos previstos y que cumplen con el sistema de gestión de calidad.
8.4.3	Información para los proveedores externos	X		El área informa a sus proveedores los requisitos que se deben tener en consideración para que estos elaboren las actividades o productos basándose y cumplimiento el SGC, además se debe

			verificar que la compañía tenga un personal calificado y por medio de diferentes evaluaciones se verifica que se cumplan los estándares previstos.
8.5	Producción y prestación del servicio		
8.5.1	Control de la producción y de la provisión del servicio	X	Por medio de diferentes portales web de intranet y por línea telefónica, se presta a los usuarios diferentes formas para solicitar servicios a la DG-T, donde se diligencia formularios para ser atendidos y además se encuentran el portafolio de servicios, estas herramientas permiten realizar un control sobre la información, recursos, personal asignado, tipos de solicitudes. Todo esto para que las actividades puedan ser controladas, además de verificar que se preste el adecuado servicio y exista respaldo para evitar errores humanos y/o prevenirlos.
8.5.2	Identificación y trazabilidad	X	Según el medio por donde se realiza la solicitud, se debe documentar en un expediente sobre el análisis del reporte, soluciones y cierre de los casos, este último con una evaluación del cliente sobre el servicio prestado, todo esto para identificar posibles problemas frecuentes, efectividades de las soluciones y desempeño del personal a cargo.
8.5.3	Propiedad perteneciente a los clientes o proveedores externos	X	La organización debe prevalecer los acuerdos firmados con los proveedores externos para los productos prestados, principalmente licencias, en donde se debe resguardar que sean utilizadas las cantidades adquiridas en el contrato y no se incumpla legalmente con estas, guardando toda la documentación relacionada.
8.5.4	Preservación	X	Se realiza la preservación de todos los documentos referentes a las actividades diarias del departamento, como también
8.5.5	Actividades posteriores a la entrega	X	Se realizan actividades para resguardar el producto final, donde se realizan mantenimientos preventivos, procedimientos para el deshecho de artículos computacionales que deban ser depositados en diferentes dispositivos para resguardar el medio ambiente, además el soporte que se presta para capacitar a los usuarios en el uso de diferentes softwares.
8.5.6	Control de los cambios	X	Al momento de presentarse cambios en la prestación de servicios, se modifican los procedimientos o procesos, en la herramienta ARIS, donde se mantiene documentado el historial de cambios y se procede a publicar según la aprobación de los responsables a cargo, para que se encuentre disponible en los documentos internos de la compañía.
8.6	Liberación de los productos y servicios	X	Se realizan pruebas de revisión antes de la liberación o entrega de un producto al cliente, por medio de diferentes procedimientos de verificación, en el caso de prestar un servicio, se solicita que autorice cerrar el caso de la solicitud, donde se verifica que esta sea cumplida a cabalidad y solucione el problema encontrado, así se verifica que los requisitos se han cumplido para los dos casos.
8.7	Control de las salidas no conformes	X	Al momento de presentarse una salida no conforme reportada por el cliente o por el personal, se documenta en los diferentes portales web sobre una solicitud más detallada por parte de los

				ingenieros para que este incidente sea evaluado y solucionado. Estas también son reportadas para las acciones de mejora que deben realizarse.
9 Evaluación del desempeño				
9.1 Seguimiento, medición, análisis y evaluación				
9.1.1	Generalidades	X		La evaluación de desempeño se realiza dependiendo del periodo acordado por cada área, donde se han definido diferentes indicadores que miden el cumplimiento de las operaciones de la DG-T y se entrega un reporte mensual sobre el nivel satisfacción de estas.
9.1.2	Satisfacción del cliente	X		Por medio de diferentes encuestas hacia los clientes, se define el nivel de satisfacción que ofrece el área hacia los posibles usuarios.
9.1.3	Análisis y evaluación	X		En una herramienta de Excel y con ayuda de SharePoint se realizan los cálculos de los diferentes indicadores, donde se encuentran definidos según una ficha técnica la fórmula de medición, objetivo, niveles de satisfacción o semáforos, como también el periodo y área encargada.
9.2	Auditoría interna	X		Se realiza un seguimiento periódico y se documentan posibles acciones de mejora y correcciones que sean necesarias para un adecuado cumplimiento del sistema de gestión.
9.3 Revisión por la dirección				
9.3.1	Generalidades	X		Anualmente, se realiza una revisión general de la alta dirección sobre el cumplimiento del sistema.
9.3.2	Entradas de la revisión por la dirección	X		Acciones de mejora documentadas durante el periodo y posibles cambios en los documentos que contempla el sistema de gestión.
9.3.3	Salidas de la revisión por la dirección	X		Informe y acta de revisión de cada punto de la reunión, con sus posibles observaciones.
10 Mejora				
10.1	Generalidades	X		El gobierno de la calidad de la DG-T como los responsables de cada área se encarga de documentar las mejoras realizadas para sus procesos.
10.2	No conformidad y acción correctiva	X		Por medio del SharePoint es posible visualizar las acciones de mejora según el área responsable.

10.3	Mejora continua	X		Se realiza un chequeo constante con todas las áreas encargadas para verificar el adecuado funcionamiento del sistema, donde se documentan y se realizan los cambios según se vayan encontrando nuevas soluciones.
------	-----------------	---	--	---

9.1.2. Norma ISO/IEC 19770-1

En la Tabla 2 se evidencia el resumen de los numerales de la norma, con su respectivo título de identificación, además se identifica si es aplicable al área de la DG-T y si actualmente se cumple cada requisito, para el caso en que se cumpla se describe la forma de dar cumplimiento a estos requisitos.

Tabla 2. Tabla resumen Norma ISO/IEC 19770-1

Numeral	Título	Aplica	No aplica	Se realiza actual	Documentos que aplica a la gestión de activos TI
4	<i>Contexto de la organización</i>				
4.1	Comprensión de la organización	X		X	Se encuentra documentado en un manual de sistema de gestión
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	X		X	Se encuentra documentado en un manual de sistema de gestión, en donde se definen los siguientes: Clientes (personas externas o entidades), Áreas usuarias (áreas internas del banco), Áreas de apoyo (áreas transversales a la DG-T) y proveedores.
4.3	Determinación del alcance del sistema de gestión de activos de TI	X		-	No existe un alcance definido para la gestión de activos TI, donde estén determinados los requisitos mencionados en el anterior numeral, ni existe una interacción definida con otros sistemas de gestión, asimismo, puesto que no hay un plan estratégico ni políticas, si se tiene definido un portafolio de productos sobre los activos.
4.4	Sistema de gestión de activos de TI	X		-	Aún no se ha establecido un plan estratégico para la gestión de activos, sin embargo, si se realizan actividades para el adquisición, mantenimiento, retiro y mejora de los activos de software y hardware que hacen referencia al ciclo de vida del activo, como también procesos sobre mitigación de riesgos, vulnerabilidades, incidentes, problemas y eventos también se encuentra establecido el catálogo de servicios
5	<i>Liderazgo</i>				

5.1	Liderazgo y compromiso	X	-	El liderazgo de la compañía se encuentra descentralizada según las actividades de operación, para el caso del área de tecnología, el principal líder es el director general, que responde al subgerente general de los servicios corporativos. Donde se aseguran los recursos, promover la colaboración multifuncional, promover la mejor continua, apoyar otros roles de gestión y asegurar el enfoque para gestionar el riesgo, sin embargo, esta norma exige algunos requisitos adicionales que por el momento no se cumple, los cuales son: Asegurar la política con plan estratégico y objetivos, asegurar la integración de los requisitos, asegurar que el sistema logre los resultados y comunicar la importancia del sistema.
5.2	Política	X	-	No existe documentada una política para la gestión de activos de TI, sin embargo, existen políticas para el retiro y reutilización de los activos, asignación de software y hardware, restricción de software, tratamiento de riesgos y mitigación de vulnerabilidades e incidentes, para controles de acceso, para resguardar la seguridad de la información.
5.3	Roles, responsabilidades y autoridades en la organización	X	-	No existe un grupo especializado que tenga responsabilidades y roles sobre la aplicación de esta norma.
6 Planificación				
6.1	Acciones para abordar los riesgos y oportunidades para la gestión de activos TI			
6.1.1	General	X	X	El grupo de apoyo que evalúa la factibilidad de implementar el sistema, ha realizado análisis sobre las posibles oportunidades y riesgos que puede llegar a producir este sistema.
6.1.2	Evaluación de riesgos de activos TI	X	X	La evaluación de riesgos es un elemento fundamental que se realiza conjuntamente con las áreas del departamento, donde evalúa riesgos de diferentes aspectos, que pueden ser asociados y homologados con la norma ISO 27000. Donde se implementan procesos para identificación de incidentes, problemas y vulnerabilidades principalmente.
6.1.3	Tratamiento del riesgo de activos TI	X	X	Este numeral es homologado a la ISO/IEC 27001:2013, 6.1.2 y 6.1.3, la cual se encuentra certificada la compañía. En donde realizan la mitigación y tratamiento de riesgos asociados con las diferentes áreas del departamento, independiente de que no se tenga un plan estratégico de gestión de activos, se realiza esta mitigación para las plataformas, software, información, equipos hardware, etc., por medio de procedimientos como gestión de vulnerabilidades, incidentes, eventos, problemas y seguridad de la información.

6.2		Objetivos de la gestión de activos de TI y planificación para alcanzarlos			
6.2.1	Especificación del proceso de operación de gestión de activos TI	X		-	Actualmente la compañía no tiene documentados algunos procedimientos que son relevantes para el proceso de gestionar los activos. Sin embargo, posee establecido algunos procedimientos para la gestión del cambio, gestión de la seguridad, asignación de recursos, mantenimiento, adquisición retiro y traslados de activos, entre otros. Pero faltan algunos temas como lo son gestión de licencias y gestión de datos básicos los cuales se ha venido realizando algunas propuestas.
6.2.2	Objetivos de gestión de activos de TI para procesos operativos	X		X	Aunque falta la inclusión de algunos procesos relevantes para dicha gestión, si existe declaración de aplicabilidad para procesos que se encuentran establecidos y cumplen con el sistema de gestión de activos TI, como son demanda y adquisiciones, todos aquellos relacionados con financiamiento como procesos de compras, presupuestos, asignación de recursos; además de procedimientos para mantenimiento y mejora de los activos, retiro y transferencia; procedimientos sobre seguridad electrónica como fuga de datos, incidentes, problemas; además de otros procesos como lo son auditorías y mejoras, informaciones de respaldo y gestión de riesgos.
6.2.3	Objetivos generales de gestión de activos de TI	X		X	Aunque no hay un documento consolidado donde se puedan reflejar los objetivos, si existe la definición de estos, puesto que la razón de ser del departamento es coordinar y dirigir la implementación de políticas y estándares de uso de tecnologías de información, telecomunicaciones, multimedia, seguridad informática y la seguridad electrónica asumida por la Subgerencia General de Servicios Corporativos que tiene como una de las áreas la dirección general de tecnología, en donde se realiza una planeación, diseño, administración y soporte de los activos TI. Por consiguiente, es posible encontrarlos por separado como objetivos de calidad, seguridad informática, objetivos de área sobre el mantenimiento, integración y funcionamiento de los activos de TI.
6.2.4	Planificación para lograr los objetivos de gestión de activos de TI	X		X	Aunque los objetivos del sistema, la política y el plan no estén consolidados en un documento integrado como lo exige esta norma, la razón de ser del área es adquirir, retirar, operar y realizar mantenimiento a todos los activos de TI, para que con ellos puedan prestar soporte a las actividades del Banco. Por consiguiente, si se realizan métodos y procesos para toda la gestión del ciclo de vida del activo, los recursos que se requiere, responsables de los activos y realizan acciones para abordar oportunidades asociadas con estos.
7	Soporte				

7.1	Recursos	X		X	La organización proporciona recursos necesarios para la mejora y establecimiento de los activos de software y hardware, la cual se encuentra en los documentos que definen el presupuesto anual, además el área de talento humano proporciona los recursos en personal calificado para desempeñar las funciones del área de la DG-T, también existen procedimientos sobre la definición del portafolio de servicios donde se encuentran los recursos con los que se trabaja en el área.
7.2	Competencia	X		X	El nivel de conocimiento de los empleados del área es muy elevado, puesto que la gran mayoría cuenta con mucha experiencia laboral y poseen grandes especializaciones.
7.3	Conciencia	X		-	El departamento aún no ha comunicado su intención de implementar esta norma a sus partes interesadas.
7.4	Comunicación	X		X	La comunicación se maneja según fuentes oficiales de intranet, o por aplicaciones de comunicación disponibles solo internamente en los computadores del Banco.
7.5	Requisitos de información	X		-	Aunque se tenga la documentación sobre las compras, información de contratos, licencias, técnica y organización, información la identificación y mitigación de vulnerabilidades, eventos e incidentes, donde se identifican y documentan amenazas y vulnerabilidades de los activos, no se describen la dificultad para controlar las características de estos, la documentación de algunos procesos y procedimientos, tampoco se han determinado algunas características básicas de los activos TI, que se encuentran descritas en el anexo C de la norma, como lo son: complejidad tecnológica (flexibilidad de ubicación, Número y complejidad de componente, tasa de cambio del activo)
7.6	Información documentada				
7.6.1	General	X		-	No tiene la información documentada de algunos requisitos que exige el documento y tampoco información necesaria para la eficacia del sistema como especifica el numeral 7.5.
7.6.2	Trazabilidad de la propiedad y la responsabilidad	X		X	La propiedad y responsabilidad de los activos de TI se encuentran documentados, según el tipo de activo, información de contrato, términos y condiciones, información sobre garantías y renovaciones, usuarios finales, autorizaciones, datos de equipo, licencias, entre otros.
7.6.3	Seguimiento de auditorías de autorización y ejecución de autorizaciones	X		X	Se documentan las autorizaciones, donde se describe la persona que lo realiza, a quien se lo otorga, el activo y fecha de dicha autorización. Además de que se posee un plan de auditorías tanto internas como externas que solo revisan el cumplimiento de los sistemas de gestión, sino que también verifica el buen funcionamiento de las diferentes tareas que realiza el departamento.

7.6.4	Creación y actualización	X		X	Al momento de crearse y/o actualizar los documentos se deben tener encuentra varios factores, principalmente el nombre, área encargada, fecha, responsable, fuente de información, versión. En los casos de documentación de software o hardware se documenta datos de proveedores, licencias, acuerdos firmados, manual de uso, entre otros.
7.6.5	Control de la información documentada	X		-	No existe la cierta información documentada requerida para el sistema, como se mencionaba en los numerales anteriores y tampoco de algunos requisitos de la norma, sin embargo, toda la información del Banco es protegida por tecnologías y herramientas que ayudan a la prevención de fuga de datos, realizan seguimiento de controles de acceso.
8 Operación					
8.1	Planificación y control operacional	X		X	Dentro de los procesos definidos por la compañía se realizan la planificación de recursos y posible demanda, como también para la parte de control operacional aquellos relacionados con el diseño, retiro, adquisición, traslado, mantenimiento, soporte y servicio a los diferentes usuarios. Donde se resaltan procesos para definición de capacidad, portafolio de productos y servicios, control de cambios de operaciones, incidentes, inclusión de software, retiro y reutilización, gestión de eventos, gestión de problemas, soporte de operaciones, gestión de la seguridad de la información, gestión de incidentes, manejo de problemas, vulnerabilidades y pruebas del servicio
8.2	Gestión del cambio	X		X	El departamento cumple con un riguroso proceso para la gestión de cambios, donde se examinan los posibles riesgos establecidos en la norma ISO /IEC 2700, además de mitigar las posibles afectaciones que estas puedan generar.
8.3	Gestión de datos básicos	X		-	Hasta el momento se han empezado a realizar verificaciones sobre la línea base, identificando los software que se encuentran autorizados, sin embargo, el proceso no ha concluido, adicional a esto, se encuentra la documentación de los datos, de manera descentralizada, haciendo que sea difícil acceso a esto, para esto, la organización se encuentra en proceso de consolidar la documentación requerida según la característica de cada activo, donde se pueda encontrar un historial de cambios, número de licencias, alcance del activo, usuarios autorizados, proveedores, cotizaciones, información sobre el ciclo de vida de este. Además, hace falta documentar el proceso sobre la gestión de datos, para que sea estandarizado y ejecutado por los responsables del sistema.
8.4	Gestión de licencias	X		-	A pesar que se revisen y se cumplan los requisitos establecidos y los derechos relacionados sobre las licencias adquiridas , no se encuentra establecido un procedimiento que verifique que se cumpla el uso de estas o de soporte a las auditorias de contratos, sobre el número total de licencias permitidas, tampoco existen medidores

				o indicadores, que ayuden a la trazabilidad para ayudar a la toma de decisiones de los diferentes software sobre los diferentes usos, sin embargo, si existen la gran mayoría de procesos donde se detallan actividades para el traspaso, retiro y adquisición de las licencias, mantenimiento y operación.
8.5	Gestión de seguridad	X	X	la organización tiene estrictas medidas para verificar la seguridad de su información y de sus activos, donde realicen la verificación de incidentes, problemas y vulnerabilidades para mitigar los riesgos existentes y fortalecer los sistemas actuales a cualquier tipo de fuga de datos, realización de pruebas de seguridad.
8.6	Otros procesos	X	X	Dentro de los otros procedimientos que se han establecido en el área, se encuentran aquellos que realizan estimación de capacidad de talento humano, auditorias, verificación de riesgos, seguimiento de indicadores, realización de pruebas de seguridad, portafolio de productos, estimación de recursos, definición de la demanda y soporte a los usuarios
8.7	Subcontratación y servicios	X	X	El departamento exige a sus contratistas el cumplimiento de las normas de seguridad ISO/IEC 27000 y de Calidad 9001, para los productos y servicios que sean adquiridos con uso organización, además se evalúan estos posibles proveedores, con el fin garantizar que sean certificados, también se examinan posibles riesgos que puedan generar los servicios o productos adquiridos, identificando las vulnerabilidades y problemas que afecten al sistema.
8.8	Responsabilidades mixtas entre la organización y su personal	X	X	Se han determinado las responsabilidades y acuerdos de confidencialidad que poseen tanto los usuarios como el prestador de servicio, de acuerdo con el uso de estos con fines laborales, además de que existen mecanismos de verificación de autenticidad y verificación de fuga de datos, para los dispositivos o los accesos de licencias que se adquirió a terceros.
9 Evaluación del desempeño				
9.1	Seguimiento, medición, análisis y evaluación	X	-	A pesar de tener establecidos métodos de análisis y evaluación de seguimiento, estos hacen mayor énfasis, en cómo se cumple de acuerdo a las expectativas de los usuarios internos y externos, hace falta implementar medidas de desempeño para determinar el nivel de rendimiento que tienen los activos con respecto al rendimiento financiero y no financiero, todo esto para determinar posibles mejoras o verificar el adecuado funcionamiento de estos de acuerdo con las tareas diarias estipuladas.
9.2	Auditoría interna	X	-	No se ha estipulado la implementación o el deseo formar de formalización de esta norma, por consiguiente, los auditores internos no tienen conocimiento a estos requisitos. Sin embargo, si se realiza un seguimiento periódico y se documentan

					posibles acciones de mejora y correcciones que sean necesarias para un adecuado cumplimiento del sistema de gestión.
9.3	Revisión por la dirección	X		-	Ya que no se ha estipulado la implementación o el deseo formar de formalización de esta norma, debido a esto, no existen resultados de seguimiento, no conformidades y acciones correctivas que puedan ser presentadas y divulgadas a la alta dirección.
10 Mejora					
10.1	No conformidad y acción correctiva	X		X	Este numeral es común con la norma ISO 9001, donde se realizan acciones correctivas para mitigar los incidentes presentados mientras se realiza el funcionamiento de las actividades del área, como también aquellas no conformidades encontradas en diferentes procesos del departamento, tanto mal funcionamiento de un software, hardware, o servicios prestados por el área realizando las respectivas modificaciones para no alterar en lo posible las actividades diarias.
10.2	Acción preventiva	X		X	El departamento realiza acciones para que el sistema actual no presente fallas futuras, donde se realizan mantenimientos preventivos y frecuentes sobre las diferentes plataformas, softwares y hardware, tanto para hacer chequeos de seguridad, como también implementar mejoras provenientes de los proveedores de estos sistemas y que estos no queden obsoletos.
10.3	Mejora continua	X		X	Se realiza un chequeo constante con todas las áreas encargadas para verificar el adecuado funcionamiento de las tereas cotidianas, donde se documentan y se realizan los cambios según se vayan encontrando nuevas soluciones.

9.1.3. Guía ITIL

A diferencia de las anteriores normas ISO, ITIL no proporciona requisitos en forma de estándares para realizar una certificación con ellos, por el contrario, es una recopilación de buenas prácticas en un manual o Guía. Para el caso de este proyecto se utilizarán como base los 5 capítulos propuesto por ITIL V4, en donde se realiza un enfoque hacia la cadena de valor del servicio.

Los capítulos mencionados anteriormente son: principios reactores, gobernanza, cadena de valor del servicio, prácticas y mejora continua. Para la documentación en este numeral, se tomará como base la norma ISO/IEC 19770-1 con cada uno de sus requisitos y se identificará el capítulo con respecto a ITIL que puede ser homologado pueda tener cierto nivel de referencia al numeral de la ISO, adicionalmente se describirán aquellas sugerencias que propone esta guía, para dar cumplimiento a estos numerales. Además de esto, se utilizarán algunas sugerencias que posee ITIL V3 para aquellos numerales sobre especifiquen sobre la operación de gestión de activos de TI.

En la Tabla 3 se encuentra el resumen de los numerales descritos por la ISO/IEC 19770-1 con el comparativo referencial de ITIL y las buenas prácticas que sugiere esta norma para aplicar a las organizaciones prestadoras de servicios de tecnología.

Tabla 3. Tabla resumen Guía ITIL.

Numeral	Título ISO 19770-1	Comparativo con ITIL	Buenas prácticas de ITIL para la Gestión de activos TI
4	Contexto de la organización	Principios reactivos (PR), Gobernanza(G), Cadena del valor del servicio (CVS), Prácticas (P) y Mejora continua (MC)	
4.1	Comprensión de la organización	PR -Piense y trabaje de manera integral.	La organización debe pensar de manera holística, donde se realice un trabajo transversal, que integre y comprenda todas las necesidades. Para esto, debe evaluar estado actual por medio de: una (FODA), un análisis equilibrado revisión del cuadro de mando, evaluaciones y auditorías internas y externas o combinación de estas.
		PR -Factores externos	Además de identificar los factores internos de la compañía es necesario verificar los factores externos puesto que se trabaja en entornos dinámicos y complejos que generan volatilidad e incertidumbre. Para esto se sugiere utilizar modelos PESTLE (o PESTEL).
		CVS -Plan	Asimismo, la organización debe comprender no solo el estado actual, sino la visión a la que desea llegar y encaminar esfuerzos para garantizar el entendimiento de esta en todas las jerarquías.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	PR -Centrarse en el valor.	Una organización debe identificar directa o indirectamente lo que genera valor para los grupos de interés, aparte de lo mencionado, también es necesario verificar la experiencia de los clientes y usuarios hacia con los servicios.
		PR -Participar	También se deben entablar buenas relaciones con estas partes para mejorar el entendimiento, transparencia y compromiso continuo, donde se vea reflejado en los servicios y productos proporcionados.
4.3	Determinación del alcance del sistema de gestión de activos de TI	MC - ¿Dónde estamos ahora?	El éxito de un sistema depende de una clara y precisa comprensión y definición del punto de partida y el impacto que pueda producir hacia las actividades, personas, infraestructura, productos y servicios de la organización y cómo es posible definir un alcance que se encuentre delimitado.
4.4	Sistema de gestión de activos de TI	PR - Piense y trabaje de manera integral.	Es importante para realizar una gestión eficaz y eficiente e integración dinámica de información, tecnología, organización, personas, prácticas, socios y acuerdos, que deben coordinarse todos para proporcionar un valor definido.

		PR- Empiece donde está.	No es necesario empezar desde cero, para definir un sistema, puesto que pueden existir servicios, procesos, programas, proyectos, personas calificadas, sistemas que se encuentren disponibles y que puedan ser aprovechado, con el fin de facilitar la implementación y ahorrar tiempo y dinero.
		P- Gestión de la estrategia	Es necesario formular un plan estratégico que identifique las metas de la organización y adoptar los cursos de acción y asignación de recursos necesarios para que se realice el logro de los objetivos. También se deben definir el catálogo de productos o servicios que cumplan con las expectativas de los usuarios/clientes y documentar las mejoras necesarias para cambios en las estrategias.
5	Liderazgo	Gobernanza (G), Principios reactivos (PR) y Prácticas (P)	
5.1	Liderazgo y compromiso	G- Gobernanza	La organización debe definir a una persona o grupo de personas para evaluar, monitorear y dirigir el desempeño y cumplimiento de las políticas, estrategias, objetivos, aseguramiento de recursos financieros, recursos tecnológicos para con el fin de cumplir las actividades diarias de la organización.
		PR- Colabora y promueve visibilidad	Un trabajo en conjunto con las personas de la organización y las partes interesadas genera mayor probabilidad de éxitos de aceptación y logro de los objetivos, el cual, requiere información compartida, comprensión y confianza.
		P- Gestión del personal y talento	La ejecución adecuada a esta práctica no solo permite que la organización tenga al personal idóneo para realizar las actividades de la compañía, sino que también crea personas con liderazgo, sean eficaces para posicionar a la organización en un crecimiento futuro.
5.2	Política	G- Gobernanza	El órgano de gobierno es responsable de definir y dar cumplimiento sobre las políticas y cualquier reglamentación externa.
5.3	Roles, responsabilidades y autoridades en la organización	P- Gestión del personal y talento	El buen funcionamiento y cumplimiento de los objetivos en una organización es responsabilidad de todos. Sin embargo, puede existir un grupo de personas que realice las tareas fundamentales para la prestación de servicios de tecnología. Estos deben poseer descripciones de tareas y los objetivos de cada empleado, así como en los contratos con proveedores y contratistas. El asignar a las personas adecuadas permite reducir los atrasos, mejorar la calidad, evita retrabajos provocados por defectos y reduce el tiempo de espera al tiempo que cierra las brechas de conocimientos y habilidades.
6	Planificación	Cadena de valor del servicio (CVS), Principios reactivos (PR) y Prácticas (P)	

6.1 Acciones para abordar los riesgos y oportunidades para la gestión de activos TI			
6.1.1	General	CVS- Plan	En esta parte del proceso, no solo se debe definir los planes estratégicos, tácticos y operativos, sino que también es necesario tomar decisiones en cuanto al financiamiento, arquitecturas, políticas, oportunidades de mejora, riesgos identificados, un portafolio de productos y servicios, requisitos de contrato y acuerdos. Todo esto con el fin de garantizar el logro de los objetivos propuestos.
		PR- Manténlo simple y práctico	Este principio proporciona valor al realizar acciones basadas en el logro de los resultados para producir soluciones prácticas que sean útiles y efectivas, eliminando procesos o servicios que generan efectos no deseados.
		P- Análisis empresarial	Esta práctica tiene como objetivo recomendar posibles soluciones para atender las distintas necesidades y diseñar solucionar un problema empresarial que ayuden al cumplimiento de los objetivos.
6.1.2	Evaluación de riesgos de activos TI	P- Gestión de riesgos	Se deben realizar procesos que integren principalmente la identificación de riesgos, mediciones de probabilidad, impactos y la proximidad de estos, adicional a esto, deben existir actividades como la planificación de las respuestas adecuadas a los riesgos, asignando propietarios y acciones y luego implementarlo, monitorearlo y controlarlo.
6.1.3	Tratamiento del riesgo de activos TI	P- Seguimiento y gestión de eventos	Por medio de un seguimiento a los servicios que se ejecutan en el área se pueden identificar cambios o anomalías que pueden ser denominadas eventos. Estos se pueden clasificar como informativos (sin ejecución de acciones inmediatas, solo análisis del caso), de advertencia (permiten tomar medidas antes de efectos no deseados) y excepciones (son de acción inmediata, puesto que incumple a una norma establecida por la organización).
		P- Administración de incidente	La administración de incidentes, busca minimizar efectos negativos y solucionar tan pronto sea posible. Dichos efectos pueden ser encontrados en sistemas software, mal funcionamiento de plataformas, fuga de datos, daño de servidores, problemas con la red corporativa. Se debe documentar esta información definiendo los síntomas, impacto, CI afectados, acciones completadas y acciones planificadas, con detalle de los tiempos en que se realizan.
		P- Manejo de problemas	Una práctica sobre el manejo de problemas relacionados con el funcionamiento de los activos o con la seguridad informática, ayuda a reducir la probabilidad e impacto de los incidentes y gestiona soluciones provisionales a errores conocidos. Dentro de las actividades que propone esta gestión, es posible encontrar análisis de riesgos, identificación de problemas reiterados, análisis de información por parte de proveedores, software, hardware.

		P- Gestión de la continuidad del servicio	A diferencia de las prácticas anteriores, esta es la encargada de que se mantenga la disponibilidad y el rendimiento de un servicio mantengan en niveles óptimos para el funcionamiento de la organización en caso de un evento de desastre., los eventos menos significativos son denominados incidentes Algunos ejemplos son: Evento político económico, terrorismo, fallo cadena de suministro, crisis pública, ataque cibernético, ingresos perdidos, entre otros.
6.2	Objetivos de la gestión de activos de TI y planificación para alcanzarlos		
6.2.1	Especificación del proceso de operación de gestión de activos TI	CVS- Diseño y transición	Principalmente se asegura de crear y modificar los requerimientos necesarios para que los productos y servicios satisfacen las expectativas de las partes interesadas en cuanto a calidad, costos y tiempo de comercialización. Dentro de esos requerimientos, es posible encontrar políticas, procesos, actividades, determinación de capacidad de personal, entre otras.
		P- Prácticas	Para la aplicación de este numeral, aplican todas aquellas prácticas que se encuentran definidas en el capítulo 5 de ITIL, puesto que, esos pueden desarrollarse como procesos y procedimientos. Las principales prácticas son: Gestión de disponibilidad, de capacidad y rendimiento, control de cambios, incidentes, activos TI, seguimiento y gestión de eventos, gestión de problemas, gestión versiones, mesa de servicio, experiencia del cliente, entre otros.
6.2.2	Objetivos de gestión de activos de TI para procesos operativos	P- Gestión de la estrategia	Se formulan planes que identifique las metas de la organización y métodos para su ejecución y asignación de recursos necesarios para el logro de los objetivos. También se deben definir el catálogo de productos o servicios que cumplan con las expectativas de los usuarios/clientes.
		P- Gestión del catálogo de servicios	Proporciona una información sobre todos los servicio y productos, que dispone el área, para dar soluciones a las necesidades de las partes interesadas, asegurando la disponibilidad para ellos, además proporciona los requisitos necesarios para realizar solicitudes, declaración de aplicabilidad de los diferentes activos software y hardware, como también para la prestación de los servicios.
6.2.3	Objetivos generales de gestión de activos de TI	P- Gestión de la estrategia	Es la misma práctica que se encuentra en el apartado 6.2.2
6.2.4	Planificación para lograr los objetivos de gestión de activos de TI	P- Gestión de la estrategia	Es la misma práctica que se encuentra en el apartado 6.2.2
		CVS- Diseño y transición	Es el mismo paso que forma parte de la cadena de valor del servicio y que se encuentra definido en el numeral 6.2.1

		P- Gestión de proyectos	Esta práctica es la encargada de la planificar, delegar, monitorear y mantener control de todos los aspectos de los proyectos que sean nuevos, de transición o de mejora. ITIL define 2 tipos de métodos los cuales son método cascada (requisitos conocidos y el trabajo es más importante que el tiempo de entrega) y método ágil (requisitos inciertos y cambiantes, se prioriza el tiempo de ejecución)
7	Soporte	<i>Cadena de valor del servicio (CVS), Principios reactores (PR) y Prácticas (P)</i>	
7.1	Recursos	P- Gestión de cartera	Según (AXELOS, 2019), esta práctica es la responsable de ejecutar estrategias de financiamiento y recursos para garantizar la ejecución de programas, proyectos, productos y servicios, que desarrolla la organización. Dentro de las actividades críticas de esta práctica, se encuentra: definición de portafolio de servicio y productos, priorización de proyectos, servicios y productos, evaluación de inversiones, toma de decisiones, evaluar costos y riesgos
		P- Gestión del catálogo de servicios	Es el proceso de diseñar y mantener información documentada sobre todos los servicio y productos del área en cuestión, que son necesario para cumplir con los requerimientos y las necesidades de las partes interesadas, donde se debe asegurar la disponibilidad de estos, y proporcionar información sobre los requisitos necesarios para realizar solicitudes, declaración de aplicabilidad de los diferentes activos software y hardware, como también para la prestación de los servicios. (AXELOS, 2019)
		P- Gestión del personal y talento	Una organización debe integrar para sus operaciones a personas con habilidades y conocimientos para prevenir o reducir los atrasos, mejorar la calidad, evita retrabajos provocados por defectos y reduce el tiempo de espera al tiempo que cierra las brechas de conocimientos y habilidades.
7.2	Competencia	P- Gestión del conocimiento	Esta práctica según (AXELOS, 2019), busca fomentar capacidades y habilidades en los colaboradores para que ellos puedan realizar las operaciones diarias de la organización de acuerdo a las mejores prácticas que están en el mercado, adicional a esto, es importante para dar cumplimiento a los objetivos propuesto y las necesidades de las partes interesadas. Para esto se pueden realizar procedimientos para la adquisición del conocimiento, incluido el desarrollo, la captura y la recolección de conocimiento, ya sea formal y documentado o informal y tácito.
7.3	Conciencia	PR- Colabora y promociona visibilidad	Este principio, busca que se realicen trabajo en conjunto, tanto el personal, organización y partes interesadas, uniendo esfuerzos para lograr los objetivos, sin embargo, para realizar este trabajo en conjunto es necesario que la información sea

			compartida, que exista una comprensión y confianza de todas las partes y que además exista conciencia entre ellos a con las tareas que deben realizar.
		CVS- Participar	Esta parte de la cadena de servicios, invita a la participación iterativa de todos los interesados en la organización y externos, con el fin de que se identifiquen necesidades y sean comprendidas por todas las partes, mejorar las relaciones y tener un compromiso continuo para realizar las actividades y lograr los objetivos propuestos. Para esta parte de la cadena es posible obtener resultados como: demandas definidas y oportunidades, requisitos de productos y servicios, actividades de soporte al usuario, soporte de oportunidades de mejora y comentarios de las partes interesadas, solicitudes de cambio o inicio de proyecto, contratos y acuerdos con proveedores y socios externos e internos.
		P- Gestión del nivel de servicio	Dentro de esta práctica es posible encontrar los acuerdos de nivel de servicio, en donde se documenta los requisitos pactados por el proveedor de servicios y también los acuerdos con los clientes en los cuales se identifica los servicios requeridos y el nivel de servicio esperado por estos, adicional a esto se realizan encuestas y métricas para capturar la percepción que tienen estos con los servicios prestados.
7.4	Comunicación	CVS- Participar	Es la misma práctica que se encuentra en el numeral 7.3.
		PR- Colabora y promociona visibilidad	Es la misma práctica que se encuentra en el numeral 7.3.
		P- Gestión de relaciones	Su principal propósito es establecer y mejorar los vínculos que tiene una organización con sus partes interesadas en los diferentes niveles estratégico y tácticos. Una buena implementación, asegura la comprensión y satisfacción de las necesidades, priorización de los distinto clientes y verificación de quejas y sugerencias.
		CVS- Entrega y soporte	Este proceso de la cadena de servicio realiza actividades como información sobre rendimiento, requisitos de contratos y términos de acuerdos, solicitudes de cambio, prestación de servicios a usuarios, información de finalización de soporte, entre otras.
7.5	Requisitos de información	P- Mejora	Dentro de las prácticas propuestas, se encuentra una específica para realizar mejoras en la organización, donde se especifica que es necesario tener documentación sobre los registros de actividades que se han mejorado en el pasado o que necesitan un cambio.
		P- Gestión de activos de TI	Dentro de estas sugerencias que propone (AXELOS, 2011) en la versión 3, se encuentra la creación de una base de datos de gestión de la configuración o en sus siglas en inglés CMDB, el cuál propone la creación de una base de datos que contenga información relacionada con el hardware, software, documentos asociados y las

			<p>relaciones que existen entre estos, es decir un lugar que contenga el inventario de los activos para poder identificar, controlar y gestionar de una forma única todos estos.</p> <p>Ahora bien, (AXELOS, 2019) versión 4, propone la gestión del ciclo de vida completo de cada activo. Esto incluye la gestión del aprovisionamiento de activos; recepción, desmantelamiento y devolución; eliminación de hardware; reutilización de software; gestión de arrendamientos; y potencialmente muchas otras actividades, donde se debe documentar y tener un registro de datos básicos para cada uno de los activos, con el fin de poder rastrear todas los cambios efectuados tan en el ciclo de vida, como en el funcionamiento de este mismo, dentro de estos documentos es posible encontrar: información de compras, términos y condiciones; solicitudes de asignación de usuario, solicitudes de traslado, soporte de renovaciones, información sobre uso de licencias y solicitudes de retiro.</p>
		P- Gestión del nivel de servicio	<p>Además de lo mencionado sobre los acuerdos de servicio, que poseen documentaciones tanto de los proveedores sobre requisitos pactados y de los clientes, donde se les informa a los acuerdos del servicio y por parte de ellos se reciben retroalimentaciones sobre el nivel esperado de estos. Esta práctica es la encargada de establecer objetivos del servicio, los cuales son evaluados, monitoreados, almacenados estos documentos con los respectivos análisis e informes de métricas.</p>
7.6 Información documentada			
7.6.1	General	P- Prácticas	<p>En este ítem se identifica al conjunto de todas las prácticas que propone ITIL, puesto que en cada una de ellas se debe asegurar una información documentada, sobre los procesos realizado, las actividades, responsables de ejecución, resultados de los servicios prestados, resultados de los activos, políticas, entre otros. Asimismo, se integran las prácticas mencionadas en el numeral anterior 7.5 sobre la mejora y gestión de activos y el proceso de entrega y soporte de la cadena de valor del servicio</p>
7.6.2	Trazabilidad de la propiedad y la responsabilidad	P- Gestión de Proveedores	<p>Dentro de una buena gestión con los proveedores, se encuentra la gestión de los contratos, donde es importante tener una documentación sobre los términos y condiciones, niveles de cumplimiento, gestionar la garantía, renovaciones y/o rescisión del contrato y posibles mejoras que puedan realizarse por parte de estos, es decir, cómo medirán, informarán y mejorarán sus servicios durante la vigencia del contrato.</p>
		P- Gestión de activos de TI	<p>Como se mencionaba en el numeral 7.5, la gestión de los activos debe permitir un adecuado manejo sobre el ciclo de vida de estos, donde para ello, es necesario una cierta documentación requerida con el fin de ser soporte para vigilar y cuidar los activos. Dentro de esto también se encuentra las solicitudes de asignación de usuario</p>

			o de traslado de licencias, donde se debe documentar el responsable del producto, la fecha de asignación, el responsable de la aprobación, el número de licencia o serial asignado, firma del responsable aceptando los términos y condiciones. Todo esto con el fin de que se asuman la responsabilidad de sus cuidados.
		P- Gestión de solicitudes de servicio	Dependiendo del tipo de solicitud gestionada por el usuario, es posible que requiera alguna autorización por parte de un superior o del responsable a cargo, como también pueda que no sea requerido una autorización. Para el manejo adecuado, es necesario crear estándares de operaciones, establecer políticas, cumplir los tiempos de entrega pactados, implementar mejoras y la documentación debe estar almacenada para futuras revisiones de auditoría.
		P- Gestión del nivel de servicio	Es la misma práctica del numeral 7.5, donde se documentan y almacenan los acuerdos de servicio que se tienen con el proveedor y con los clientes.
7.6.3	Seguimiento de auditorías de autorización y ejecución de autorizaciones	P- Gestión de activos de TI	Es la misma práctica mencionada en el numeral 7.6.2.
		P- Gestión de solicitudes de servicio	Es la misma práctica mencionada en el numeral 7.6.2.
7.6.4	Creación y actualización	P-Mejora continua	Dentro de las prácticas propuestas, se encuentra una específica para realizar mejoras en la organización, donde se especifica que es necesario tener documentación sobre los registros de actividades que se han mejorado en el pasado o que necesitan un cambio. Sin embargo, esta práctica y en general ITIL, No especifica el tema de documentación con formatos, fechas, versiones y actualización de estos datos.
		P-Mejora continua	Es la misma práctica mencionada en el numeral 7.6.4
7.6.5	Control de la información documentada	PR- Colabora y promueve la visibilidad	Como se mencionaba en numerales anteriores, esta práctica busca la colaboración de todos los implicados en los diferentes procesos de la organización, donde es primordial que la información sea compartida, que se encuentre disponible para que cada persona pueda verificar los compromisos adquiridos y como se encuentra los procesos.
		P- Gestión de la seguridad de la información	Ahora bien, no solo se debe mantener una información disponible para todos los implicados en los procesos como se mencionaba en las dos actividades anteriores, también es necesario proteger la información por medio de la preservación y gestión de riesgos de confidencialidad, disponibilidad de la información, autenticación y no repudio, revisión y auditoría de control, gestión de identidad y acceso.

8	<i>Operación</i>	<i>Cadena de valor del servicio (CVS), Principios reactores (PR) y prácticas (P)</i>	
8.1	Planificación y control operacional	CVS- Obtener/construir	Esta parte de la cadena de valor del servicio pretende realizar la gestión para asegurar que estén disponibles los servicios, cuando y donde sean solicitados, además de que estos cumplan con las especificaciones acordadas para los clientes. Para esto, es necesario realizar un monitoreo sobre las actividades ejecutadas y si es necesario realizar acciones de mejora para cumplir con los objetivos propuestos.
		P- Mejora	Al igual que en el requisito número 7.5, esta práctica ayuda al control y planificación de las operaciones al tener una información documentada sobre las mejoras en la organización, donde se especifica las actividades que se han mejorado en el pasado o que necesitan un cambio., esto con el fin de tener un monitoreo e identificación clara sobre las mejoras, que pueden ser seguidas hasta la acción final.
		CVS- Entrega y soporte	Al igual que en el requisito número 7.5, esta parte de la cadena de valor del servicio busca que sean entregados y respaldados los servicios con las especificaciones pactadas a los clientes, en donde se obtienen información sobre rendimiento, requisitos de contratos y términos de acuerdos, solicitudes de cambio, prestación de servicios a usuarios, información de finalización de soporte, entre otras.
		P- Gestión de riesgos	Es la misma práctica del numeral 6.1.2, la cual se definió como aquellos procesos que integren principalmente la identificación de riesgos, mediciones de probabilidad, impactos y la proximidad de estos, adicional a esto, deben existir actividades como la planificación de las respuestas adecuadas a los riesgos, asignando propietarios y acciones y luego implementarlo, monitorearlo y controlarlo.
		P- Prácticas	En este ítem se identifica al conjunto de todas las prácticas que propone ITIL, puesto que en cada una de ellas se debe asegurar una información documentada, sobre los procesos realizados, las actividades, responsables de ejecución, resultados de los servicios prestados, resultados de los activos, políticas, entre otros. Asimismo, se integran las prácticas mencionadas en el numeral anterior 7.5 sobre la mejora y gestión de activos y el proceso de entrega y soporte de la cadena de valor del servicio, controles sobre la ejecución de las actividades de operación, controles sobre los resultados obtenidos y satisfacción del cliente.
8.2	Gestión del cambio	PR- Manténlo simple y práctico	La organización debe implementar principios sobre la simplicidad y practicidad de las cosas, donde si un proceso, servicio, acción o métrica no arroja los resultados acordados con las expectativas, es necesario eliminarlo. Por consiguiente, este principio busca generar un pensamiento de cambio práctico, sencillo y útil.

8.3	Gestión de datos básicos	P-Gestión del cambio organizacional	El objetivo de esta práctica según (AXELOS, 2019) asegurar que se implementen los cambios sin problemas y con éxito, generando beneficios duraderos, por medio del establecimiento de objetivos claros, liderazgo fuerte y comprometido, participantes dispuestos y preparados (a través de capacitación, concientización y comunicaciones) y una mejora sostenida.
		P- Control de cambios	El propósito de esta práctica es asegurar que los cambios que sean efectuados se hayan implementado con éxito y que tengan una evaluación de riesgos, en donde por lo general, esta práctica solo se realiza a productos y servicios. Todos estos cambios deben ser autorizados y evaluados por personas que comprenden los riesgos y beneficios y se implemente un cronograma para planificar y ayudar en la comunicación, evitar conflictos y asignar recursos. Según (AXELOS, 2019), identifica tres tipos de cambios: Estándar: son de bajo riesgo y no necesitan autorización adicional. Normal: deben programarse, evaluarse y autorizarse siguiendo un proceso, pueden ser de bajo riesgo, son muy importantes y la autoridad puede tomar decisiones rápidas. De emergencia: se deben implementar tan pronto como sea posible, no se incluyen en el programa de cambios y el proceso de evaluación y autorización se agiliza para implementarse rápidamente.
		P- Gestión de riesgos	Igual al 8.1 integrando los procedimientos, incluyendo la evaluación e implementación de procedimientos de vulnerabilidades, incidentes, problemas y gestión de continuidad del servicio, que han sido nombrados anteriormente.
		P- Gestión de activos de TI	Dentro de estas sugerencias que propone (AXELOS, 2011) en la versión 3, se encuentra la creación de una base de datos de gestión de la configuración o en sus siglas en inglés CMDB, el cual propone la creación de una base de datos que contenga información relacionada con el hardware, software, documentos asociados y las relaciones que existen entre estos, es decir un lugar que contenga el inventario de los activos para poder identificar, controlar y gestionar de una forma única todos estos. Ahora bien, (AXELOS, 2019) versión 4, propone la gestión del ciclo de vida completo de cada activo. Esto incluye la gestión del aprovisionamiento de activos; recepción, desmantelamiento y devolución; eliminación de hardware; reutilización de software; gestión de arrendamientos; y potencialmente muchas otras actividades, donde se debe documentar y tener un registro de datos básicos para cada uno de los activos, con el fin de poder rastrear todas los cambios efectuados tan en el ciclo de vida, como en el funcionamiento de este mismo, dentro de estos documentos es posible encontrar: información de compras, términos y condiciones; solicitudes de asignación de

			usuario, solicitudes de traslado, soporte de renovaciones, información sobre uso de licencias y solicitudes de retiro, políticas de reutilizar y desmantelar activos.
8.4	Gestión de licencias	P- Gestión de Proveedores	Es la misma práctica del numeral 7.6.2, en donde se define que, dentro de una buena gestión con los proveedores, se encuentra la gestión de los contratos, donde es importante tener una documentación sobre los términos y condiciones, niveles de cumplimiento, gestionar la garantía, renovaciones y/o recisión del contrato y posibles mejoras que puedan realizarse por parte de estos, es decir, cómo medirán, informarán y mejorarán sus servicios durante la vigencia del contrato.
		P- Gestión de activos de TI	Como se mencionaba en el numeral 7.5 y 7.6.2, la gestión de los activos debe permitir un adecuado manejo sobre el ciclo de vida de estos, donde para ello, es necesario una cierta documentación requerida con el fin de ser soporte para vigilar y cuidar los activos. Dentro de esto también se encuentra las solicitudes de asignación de usuario o de traslado de licencias, donde se debe documentar el responsable del producto, la fecha de asignación, el responsable de la aprobación, el número de licencia o serial asignado, firma del responsable aceptando los términos y condiciones. Todo esto con el fin de que se asuman la responsabilidad de sus cuidados.
		CVS- Entrega y soporte	Es la misma parte de la cadena de servicio mencionada en el apartado 7.5, en donde se realiza actividades como información sobre rendimiento, requisitos de contratos y términos de acuerdos, solicitudes de cambio, prestación de servicios a usuarios, información de finalización de soporte, entre otras.
8.5	Gestión de seguridad	P- Seguridad de la información	Adicional de lo mencionado en esta práctica en el numeral 7.65, sobre mantener la información documentada, también es necesario que se realicen políticas, procesos, comportamientos, riesgos y controles, detecten incidentes o problemas de forma confiable y rápida y se corrijan, adicional a esto es primordial que esta práctica se realice de manera transversal con las demás prácticas. Los procesos incluidos para esta gestión son los siguientes: gestión de incidentes de seguridad de la información, gestión de riesgos, revisión y auditoría de control, gestión de identidad y acceso, gestión de eventos, procedimientos para pruebas de penetración, escaneo de vulnerabilidades, procedimientos para administrar cambios relacionados con la seguridad de la información, como firewall. cambios de configuración

8.6	Otros procesos	P- Seguimiento y gestión de eventos	Es la misma práctica del apartado 6.1.3, donde por medio de un seguimiento a los servicios que se ejecutan en el área se pueden identificar cambios o anomalías que pueden ser denominadas eventos. Estos se pueden clasificar como informativos (sin ejecución de acciones inmediatas, solo análisis del caso), de advertencia (permiten tomar medidas antes de efectos no deseados) y excepciones (son de acción inmediata, puesto que incumple a una norma establecida por la organización).
		P- Administración de incidente	Es la misma práctica del numeral 6.1.3, donde se busca minimizar efectos negativos y solucionar tan pronto sea posible. Dichos efectos pueden ser encontrados en sistemas software, mal funcionamiento de plataformas, fuga de datos, daño de servidores, problemas con la red corporativa. Se debe documentar esta información definiendo los síntomas, impacto, CI afectados, acciones completadas y acciones planificadas, con detalle de los tiempos en que se realizan.
		P- Manejo de problemas	Esta definición es igual al encontrado en el requisito 6.1.3, donde el manejo de problemas relacionados con el funcionamiento de los activos o con la seguridad informática, ayuda a reducir la probabilidad e impacto de los incidentes y gestiona soluciones provisionales a errores conocidos. Dentro de las actividades que propone esta gestión, es posible encontrar análisis de riesgos, identificación de problemas reiterados, análisis de información por parte de proveedores, software, hardware.
		P- Mesa de servicio	Es la encargada de crear vínculos entre el proveedor del servicio y sus usuarios, donde se reciben solicitudes de información sobre soporte, incidentes presentados y problemas. Estas solicitudes pueden ser provenientes de llamadas telefónicas, portales de servicio y aplicaciones móviles, chatbots, correo electrónico, medio autorizados por las organizaciones para comunicaciones internas como redes sociales corporativas y foros de discusión.
		P- Gestión de solicitudes de servicio	Es la responsable de respaldar la calidad acordada de un servicio mediante el manejo de todos los servicios predefinidos e iniciados por el usuario con solicitudes de manera eficaz. Dependiendo del tipo de solicitud gestionada por el usuario, es posible que requiera alguna autorización por parte de un superior o del responsable a cargo, como también pueda que no sea requerido una autorización. Para el manejo adecuado, es necesario crear estándares de operaciones, establecer políticas, cumplir los tiempos de entrega pactados, implementar mejoras y la documentación debe estar almacenada para futuras revisiones de auditoría
		P- Gestión de cartera	Según (AXELOS, 2019), esta práctica es la responsable de ejecutar estrategias de financiamiento y recursos para garantizar la ejecución de programas, proyectos, productos y servicios, que desarrolla la organización. Dentro de las actividades críticas de esta práctica, se encuentra: definición de portafolio de servicio y productos,

			priorización de proyectos, servicios y productos, evaluación de inversiones, toma de decisiones, evaluar costos y riesgos y llevar la contabilidad
		P- Gestión de proyectos	Esta práctica es la encargada de la planificar, delegar, monitorear y mantener control de todos los aspectos de los proyectos que sean nuevos, de transición o de mejora. ITIL define 2 tipos de métodos los cuales son método cascada (requisitos conocidos y el trabajo es más importante que el tiempo de entrega) y método ágil (requisitos inciertos y cambiantes, se prioriza el tiempo de ejecución)
		P- Validación y prueba del servicio	Garantiza que los nuevos productos y servicios modificados cumplen los requisitos definidos para el cumplimiento de las expectativas de las partes interesadas, los insumos principales son los aportes dados por los clientes, los objetivos comerciales y requisitos. En la validación se gestiona la implementación de servicios y cambios y las versiones, en donde se debe verificar y documentar los criterios de aseguramiento del servicio centrados en la utilidad y la garantía. En cuanto a las pruebas deben llevarse a cabo tanto en sistemas desarrollados internamente como en sistemas desarrollados externamente soluciones, alguna de ellas es: prueba del sistema, integración, rendimiento y capacidad, seguridad, vulnerabilidades, cumplimiento, respaldo, requisitos de garantías, aceptación de usuarios, entre otras.
		P- Gestión del nivel de servicio	Dentro de esta práctica es posible encontrar los acuerdos de nivel de servicio, en donde se documenta los requisitos pactados por el proveedor de servicios y también los acuerdos con los clientes en los cuales se identifica los servicios requeridos y el nivel de servicio esperado por estos, adicional a esto se realizan encuestas y métricas para capturar la percepción que tienen estos con los servicios prestados, incluyendo informes de rendimiento, además se deben realizar revisiones continuos para garantizar que todo eso se cumpla En los acuerdos de nivel de servicio se debe poseer documentaciones tanto de los proveedores sobre requisitos pactados y de los compromisos con los clientes, donde se les informa a los acuerdos del servicio y por parte de ellos se reciben retroalimentaciones sobre el nivel esperado de estos. Esta práctica es la encargada de establecer objetivos del servicio, los cuales son evaluados, monitoreados, almacenados estos documentos con los respectivos análisis e informes de métricas.
8.7	Subcontratación y servicios	CVS- Participar	Es la misma encontrada en el numeral 7.3, la cual invita a la participación iterativa de todos los interesados en la organización y externos, con el fin de que se identifiquen necesidades y sean comprendidas por todas las partes, mejorar las relaciones y tener un compromiso continuo para realizar las actividades y lograr los objetivos propuestos. Para esta parte de la cadena es posible obtener resultados como: demandas definidas y oportunidades, requisitos de productos y servicios, actividades de soporte

			al usuario, soporte de oportunidades de mejora y comentarios de las partes interesadas, solicitudes de cambio o inicio de proyecto, contratos y acuerdos con proveedores y socios externos e internos.
		P- Mejora continua	Dentro de la información documentada que propone esta práctica debe encontrarse detalles sobre como los proveedores medirán, informaran y mejoraran los servicios durante la vigencia del contrato. Si se requerirán datos de los proveedores para operar mejoras internas, que también deben especificarse en el contrato.
		P- Gestión del nivel de servicio	Es la misma práctica que se encuentra en el numeral 8.6.
		P- Gestión de solicitudes de servicio	Es la misma práctica que se encuentra en el numeral 8.6.
		P- Gestión de riesgos	Es la misma práctica del numeral 6.1.2, la cual se definió como aquellos procesos que integren principalmente la identificación de riesgos, mediciones de probabilidad, impactos y la proximidad de estos, adicional a esto, deben existir actividades como la planificación de las respuestas adecuadas a los riesgos, asignando propietarios y acciones y luego implementarlo, monitorearlo y controlarlo. Integrando los procedimientos, incluyendo la evaluación e implementación de procedimientos de vulnerabilidades, incidentes, problemas y gestión de continuidad del servicio, que han sido nombrados anteriormente.
8.8	Responsabilidades mixtas entre la organización y su personal	P- Gestión de riesgos	Es la misma práctica que se encuentra en el numeral 8.7.
		P- Gestión de la seguridad de la información	Es la misma práctica que se encuentra en el numeral 8.6.
		P- Gestión de solicitudes de servicio	Es la misma práctica que se encuentra en el numeral 8.6.
9	Evaluación del desempeño	Prácticas (P) y Mejora continua (MC)	
9.1	Seguimiento, medición, análisis y evaluación	MC- ¿Dónde estamos ahora?	Para identifica el punto de partida del funcionamiento de las operaciones de la organización, es necesario evaluar servicios existentes, incluida la percepción de los usuarios del valor recibido, las personas, competencias y habilidades, los procesos y procedimientos involucrados, y / o las capacidades de las soluciones tecnológicas disponibles.

		P- Mediciones e informes	Se recomienda medir el comportamiento de las actividades para determinar el cumplimiento de los objetivos propuestos, en donde se pueden utilizar Factores críticos de éxito (CSF) e Indicadores clave de rendimiento (KPI). Los datos recolectados en estas métricas deben presentarse en informes o cuadros de mando donde faciliten la toma de decisiones.
		P- Experiencia del cliente y del usuario	Es la medición de la percepción que tiene el cliente sobre los productos y servicios prestados por la organización, donde se incluye el tiempo, la calidad, el coste, fiabilidad y eficacia, la facilidad de uso del producto o servicio, la exposición al riesgo y tratamiento de este. Todos estos parámetros, son fuente para realizar informes.
		P- Validación y prueba del servicio	Garantiza que los nuevos productos y servicios modificados cumplen los requisitos definidos para el cumplimiento de las expectativas de las partes interesadas, los insumos principales son los aportes dados por los clientes, los objetivos comerciales y requisitos. En la validación se gestiona la implementación de servicios y cambios y las versiones, en donde se debe verificar y documentar los criterios de aseguramiento del servicio centrados en la utilidad y la garantía. En cuanto a las pruebas deben llevarse a cabo tanto en sistemas desarrollados internamente como en sistemas desarrollados externamente soluciones, alguna de ellas es: prueba del sistema, integración, rendimiento y capacidad, seguridad, vulnerabilidades, cumplimiento, respaldo, requisitos de garantías, aceptación de usuarios, entre otras.
9.2	Auditoría interna	-	ITIL no especifica temas relacionados con las auditorías internas.
9.3	Revisión por la dirección	-	ITIL no especifica alguna práctica o parte de la cadena de valor del servicio, donde se relacionen temas de la revisión por la alta dirección, sin embargo, las actividades y prácticas incluyen mediciones e informes que permiten ser presentados para la toma de decisiones sobre la operabilidad de los servicios y productos.
10	Mejora	Mejora Continua (MC)	
10.1	No conformidad y acción correctiva	MC- Mejora continua	Es una actividad que debe realizarse recurrentemente en todos los niveles de la organización, para asegurar que el desempeño cumple con los de las partes interesadas y sus expectativas. involucra la planificación e implementación de acciones de mejora, identificar y registra, evalúa y prioriza oportunidades de mejora. ITIL propone una serie de pasos, con el fin de facilitar el entendimiento del proceso por medio de este modelo:

10.2	Acción preventiva	
10.3	Mejora continua	<ol style="list-style-type: none"> 1. ¿Cuál es la visión?: es necesario crear una visión para las mejoras planeadas, además de que debe ser traducida a necesidades específicas, como también debe entender las partes interesadas y los roles de modo que los objetivos sean medibles. 2. ¿Dónde estamos ahora?: El éxito de una iniciativa de mejora depende de una clara y precisa comprensión del punto de partida y el impacto de la iniciativa. 3. ¿Dónde queremos estar?: Este paso debe definir uno o más acciones priorizadas a lo largo del camino para completar la visión de mejora, basado en lo que se conoce en el punto de partida. 4. ¿Cómo llegamos allí?: Basado en lo anterior se puede elaborar un plan para abordar los desafíos de la iniciativa. Donde se pueden experimentar pruebas para elegir los caminos y trabajar en una serie de iteraciones que ayuden a progresar, reevaluar el enfoque y si es necesario cambiar la dirección. 5. Actúe: Esto podría implicar un enfoque tradicional de estilo cascada, pero podría ser más apropiado seguir un enfoque ágil experimentando, iterando, cambiando de dirección o incluso volviendo a los pasos anteriores. No importa si el cambio es pequeño, en algunos casos el mayor cambio es la implementación de múltiples mejoras menores. 6. ¿Llegamos allí?: Debe verificar si se ha alcanzado el punto de a dónde queremos llegar. 7. ¿Cómo mantenemos el impulso?: En este punto son importantes las prácticas de gestión del cambio organizacional y gestión del conocimiento. Si la mejora fue un éxito, es necesario empezar a reforzar cualquier nuevo método introducido, con el equipo de trabajo para garantizar que el progreso realizado no se pierda y generar mayores impulsos. Si los resultados no fueron los deseados, se debe realizar un análisis de mejora del porqué no funciono y comunicar a las partes interesadas documentando las lecciones aprendidas y cómo es posible realizar de otras maneras.

9.1.4. Guía IAITAM

El objetivo propuesto por este trabajo para este numeral era la identificación y documentación de las buenas prácticas propuestas por IAITAM que apliquen a la gestión de activos de tecnología de información propios para el Banco de la República. Sin embargo, no fue posible realizarse la adquisición de esta guía en el tiempo destinado para la realización de esta práctica empresarial, por consiguiente, se optó por realizar un cambio de marco de referencia, en donde fueron evaluados los diferentes marcos gratuitos, disponibles en el mercado y que sean referentes en servicios de tecnología, donde se seccionó la guía NIST.

El National Institute of Standards and Technology o en sus siglas en inglés NIST, posee una documentación sobre diferentes estándares realizados para ayudar a las empresas de Estados Unidos a ser más competitivas. Para el caso de este proyecto, se utilizará el marco de referencia NIST 1800-5, denominada Gestión de activos de TI.

Esta guía consiste en un estudio realizado por este instituto con base a las empresas del sector financiero, donde presenta diferentes soluciones enfocadas únicamente sobre las tecnologías a implementar para rastrear la ubicación y configuración de dispositivos y software en red en una empresa. Abarca el seguimiento de activos físicos tradicionales, información de activos de TI, seguridad física e información de vulnerabilidad y cumplimiento (NIST, 2012).

Ahora bien, esta guía como ITIL no proporciona requisitos en forma de estándares, simplemente es una recopilación de buenas prácticas, en donde su documento consiste en

3 volúmenes, el primero es un resumen ejecutivo, el segundo es el enfoque, arquitectura y características de seguridad y el último es una guía de prácticas sobre la adecuación de tecnologías para que ayuden la implementación de los enfoques explicados en el anterior. Para el caso de este proyecto se utilizarán como base los dos primeros volúmenes, puesto que, las tecnologías de implementación no cubren el alcance de este proyecto.

En la Tabla 4 se encuentra el resumen de los numerales descritos por la ISO/IEC 19770-1 con el comparativo de las buenas prácticas que sugiere la guía NIST para aplicar a las organizaciones de los sectores financieros.

Tabla 4. Tabla resumen Guía NIST

Numeral	Título ISO 19770-1	¿Existe información relacionada?	Comparativo con guía NIST
4 Contexto de la organización			
4.1	Comprensión de la organización	NO	Esta guía no especifica acciones que se deben emprender para la comprensión de la organización, como tampoco acciones sobre la comprensión de necesidades y expectativas de las partes interesadas, ni una determinación del alcance del sistema, proporciona propuestas a los problemas más comunes que poseen las empresas del sector financiero, en cuanto al manejo de la seguridad y mitigación de riesgos informáticos, como también a la gestión de activos de TI.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	NO	
4.3	Determinación del alcance del sistema de gestión de activos de TI	NO	
4.4	Sistema de gestión de activos de TI	SI	La gestión de activos de TI, no es una implementación de diferentes actividades independientes que cumplan a diferentes problemas identificados, este sistema debe tener una planificación y definición de los objetivos, procesos, métodos de monitoreo, identificación de riesgos y mitigación de estos y políticas de retiro, para que sea una implementación conjunta, que se interrelacione con diferentes prácticas y pueda dar el adecuado seguimiento al ciclo de vida del activo, con el fin de tener una gestión perdurable.
5 Liderazgo			
5.1	Liderazgo y compromiso	NO	Como se mencionaba anteriormente, esta guía no proporciona acciones o indica como debe apoyar la alta dirección para la implementación de esta gestión, por consiguiente, no detalla el compromiso y liderazgo que deben tener los colaboradores.
5.2	Política	SI	La organización debe establecer políticas para la gestión del sistema, en donde aparte de estas generales, la guía propone que deben establecerse políticas para la gestión del ciclo de vida, y seguridad, tales como: retiro de los activos, restricción de software, para el tratamiento de riesgos y mitigación de vulnerabilidades e incidentes, para controles de acceso, para resguardar la seguridad de la información, entre otras.
5.3	Roles, responsabilidades y autoridades en la organización	NO	No se detallan acciones para la definición de roles y responsabilidades de la organización a con el sistema.
6 Planificación			

6.1 Acciones para abordar los riesgos y oportunidades para la gestión de activos TI			
6.1.1	General	SI	Esta guía especifica que, para una implementación adecuada del sistema integrado en cuanto a la seguridad informática y la gestión de activos, es necesario que se realicen procesos sobre la evaluación y mitigación de riesgos, en donde se deben realizar actividades de establecimiento de políticas, identificación, estimación, priorización de los riesgos referentes con la operación tanto las actividades organizacionales, como de los activos de TI. Otra parte de esta gestión incluye procesos para la identificación, análisis y tratamiento de las amenazas y vulnerabilidades. Algunos de los controles de seguridad que propone esta guía son los siguientes: Creación de políticas para el control de acceso, auditoria de eventos, detección e informes de anomalías, escaneo de vulnerabilidades, monitoreo de las actividades del usuario, monitoreo y seguimiento continuo de los activos conectados a la red y una transmisión de datos segura, para prevenir la fuga de información.
6.1.2	Evaluación de riesgos de activos TI	SI	
6.1.3	Tratamiento del riesgo de activos TI	SI	
6.2 Objetivos de la gestión de activos de TI y planificación para alcanzarlos			
6.2.1	Especificación del proceso de operación de gestión de activos TI	SI	Las organizaciones que deseen tener éxito en la implementación de un sistema de gestión TI, deben realizar procesos para conocer y controlar qué activos posee la compañía tanto virtuales como físicos, planificar los recursos tanto financieros como de activos y servicios, implementar políticas y objetivos para determinar el buen funcionamiento y que la organización cumpla con los requerimientos tanto en términos y condiciones de los productos, acuerdos de servicios, seguridad en la información, prevención de fuga de datos, realizar adquisiciones y todo lo que implica con el tratamiento de elegir la mejora herramienta o sistema acorde con las necesidades, permitir a los administradores definir y controlar el hardware y el software que se pueden conectar al entorno corporativo, definir los servicios proporcionados a los clientes, monitorear y evaluar el ciclo de vida del activo, realizar inventarios de los activos, gestionar los datos e información documentada necesaria, retirar y reutilizar software o hardware, detectar, prevenir y responder a incidentes, monitoreo continuo de hardware y software no aprobados y monitoreo continuo de vulnerabilidades y aplicación de parches / actualizaciones aprobadas por la empresa.
6.2.2	Objetivos de gestión de activos de TI para procesos operativos	SI	
6.2.3	Objetivos generales de gestión de activos de TI	SI	
6.2.4	Planificación para lograr los objetivos de gestión de activos de TI	SI	
7 <i>Soporte</i>			
7.1	Recursos	SI	Esta guía no proporciona una idea sobre los recursos de infraestructura, ni de personal a cargo, sin embargo, hacer referencia y recalca que es importante tener recursos financieros para la adquisición de las diferentes herramientas que ayudan a gestionar los activos de TI,

			como también las que soportan las actividades diarias para el software y hardware, por consiguiente debe existir un procedimiento donde se asigne y planifiquen estos recursos económicos y como se mencionaba anteriormente la definición de productos y servicios para la prestación de los servicios.
7.2	Competencia	NO	Esta guía no contempla nada referente al personal a cargo, donde no identifica si estos deben tener algún tipo de conocimiento, competencias de estos ni tampoco como se interactúa entre la organización para tener un mejor entendimiento sobre lo implementado
7.3	Conciencia	NO	
7.4	Comunicación	NO	
7.5	Requisitos de información	SI	<p>En cuanto a los requisitos de información que propone esta guía se encuentran aquellos que sean referentes a la identificación y mitigación de vulnerabilidades, eventos e incidentes, donde se identifican y documentan amenazas y vulnerabilidades de los activos, fuentes y foros de intercambio de información, adicionalmente, los registros de auditoría en donde se documentan, implementan y revisan de acuerdo con las políticas establecidas.</p> <p>Otro tipo de información necesaria es la recopilación de licencias, términos y condiciones, almacenamiento de datos, es decir realizar copias de seguridad, inventario de los activos, información de los activos que apliquen para el monitoreo del ciclo de vida, como renovaciones, versiones, actualizaciones, funciones, propietario de este, facturas de compras y contratos y la información sobre el software instalado y autorizado.</p>
7.6	Información documentada		
7.6.1	General	SI	En el numeral 7.5 se incluye toda la información documentada que debe tener la organización sobre el sistema, sin embargo, no especifica en información documentada para todas las operaciones fuera de la gestión de TI.
7.6.2	Trazabilidad de la propiedad y la responsabilidad	SI	<p>Las políticas y el gobierno corporativo son todas las reglas que se imponen a los activos de TI. Estas reglas pueden incluir la red / sitios web que los empleados pueden visitar, qué software se puede instalar y qué servicios de red están permitidos, estas políticas deben ser comunicadas y estar disponibles para ser consultadas por los usuarios, adicional a esto, se debe mantener información referente a los contratos y términos y condiciones con los proveedores, con el fin de cumplir y hacer llegar esto a los usuarios.</p> <p>A pesar de esto, no existe una mención sobre las responsabilidades que tienen los proveedores de los activos y servicios a con la organización sobre información de actualizaciones y mejoramiento de versiones.</p>

7.6.3	Seguimiento de auditorías de autorización y ejecución de autorizaciones	NO	No se hace referencia sobre las autorizaciones que deben recibir los usuarios por parte de los directivos o jefes inmediatos para que puedan ser asignados un activo de hardware o software.
7.6.4	Creación y actualización	NO	No existe nada relacionado sobre la creación y actualización de los formatos tanto para el sistema, como para una norma.
7.6.5	Control de la información documentada	SI	Toda la información documentada mencionada en el numeral 7.5 debe estar protegida, por medio de tecnologías que aseguren la visibilidad solo a personal autorizado, es decir, realizar controles de acceso, con el fin de prevenir fuga de datos, esto por medio de y sistemas de seguridad, como firewalls y sistemas de detección de intrusos y administración de identidad y acceso (IDAM).
8 Operación			
8.1	Planificación y control operacional	SI	En cuanto a la planificación y control operacional, se deben mantener principalmente la información documentada de los procesos realizados, como también de la documentación descrita en el numeral 7.5, adicional a esto, es necesario realizar auditorías para mantener el control adecuado de los operaciones diarias e identificar los criterios sobre los cuales se van a basar lo procesos que soporten la gestión de activos y como puede integrarse con todas las actividades para mitigar los riesgos como se menciona en los numerales del 6.1
8.2	Gestión del cambio	SI	No se especifica nada sobre como implementar los cambios en la organización pero si como identificar los riesgos que puedan generar dichos cambios, dichos riesgos se evidencian en los numerales del 6.1, donde se debe incorporar análisis de amenazas y vulnerabilidades, y considera las mitigaciones proporcionadas por los controles de seguridad planificados o implementados, además, de proteger el control de acceso y realizar monitoreo de personal, conexiones, dispositivos y software utilizados, para detectar posibles eventos de ciberseguridad.
8.3	Gestión de datos básicos	SI	Dentro de la gestión de datos básicos, las organizaciones deben realizar procesos para conocer y controlar qué activos posee la compañía tanto virtuales como físicos, permitir a los administradores definir y controlar el hardware y el software que se pueden conectar al entorno corporativo, realizar inventarios de los activos, gestionar los datos e información documentada necesaria para el ciclo de vida como renovaciones, versiones, actualizaciones, funciones, propietario de este, facturas de compras y contratos, la información sobre el software instalado y autorizado, propietario, etiquetar un activo, registrar número de serie y otros atributos de la base de datos.
8.4	Gestión de licencias	SI	En cuanto a la gestión de licencias, se deben establecer políticas para que se cumplan los acuerdos de servicios pactados con los proveedores, auditorias para revisar el cumplimiento de los contratos, es decir que las licencias adquiridas sean las utilizadas, también, procesos

			para retirar y reutilizar software e implementación y monitoreo continuo sobre las actualizaciones y nuevos parches a implementar, que han sido recibidos por los proveedores.
8.5	Gestión de seguridad	SI	En cuanto la gestión de la seguridad, la guía identifica los procedimientos claves que debe tener toda organización prestadora de servicios financieros, los cuales son: identificación y mitigación de vulnerabilidades, gestión de riesgos, gestión de incidentes y problemas relacionados con la ciberseguridad. Donde con ellos permite respuestas más rápidas a las alertas de seguridad al revelar la ubicación y el propietario de un dispositivo, ayuda a centrarse en los activos críticos, reduce el ataque de las máquinas, detecta y alerta cuando dispositivos no autorizados intenten acceder a la red, hace cumplir las políticas de restricción de software relacionadas con el software que puede ejecutarse en el entorno corporativo.
8.6	Otros procesos	SI	Dentro de los otros procesos que se deben realizar para la gestión de activos se encuentran aquellos relacionados con la atención del servicio y solución de problemas a los usuarios, donde lo determinan como mesa de ayuda, que permite ser un soporte de colaboración con el personal cuando este tenga algún inconveniente con un producto y otro proceso que menciona la guía es el del retiro y re utilización de activos hardware, en donde se establecen políticas para eliminación de datos, número de serie en la base de datos y retiro físico de las instalaciones de la empresa.
8.7	Subcontratación y servicios	NO	No se especifican temas relacionados con la subcontratación de servicios.
8.8	Responsabilidades mixtas entre la organización y su personal	NO	No se hace referencia sobre los procesos y actividades, implicaciones y responsabilidades que se ven afectados por responsabilidades mixtas entre la organización y su personal.
9 Evaluación del desempeño			
9.1	Seguimiento, medición, análisis y evaluación	SI	Se deben hacer seguimientos, informes, análisis y evaluaciones a los informes sobre software instalado, software utilizado, monitoreo a hardware y software no aprobados vulnerabilidades, donde se evalúen conexiones, dispositivos, actividad del personal estado de cumplimiento de políticas, y transmisión de datos.
9.2	Auditoría interna	NO	En cuanto a las auditorías, solo especifica estas acciones para verificar el cumplimiento de la seguridad, el cumplimiento de la gestión de activos y sobre problemas, incidentes y vulnerabilidades encontradas en el transcurso de la operación.
9.3	Revisión por la dirección	NO	No existe referencia como se mencionaba en el capítulo 4 sobre las implicaciones que tiene la alta dirección en esta guía de gestión de activos de TI y seguridad.

10 Mejora			
10.1	No conformidad y acción correctiva	NO	No se realizan documentaciones sobre no conformidades para una norma específica, como tampoco acciones correctivas necesarias para cumplir con los estándares de esta, sin embargo, la gestión de vulnerabilidades e incidentes, realiza acciones correctivas sobre problemas identificados en el transcurso de las operaciones diarias, tampoco donde especifique acciones preventivas que debe realizar la organización, ni que es necesario realizar mejoras al sistema para evitar el deterioro de este, solo recalca la importancia de la seguridad informática.
10.2	Acción preventiva	NO	
10.3	Mejora continua	NO	

9.2 Integración documental normas, guías y procedimientos para el área de Dirección General de Tecnología Banco de la República

Según los resultados obtenidos en el numeral anterior se identificaron las mejores prácticas de la gestión de activos TI y se documentaron según los numerales que exige la norma ISO 19770-1, además, se integraron de acuerdo con el Sistema de Gestión de Calidad ISO 9001:2015, donde se identifican aquellos requisitos que son comunes; es decir que las exigencias son similares; homólogos, que poseen características similares. Además, se describen las buenas prácticas que ofrecen las guías ITIL y NIST para algunos de estos requisitos y que pueden ser integradas a los procedimientos actuales de la organización. Esto se puede observar en la Tabla 5 del resumen de la integración documental normas y guías.

Tabla 5. Resumen de la integración documental normas y guías.

Numeral	Título ISO/IEC 19770-1	ISO 9001	ITIL	NIST	Integración a documentación actual
4 Contexto de la organización					
4.1	Comprensión de la organización	Numeral 4.1 (común)	ITIL sugiere realizar una (FODA), evaluaciones y auditorías internas y externas, como también un modelo de PESTEL para verificar los factores externos puesto que se trabaja en entornos dinámicos de incertidumbre.	No especifica	Estas evaluaciones y auditorías han dado como resultado un manual de sistema de gestión que abarca la comprensión de la organización.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	Numeral 4.2 (común)	Como primera medida se debe identificar a los grupos de interés, seguido de esto debe investigar las formas de generar valor para esto, en el caso de los clientes se puede revisar los informes que dan la experiencia de estos hacia con los servicios.	No especifica	Existe identificación de las partes interesadas y cómo es posible crear valor para ellas, es decir, las expectativas que tienen con la organización
4.3	Determinación del alcance del sistema de gestión de activos de TI	Numeral 4.3 (común)	Antes de definir un alcance es necesario saber el punto de partida y el impacto que se desea generar con dicho sistema. Esto puede ser realizado por medio de auditorías.	No especifica	Se sugiere realizar un análisis para definir lo que se tiene establecido en la organización y puede servir para el sistema, además de identificar el alcance de la iniciativa y cómo es posible integrarse a otras prácticas actuales.
4.4	Sistema de gestión de activos de TI	Numeral 4.4 (Homologo)	Principalmente es necesario pensar de manera integral y conocer el punto de partida de cómo se encuentra el sistema, todo esto para formalizar un plan estratégico que identifique las metas de la organización y adoptar los cursos de acción y asignación de recursos necesarios para que se realice el logro de los objetivos. También se deben definir el catálogo de productos o servicios que cumplan con las expectativas de los usuarios/clientes y documentar las mejoras necesarias para cambios en las estrategias.	El sistema debe tener una planificación y definición de los objetivos, procesos, métodos de monitoreo, identificación de riesgos y mitigación de estos y políticas de retiro, para que sea una implementación conjunta, que se interrelacione con diferentes prácticas y pueda dar el adecuado seguimiento al ciclo de vida del	Para definir el sistema primero debe ver que puede integrarse con el sistema de gestión actual y con la evaluación realizada ya sea por medio de auditorías internas y externas, como también de con las mediciones e informes de las operaciones, documentar el sistema de gestión de activos de TI, como lo exige esta norma, puesto que con las actividades

				activo, con el fin de tener una gestión perdurable.	realizadas actualmente ya da cabida para la ejecución del sistema.
5 Liderazgo					
5.1	Liderazgo y compromiso	Numeral 5.1 (común)	Como parte de una organización, es importante resaltar y hacer ver a los colaboradores el nivel de compromiso que se debe tener para cumplir con los objetivos, tomando las mejores decisiones para con los empleados como con la compañía, para esto desde los altos mandos se debe fomentar el liderazgo.	No especifica	Es necesario asegurar la política con plan estratégico y objetivos, asegurar la integración de los requisitos, asegurar que el sistema logre los resultados y comunicar la importancia del sistema.
5.2	Política	Numeral 5.2 (común)	Debe ser establecida por las directivas de acuerdo a las actividades de la organización y cualquier reglamentación externa.	Aparte de las políticas del sistema, es necesario definir políticas para la gestión del ciclo de vida, y seguridad, tales como: retiro de los activos, restricción de software, para el tratamiento de riesgos y mitigación de vulnerabilidades e incidentes, para controles de acceso, para resguardar la seguridad de la información, entre otras.	Realizar políticas generales sobre el sistema de gestión de TI y consolidar en un solo documento las políticas de las prácticas del ciclo de vida y seguridad de la información.
5.3	Roles, responsabilidades y autoridades en la organización	Numeral 5.3 (común)	Se debe delegar en un grupo de personas la ejecución de las actividades del sistema, dejando documentado las descripciones de las tareas a realizar como también los objetivos que se desean alcanzar con ellas	No especifica	Es necesario definir a un grupo de personas responsables de la ejecución del sistema, que verifique la planificación, operación y mejoras de todo el sistema de gestión de TI.
6 Planificación					
6.1	Acciones para abordar los riesgos y oportunidades para la gestión de activos TI				

6.1.1	General	Numeral 6.1 (Homólogo)	Definir los planes estratégicos, tácticos y operativos, tipos de financiamiento, arquitecturas, políticas, oportunidades de mejora, riesgos identificados, un portafolio de productos y servicios, requisitos de contrato y acuerdos. Todo esto con el fin de garantizar el logro de los objetivos propuestos.	Propone prácticas para seguridad informática y la gestión de activos, es necesario que se realicen procesos sobre la evaluación y mitigación de riesgos, en donde se deben realizar actividades de establecimiento de políticas, identificación, estimación, priorización de los riesgos referentes con la operación tanto las actividades organizacionales, como de los activos de TI. Otra parte de esta gestión incluye procesos para la identificación, análisis y tratamiento de las amenazas y vulnerabilidades.	Actualmente el área cumple con este requisito
6.1.2	Evaluación de riesgos de activos TI	Numeral 6.1 (Homólogo)	Se deben realizar procesos que integren principalmente la identificación de riesgos, mediciones de probabilidad, impactos y la proximidad de estos, adicional a esto, deben existir actividades como la planificación de las respuestas adecuadas a los riesgos, asignando propietarios y acciones y luego implementarlo, monitorearlo y controlarlo.	Algunos de los controles de seguridad que propone esta guía son los siguientes: Creación de políticas para el control de acceso, auditoria de eventos, detección e informes de anomalías, escaneo de vulnerabilidades, monitoreo de las actividades del usuario, monitoreo y seguimiento continuo de los activos conectados a la red y una transmisión de datos segura, para prevenir la fuga de información.	La evaluación de riesgos del área se encuentra definido en el sistema de seguridad de información que da cumplimiento a la norma ISO/IEC 27001:2013.
6.1.3	Tratamiento del riesgo de activos TI	Numeral 6.1 (Homólogo)	ITIL propone la implementación de prácticas para la <i>administración de incidentes</i> para minimizar los efectos de estos y solucionarlos lo más pronto posible; también, propone una práctica sobre el <i>manejo de problemas</i> donde se analice riesgos, identificación de problemas reiterados y análisis de información por parte de proveedores, software, hardware.; por último la práctica sobre la <i>gestión de la continuidad del servicio</i> que permite mantener en niveles óptimos disponibilidad y rendimiento de los servicios en caso de un evento de desastre.		Este numeral es homologo a la ISO/IEC 27001:2013, 6.1.2 y 6.1.3, la cual se encuentra certificada la compañía. Donde se están implementando los procedimientos propuestos tanto por ITIL, como por NIST.
6.2	Objetivos de la gestión de activos de TI y planificación para alcanzarlos				

6.2.1	Especificación del proceso de operación de gestión de activos TI	Específico	Es necesario determinar políticas, procesos, actividades, determinación de capacidad de personal, implementación de prácticas como: <i>Gestión de disponibilidad, de capacidad y rendimiento, control de cambios, incidentes, activos TI, seguimiento y gestión de eventos, gestión de problemas, gestión versiones, mesa de servicio, experiencia del cliente, gestión del catálogo de servicios, gestión de solicitudes de servicio, gestión de la seguridad de la información, gestión de cambios, administración de incidentes, manejo de problemas, validación y prueba del servicio, gestión del nivel de servicio.</i>	realizar procesos para conocer y controlar qué activos posee la compañía tanto virtuales como físicos, planificar los recursos tanto financieros como de activos y servicios, implementar políticas y objetivos para determinar el buen funcionamiento y que la organización cumpla con los requerimientos tanto en términos y condiciones de los productos, acuerdos de servicios, seguridad en la información, prevención de fuga de datos, realizar adquisiciones y todo lo que implica con el tratamiento de elegir la mejor herramienta o sistema acorde con las necesidades, permitir a los administradores definir y controlar el hardware y el software que se pueden conectar al entorno corporativo, definir los servicios proporcionados a los clientes, monitorear y evaluar el ciclo de vida del activo, realizar inventarios de los activos, gestionar los datos e información documentada necesaria, retirar y reutilizar software o hardware, detectar, prevenir y responder a incidentes, monitoreo continuo de hardware y software no aprobados y monitoreo continuo de vulnerabilidades y aplicación de parches / actualizaciones aprobadas por la empresa	Se propone implementar temas referentes a la gestión de licencias, donde cumpla las actividades de monitorear los acuerdos y términos del producto, también gestión de datos básicos, donde se realicen inventarios de procedimientos, gestión de información documentada sobre los activos, experiencia del cliente y gestión de solicitudes de servicio.
6.2.2	Objetivos de gestión de activos de TI para procesos operativos	Numeral 6.2 (Homólogo)	Se deben definir planes que sean acordes con las metas de la organización y métodos para su ejecución y asignación de recursos necesarios para el logro de los objetivos. También se deben definir el catálogo de productos o servicios que cumplan con las expectativas de los usuarios/clientes y posea declaración de aplicabilidad.	monitorear y evaluar el ciclo de vida del activo, realizar inventarios de los activos, gestionar los datos e información documentada necesaria, retirar y reutilizar software o hardware, detectar, prevenir y responder a incidentes, monitoreo continuo de hardware y software no aprobados y monitoreo continuo de vulnerabilidades y aplicación de parches / actualizaciones aprobadas por la empresa	Falta incluir objetivos sobre los procedimientos que se proponen en el numeral anterior
6.2.3	Objetivos generales de gestión de activos de TI	Numeral 6.2 (Homólogo)	Establecer objetivos ayuden al cumplimiento de las metas del sistema de gestión de activos de TI.	Adicional de lo mencionado en el los dos numerales anteriores, ITIL propone la implementación de la práctica de <i>gestión de</i>	El área cumple con los objetivos, puesto que, la razón de ser del departamento es coordinar y dirigir la implementación de políticas y estándares de uso de tecnologías de información, telecomunicaciones, multimedia, seguridad informática y la seguridad electrónica asumida por la Subgerencia General de Servicios Corporativos
6.2.4	Planificación para lograr los objetivos de gestión de activos de TI	Numeral 6.3 (Homólogo)	Adicional de lo mencionado en el los dos numerales anteriores, ITIL propone la implementación de la práctica de <i>gestión de</i>	Adicional de lo mencionado en el los dos numerales anteriores, ITIL propone la implementación de la práctica de <i>gestión de</i>	El área cumple con este ítem, puesto que, la razón de ser del área es adquirir, retirar, operar y realizar mantenimiento

			<i>proyectos</i> , para planificar, delegar, monitorear y mantener control de todos los aspectos de los proyectos que sean nuevos, de transición o de mejora. Ya sea con método cascada o método ágil.		a todos los activos de TI, para que con ellos puedan prestar soporte a las actividades del Banco. Por consiguiente, si se realizan métodos y procesos para toda la gestión del ciclo de vida del activo. Donde por medio de los BRM se identifican y se priorizan los nuevos proyectos o proyectos de transición, en los cuales dependiendo de este se implementan esas metodologías de cascada o ágil
7	Soporte				
7.1	Recursos	Numeral 7.1 (Homólogo)	ITIL propone 3 prácticas, donde la primera <i>gestión de recursos</i> se encuentra: definición de portafolio de servicio y productos, priorización de proyectos, servicios y productos, evaluación de inversiones, toma de decisiones, evaluar costos y riesgos; la segunda es la <i>gestión del catálogo de servicios</i> , donde principalmente se encuentran los productos y servicios ofrecidos a los usuarios como también la declaración de aplicabilidad; por último se encuentra la <i>gestión del personal y talento</i> , que garantiza tener el personal adecuado, con habilidades requeridas para la ejecución de las actividades.	Menciona temas de recursos financieros para adquirir diferentes herramientas que ayuden a gestionar los activos como también las que soportan las actividades diarias para el software y hardware, por consiguiente, debe existir un procedimiento donde se asigne y planifiquen estos recursos económicos y como se mencionaba anteriormente la definición de productos y servicios para la prestación de los servicios.	Hace falta definir recursos para la adquisición de herramientas que ayuden al seguimiento y mejora del sistema de gestión de activos, donde realicen actividades de monitoreo automático y permitan facilitar al personal encargado de esto, las actividades diarias.
7.2	Competencia	Numeral 7.2 (común)	En la práctica de la gestión del conocimiento se deben realizar actividades para realizar la adquisición de este, incluido el desarrollo, la captura y la recolección de conocimiento, ya sea formal y documentado o informal y tácito.	No especifica	El nivel de conocimiento de los empleados del área es muy elevado, puesto que la gran mayoría cuenta con mucha experiencia laboral y poseen grandes especializaciones.
7.3	Conciencia	Numeral 7.3 (común)	El trabajo en conjunto tanto del personal, organización y partes interesadas ayuda al cumplimiento de los objetivos, sin embargo, para realizar este trabajo en conjunto es necesario que la información sea compartida, que exista una	No especifica	Para esto se sugiere, definir la implementación del sistema y comunicarles a los colaboradores sobre la importancia de esta gestión, con el fin de que se implemente con éxito.

			comprensión y confianza de todas las partes y que además exista conciencia entre ellos a con las tareas que deben realizar		
7.4	Comunicación	Numeral 7.4 (común)	La práctica de la gestión de relaciones busca establecer y mejorar los vínculos que tiene una organización con sus partes interesadas en los diferentes niveles estratégico y tácticos. Una buena implementación, asegura la comprensión y satisfacción de las necesidades, priorización de los distintos clientes y verificación de quejas y sugerencias	No especifica	La comunicación en el área se realiza con los usuarios/clientes, colaboradores y altos directivos, por medio de la intranet del Banco, sin embargo, es necesario fortalecer los vínculos con los proveedores de servicios donde se tenga un canal directo de comunicación.
7.5	Requisitos de información	Numeral 7.5.3 (Homólogo)	Los requisitos de información deben ser contratos y términos de acuerdos, solicitudes de cambio, prestación de servicios a usuarios, información de finalización de soporte, actividades de mejora, base de datos que contenga información relacionada con el hardware, software, el inventario de los activos, información de compras, términos y condiciones; solicitudes de asignación de usuario, solicitudes de traslado, soporte de renovaciones, información sobre uso de licencias y solicitudes de retiro. documentaciones tanto de los proveedores sobre requisitos pactados y de los clientes, donde se les informa a los acuerdos del servicio.	Los requisitos de información la identificación y mitigación de vulnerabilidades, eventos e incidentes, donde se identifican y documentan amenazas y vulnerabilidades de los activos, recopilación de licencias, términos y condiciones, almacenamiento de datos, es decir realizar copias de seguridad, inventario de los activos, información de los activos que apliquen para el monitoreo del ciclo de vida, como renovaciones, versiones, actualizaciones, funciones, propietario de este, facturas de compras y contratos y la información sobre el software instalado y autorizado.	Hace falta información documentada sobre procesos y procedimientos que hacen falta implementar, tampoco se han determinado algunas características básicas de los activos TI, que se encuentran descritas en el anexo C de la norma, como lo son: complejidad tecnológica (flexibilidad de ubicación, Número y complejidad de componente, tasa de cambio del activo).
7.6	Información documentada				
7.6.1	General	Numeral 7.5.1 (común)	En este ítem se identifica al conjunto de todas las prácticas que propone ITIL, puesto que en cada una de ellas se debe asegurar una información documentada, sobre los procesos realizado, las actividades, responsables de ejecución, resultados	En el numeral 7.5 se incluye toda la información documentada que debe tener la organización sobre el sistema, sin embargo, no especifica en información documentada para	Hace falta la información documentada mencionada en el anterior numeral.

			de los servicios prestados, resultados de los activos, políticas, entre otros. Asimismo, se integran las prácticas mencionadas en el numeral anterior 7.5 sobre la mejora y gestión de activos y el proceso de entrega y soporte de la cadena de valor del servicio.	todas las operaciones fuera de la gestión de TI	
7.6.2	Trazabilidad de la propiedad y la responsabilidad	Especifico	En la práctica de <i>gestión de proveedores</i> se pueden encontrar gestión de contratos, términos y condiciones, niveles de cumplimiento, gestionar la garantía, renovaciones y/o rescisión del contrato; en la <i>gestión de activos de ti</i> se encuentra solicitudes de asignación de usuario o de traslado de licencias, donde se debe documentar el responsable del producto, la fecha de asignación, el responsable de la aprobación, el número de licencia o serial y firma del responsable; en la <i>gestión del nivel de servicio</i> documentaciones tanto de los proveedores sobre requisitos pactados y de los clientes, donde se les informa a los acuerdos del servicio.	información referente a los contratos y términos y condiciones con los proveedores, con el fin de cumplir y hacer llegar esto a los usuarios. A pesar de esto, no existe una mención sobre las responsabilidades que tienen los proveedores de los activos y servicios a con la organización sobre información de actualizaciones y mejoramiento de versiones.	Cumple con este requisito
7.6.3	Seguimiento de auditorías de autorización y ejecución de autorizaciones	Especifico	Misma documentación requerida sobre la gestión de activos de ti del numeral anterior	No especifica	Cumple con este requisito
7.6.4	Creación y actualización	Numeral 7.5.2 (común)	Para las mejoras es necesario tener documentación sobre los registros de actividades que se han mejorado en el pasado o que necesitan un cambio. Sin embargo, esta práctica y en general ITIL, No especifica el tema de documentación con formatos, fechas, versiones y actualización de estos datos.	No especifica	Hace falta crear la documentación requerida exigida por esta norma para la implementación del sistema
7.6.5	Control de la información documentada	Numeral 7.5.3 (común)	No solo se debe mantener una información disponible, también es necesario proteger la información por medio de la compresión y gestión de riesgos de confidencialidad, disponibilidad de la información, autenticación y no repudio,	Se debe proteger, por medio de tecnologías que aseguren la visibilidad solo a personal autorizado, es decir, realizar controles de acceso, con el fin de	Hace falta la documentación requerida para esta norma.

			revisión y auditoría de control, gestión de identidad y acceso.	prevenir fuga de datos, esto por medio de y sistemas de seguridad, como firewalls y sistemas de detección de intrusos y administración de identidad y acceso (IDAM).	
8 Operación					
8.1	Planificación y control operacional	Numeral 8.1 (Homólogo)	La planificación sirve para asegurar, entregar y respaldar que estén disponibles los servicios, cuando y donde sean solicitados, además de que estos cumplan con las especificaciones acordadas para los clientes y realizar acciones de mejora para cumplir con los objetivos propuestos. Adicional a esto se deben identificar los riesgos, mediciones de probabilidad, impactos y la proximidad de estos. Las prácticas que propone ITIL son: <i>Gestión de disponibilidad, de capacidad y rendimiento, control de cambios, incidentes, activos TI, seguimiento y gestión de eventos, gestión de problemas, gestión versiones, mesa de servicio, experiencia del cliente, gestión del catálogo de servicios, gestión de solicitudes de servicio, gestión de la seguridad de la información, gestión de cambios, administración de incidentes, manejo de problemas, validación y prueba del servicio, gestión del nivel de servicio.</i>	Se deben mantener principalmente la información documentada de los procesos realizados, como también de la documentación descrita en el numeral 7.5, adicional a esto, es necesario realizar auditorías para mantener el control adecuado de las operaciones diarias e identificar los criterios sobre los cuales se van a basar lo procesos que soporten la gestión de activos y como puede integrarse con todas las actividades para mitigar los riesgos como se menciona en los numerales del 6.1	Cumple con el requisito ya que cuenta con procesos definidos por la compañía se realizan la planificación de recursos y posible demanda, como también para la parte de control operacional aquellos relacionados con el diseño, retiro, adquisición, traslado, mantenimiento, soporte y servicio a los diferentes usuarios.
8.2	Gestión del cambio	Especifico	La práctica de <i>gestión del cambio organizacional</i> asegurar por medio de la definición de objetivos, liderazgo y participantes dispuestos es posible realizar cambios sin problemas y con éxito; la práctica de <i>control de cambios</i> identifica los 3 cambios posibles: estándar (bajo riesgo), normal (bajo riesgo, pero importantes) y de emergencia (implementación tan pronto sea posible). Por	No específica sobre cómo implementar los cambios en la organización, pero si como identificar los riesgos que puedan generar dichos cambios, donde se debe incorporar análisis de amenazas y vulnerabilidades, y considera las mitigaciones proporcionadas por los controles de	Si cumple con el requisito

			último, es necesario implementar la práctica de <i>gestión de riesgos</i>	seguridad planificados o implementados, además, de proteger el control de acceso y realizar monitoreo de personal, conexiones, dispositivos y software utilizados, para detectar posibles eventos de ciberseguridad.	
8.3	Gestión de datos básicos	Especifico	ITIL propone la creación de una base de datos de gestión de la configuración que contenga información relacionada información de compras, términos y condiciones; solicitudes de asignación de usuario, solicitudes de traslado, soporte de renovaciones, información sobre uso de licencias y solicitudes de retiro, políticas de reutilizar y dismantelar activos, también se debe incluir un registro de inventario.	conocer y controlar qué activos posee la compañía tanto virtuales como físicos, realizar inventarios de los activos, gestionar los datos e información documentada necesaria para el ciclo de vida como renovaciones, versiones, actualizaciones, funciones, propietario de este, facturas de compras y contratos, la información sobre el software instalado y autorizado, propietario, etiquetar un activo, registrar número de serie y otros atributos de la base de datos.	Se propone un procedimiento para la gestión de datos básicos donde se realice inventario sobre la línea base del Banco e identifique las software autorizados e instalados, adicional a esto, también se propone un documento donde sea posible anexar la documentación de datos básicos de cada activos software, es decir una ficha técnica donde incluye solicitudes de asignación de usuario, solicitudes de traslado, soporte de renovaciones, información sobre uso de licencias y datos básicos generales de este. Para dar soporte a esta ficha, también se propone un procedimiento que detalla la documentación de esta ficha.
8.4	Gestión de licencias	Especifico	<i>Práctica de gestión de proveedores</i> mantiene información sobre el uso de licencias y evitar la copia ilegal, es necesario tener documentación sobre los términos y condiciones, niveles de cumplimiento, gestionar la garantía, renovaciones y/o rescisión del contrato y posibles mejoras que puedan realizarse por parte de estos, es decir; <i>práctica de gestión de activos TI</i> mantiene información sobre solicitudes de asignación de usuario o de traslado de licencias, donde se debe documentar el responsable del producto, la fecha de asignación, el responsable de la aprobación, el número de licencia o serial asignado, firma del	establecer políticas para que se cumplan los acuerdos de servicios pactados con los proveedores, auditorias para revisar el cumplimiento de los contratos, también, procesos para retirar y reutilizar software e implementación y monitoreo continuo sobre las actualizaciones y nuevos parches a implementar, que han sido recibidos por los proveedores.	Se propone un procedimiento que ayude de soporte para auditar los requisitos de las licencias, en cuanto a número total de usuarios asignados por cada una y permita evitar la copia ilegal e incumplimiento de contratos.

			responsable aceptando los términos y condiciones.		
8.5	Gestión de seguridad	Especifico	<p>la <i>seguridad de la información</i> mantiene políticas, procesos, comportamientos, riesgos y controles, detecten incidentes o problemas de forma confiable y rápida y se corrijan, los procesos incluidos para esta gestión son los siguientes: <i>gestión de incidentes</i> de seguridad para minimizar los efectos de estos y solucionarlos lo más pronto posible; también, propone una práctica sobre el <i>manejo de problemas</i> donde se analice riesgos, identificación de problemas reiterados y análisis de información por parte de proveedores, software, hardware.; la <i>gestión de la continuidad del servicio</i> que permite mantener en niveles óptimos disponibilidad y rendimiento de los servicios en caso de un evento de desastre de la información. Otros procesos son <i>gestión de riesgos, revisión y auditoría de control, gestión de identidad y acceso, gestión de eventos, procedimientos para pruebas de penetración, escaneo de vulnerabilidades, procedimientos para administrar cambios relacionados con la seguridad de la información</i>, como firewall. cambios de configuración.</p>	<p>los procedimientos claves que debe tener toda organización prestadora de servicios financieros, son: identificación y mitigación de vulnerabilidades, gestión de riesgos, gestión de incidentes y problemas relacionados con la ciberseguridad. revelar la ubicación y el propietario de un dispositivo, ayuda a centrarse en los activos críticos, reduce el ataque de las máquinas, detecta y alerta cuando dispositivos no autorizados intenten acceder a la red, hace cumplir las políticas de restricción de software relacionadas con el software que puede ejecutarse en el entorno corporativo.</p>	Sí cumple con el requisito
8.6	Otros procesos	Especifico	<p>Los otros procesos identificados por ITIL son: <i>Mesa de servicio</i> donde se presta soporte a los usuarios para resolver los problemas identificados con los activos o servicios; <i>Gestión de solicitudes de servicio</i> respalda la calidad acordada de un servicio predefinido que ha sido iniciado por el usuario; <i>Gestión de cartera</i> responsable del financiamiento para mantener el portafolio de servicio y productos, priorización de proyectos, servicios y productos, evaluación de inversiones, toma de decisiones, evaluar costos y riesgos y</p>	<p>la atención del servicio y solución de problemas a los usuarios, donde lo determinan como mesa de ayuda, que permite ser un soporte de colaboración con el personal cuando este tenga algún inconveniente con un producto y otro proceso que menciona la guía es el del retiro y reutilización de activos hardware, en donde se establecen políticas para</p>	Cumple con el requisito

			llevar la contabilidad; <i>Gestión de proyectos</i> para planificar, delegar, monitorear y mantener control de todos los aspectos de los proyectos que sean nuevos, de transición o de mejora. Ya sea con método cascada o método ágil; <i>Validación y prueba del servicio</i> donde se realicen prueba del sistema, integración, rendimiento y capacidad, seguridad, vulnerabilidades, cumplimiento, respaldo, requisitos de garantías, aceptación de usuarios, entre otras; y por último la <i>gestión del nivel de servicio</i> donde se identifican los acuerdos pactados tanto por los proveedores como con los usuarios sobre la prestación del servicio y se realizan informes y métricas con estos.	eliminación de datos, número de serie en la base de datos y retiro físico de las instalaciones de la empresa.	
8.7	Subcontratación y servicios	Específico	Define las métricas que deben encontrarse sobre como los proveedores medirán, informaran y mejoraran los servicios durante la vigencia del contrato. Si se requerirán datos de los proveedores para operar mejoras internas, que también deben especificarse en el contrato, como también, la definición de los productos o servicios subcontratados.	No especifica	El departamento exige a sus contratistas el cumplimiento de las normas de seguridad ISO/IEC 27000 y de Calidad 9001 para realizar subcontrataciones, por consiguiente, cumple con el requisito
8.8	Responsabilidades mixtas entre la organización y su personal	Específico	Incluye todas aquellas actividades mencionadas en la gestión de riesgos sobre la planificación de las respuestas adecuadas a los riesgos, asignando propietarios y acciones y luego implementarlo, monitorearlo y controlarlo, adicional a esto también esta información debe estar protegida, para evitar fuga de datos.	No especifica	Si cumple con el requisito ya que se cumplen los acuerdos de confidencialidad que poseen tanto los usuarios como el prestador de servicio, además de que existen mecanismos de verificación de autenticidad y verificación de fuga de datos, para los dispositivos o los accesos de licencias que se adquirió a terceros.
9 <i>Evaluación del desempeño</i>					
9.1	Seguimiento, medición, análisis y evaluación	Numeral 9.1 (Homólogo)	Se recomienda hacer análisis sobre cómo se encuentra el sistema, para identificar el punto donde se encuentra, además ITIL propone que se	Se deben hacer seguimientos, informes, análisis y evaluaciones a los informes sobre software	Hace falta medidas de desempeño para determinar el nivel de rendimiento que tienen los activos con respecto al

			utilicen factores críticos de éxito (CSF) e indicadores clave de rendimiento (KPI), para facilitar la recolección de los datos e información arrojada por las actividades de las operaciones, también es importante evaluar la experiencia que tiene el usuario a con los servicios y productos prestados, para identificar los posibles fallos y mejorar las expectativas de este.	instalado, software utilizado, monitoreo a hardware y software no aprobados vulnerabilidades, donde se evalúen conexiones, dispositivos, actividad del personal estado de cumplimiento de políticas, y transmisión de datos.	rendimiento financiero y no financiero, todo esto para determinar posibles mejoras o verificar el adecuado funcionamiento de estos de acuerdo con las tareas diarias estipuladas
9.2	Auditoría interna	Numeral 9.2 (común)	No especifica	Solo especifica las auditorias para verificar el cumplimiento de la seguridad, cumplimiento de gestión de activos y problemas encontrados en el transcurso de las operaciones	No se ha estipulado la implementación o el deseo formar de formalización de esta norma, por consiguiente, los auditores internos no tienen conocimiento a estos requisitos. Sin embargo, si se realiza un seguimiento periódico y se documentan acciones de mejora para los demás sistemas de gestión.
9.3	Revisión por la dirección	Numeral 9.3 (Homólogo)	No especifica	No especifica	Como no se ha implementado esta norma, no existe revisión por la alta dirección sobre el cumplimiento de estos requisitos.
10	Mejora				
10.1	No conformidad y acción correctiva	Numeral 10.2 (común)	ITIL propone una serie de pasos, con el fin de facilitar el entendimiento del proceso de mejora continua por medio de este modelo:	No especifica	Sí cumple, ya que es un numeral común con la norma ISO 9001
10.2	Acción preventiva	Numeral 10.1 (Homólogo)	<ol style="list-style-type: none"> 1. ¿Cuál es la visión?: es necesario crear una visión para las mejoras planeadas, además de que debe ser traducida a necesidades específicas. 2. ¿Dónde estamos ahora?: El éxito de una iniciativa de mejora depende de una clara y precisa comprensión del punto de partida y el impacto de la iniciativa. 3. ¿Dónde queremos estar?: definir uno o más acciones priorizadas a lo largo del camino para 	No especifica	La realización del proceso de pruebas tanto de seguridad como de soporte, permite identificar problemas y solucionarlos, también se realizan mantenimiento en los activos tanto de software como de hardware.
10.3	Mejora continua	Numeral 10.3 (común)		No especifica	Sí cumple este requisito, ya que tiene una metodología enfocada a detectar y mejorar los sistemas, procesos y servicios del área.

		<p>completar la visión de mejora, basado en lo que se conoce en el punto de partida.</p> <p>4. ¿Cómo llegamos allí?: elaborar un plan para abordar los desafíos de la iniciativa. Donde se pueden experimentar pruebas para elegir los caminos y trabajar en una serie de iteraciones que ayuden a progresar, reevaluar el enfoque y si es necesario cambiar la dirección.</p> <p>5. Actúe: Esto podría implicar un enfoque tradicional de estilo cascada, pero podría ser más apropiado seguir un enfoque ágil.</p> <p>6. ¿Llegamos allí?: Debe verificar si se ha alcanzado el punto de a dónde queremos llegar.</p> <p>7. ¿Cómo mantenemos el impulso?: Si la mejora fue un éxito, es necesario empezar a reforzar cualquier nuevo método introducido, con el equipo de trabajo para garantizar que el progreso realizado no se pierda y generar mayores impulsos. Si los resultados no fueron los deseados, se debe realizar un análisis de mejora del porqué no funciona y comunicar a las partes interesadas documentando las lecciones aprendidas y cómo es posible realizar de otras maneras</p>		
--	--	--	--	--

9.3 Documentación de procedimientos área de Dirección General de Tecnología

Banco de la República

Ahora bien, según las recomendaciones que ofrecen las diferentes normativas y guías sobre la forma es que se deben administrar adecuadamente los activos de tecnología, se identificaron y priorizaron 3 procedimientos que requiere actualmente el área de la DG-T y que es primordial para el buen funcionamiento de los activos TI; además de esto, para dar cumplimiento a la verificación de algunos requisitos se elaboró una plantilla de ficha técnica de software, la cual sirve como soporte para el procedimiento de gestión de datos básicos, donde se integran los requisitos mínimos, información sobre proveedores, historial de renovaciones, personal autorizado, entre otros en un solo documento.

Se realiza una propuesta a nivel de procedimientos al área para que sea estudiada por sus directivos y se evalúe la implementación de estos en sus procesos y procedimientos actuales. Esta propuesta se realiza en una herramienta tecnológica llamada ARIS CLOUD, donde consiste en realizar un flujograma de actividades que se deben cumplir para culminar el procedimiento. En esta herramienta, se diagraman todos los procesos, organigramas, procedimientos e instructivos necesarios para la realización de cada una de las tareas del personal del Banco. Todo esto se realiza según un enfoque basado en procesos, los cuales cuentan con lineamientos establecidos por las directrices de la empresa.

Ahora bien, según los resultados arrojados por la integración de las normas y guías, uno de los temas que se deben ser tratados es la gestión de datos básicos, descrito en el numeral 8.3 de la ISO/IEC 19770-1, en donde su objetivo primordial es elaborar y mantener una base de datos sobre el hardware y software, sus documentos asociados y las

relaciones entre ellos, de forma que puedan ser identificado como un almacén o inventario de activos que sean monitoreados y controlados de manera única.

Según esa definición y de acuerdo con lo examinado en el área y arrojado en esta evaluación preliminar de requisitos, se identificó la falta de prácticas que se verifique el nivel de inventario de software que encuentra instalado en los computadores del Banco.

Por consiguiente, dentro de los procedimientos propuestos para este presente trabajo se encuentra uno nuevo denominado “*Recirculación de software*”; el cual, consiste en actualizar la línea base del software que se encuentra instalado en el Banco, donde se coteja con los que están autorizados para su uso, esto con el objetivo de identificar si los computadores cuentan con licencias o software libres que son de procedencia dudosa o que no cumplen para la realización de las funciones estrictamente laboral.

Este procedimiento cuenta con 21 actividades, en donde inicia con un evento en el cual se realiza una solicitud para revisar el inventario de software, seguido de esto se generan los respectivos reportes del software instalado, el libre y el que se encuentra autorizado, esto se realiza en una herramienta tecnológica llamada ALTIRIS/ITAM y puede ser realizado por una unidad interna de computación personal o un outsourcing.

Esos reportes generados ingresan a una actividad de control que verifica el software que no está autorizado y genera otro reporte que es publicado por medio de TEAMS y notificado al correo electrónico al personal de la DG-T, para que ellos realicen otra verificación y determinen si los softwares que se encuentran en esa lista son utilizados o no.

Cuando el software cuenta con un uso confirmado se clasifica según las características de este y se identifica los posibles usuarios; además se determina una ficha técnica para un posterior uso, se integra el nuevo software a la línea base y dispara un procedimiento llamado incluir un nuevo software dentro del catálogo. Por el contrario, cuando no cuenta con un uso confirmado se verifica si puede ser autorizado o no; para el primer caso, es necesario evaluar si el software necesita licencia o no, de necesitarla primeramente debe ser bloqueado, puesto que por temas de legalidad no es posible contar con un software que no cuente con una autorización del prestador del servicio, después de esto se notifica a las áreas que deben ejecutar una solicitud para incluir la compra de la licencia y se transfiere al procedimiento de incluir nuevo software dentro del catálogo. Cuando no es necesario adquirir una licencia, es decir el software es libre, se realiza la clasificación y se integra a la línea base.

Ahora bien, cuando el software no está confirmado de uso, además no es autorizado para utilizar por ciertas dependencias del Banco o por todos en general, se debe verificar si es posible desinstalar, si es factible esto, debe identificarse si puede desinstalarse de manera automática por medio de ALTIRIS o de lo contrario, manualmente, donde se deben solicitar las contraseñas de acceso a cada computador y desinstalarlo en cada uno. Si no es posible desinstalar el software debe ser bloqueado para que nadie tenga acceso a este.

Para la realización de los siguientes 2 procedimientos se realizó una propuesta en una herramienta tecnológica llamada ARIS CLOUD, donde consiste en realizar un flujograma de actividades que se deben cumplir para culminar el procedimiento.

La compañía cuenta con una suscripción al software ARIS ARCHITECT, en donde se diagraman todos los procesos, organigramas, procedimientos e instructivos necesarios para la realización de cada una de las tareas del personal del Banco. Todo esto se realiza según un enfoque basado en procesos, los cuales cuentan con lineamientos establecidos por las directrices de la empresa.

Para la diagramación de estos procedimientos se emplean objetos representados por símbolos y atributos con campos descriptivos que permiten registrar la información relacionada con un proceso. A continuación, en la ilustración 9, se pueden observar los objetos con su respectiva definición al frente de estos.



Ilustración 9 Objetos ARIS CLOUD

Fuente: Elaboración propia en la herramienta ARIS CLOUD

Como se puede observar en la anterior ilustración, para el caso de los procedimientos realizados se utilizaron 7 objetos, en donde:

- Evento: es un hito que representa el inicio, fin y cualquier decisión que deba tomar en el proceso.
- Actividad o Función: Indica las etapas de un proceso, actividades o tareas que deben ser ejecutadas.
- Interfaz de procedimiento: Enlace en el documento con otro procedimiento existente.
- Conector O exclusivo: Permite abrir secuencia en dos o más caminos, los cuales solo uno se puede ejecutar.
- Rol: son personas o grupo de personas encargadas de desempeñar funciones descritas.
- Documento: Documentos que pueden ser la entrada o insumo para una actividad o que sean generados como salida de esta.
- Sistema tecnológico: aplicaciones tecnológicas que han sido diseñadas por las dependencias del Banco o que han sido adquiridas por terceros para ser ejecutadas en una actividad.

En cuanto a la forma de diagramación, se establecen unas reglas básicas, que han sido determinadas por las directrices del Banco, donde las actividades pueden tener un sistema de entradas y salidas, además se debe especificar quien ejecuta cada acción y por medio de cual herramienta tecnológica se realiza. Todo esto para que sirva como soporte de la descripción de funciones de cada área y cargo de la compañía.

En la ilustración 10, se puede evidenciar la estructura de diseño de un procedimiento

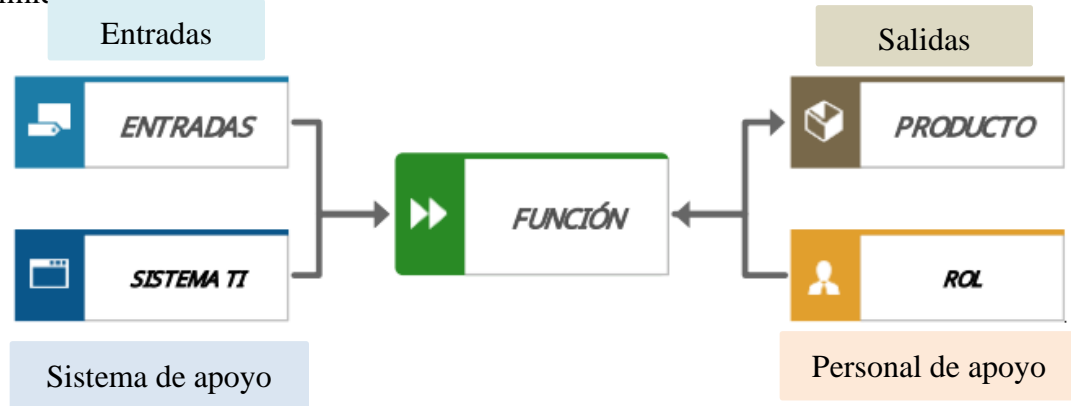
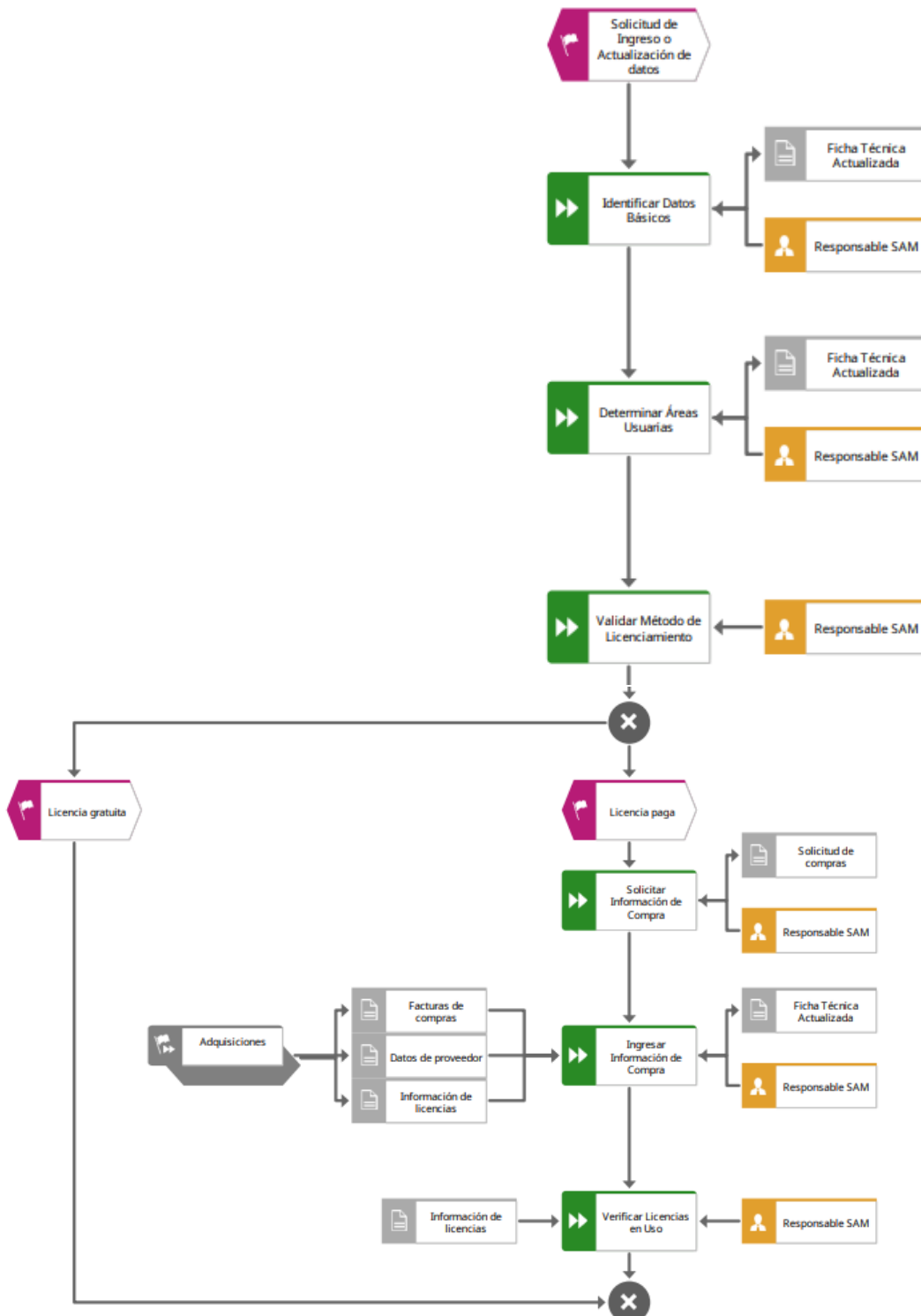


Ilustración 10 Estructura procedimiento ARIS.

Fuente: Elaboración propia en la herramienta ARIS CLOUD

Como segunda propuesta, se encuentra el procedimiento denominado **“Gestión de datos básicos”**, el cual busca estandarizar y centralizar la información sobre los diferentes activos de software que posee la compañía, donde según especifica numeral 8.3 de la ISO/IEC 19770-1 y la sugerencias propuesta por la guía ITIL, es necesario que se tenga una documentación sobre los activos en los diferentes puntos del ciclo de vida de estos, con el fin de poder monitorear, adquirir, retirar y realizar traslados.

En la ilustración número 11 es posible evidenciar el flujograma realizado para este procedimiento.



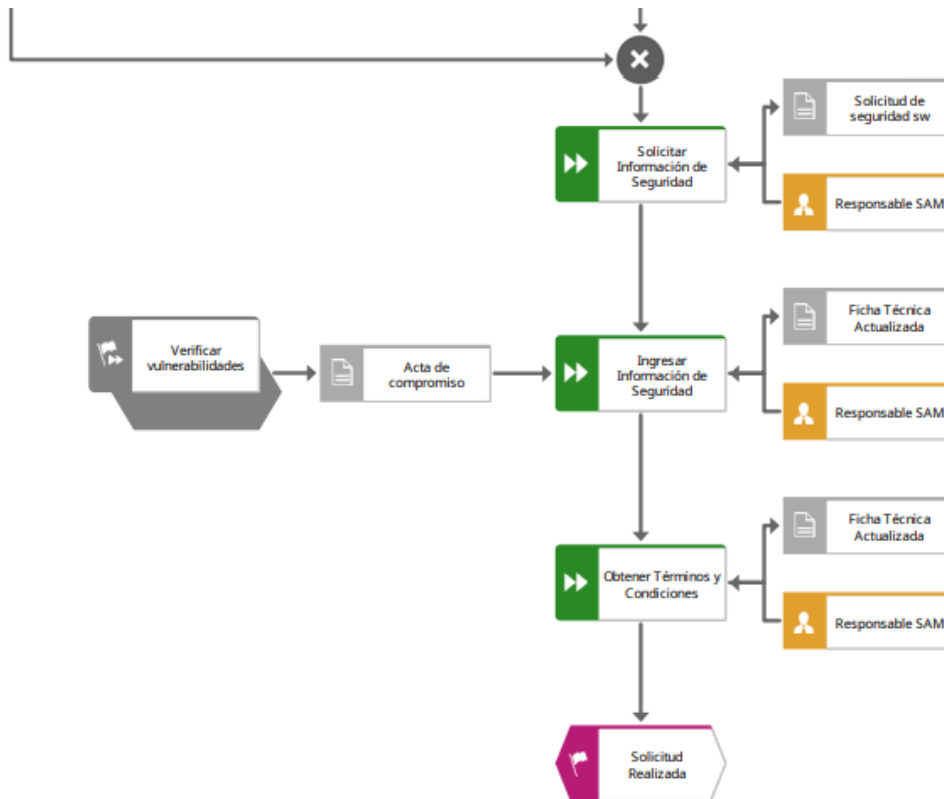


Ilustración 11 Gestión de datos básicos

Fuente: Elaborado por el autor

Por consiguiente, este procedimiento cuenta con 13 actividades, que tienen como alcance realizar y documentar los datos básicos de los diferentes softwares de la compañía, iniciando con una solicitud de ingresar o actualizar los datos de un software, seguido de la identificación de los datos básicos, dentro de ellos es posible encontrar nombre, objetivo, funcionalidad, tipo de versión, clasificación del software, tamaño, datos del desarrollador y especificaciones de compatibilidad para instalación. Esta actividad es realizada por el

responsable SAM y documentada en la ficha técnica del software, la cual también es una propuesta de este proyecto.

Después de identificado estos datos, el responsable SAM, debe determinar los usuarios o áreas autorizadas para la utilización de este software, según la funcionalidad de estos, pueden tener diferentes usuarios objetivo, adicional a esto, debe documentar las áreas solicitantes de la adquisición, esto debe ser diligenciado en el mismo formato de Excel de Ficha técnica de software.

Seguido a esto el responsable SAM, debe validar el método del licenciamiento, identificando el tipo de software que se desea adquirir o actualizar, ya sea Software libre, el cuál es gratuito o software por suscripción, por uso, as a service, a perpetuidad o Cloud, los cuales por lo general son licencias pactadas a un año y poseen un costo, dependiendo ya sea por número de licencias o por prestación del servicio.

Cuando la licencia es paga, se debe solicitar la información de compra al área de adquisiciones, por medio de una solicitud vía correo electrónico, donde ellos envían información sobre facturas de compra, datos del proveedor (NIT, nombre, teléfono de contacto, clasificación del proveedor) y número de licencias adquiridas, este último es el insumo para realizar una verificación de licencias en uso, donde se coteja las licencias compradas con las utilizadas e identificar si existe alguna sobre utilización o sub utilización de estas. Estos datos también deben ser diligenciados en la ficha técnica y dejar el soporte que sea necesario.

Cuando el software es libre, no es necesario solicitar ninguna información sobre licencias, soportes de pago ni tipo de proveedor, puesto que se encuentran disponibles para

todo el público y su uso es gratuito, por consiguiente, se salta estas actividades y se une a la licencia paga para solicitar información de seguridad, la cual debe ser diferida al departamento de seguridad de información, donde se realiza un chequeo en otro procedimiento transversal sobre las vulnerabilidades del software. Por parte de este departamento se envía un acta de compromiso, donde se encuentra la autorización para la instalación o uso interno de este producto.

Por último, se deben adjuntar todos los términos y condiciones que se obtienen con la adquisición del software, es decir, firma de contrato, si se dispone a actualizaciones futuras, mantenimiento, entrega de seriales, manuales de servicio, soporte técnico e inducción funcional al producto, esto se diligencia en la ficha técnica y finaliza la solicitud tramitada.

Además de estos procedimientos, se propone una plantilla en Excel que sirva como modelo de ficha técnica para cualquier software que se encuentre disponible o que se desee adquirir por el Banco. Ahora bien, el funcionamiento de esta herramienta consiste en rellenar los campos descritos, para obtener una base documental sobre diferentes aspectos con el fin de tener una adecuada administración de las licencias software y ser soporte del procedimiento anteriormente descrito.

Esta ficha técnica permite proporcionar datos para generar mediciones por medio de indicadores sobre el uso de estas y ser soporte documental para las auditorias. En la ilustración 12, se puede observar una captura del menú de inicio de esta herramienta.

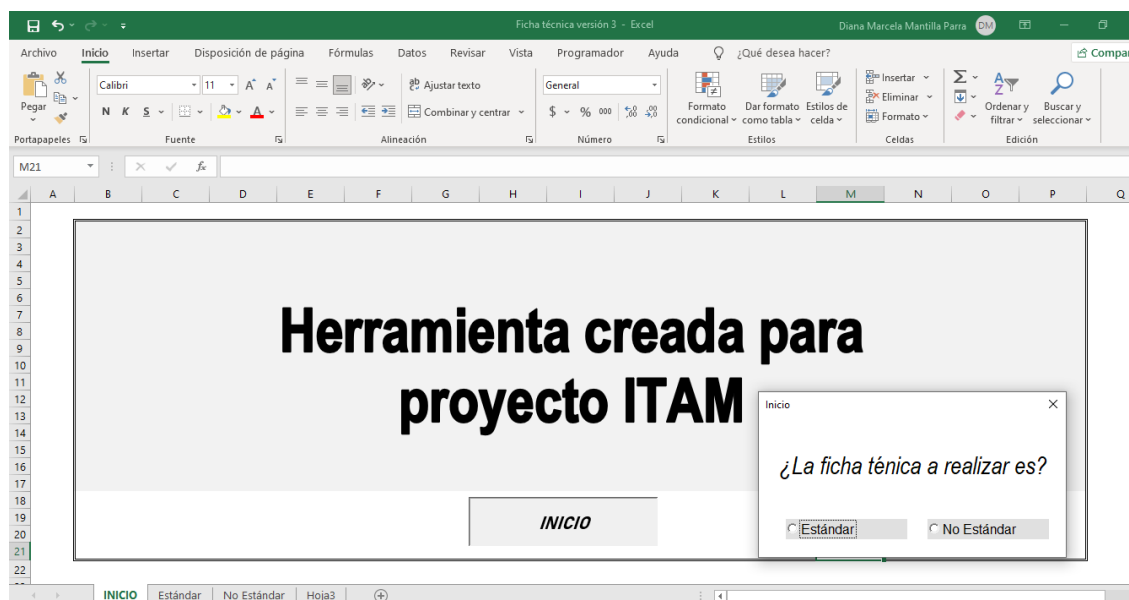


Ilustración 12 Menú inicio- Ficha técnica.

Fuente: Elaboración propia

Al ingresar al documento se puede observar este menú, donde por medio de un formulario creado en Visual Basic el responsable puede identificar y realizar la inscripción del tipo de software que desea, donde se identifica como estándar, aquel que se encuentra autorizado y definido con uso en la organización y como no estándar aquellos nuevos softwares que no han sido evaluados para una posible autorización.

Para el caso de la ficha técnica estándar, se encuentra todos los campos de datos básicos, áreas usuarias y autorizadas, grupo de usuarios, método y costo del licenciamiento, especificaciones mínimas del producto, datos de los proveedores, servicios contratados adicionales o incluidos en la compra, renovaciones y firma del BRM. Por el contrario, para la ficha no estándar solo se encuentran los campos de datos básicos, áreas usuarias y autorizadas, especificaciones mínimas y firma del BRM.

FICHA TÉCNICA ESTÁNDAR		FECHA DE APROBACION:	
NOMBRE DE SOFTWARE		FECHA:	
Clasificación:	Software Libre	Ingresar datos	Tamaño: [Tamaño de la aplicación en KB, MB, GB o TB.]
Datos del Desarrollador:	[Identifique el nombre del creador de este software.]	Página del Fabricante:	[Ingrese el link de acceso del fabricante.]
Descripción:	[Describe el objetivo principal del software.]		
Aplicación y Funciones:	[Describe brevemente las principales funciones que presenta el software.]		
Áreas interesadas:	[Aquellas áreas que tiene interés en que el software se adquiera, o que por sus funciones sirven para cumplir las distintas tareas del área.]	Áreas autorizadas:	[Aquellas áreas que tienen autorización para adquirir y utilizar este software.]

Ilustración 13 Ficha técnica.

Fuente: Elaboración propia

Ahora bien, dentro de los campos que posee este documento se encuentra primeramente un macro en Visual Basic que arroja un formulario dentro de una ventana, en la cual solicita que identifique primeramente la clasificación del software (libre, perpetuidad, por uso, SaaS, Cloud y suscripción), el periodo de licenciamiento y dependiendo del caso el costo de este con su respectivo costo de soporte de mantenimiento. Estos datos son almacenados en una hoja diferente en donde se calcula el costo asociado total y se guarda el historial para futuras comparaciones. En la ilustración 14 es posible ver el formulario de Excel.

The image shows a web form titled "Seleccione el tipo de licencia" (Select the type of license) within a window labeled "Datos". The form includes a dropdown menu with the following options: "Software Libre", "Software a perpetuidad", "Software por uso", "SaaS", "Software Cloud", and "Software por suscripción". Below the dropdown, there are two input fields: "Periodo del licenciamiento" (License period) with a dropdown set to "Anualmente" (Annually), and "Costo de licenciamiento" (License cost) with a dollar sign and an empty input box. A red instruction reads "Para software libre por favor ingresar 0" (For free software please enter 0). Below this, there is another input field for "Costo de soporte" (Support cost) with a dollar sign and an empty box. At the bottom of the form is a "Guardar" (Save) button.

Ilustración 14 Formulario datos

Fuente: Elaboración propia

Asimismo, se solicita que sean diligenciados datos del fabricante, proveedores autorizados según las categorías aceptadas en el Banco, áreas solicitantes y autorizadas para adquirir el software, cantidad de licencias adquiridas, especificaciones mínimas para dispositivos, tipo de soporte adquirido, método de contratación y método de activación del producto. Algunas de estos campos son de diligenciamiento libre y otros se encuentran ligados a las opciones que se utilizan actualmente por medio de listas. En la siguiente ilustración se mostrarán los demás campos de la ficha técnica.

Método de adquisición:	<i>Seleccione dependiendo del caso</i>		Costo del Licenciamiento:		<i>Digite el valor</i>	
Datos del Proveedor:			Clasificación del proveedor		Seleccione dependiendo del caso	
Nombre:		Razón social:		NIT:		
Cámara de comercio:		RUT:		Representante legal:		
Gerente de cuenta:			Dirección:			
Teléfono (s) de contacto:			Correo electrónico:			
Categoría del producto de Software	<i>Identifique según sea el caso cada categoría con su sub-clase</i>					
Renovaciones:	<i>[Marque con una X cuando sea el caso.]</i>					
Se contrata soporte técnico:	<i>[Escriba SÍ o NO dependiendo del caso.]</i>					
Se dispone de derecho a:	<i>[Si la respuesta anterior fue Sí, conteste las siguientes seleccionando SÍ o NO dependiendo del caso.]</i>					
Soporte	<i>Seleccione dependiendo del caso</i>	Intalación por fabricante	<i>Seleccione dependiendo del caso</i>	Transferencia proceso de instalación o	<i>Seleccione dependiendo del caso</i>	
Mantenimiento	<i>Seleccione dependiendo del caso</i>	Medios para actualizar nueva versión entrega manuales, guías, seriales y acceso a material físico o digital	<i>Seleccione dependiendo del caso</i>	Inducción funcional del producto	<i>Seleccione dependiendo del caso</i>	
Entrega medios de instalación	<i>Seleccione dependiendo del caso</i>		<i>Seleccione dependiendo del caso</i>	Entrega de certificado de licenciamiento	<i>Seleccione dependiendo del caso</i>	
Método de activación del producto:	<i>Seleccione dependiendo del caso</i>					
Cantidad y relación de licencias del producto	<i>[Identifique con números en cada caso.]</i>					
Cantidad de licencias del producto	0	Cantidad de licencias utilizadas	0	Cantidad de licencias disponibles	0	<i>No tiene licencias disponibles</i>
Especificaciones técnicas mínimas	<i>[Identifique con números en cada caso.]</i>				<i>Cliente</i>	<i>Servidor</i>
Equipo cliente Posee los PC'S clientes según especificaciones del producto		Equipo servidor Posee servidores según especificaciones del producto		Microprocesador		
<i>Revisión por BRM</i>				Unidad de disco óptico		
<i>Seleccione según el caso</i>		<i>Fecha revisión</i> 11/05/2021		Unidad de disco duro		
Nombre:				Periféricos de video (tarjeta de expansión o)		
Comentario				Compatibilidad con sistema operativo 32 Bit o 64 Bit		
Firma:	_____			Comunicaciones o compatibilidad		
Cargo:				Exclusiones Firewall, Proxy		

Ilustración 15 Campos ficha técnica

Fuente: Elaboración propia

Como último, se propone el procedimiento de **Gestión de licencias en uso**, donde su principal objetivo es verificar que las licencias que se encuentran en utilización, son las mismas que están pactadas por los contratos de adquisiciones. Este procedimiento es posible observarlo en la ilustración 16 de a continuación.

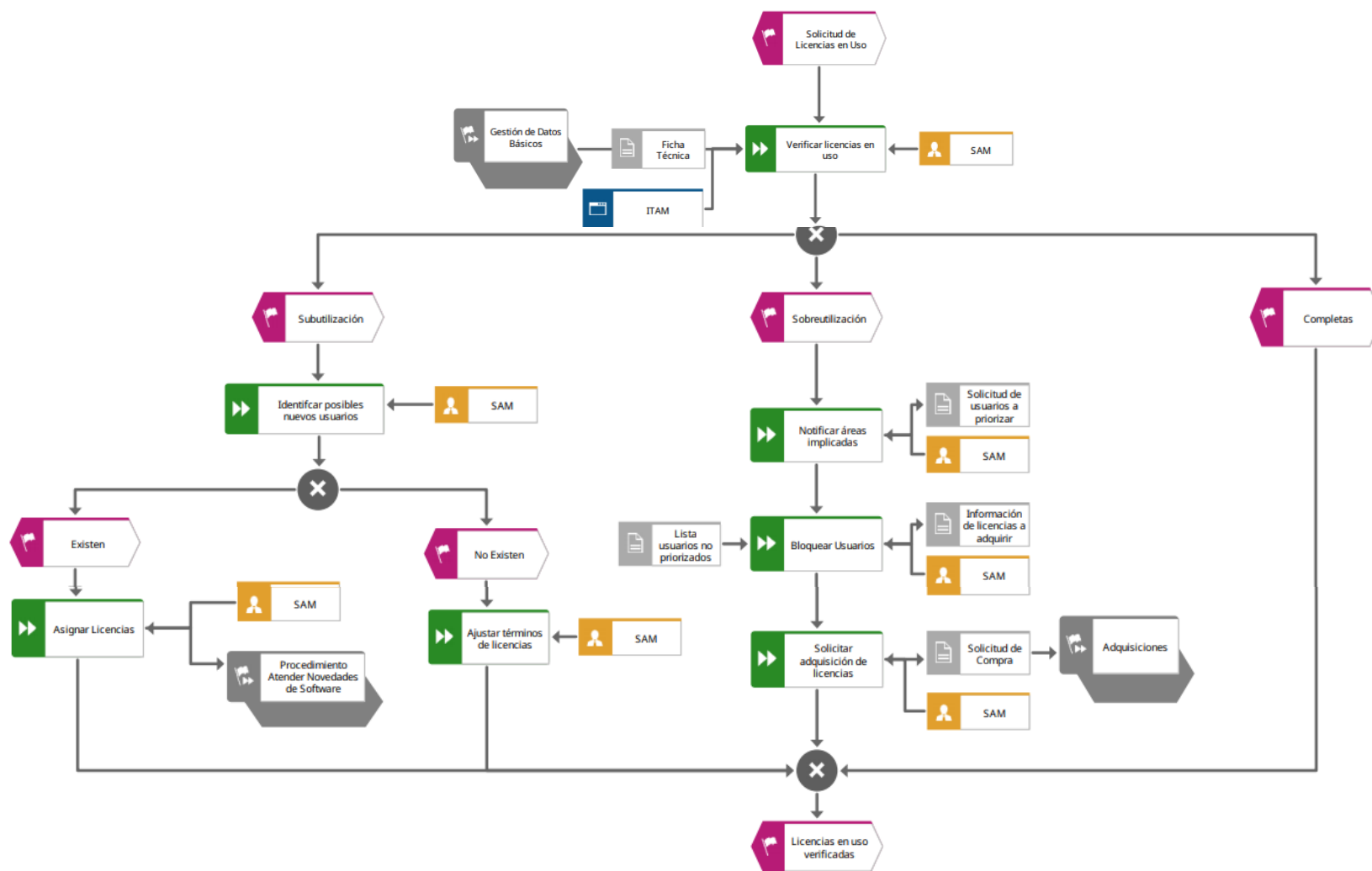


Ilustración 16 Gestión de licencias en uso

Fuente: Elaboración propia en la herramienta ARIS CLOUD

Este procedimiento cuenta con 14 actividades, donde se inicia con un evento de solicitud de licencias en uso de los diferentes softwares pagos, donde seguido de esto, el responsable SAM debe realizar una verificación de las licencias, con los datos proporcionados por el procedimiento de gestión de datos básicos, los cuales proporcionan la ficha técnica en donde se encuentran el número de licencias compradas y utilizadas, esta última actividad es posible verificarse por medio de la herramienta ITAM.

Al momento de realizar dicha verificación, es posible que arrojen 3 distintos caminos, cuando el resultado es completo, es decir, que las licencias compradas todas han sido utilizadas por los usuarios, el procedimiento concluye; sin embargo, si la verificación da como resultado una sub utilización, es decir, que del total de licencias pactadas con el proveedor, existen algunas que no tienen un usuario asignado, se debe identificar los posibles nuevos usuarios siguiendo con las políticas, acuerdos, usuarios autorizados y solicitudes de asignación, esto lo debe realizar el personal de SAM, si es afirmativa esta búsqueda se realiza la asignación de la licencia y se envía al procedimiento de atención de necesidades de software para que realicen la gestión de asignación e instalación. Por otro lado, si la respuesta es negativa, es necesario evaluar las métricas de uso y verificar si es posible realizar ajustes en los términos de las licencias para una futura renovación.

El tercer camino o respuesta posible a esta verificación, es la de sobre utilización, la cual significa que del total de licencias hay más usuarios que poseen el software, esto debe ser examinado, puesto que pueda que el usuario tenga el software instalado pero no posea acceso o no lo utilice, por consiguiente se debe informar a las áreas implicadas para

solicitar una priorización de los usuarios, con el fin de definir una lista de aquellos que no la están utilizando o que no es esencial para sus labores, seguido de esto, con esta lista es posible bloquear el acceso a los usuarios no priorizados o no autorizados y definir si es necesario adquirir nuevas licencias para ellos, por último, se debe solicitar al departamento de adquisiciones la compra de las licencias que faltan y con ello dar finalización al procedimiento con la verificación de licencias en uso.

9.4 Sensibilización y socialización en el área de Dirección General de Tecnología de la integración documental ISO 9001, ISO 19770-1, ITIL e IAITAM

Para lograr este objetivo, se realizaron algunas videoconferencias con las personas responsables del proyecto, en donde se hacían resúmenes de los logros realizados, desafíos nuevos, avances de propuestas estudiadas, planificación de los tiempos para realizar las actividades propuestas en este proyecto, además de consultas sobre diferentes temas de interés y sobre todo los resultados obtenidos. Este trabajo en conjunto, fue elaborado con el asesoramiento del responsable de este nuevo proyecto el ingeniero especializado, que cubre tareas sobre computación personal y responsable SAM. Además de la supervisión directa de los tutores asignados a este tema.

Ahora bien, no es posible detallar alguna evidencia sobre estas socializaciones puesto que estas reuniones hacen parte de las tareas diarias de la compañía, en donde por temas de confidencialidad, las reuniones no pueden ser grabadas ni los datos obtenidos en estas pueden ser utilizadas con otro fin diferente a las actividades del Banco, por consiguiente, no es posible anexar una fotografía sobre dichas reuniones.

Capítulo 10

Conclusiones y Recomendaciones

A través de los resultados de esta investigación, se logra identificar la importancia que posee en los sistemas de gestión, la adecuada gestión de las licencias y almacenamiento de activos. Como esto brinda una ventaja hacia la organización no solo para el dominio de las TIC, sino también para la gestión financiera, contractual, estratégica, de toma de decisiones.

El área de la DG-T posee en su mayoría varias características implementadas sobre la gestión de activos de TI, que han sido definidas por la norma ISO/IEC 19770-1 y guías ITIL y NIST estudiadas para este proyecto, por lo tanto, el sistema que se encuentra actualmente, cumple con los objetivos propuestos no solo para la gestión de activos, sino para la integración del sistema actual de gestión ISO 9001 e ISO/IEC 27000.

El Banco de la República, en especial el área de Dirección General de Tecnología, puede tomar como base para futuras documentaciones este proyecto, en donde se encuentran los estándares y buenas prácticas consolidadas de las normas y guías estudiadas, para la construcción de políticas y procedimientos diferentes a los propuestos en el numeral 9.3, que ayudarán a la toma de decisiones sobre los activos en todo su ciclo de vida.

Se recomienda la implementación de los procedimientos y actividades para la gestión de los datos básicos, realización de inventario de software y gestión del uso de licencias, que además de servir para estandarizar las funciones, es posible con ellas determinar parámetros y métricas con las cuales se pueden optimizar los productos

ofrecidos a los usuarios, como también minimizar los costos en cuanto a productos software adquirido que no está siendo utilizado y no es de utilidad para la organización.

Se recomienda concientizar en los trabajadores de la DG-T la importancia de la implementación y documentación de este sistema, con el fin de dar a conocer el alcance y objetivos y por medio de ellos realizar mejoras sustanciales a las operaciones diarias y mantener los sistemas de gestión adecuados y perdurables.

Referencias

- Alcántara, R., Palacios, C., & Vigo, J. (Febrero de 2018). *Repositorio académico UPC*. Obtenido de <https://repositorioacademico.upc.edu.pe/handle/10757/623573>
- AXELOS. (2011). *ITIL V3*. Norwich: TSO.
- AXELOS. (2019). *ITIL V4*. Norwich: TSO.
- Banco de la República. (28 de Septiembre de 2020). *Banco de la República*. Obtenido de <https://www.banrep.gov.co/es/el-banco/contenidos/page/historia>
- Banco de la República. (28 de Septiembre de 2020). *Banco de la República*. Obtenido de <https://www.banrep.gov.co/es/organigrama>
- Caillaux, C. (13 de Octubre de 2020). *Conexiónesan*. Obtenido de <https://www.esan.edu.pe/conexion/actualidad/2020/10/13/cuanto-ha-transformado-la-tecnologia-nuestras-vidas-durante-la-pandemia/>
- CORNELEC. (2020). *CORNELEC*. Obtenido de <https://cornelec.cl/iec/>
- DELOITTE. (2016). *DELOITTE*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Administracion_activos_software-2016.pdf
- Deloitte.insights. (2019). *Tendencias tecnologicas 2019*. New York.
- DG-T. (28 de Septiembre de 2020). *Banco de la República*. Obtenido de <https://www.banrep.gov.co/es/organigrama-sgsc>

DG-T. (2021). *BANCO DE LA REPÚBLICA*. Obtenido de <https://d11oz1xo3vrzp6.cloudfront.net/publish/2020/12/2/8e315d9515ce4834900e3805abec273f.mp4>

Economipedia. (2016). *Economipedia*. Obtenido de <https://economipedia.com/actual/las-ventajas-la-tecnologia-las-empresas.html>

Freshservice. (2018). *Freshservice.com*. Obtenido de <https://freshservice.com/latam/it-asset-management-software/>

Gonzales, J. (2018). *Repositorio Universidad Norbert Wiener*.

González, P. (17 de Septiembre de 2018). *Library*. Obtenido de <https://1library.co/document/8ydop0gz-diseno-analisis-implementacion-gestion-software-recomendaciones-entornos-empresariales.html>

IAITAM. (2019). *IAITAM*. Obtenido de <https://iaitam.org/what-is-it-asset-management/>

IAITAM. (2020). *IAITAM*. Obtenido de <https://iaitam.org/about-us/>

IAITAM. (2020). *IAITAM*. Obtenido de <https://iaitam.org/citam/>

IEC. (2020). *IEC*. Obtenido de <https://www.iec.ch/what-we-do>

ISO . (2015). *ISO*. Obtenido de <https://www.iso.org/home.html>

ISO. (Septiembre de 2015). *Nueva ISO*. Obtenido de <https://www.nueva-iso-9001-2015.com/2016/09/desarrollo-concepto-calidad/>

ISO 9001. (2015). *Sistemas de gestión de la calidad*. Londres: ISO.

ISO. (s.f.). *ISO*. Obtenido de <https://www.iso.org/isoiec-jtc-1.html>

ISO/IEC 19770-1. (2017). *Sistema de gestión de activos TI*.

ISOTools. (2010). *ISOTools*. Obtenido de [https://www.isotools.com.co/normas/ntc-iso-9001/#:~:text=La%20NTC%20ISO%209001%20es,T%C3%A9cnicas%20y%20Certificaci%C3%B3n%20\(ICONTEC\),&text=Con%20la%20NTC%20ISO9001%20C%20las,calidad%20exigida%20a%20nivel%20internacional.](https://www.isotools.com.co/normas/ntc-iso-9001/#:~:text=La%20NTC%20ISO%209001%20es,T%C3%A9cnicas%20y%20Certificaci%C3%B3n%20(ICONTEC),&text=Con%20la%20NTC%20ISO9001%20C%20las,calidad%20exigida%20a%20nivel%20internacional.)

ITIL FUNDATION. (2019). *ITIL 4 edición*. Londres: AXELOS.

Loja, J. (13 de Febrero de 2015). *Universidad Politecnica Salesiana de Ecuador*. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/7805/1/UPS-CT004654.pdf>

Maisterra, O. (Diciembre de 2008). *Repositorio Tecnológico de Monterrey*. Obtenido de https://repositorio.tec.mx/bitstream/handle/11285/568961/DocsTec_6821.pdf?sequence=1&isAllowed=y

ManageEngine. (2019). *ManageEngine.com*. Obtenido de <https://www.lifeder.com/investigacion-descriptiva/>

Manga, R. (2016). *Wordpress*. Obtenido de <https://solinfocol.wordpress.com/2016/12/05/ley-603-de-2000/>

Mejía, T. (2020). *Lifeder.com*. Obtenido de <https://www.lifeder.com/investigacion-descriptiva/>

Morales, F. (2017). *Economipedia*. Obtenido de <https://economipedia.com/definiciones/estandarizacion.html>

NIST. (2012). *NIST*. Obtenido de <https://www.nist.gov/about-nist/our-organization/mission-vision-values>

Quintero, D. (2009). *Repositorio UPB*. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/708/digital_17345.pdf?sequence=1&isAllowed=y

SIC. (2016). *Super intendencia de industria y comercio*. Obtenido de <https://www.sic.gov.co/preguntas-frecuentes-rnbd>

Taslaviña, J., & Miguel, G. (2018). *Repositorio Universidad Distrital*. Obtenido de <https://repository.udistrital.edu.co/bitstream/handle/11349/13717/GarciaCardozoMiguelAngel2018.pdf?sequence=1&isAllowed=y>