MAESTRÍA EN GERENCIA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN PARA ROCHE ECUADOR S.A. EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA, PARA EL AÑO 2014.

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Magíster en Gerencia de Sistemas y Tecnologías de la Información

Profesor Guía
Dr. Hugo Banda Gamboa

Autor
Jorge Burgos Donoso

2014

DECLARACIÓN DEL PROFESOR – GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Hugo Banda
Philosophy Doctor (PhD)
C. C.: 1710277950-3

DECLARACIÓN DE AUTORÍA

Declaro (amos) que este trabajo es original, de mi (nuestra) autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

Jorge Burgos Donoso
C. C.: 171457080-9

AGRADECIMIENTOS

El presente trabajo no podría haber sido posible sin el apoyo constante y caluroso de mi familia, base de mis logros y mis esfuerzos. Quiero agradecerles infinitamente por su amor y fomento.

De manera especial, deseo manifestar mi profunda gratitud a la Universidad de las Américas, a su personal docente, administrativo y de servicios y de manera particular al doctor Hugo Banda Gamboa por su permanente apoyo y enseñanza durante la realización del presente trabajo investigativo.

De la misma manera, quiero agradecer a ROCHE Ecuador, por haberme permitido realizar la investigación dentro de la empresa. Espero de todo corazón que los resultados y la propuesta sean de ayuda dentro de las operaciones de la organización.

DEDICATORIA

A mi esposa y mis hijos, con todo mi amor por su apoyo irrestricto y caminar conmigo a través de los sacrificios que han significado el cursar mi Maestría; a mis padres, por estar siempre a mi lado; a mis hermanas y a mi familia.

RESUMEN

El presente trabajo determina las vulnerabilidades del área de tecnologías de la información (TI) en la empresa ROCHE del Ecuador, con el fin de diseñar un modelo de gestión de riesgos acorde a las necesidades de la organización.

Tras la aplicación de un estudio descriptivo, se encontró que las principales falencias de la gestión de riesgos de TI son: falta de capacitación de los usuarios sobre los riesgos y políticas de TI, inadecuado plan de mantenimiento preventivo, exceso de mantenimiento correctivo y cambios y mejoras de los componentes de manera desordenada. Todos estos elementos abonan a la paralización irregular de las operaciones de ROCHE del Ecuador.

La evaluación de los elementos estudiados permitió definir las siguientes medidas para el modelo de gestión de riesgos de TI: capacitación de los usuarios, mejoramiento del plan de mantenimiento preventivo, procesos claros de mantenimiento correctivo y su reducción; y, cambios y mejoras en los componentes de manera más ordenada.

El modelo propuesto, así como los hallazgos en la evaluación de los procesos actuales de gestión de riesgos de TI, ha sido presentado a las autoridades respectivas de la entidad estudiada y ha sido aprobada su implementación.

ABSTRACT

The following document identifies vulnerabilities of the information technology (IT) area in ROCHE - Ecuador, in order to design a risk management model based on the needs of the organization.

After the application of a descriptive study, it was found that the main shortcomings of IT managing risks are: lack of user training on risks and IT policies, inadequate maintenance plan, excessive corrective maintenance and changes and improvements of the IT components with a disorderly manner. All these elements paid to irregular cessation of operations of ROCHE.

The evaluation of the studied elements allowed the following steps to define the model of IT risk management: user training, improve the maintenance plan, clear processes for corrective maintenance, and more orderly changes and improvements in the components.

The proposed model, as well as the findings in the evaluation of the current processes of IT risk management, has been submitted to the respective authorities of the studied entity and approved its implementation.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Las acciones de gestión de riesgos de TI permiten la identificación y evaluación de vulnerabilidades así como la selección de alternativas óptimas para el mantenimiento de componentes con el fin de reducir las vulnerabilidades detectadas y, finalmente, el control y evaluación de las acciones desarrolladas.

La gestión de riesgos de TI, ha ido incrementando su importancia con los años debido a la dependencia, cada vez más profunda, de las operaciones de las compañías hacia su información gerencial y los componentes tecnológicos para su administración y almacenamiento.

Una de estas empresas es ROCHE Ecuador, empresa farmacéutica de gran prestigio que requiere para sus operaciones de componentes tecnológicos que, en la actualidad presentan varias vulnerabilidades.

El objetivo del presente trabajo es definir las causas y los efectos de los problemas actuales de TI de la empresa estudiada y proponer un modelo que permita la solución de los mismos.

La presente investigación se encuentra estructurada de la siguiente manera:

CAPÍTULO I. GENERALIDADES: En este capítulo se determina el tema, los antecedentes, los objetivos de la investigación y su justificación, además de un acercamiento a la metodología utilizada.
CAPÍTULO II. FUNDAMENTACIÓN TEÓRICA: En este espacio se hace un resumen de análisis teórico de elementos que servirán para la investigación y la propuesta posteriores.
CAPÍTULO III. ANÁLISIS DEL DOMINIO DEL PROBLEMA: Este capítulo determina cuál es el problema de la investigación, además de determinar los componentes y actores que posteriormente serán evaluados.

CAPÍTULO IV. INTEGRACIÓN SISTÉMICA: Este capítulo ofrece una visión más específica acerca de los actores y componentes así como de sus relaciones y problemas. De manera adicional, se presentan opciones de sistemas integrados para su evaluación.

CAPÍTULO V. REQUERIMIENTOS Y CASOS DE USO: En este espacio se hará un recuento de los usos del sistema seleccionado y las funciones de los actores determinados previamente.

CAPÍTULO VI. ESPECIFICACIONES ARQUITECTÓNICAS: En este capítulo se hace un análisis pormenorizado de la arquitectura de los componentes y los procesos con el fin de proponer alternativas y seleccionar aquellas que se consideren óptimas para su aplicación en el modelo.

CAPÍTULO VII. DISEÑO FÍSICO: En este apartado se define cuáles serán los componentes, las políticas y los procesos, seleccionados previamente, y su determinación concreta, lo que incluye mapas de procesos a ser llevados a cabo en el modelo propuesto.

CAPÍTULO VIII. CONCLUSIONES Y RECOMENDACIONES: Derivadas de la investigación y la propuesta presentadas.

CAPÍTULO I

GENERALIDADES

1.1 TEMA

Elaboración del Plan de Gestión de Riesgos de las Tecnologías de la Información para Roche Ecuador S.A. en la ciudad de Quito, provincia de Pichincha, para el año 2014.

1.2 ANTECEDENTES

Roche Ecuador S.A. es una empresa multinacional de origen suizo con sede en Basilea que se dedica a la investigación y el desarrollo de productos farmacéuticos, equipos de diagnóstico clínico y productos biológicos para el tratamiento de algunas enfermedades, especialmente de patologías de tipo catastróficas como son el cáncer, la artritis reumatoide, el SIDA y la fibrosis quística.

En el Ecuador, la empresa cuenta con una presencia de 30 años aproximadamente y tiene oficinas en las ciudades de Quito y Guayaquil, donde laboran cerca de 300 empleados en diferentes áreas de la organización. Roche Ecuador S.A. es una compañía sólida que apalanca su operación de manera muy fuerte con las Tecnologías de la Información y brinda a sus empleados equipos y sistemas de última generación para así, optimizar el tiempo y la eficiencia de sus colaboradores (ROCHE, 2010).

Lo señalado, junto al manejo de información sensible y confidencial, hace necesario contar con un plan de Gestión de Riesgos basado en los estándares de gestión de seguridad, lo cual permita la detección, identificación, mitigación

y control de los factores de riesgo que atenten contra la integridad de la información, equipos tecnológicos y la normal operación del negocio en el país.

En la actualidad, Roche Ecuador S.A. no cuenta con un Plan de Gestión de Riesgos lo cual supone dejar a la compañía en un estado de vulnerabilidad ante sus competidores y pone en alto compromiso el normal desempeño de su gestión comercial en el Ecuador así como también el alcanzar sus objetivos y metas de manera segura y eficiente.

1.3 OBJETIVOS

1.3.1 Objetivo general

Desarrollar un Plan de Gestión de Riesgos para Roche Ecuador S.A. apalancado por los estándares aplicables a dicho efecto, con la finalidad de influir positivamente en la eficacia y eficiencia operativa de la compañía.

1.3.2 Objetivos específicos

- Determinar la fundamentación teórica como sustento para el desarrollo del plan.
- Verificar la situación actual de Roche Ecuador S. A. con el fin de identificar sus sistemas y procesos de TI así como su grado de vulnerabilidad.
- Mejorar el Gobierno de TI mediante la Gestión de Riesgos y establecer un adecuado Plan de Comunicación para la difusión de las normativas adoptadas por TI.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Por medio de la investigación propuesta, se presenta un escenario apropiado en cuanto a la Gestión de Riesgos en Roche Ecuador S.A., donde exista un conocimiento y un orden en las actividades que permitan la identificación, mitigación y el control de los riesgos relativos a TI. Esto ayudará de manera efectiva al mejoramiento de la Organización a través del alineamiento del departamento de TI con los objetivos estratégicos de la Organización.

1.5 ASPECTOS METODOLÓGICOS

El estudio es de tipo no experimental (debido a que no se considera la intervención del investigador en variable alguna) y descriptivo (ya que permite la reseña e identificación de hechos relacionados con el objeto de estudio con el fin de diseñar modelos para su solución (Bernal, Metodología de la Investigación , 2006, pág. 112).

Se utilizan los métodos inductivo y deductivo que permiten encontrar “conclusiones generales que parten de hechos particulares” y en “tomar conclusiones generales para explicaciones particulares” (Eyssautier de la Mora, 2006, pág. 98), respectivamente. Estos métodos permiten la relación entre la fundamentación teórica y los resultados verificados. También se hace uso del método cualitativo-cuantitativo que permite recopilar, tabular y analizar la información obtenida por las técnicas de investigación (Eyssautier de la Mora, 2006, pág. 99) que se aplican.

Entre las técnicas de las que se vale el estudio para fundamentar sus conclusiones y el plan de gestión de riesgos para Roche Ecuador S. A. se encuentran:

- Entrevista estructurada a los empleados del departamento de TI con la finalidad de conocer sus criterios acerca del estado de la estructura informática de la organización, así como la identificación de los riesgos.
- Estudio biblioFigura y documental con el propósito de desarrollar tanto la fundamentación teórica como el análisis situacional de la empresa.
- Observación directa para determinar los equipos, sistemas y procesos pertinentes para la investigación.

Los resultados de las técnicas mencionadas se recopilan, tabulan y analizan mediante las siguientes herramientas:

- Entrevista: se aplican las preguntas determinadas en el cuestionario de entrevista (Anexo 2) y se procede a realizar una grabación de la conversación, previa autorización del entrevistado. Al tratarse de datos cualitativos, no se requiere de tabulación.
- Estudio biblioFigura / documental: los datos se registraron en fichas y otros instrumentos adecuados para este tipo de estudio.
- Observación directa: se registra de manera textual a través de visitas con previa autorización de los funcionarios a cargo.

La población determinada como usuarios de TI está conformada por la totalidad de empleados de Roche Ecuador S. A. en Quito, provincia de Pichincha, Ecuador, que asciende a 150 empleados. No se considera una técnica que involucre a los usuarios debido a su falta de relación directa y conocimiento sobre la implementación de políticas y gestión de riesgo de TI.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1 TECNOLOGÍAS DE LA INFORMACIÓN

La tecnología de la comunicación es parte importante de la vida actual, ya que está dentro de todos los estratos de la sociedad, integrando desde las más grandes corporaciones, hasta el microempresario, e igualmente en el ámbito personal.

Actualmente, muchos instrumentos que hasta hace 10 años no existían o no eran lo suficientemente avanzados, son usados no solo para su función principal, sino también para comunicarse entre usuarios. El ejemplo por excelencia de esta transición es el Smartphone, el cual ha dejado muy por detrás su principal función la cual es recibir y hacer llamadas, ya que es usado más como un instrumento multimedia de entretenimiento. Dentro de este mismo grupo de objetos se encuentran las actuales smart tv, mp3, tablets, entre otros dispositivos.

2.1.1 Antecedentes históricos

El ordenador, base de la información, es una máquina electrónica que procesa de forma automática los datos. Además, permite almacenarlos, recuperarlos y transmitirlos (Alonso, 2010).

Históricamente, el hombre siempre ha necesitado realizar a la perfección diversas tareas matemáticas, por lo cual el hombre creó su propia forma de mantener sus operaciones matemáticas.

La primera herramienta que se utilizó para esta tarea en el viejo continente fue el ábaco, el cual fue usado por diferentes sociedades como la griega, babilonia, romana, china, entre otras.

En América Latina, se conoce que los Incas usaban un sistema de nudos llamado “Quipus” para mantener la contabilidad por los quipucamayoc, los administradores del imperio.

A mediados del siglo XVII, el matemático Blaise Pascal desarrolló la primera calculadora mecánica, la cual permitía realizar sumas y restas. En 1670, el científico alemán Gottfried Wilhelm Leibniz construyó otra máquina que tenía la capacidad de multiplicar y dividir.

En 1835, el inglés Charles Babbage construyó una máquina que realizaba análisis y cálculos, la cual se considera el primer ejemplo de computador. Esta máquina originó el concepto de codificación digital (1= sí, 0=no), y un sistema de programación, el cual fue realizado por Augusta Ada Byron, quien fue la primera programadora de la historia.

Paralelamente, el primer modelo de telégrafo fue diseñado en 1837, con experimentos previos sobre la corriente eléctrica. Años después en 1860, Antonio Meucci presenta su invento llamado el “teletrófono”, que reproducía la voz de un cantante a larga distancia la voz de un cantante. Pocos años después Alexander Graham Bell patentó un artefacto que se conoce hasta ahora como el teléfono común.

A finales de siglo XIX, Hermann Hollerith diseñó una máquina que leía tarjetas perforadas, con el objetivo de mecanizar el censo en estados unidos.

En 1924, se inaugura la compañía IBM, la cual en la década de los 30 empezó a utilizar interruptores y contactos electromagnéticos en estado de encendido y apagado, así comenzando la era del computador digital.

En 1945 John Mauchly y John Eckert crearon el primer computador, el cual se trataba de una máquina programable y universal llamada ENIAC. Esta máquina ocupaba 160 metros cuadrados, pesaba 30 toneladas y funcionaba con 17468 válvulas de vacío. Este masivo proyecto se terminó en 30 meses de trabajo en equipo por científicos capacitados en electromagnetismo.

Al año 1965, se estaban llevando a cabo el desarrollo de los primeros circuitos integrados, los cuales albergaban un circuito integrado en un chip, llegando a ocupar un espacio muy reducido. El tamaño de este último se redujo tanto que para 1970 se creó el primer microprocesador comercial, el cual se llamaba 8008, creado por la compañía Intel.

En los sesenta, compañías como Apple crearon los primeros modelos de microordenador, los cuales incluían pantalla teclado y unidades de almacenamiento. Al mismo tiempo, nació Microsoft, compañía que facilitó un sistema operativo MS-DOS y el lenguaje de programación BASIC, lo cual facilitaba la programación.

El teléfono móvil fue creado por Motorola, siendo este un artefacto de tamaño bastante considerable, de tal manera que coloquialmente la gente lo conoce como “bloque”. El 3 de abril de 1973, Martin Cooper, el director de I+D de Motorola usó el primer prototipo funcional de teléfono celular (predecesor al DynaTAC 8000X de la misma compañía) para llamar a su compañero y rival Joel Engel, quien estaba a cargo de los Laboratorios Bell, mientras caminaba tranquilamente por la calle.

Desde los noventa hasta la actualidad, la evolución de la tecnología no ha tenido limitantes, puesto que esta es cada vez más potente y accesible al igual que pequeña y práctica.

2.1.2 Elementos

2.1.2.1 Hardware:

Básicamente, el hardware consiste en el físico de un computador o de un artefacto tecnológico, entre los cuales comúnmente se encuentra un case, un teclado, tarjetas, microprocesadores, memorias, entre otros. Igualmente, el hardware se divide en dos:

- Hardware básico, el cual comprende todo lo previamente mencionado y que sirve para el funcionamiento del dispositivo
- Hardware complementario, el cual contiene cámaras, impresoras, faxes, y otros dispositivos que sirven como elementos que mejoran o incrementan la funcionalidad o servicios del artefacto.

2.1.2.2. Software:

Comprende la parte intangible de un artefacto tecnológico, como lo es el sistema operativo y programas varios, los cuales permiten al ordenador realizar una tarea comandada por el usuario.

El software está compuesto por una secuencia de instrucciones que son ejecutadas para cada gestión.

Este puede ser ejecutado por cualquier dispositivo capaz de interpretar y llevar a cabo las instrucciones para la cual es creado. El software se clasifica en:

- Software de sistema: Comprende el sistema operativo, controladores de dispositivos y toda herramienta que sirva para el control específico de las características de las computadoras.
- Software de aplicación: Son aquellos programas creados para llevar a cabo una tarea específica, en el cual podemos encontrar procesadores de texto como Word o diseño Figura como Photoshop.

2.1.2.3 Redes y Protocolos (interconexión)

En el mundo de las telecomunicaciones, esta se refiere a la vinculación de recursos físicos y soportes lógicos, la cual incluye las instalaciones necesarias con el motivo de permitir el interfuncionamiento de las redes y la interoperabilidad de servicios de comunicaciones (Ministerio de Tecnologías de la información y Comunicaciones, 2013). En otras palabras, esta es una estructura que sirve para manejar una sola conexión entre varios usuarios.

“Por su parte, la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha definido interconexión como “la forma por la cual diferentes redes están conectadas para permitir el tráfico pasar entre ellas, incluyendo el conducir el tráfico sobre la red de un operador por cuenta de otro operador o proveedor del servicio.” (Observatel.ac, 2010)

2.1.2.4 Base de datos:

La base de datos es similar a una biblioteca, ya que este es un lugar donde toda la información se almacena para su uso posterior.

La base de datos es de suma importancia puesto que sin esta, un computador no tiene referencias o un uso clave en el que pueda ser usado.

La base de datos mundialmente conocida en la actualidad es la internet, ya que esta almacena toda la información que se desee compartir, al igual que existe otro método más profundo que se llama la Deepweb, que igualmente es una base de datos, pero esta posee información clasificada.

La web de Office dice que una base de datos es una herramienta que sirve para recopilar y organizar información. En la base de datos se puede almacenar información sobre cualquier cosa. Igualmente, dice que una base de datos empieza siendo una lista, pero a medida que esta crece, suelen aparecer incongruencias en los datos, los cuales deben ser remediados de manera satisfactoria para que la base de datos sea idónea.

2.1.3 Tipos de sistemas en la organización

2.1.3.1 Sistema de procesamiento de transacciones (Transaction Processing System, TPS)

Este es un sistema que recolecta toda la información que sale a partir de transacciones producidas por una organización. Una organización es un evento que genera o modifica los datos que se encuentran almacenados dentro de un sistema de información (Rosas, 2012).

El TPS es un sistema que mantiene monitoreado todos los programas transaccionales.

Este sistema soporta y disminuye el trabajo manual, maneja un gran volumen de transacciones, apoyan actividades que se realizan en el nivel operativo, brinda fiabilidad a las transacciones al igual que rapidez de respuesta, inflexibilidad y un procesamiento controlado, por lo cual es de suma importancia dentro de una organización.

2.1.3.2 Sistemas de oficina

Los sistemas de automatización de oficina, mejor conocido como OAS, que consiste en un paquete de aplicaciones con las cuales están destinadas a mejorar el trabajo de un empleado y por lo tanto, a la empresa.

Comúnmente, este paquete incluye un procesador de textos, una hoja de cálculo y un software de presentación. El ejemplo más claro de este tipo de OAS es por supuesto Microsoft Office.

2.1.3.3 Sistemas de trabajo de conocimiento (Knowledge Work Systems, KWS)

Este es un sistema de información que apoya a los trabajadores con la creación de nuevo conocimiento en una organización. Fue diseñado para promover la creación de conocimiento y garantizar que el nuevo conocimiento y la experiencia técnica se integra adecuadamente en la empresa.

Este sistema de información ayuda a los administradores y trabajadores a analizar los problemas, visualizar aspectos complejos y crear nuevos productos de manera más eficiente.

2.1.3.4 Sistemas de Información Gerencial (Management Information Systems, MIS)

También conocido como SIG es un sistema integrado usuario-máquina, el cual implica que algunas tareas son mejor realizadas por la mano del hombre, mientras que otras son muy bien hechas por la máquina.

Además, estos sistemas conforman un conjunto de información extensa y coordinada se subsistemas racionalmente integrados que transforman los

datos e información en una variedad de formas para cumplir con cabalidad los requerimientos de los administradores.

2.1.3.5 Sistemas de Soporte de Decisión (Decision Support System, DSS)

Un sistema de soporte de decisión es una herramienta de negocios, la cual se enfoca al análisis de los datos de una organización.

Es una herramienta de gran uso, ya que esta permite resolver los problemas y limitaciones de manera más optimizada. Es decir, los DSS son un sistema interactivo, el cual está basado en software hecho con la intención de ayudar a las personas que deban tomar decisiones.

En conclusión se puede decir que un DSS es un sistema de información que combinan datos y modelos, analíticos sofisticados o herramientas de análisis de datos para apoyar la toma de decisiones semi-estructurada y no estructurada.

2.1.3.6 Sistema de Apoyo a Ejecutivos (Executive Support Sistems, ESS)

Este es un sistema de información para los directivos que permite automatizar la labor de obtener los datos más importantes de una organización, resumirlos y presentarlos de la forma más comprensible posible, provee al ejecutivo acceso fácil a información interna y externa al negocio con el fin de dar seguimiento a los factores críticos del éxito. Se enfocan primordialmente a proporcionar información de la situación actual de la compañía y dejan en un plano secundario la visualización o proyección de esta información en escenarios futuros. En un entorno característico de sistemas de información, el sistema consolida y administra muchas de las funciones de información diarias

en relación con las áreas de oficina, administrativas, financieras y cualquier otra índole que el ejecutivo requiera.

Los Sistemas de Soporte a Ejecutivos se construyen generalmente mediante la integración de software diseñado para operar conjuntamente con la infraestructura y las aplicaciones de información existentes en la institución.

2.2 Information Technology Infrastructure Library ITIL v.3

2.2.2 Antecedentes

ITIL fue desarrollado en los años 80, sin embargo, no fue hasta la década del 90 que fue ampliamente adoptada. Este fue desarrollado por la CCTA, una agencia británica estatal. El objetivo de esta herramienta es encontrar una vía para mejorar de forma duradera estos servicios reduciendo al mismo tiempo los costes. Igualmente desarrolla procedimientos efectivos y económicos para la oferta de servicios de TI, que se encuentra hoy en día documentadas en ITIL.

2.2.2.1 Ciclo de vida del servicio

En 2007 se editó una nueva versión de ITIL, totalmente revisada y mejorada: ITIL V3. ITIL V3 recoge las experiencias de las versiones anteriores y se centra al mismo tiempo en apoyar el negocio base de las empresas e intentar que las mismas puedan conseguir a largo plazo ventajas sobre la competencia mejorando la labor de la organización de TI.

En comparación con ITIL V2, el cual se basa en un total de nueve libros, ITIL V3 está claramente focalizada. Se constituye de cinco publicaciones primordiales que reproducen conjuntamente el Ciclo de Vida del Servicio:

- Estrategia del Servicio

- Diseño del Servicio
- Transición del Servicio
- Operación del Servicio
- Perfeccionamiento Continuo del Servicio

Para mejorar el Ciclo de Vida del Servicio se cambió la estructuración de la oferta de servicios, dividida en ITIL V2 en las disciplinas Soporte de Servicio y Servicio de Envío, por una nueva, orientada claramente a las cinco fases del Ciclo de Vida del Servicio de TI.

En ITIL V3, los procesos ya conocidos de ITIL V2 se complementan con numerosos procesos nuevos. Estas novedades se caracterizan por una mayor orientación al cliente a la hora de ofrecer servicios de TI. Se trata de conseguir para el cliente un valor agregado positivo y, con ello, una significativa plusvalía para la empresa. Este nuevo enfoque no cuestiona, sin embargo, los principios en los que se basa ITIL. Éstos quedan casi inalterados.

2.2.2.2. Estrategia del servicio

Para conseguir determinar las estrategias de servicio, es imprescindible determinar en primer lugar qué servicios deben ser prestados y por qué han de ser prestados desde la perspectiva del cliente y el mercado.

Por lo tanto, una correcta estrategia debe:

- Servir de guía a la hora de establecer y priorizar objetivos y oportunidades.
- Conocer el mercado y los servicios de la competencia.
- Armonizar la oferta con la demanda de servicios.
- Proponer servicios diferenciados que aporten valor añadido al cliente.

- Gestionar los recursos y capacidades necesarios para prestar los servicios ofrecidos teniendo en cuenta los costes y riesgos asociados.
- Alinear los servicios ofrecidos con la estrategia de negocio.
- Elaborar planes que permitan un crecimiento sostenible.
- Crear casos de negocio para justificar inversiones estratégicas.

Definir las estrategias es el eje que permite que las fases de Diseño, Transición y Operación del servicio se ajusten a las políticas y visión futura del negocio.

2.2.2.3. Diseño del servicio

El diseño es la segunda fase del ciclo de vida del Servicio y trata de la producción y mantenimiento de políticas informáticas, arquitecturas y documentos para el diseño adecuado de procesos y soluciones de servicios de infraestructura informática innovadora.

Los términos a conocer de esta fase son:

- SLA (Acuerdo de nivel de servicio): Contrato con el cliente externo. Todo lo que se incluye en el SLA se ha de poder medir o monitorizar. Un SLA no puede incluir lenguaje legal o técnico que pueda crear ambigüedades, por lo que se incluirá un glosario. El SLA incluirá: unas 10 páginas de texto, niveles de disponibilidad del servicio, tiempos de respuesta y tiempos de respuesta en caso de emergencia, plazos y precios.
- OLA (Acuerdo de nivel operativo): Contrato entre dos partes de la misma organización (interno).
- UC (Contrato de soporte): Sería con un proveedor externo.
- CSF: Factores Críticos de Éxito.
- KPI: indicadores Clave de Rendimiento.

- Caída del Servicio: Casos de desastre. Se entiende por Desastre: Fallo o interrupción del servicio o del funcionamiento normal del mismo, que requiere de muchos recursos para su recuperación o restauración.
- CAU: Centro de atención al usuario. Actúa de filtro. Atiende llamadas y las pasa.
- CSU: Service Desk. Registra la incidencia. Es quien da la solución.
- Principios del diseño del Servicio.
- Diseño de la Cartera de Servicios.
- Requisitos del negocio en el diseño del servicio.
- Diseño de la Tecnología.
- Diseño del Proceso.
- Diseño de la Medición.

Como fundamento del diseño del servicio debemos tener en cuenta las 4 P's del Diseño:

- Personas.
- Proyecto.
- Procesos.
- Productos/Tecnología.

Estas 4 P's conforman lo primero a tener en cuenta para implementar ITIL

Los siete procesos de la fase de diseño que se deben desarrollar son:

- Gestión del Catálogo de Servicios.
- Gestión del Nivel de Servicio (SLM).
- Gestión de la Capacidad.
- Gestión de la Disponibilidad.
- Gestión de la Continuidad del Servicio.
- Gestión de la Seguridad de la Información.

- Gestión de suministradores/proveedores.

Las etapas en el diseño del proceso son:

- Desencadenante.
- Entrada.
- Proceso Genérico: controles, procesos, facilitadores.
- Salida.

2.3 MEJORA CONTINUA DEL SERVICIO

2.3.1 Otras normas de gestión de TI

2.3.1.1 Normas ISO (International Organization for Standardization)

Las normas ISO son creadas para satisfacer necesidades en los campos económico, financiero, industrial y técnico, siendo este el resultado de un consenso internacional emanado de los diferentes comités técnicos para un fin determinado. Hasta el actual momento un número definido de estos, que se pueden identificar según la especialidad de su dedicación. Los diferentes comités técnicos especializados de la ISO, realizan estudios y publicaciones sobre los diferentes campos del conocimiento, quienes han publicado más de 8000 normas internacionales e informes técnicos.

ISO-20000

> “La ISO 20000 fue desarrollada en diciembre de 2005 y es la primera norma en el mundo específicamente dirigida a la gestión de los servicios de TI. La ISO 20000 fue desarrollada en respuesta a la

> necesidad de establecer procesos y procedimientos para minimizar los riesgos en los negocios provenientes de un colapso técnico del sistema de TI de las organizaciones" (Maeztu, 2011).

ISO20000 describe un conjunto integrado de procesos que permiten prestar en forma eficaz servicios de TI a las organizaciones y a sus clientes. La esperada publicación de la ISO 20000 el 15 de diciembre de 2005 representa un gran paso adelante hacia el reconocimiento internacional y el desarrollo de la certificación de ITSM.

Actualmente, la aparición de la norma ISO 20000 está causando un aumento considerable del interés en aquellas organizaciones interesadas en implementar ITSM. Estudios revelan como dicho anhelo crecerá internacionalmente tomando como base la reconocida certificación ISO 20000.

ISO-27000

Es un conjunto de estándares desarrollados por ISO, el cual proporciona un marco de gestión por la seguridad de la información que se puede utilizar por cualquier tipo de organización, ya sea esta pública o privada.

La norma ISO 27001, al igual que su antecesora BS 7799-2, es certificable; es decir, empresas pueden contar con un documento certificatorio de la aplicación de esta norma lo que se produce tras una auditoría y la presentación de documentación sustentatoria de la aplicación.

> "El número de certificaciones ha aumentado considerablemente en los últimos años como demostración de la relevancia que tiene la protección de la información para el desarrollo de las actividades de las organizaciones y para mantener y desarrollar el tejido industrial de los diferentes países y en todo el mundo" (ISO 27000.es, 2013).

2.3.1.2 ISO/IEC-38500

Esta norma fue creada en Junio de 2008, basándose en la norma australiana AS8015:2005. Su objetivo es el de proporcionar un marco de principios para que la dirección de las organizaciones los usen al evaluar, dirigir y monitorear el uso de las TI.

La norma se emplea al gobierno de los procesos de gestión de las TI en todo tipo de empresas que utilicen las tecnologías de la información, proporcionando unas bases para la evaluación objetiva del gobierno de TI.

Entre los beneficios de un buen gobierno de TI estaría la conformidad de la organización con:

- los estándares de seguridad
- legislación de privacidad
- legislación sobre el spam
- legislación sobre prácticas comerciales
- derechos de propiedad intelectual, incluyendo acuerdos de licencia de software
- regulación medioambiental
- normativa de seguridad y salud laboral
- legislación sobre accesibilidad
- estándares de responsabilidad social

Además la búsqueda de un buen rendimiento de la TI mediante:

- apropiada implementación y operación de los activos de TI
- clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización
- continuidad y sostenibilidad del negocio

- alineamiento de las TI's con las necesidades del negocio
- asignación eficiente de los recursos
- innovación en servicios, mercados y negocios
- buenas prácticas en las relaciones con los interesados
- reducción de costes
- materialización efectiva de los beneficios esperados de cada inversión en TI

2.3.1.3 Manual de Operaciones y Funciones (MOF)

El manual de operaciones y funciones es un documento que las empresas llevan a cabo para implementar parte de la forma de la organización que han adoptado, y que sirve como guía para todo el personal.

El MOF contiene la estructura organizacional, la cual es llamada comúnmente organigrama y la descripción de cada puesto el perfil y los indicadores de evaluación.

Para llevar a cabo la elaboración de un MOF se debe tener en cuenta los siguientes puntos.

- La participación y compromiso de toda la organización, especialmente de los líderes como promotores.
- Que los líderes que toman las decisiones separen unas horas para las decisiones referentes a estos temas.
- Formar un equipo técnico que lidere el proceso. Puede ser interno como externo.
- Que la organización tenga su plan estratégico vigente, pues sin esto no se podrá realizar el MOF
- Que el equipo técnico use una metodología para la elaboración del cronograma y para que el plan estratégico se refleje en las funciones.

- Hacer un plan de implantación de este manual. especialmente con los cambios fuertes.
- Poner el manual a plena disponibilidad del personal. Por ejemplo, colgarlo en la intranet institucional.

2.4 GESTIÓN DE RIESGOS DE TI

La gestión de riesgos es la actividad que permite a la empresa ser consciente de las vulnerabilidades que tienen sus componentes (entendiéndose como tales a componentes físicos y digitales), y, por ende, las amenazas que esas vulnerabilidades pueden acarrear. De esta manera, la organización puede planificar contramedidas y aclarar responsabilidades en caso de amenaza.

"Existen múltiples metodologías de gestión de riesgos como Magerit, ISO 27005, Octave o Mehari" (González, 2012), que ya han sido descritos previamente.

En general, la metodología de gestión de riesgos consta de los siguientes pasos:

- Identificación de los riesgos
- Evaluación
- Decisión sobre alternativas óptimas
- Control de resultados (González, 2012)

2.5 CONCLUSIONES PARCIALES DEL CAPÍTULO

Tras la exposición de la fundamentación teórica, resaltan los siguientes elementos:

- Las tecnologías de la información y comunicación forman una parte de gran importancia en la vida actual por ser parte extendida en actividades sociales, académicas, económicas y profesionales.
- Los elementos de las tecnologías de la información se pueden dividir como hardware, software, redes y protocolos de información; y, bases de datos.
- La gestión de riesgos de TI permite a una empresa conocer sus vulnerabilidades que pueden convertirse en amenazas; sirve para identificar y evaluar el riesgo, determinar la alternativa óptima de solución y realizar controles de resultados.
- Existen varios criterios o normas de gestión de riesgos de TI como ISO-27000, ISO/IEC-38500, MOF, entre otros, que ofrecen lineamientos para evitar amenazas en los componentes de TI.

CAPÍTULO III

ANÁLISIS EN EL DOMINIO DEL PROBLEMA

3.1 IDENTIFICACIÓN Y ANÁLISIS DEL PROBLEMA

Roche Ecuador S.A. es una empresa farmacéutica multinacional de origen suizo que se dedica a la investigación y el desarrollo. En el Ecuador, la empresa cuenta con una presencia de 30 años y tiene oficinas en las ciudades de Quito y Guayaquil. En Roche Ecuador S.A. laboran cerca de 300 empleados en diferentes áreas.

Además de la importancia de las actividades de la empresa, se presenta el manejo de información sensible y confidencial, lo que hace necesario contar con un plan de Gestión de Riesgos para los sistemas de tecnología de información basado en los estándares de gestión de seguridad, con el fin de lograr la detección, identificación, mitigación y control de los factores de riesgo que atenten contra la integridad de la información, equipos tecnológicos y la normal operación de Roche Ecuador S. A.

Al no contar con el Plan de Gestión de Riesgos para el Área de TI, se han identificado 4 grupos claros como componentes de este problema los cuales son Hardware, Software, las Redes e Interconexión y las Bases de Datos. Los componentes mencionados se relacionan con el problema como se detalla a continuación:

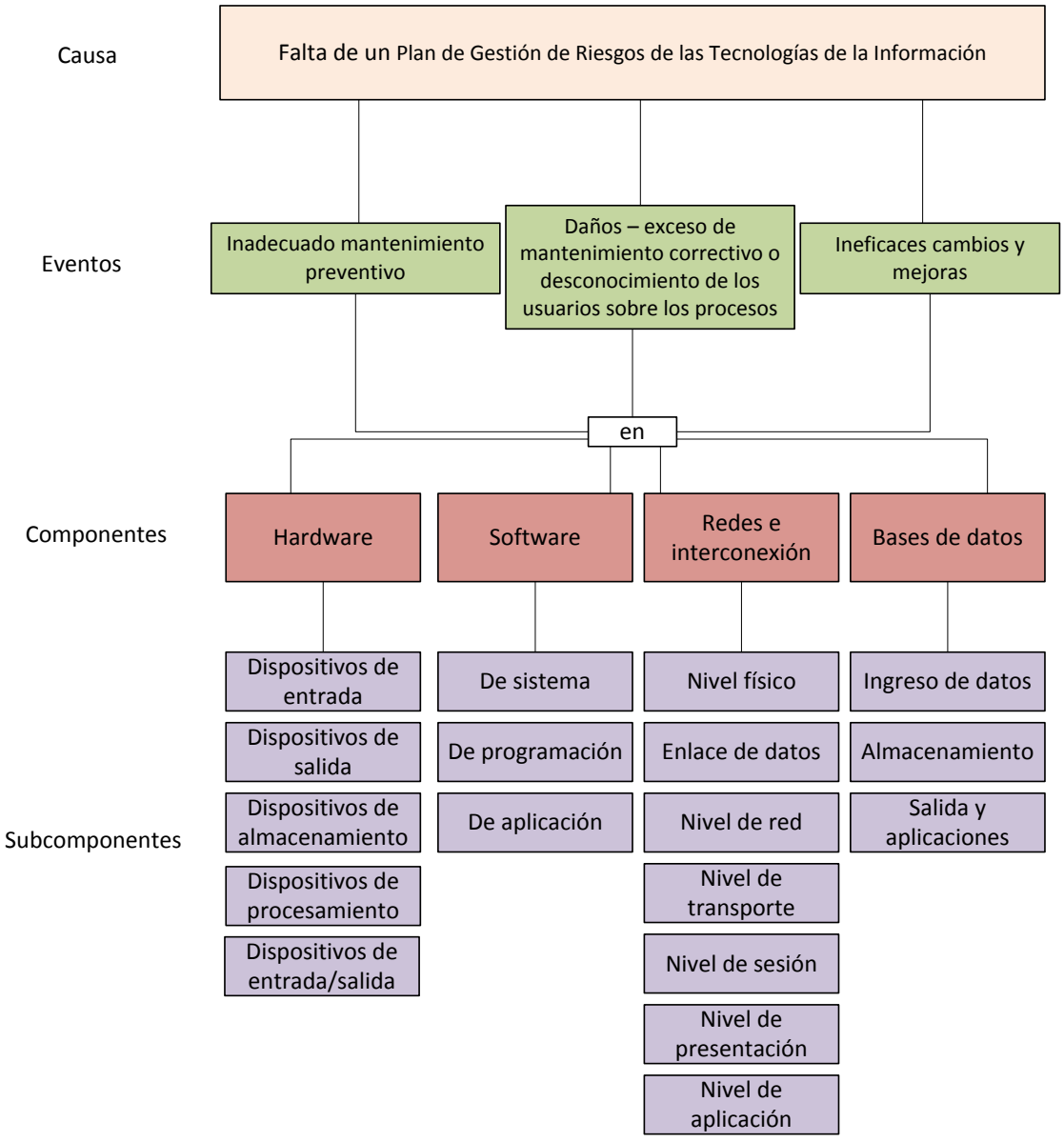


Figura 1. Modelo del problema

El objetivo de la presente investigación es determinar los riesgos y reducirlos o eliminarlos a través de estrategias adecuadas a las operaciones y características propias de la empresa.

3.1.1 Elementos del dominio de problema

Los elementos del dominio del problema se presentan a continuación, así como las técnicas e instrumentos de recolección de datos:

Tabla 1. Análisis de los elementos del dominio del problema

Elementos	Fuentes	Técnicas	Instrumentos
Asesoramiento experto	Asesor de trabajo Experto en TI de la empresa estudiada	Entrevista no estructurada Entrevista estructurada	Cuaderno de notas Guion de entrevista
Investigación documental y de campo	Empresa estudiada	Observación directa Estudio documental	Guía de observación Fichas de recolección de datos
Marco referencial	Bibliográficas y estadísticas	Análisis biblioFigura	Fichas bibliográficas y mnemotécnicas
Análisis de involucrados	Empleados del área de TI de Roche Proveedores Externos y Entidades de Control	Entrevista estructurada Regulación, SLA’s	Guion de entrevista Contratos

3.3.2 Características del problema

El problema a estudiar presenta los siguientes componentes y eventos:

Tabla 2. Eventos de riesgo de los componentes

Componente	Eventos
Hardware	Inadecuado mantenimiento preventivo
	Daños – exceso de mantenimiento correctivo o desconocimiento de los usuarios sobre los procesos
	Ineficaces cambios y mejoras
Software	Inadecuado mantenimiento preventivo
	Daños – exceso de mantenimiento correctivo o desconocimiento de los usuarios sobre los procesos
	Ineficaces cambios y mejoras
Redes y protocolos	Inadecuado mantenimiento preventivo
	Daños – exceso de mantenimiento correctivo o desconocimiento de los usuarios sobre los procesos
	Ineficaces cambios y mejoras
Bases de datos	Inadecuado mantenimiento preventivo
	Daños – exceso de mantenimiento correctivo o desconocimiento de los usuarios sobre los procesos
	Ineficaces cambios y mejoras

De manera general, se han identificado como eventos riesgosos en todos los componentes el inadecuado mantenimiento preventivo, los daños provocados por falta de conocimiento en el uso de los componentes y fallas en las acciones de cambios y mejoras que pueden retrasar las operaciones. En base al análisis de los riesgos señalados, se analizarán y evaluarán las estrategias a ser implementadas.

3.3.3 Atributos de los componentes del problema

Los componentes del Dominio del Problema se definen de la siguiente manera:

Tabla 3. Análisis del componente: Hardware

Componente:	**Hardware**				
Atributo:	Componentes físicos o tangibles que componen el sistema informático				
Clases:	Dispositivos de entrada	Dispositivos de salida	Dispositivos de almacenamiento	Dispositivos de procesamiento	Dispositivos de entrada / salida (mixtos)
Objetos:	Teclado Ratón Escáner Micrófono Cámara web Lector de CD o DVD Lector de códigos	Monitor Impresora Parlante Grabador de CD o DVD	Disco duro Discos portátiles Pendrives Memorias flash	Unidad central de procesamiento Unidades de procesamiento de Figuras	Pantalla táctil Micrófono con audífonos Impresoras multifunción

Fuente: Investigación propia

Elaborado por: Jorge Burgos

El cuadro anterior define el hardware como el conjunto de elementos físicos de un sistema tecnológico y señala sus clases: los dispositivos de entrada permiten el ingreso de información, los de salida son aquellos que retornan información al usuario, los dispositivos de almacenamiento permiten guardar información de manera digital, los dispositivos de procesamiento permiten el funcionamiento interno de la máquina y, finalmente, los dispositivos mixtos permiten el ingreso y arrojan información al usuario. De esta manera se presentan algunos ejemplos de este componente para una mayor comprensión del mismo.

Tabla 4. Análisis del componente: Software

Componente:	**Software**		
Atributo:	Equipamiento lógico o componente digital de un sistema informático		
Clases:	Software de sistema	Software de programación	Software de aplicación
Objetos:	Sistemas operativos Controladores de dispositivos Herramientas de diagnóstico Herramientas de Corrección y Optimización Servidores Utilidades	Editores de texto Compiladores Intérpretes Enlazadores Depuradores	Aplicaciones para Control de sistemas y automatización industrial Aplicaciones ofimáticas Software educativo Software empresarial Bases de datos Telecomunicaciones (por ejemplo Internet y toda su estructura lógica)

Fuente: Investigación propia

Elaborado por: Jorge Burgos

La tabla anterior muestra la definición general de software y se divide al mismo en software de sistema que permite el uso del mecanismo y sus funciones, software de programación que permiten el desarrollo de aplicaciones y el software de aplicación que es el sistema computacional que permite la ejecución de actividades específicas.

Tabla 5. Análisis del componente: Redes e interconexión

Componente:	**Redes e interconexión**						
Atributo:	Conjunto de elementos, reglas y normas que permiten que dos o más entidades de un sistema informático se comuniquen entre ellos para transmitir información						
Clases:	Nivel físico	Nivel de enlace de datos	Nivel de red	Nivel de transporte	Nivel de sesión	Nivel de presentación	Nivel de aplicación
Objetos:	Conectores eléctricos y cables Línea de transmisión Frecuencia, ancho de banda	Direccionamiento MAC LLC	Datagramas Circuitos virtuales	Direccionamiento Establecimiento de una conexión Liberación de una conexión Control de Flujo almacenamiento en buffer Multiplexión Recuperación de caídas	Control del diálogo Agrupamiento Recuperación	Formateo de datos Cifrado de datos Compresión de datos	Protocolos Servicios

Las redes permiten la transmisión de información de un dispositivo a otro. La tabla anterior muestra los diferentes niveles de transmisión y objetos que los incluyen.

Tabla 6. Análisis de componentes: Base de datos

Componente:	**Base de datos**		
Atributo:	conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso		
Clases:	Ingreso	Almacenamiento	Salida
Objetos:	Hardware Software	Hardware Software	Hardware Software

En la tabla anterior se muestra la definición de base de datos y sus clases. Este elemento es de singular importancia en el análisis de los riesgos debido a que las bases de datos suelen contener información sensible que requiere un nivel alto de precaución.

De manera general, las tablas precedentes caracterizan a los componentes del problema que serán tomados en cuenta a lo largo del desarrollo de la presente investigación: hardware, software, redes y bases de datos.

3.3.4 Involucrados

Los componentes descritos se interrelacionan a su vez entre varios involucrados, llamados también actores, a los cuales es posible discriminarlos como actores internos y actores externos, según el siguiente esquema basado en la estructura organizacional de Roche Ecuador S.A.

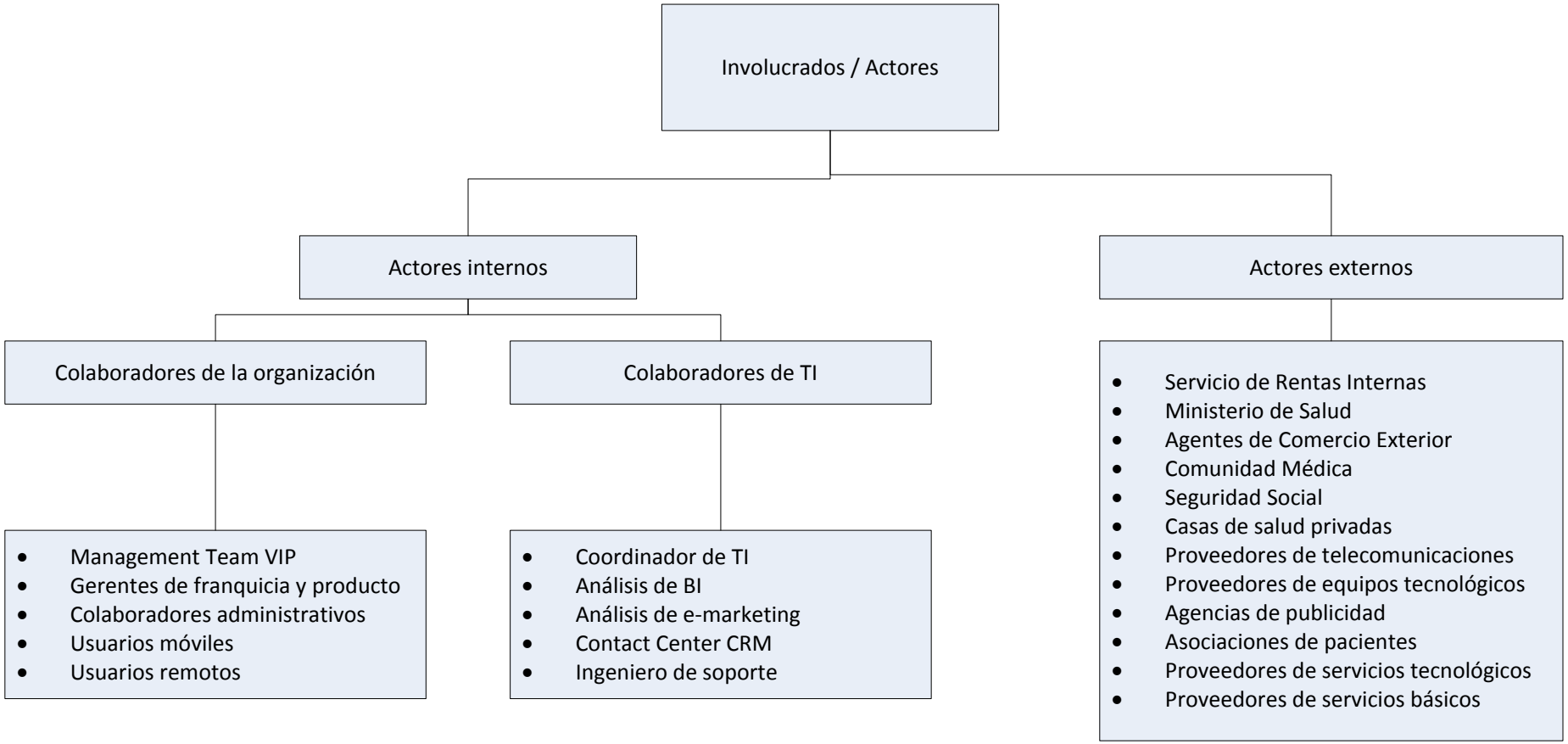


Figura 2. Descripción de actores internos y externos

3.3.5 Comportamiento de los componentes

Los componentes del problema se encuentran en constante manipulación y trabajo por parte de los usuarios y el departamento de IT de Roche; este uso constante da pie a que se produzcan fallos que son atendidos por el departamento especializado, pero que representan un costo para la compañía tanto en tiempo como en recursos.

A lo anterior se suma que información sensible y de gran importancia es manejada a través de los componentes y una pérdida de esta información representa un gran perjuicio para la organización.

La investigación documental y otras técnicas a ser aplicadas ofrecen información acerca de periodicidad de los eventos, niveles de impacto, ponderación del riesgo y otros datos que permiten el diseño de un plan de gestión de riesgos para Roche.

3.2 DESCRIPCIÓN DE LA SITUACIÓN

Como se ha mencionado, en la actualidad, Roche Ecuador S.A. no cuenta con un Plan de Gestión de Riesgos para sus sistemas de TI, por lo que existe un alto nivel de vulnerabilidad ante posibles daños de los componentes, pérdidas de información sensible, ineficiente actualización de los elementos tecnológicos y, a través de lo anterior, una desventaja competitiva sustancial frente a competidores.

Se han determinado cuatro componentes de este problema que son Hardware, Software, las Redes e Interconexión y las Bases de Datos. Todos estos elementos presentan una interacción con el componente humano que hace uso de ellos; sobre todo, el departamento de TI.

Con la finalidad de realizar un primer diagnóstico de la situación investigada, se ha realizado una investigación a través de observación directa y entrevistas no estructuradas a personas pertenecientes a la empresa. A continuación, se presenta una descripción más detallada de la situación actual de la gestión de TI en Roche Ecuador S. A., en base a los componentes señalados:

3.2.1 Hardware

- Los elementos físicos que conforman el sistema de TI de la empresa se encuentran en buenas condiciones, son actualizados y suficientes para los requerimientos actuales de la organización.
- El componente está conformado por dispositivos relativamente nuevos; cumplen con un estándar corporativo y son seleccionados según el perfil de las diferentes áreas de la empresa.
- En el departamento de TI no existe un plan estructurado de mantenimiento preventivo de hardware en la empresa.
- En caso de averías o problemas en general de este componente, el departamento de TI reacciona con mantenimiento correctivo, lo cual hace que se detengan inesperadamente las operaciones que requieren del dispositivo dañado.
- La adquisición de nuevos dispositivos se realizan según las condiciones y necesidades de cada departamento o área en un tiempo determinado. No existe planificación en la renovación de dispositivos o en mejoras.

3.2.2 Software

- Los elementos de este componente responden a las necesidades de cada área. En este sentido se verifica la presencia de software de sistemas y de programación (aplicaciones de oficina) al igual que programas de protección contra virus y otros elementos de riesgo en

todas las computadoras de la empresa y software de aplicación empresarial diseñado por la oficina matriz y que permite la entrada, almacenamiento, procesamiento y salida de información referente a las operaciones, a la gestión financiera y bases de datos de clientes en las computadoras de los respectivos departamentos.

- El componente tiene versiones actualizadas y se ajustan a las necesidades de la empresa.
- Existen políticas claras acerca de la instalación de software adicional en las computadoras; sin embargo, varias de ellas cuentan con aplicaciones y programas descargados que pueden representar un riesgo para la compañía ya que pueden instalar, al momento de su descarga, software malintencionado.
- En el departamento de TI no existe un plan estructurado de mantenimiento preventivo de los programas computacionales.
- En caso de problemas con el software, se procede a realizar mantenimiento correctivo a cargo del departamento de TI (ingeniero de soporte), lo cual hace que se detengan inesperadamente las operaciones, se escalan los problemas al equipo de soporte regional.
- El diseño, instalación, mantenimiento y mejoras de los sistemas informáticos se hace de acuerdo a las necesidades de la empresa. El coordinador de TI organiza y articula estas acciones, basado en las instrucciones recibidas por el equipo de soporte regional.

3.2.3 Redes e interconexión

- Tanto los elementos físicos como los protocolos de comunicación se encuentran en buenas condiciones. Todas las computadoras se encuentran enlazadas en una red corporativa y también tienen acceso a internet.

- En el departamento de TI no existe un plan estructurado de mantenimiento preventivo de redes e interconexión de la empresa.
- En caso de averías o problemas en general de este componente, el departamento de TI reacciona con mantenimiento correctivo, lo cual hace que se detengan inesperadamente las operaciones, ya que debe recurrir al proveedor de servicios de telecomunicaciones.
- Existen políticas claras acerca de la interconexión de las computadoras de cada usuario.
- El mejoramiento o cualquier cambio que se requiere dentro del componente de redes e interconexión de la compañía es realizado por el departamento de TI. No existe planificación en las mejoras o cambios, se lo realiza en base a las instrucciones del equipo de soporte regional.

3.2.4 Bases de datos

- La compañía realiza acciones de entrada, almacenamiento, procesamiento y salida de grandes cantidades de datos referentes a los siguientes procesos: operaciones, financieros, administración, recursos humanos, contabilidad y clientes.
- El almacenamiento se realiza en el servidor de la empresa y se realizan respaldos con frecuencia. No obstante, no existe planificación para el mantenimiento y depuración de las bases de datos.
- En caso de problemas en general de este componente, el departamento de TI reacciona con mantenimiento correctivo, lo cual hace que se detengan inesperadamente las operaciones.
- El mejoramiento o cualquier cambio que se requiere dentro de las bases de datos de la compañía es realizado por el departamento de TI. No existe planificación en las mejoras o cambios.

3.2.5 Usuarios y departamento de TI

- Los usuarios tienen cierto nivel de experiencia en el uso de los componentes físicos a su cargo.
- Algunos de los actores internos, especialmente aquellos que usan software de programación de oficina (procesamiento de textos, hojas de cálculo), tienen algunas deficiencias en el uso del software.
- Existe desconocimiento de políticas relativas a interconexión y uso general de sistemas de TI implementadas en Roche Ecuador S. A.
- En presencia de problemas en alguno de los componentes, muchas veces los usuarios no saben cómo actuar. Si el problema no impide el desenvolvimiento de sus actividades, no lo comunican al departamento de TI de inmediato.
- El departamento de TI está conformado por: un coordinador de TI, un analista de BI, un analista de e-marketing, el contact center de la empresa y un ingeniero en sistemas que da soporte al departamento.
- La estructura organizativa del departamento atiende adecuadamente a las necesidades actuales de la empresa por lo que se considera que no se requiere de incremento de personal o reorganización del departamento.

De manera general, se verifican los siguientes problemas para todos los componentes del problema estudiado: a) falta de planeación de mantenimiento preventivo; b) exceso de ocurrencia de mantenimiento correctivo; c) mejoras y cambios en los componentes de manera no planificada; y, d) desconocimiento de las políticas de TI de la organización.

3.3 ANÁLISIS DE LOS INVOLUCRADOS

3.3.1 Interacciones de los componentes y los actores identificados

Los actores identificados para la implementación de una solución al problema son:

Usuarios y administrativos: Talento humano que trabaja en Roche Ecuador S. A. que laboran en las instalaciones de la compañía y que hacen uso de los componentes. Los niveles administrativos de la empresa también se encuentran ubicados en esta categoría.

Departamento de TI: Área de la compañía que está encargada de la gestión y desarrollo de las tecnologías de la comunicación y, por ende, de los componentes del dominio del problema. Sirven como elemento de intermediación entre los usuarios internos y los componentes.

Actores externos: diferentes personas naturales y jurídicas que se relacionan con la compañía debido a sus operaciones. La relación entre los actores internos y externos se da debido a las actividades propias de la compañía y de cada uno de los actores externos. Como actores externos de más importancia destacan los clientes de la empresa.

Los actores descritos y su relación con los componentes identificados, se exponen gráficamente en función de lograr un mejor entendimiento.

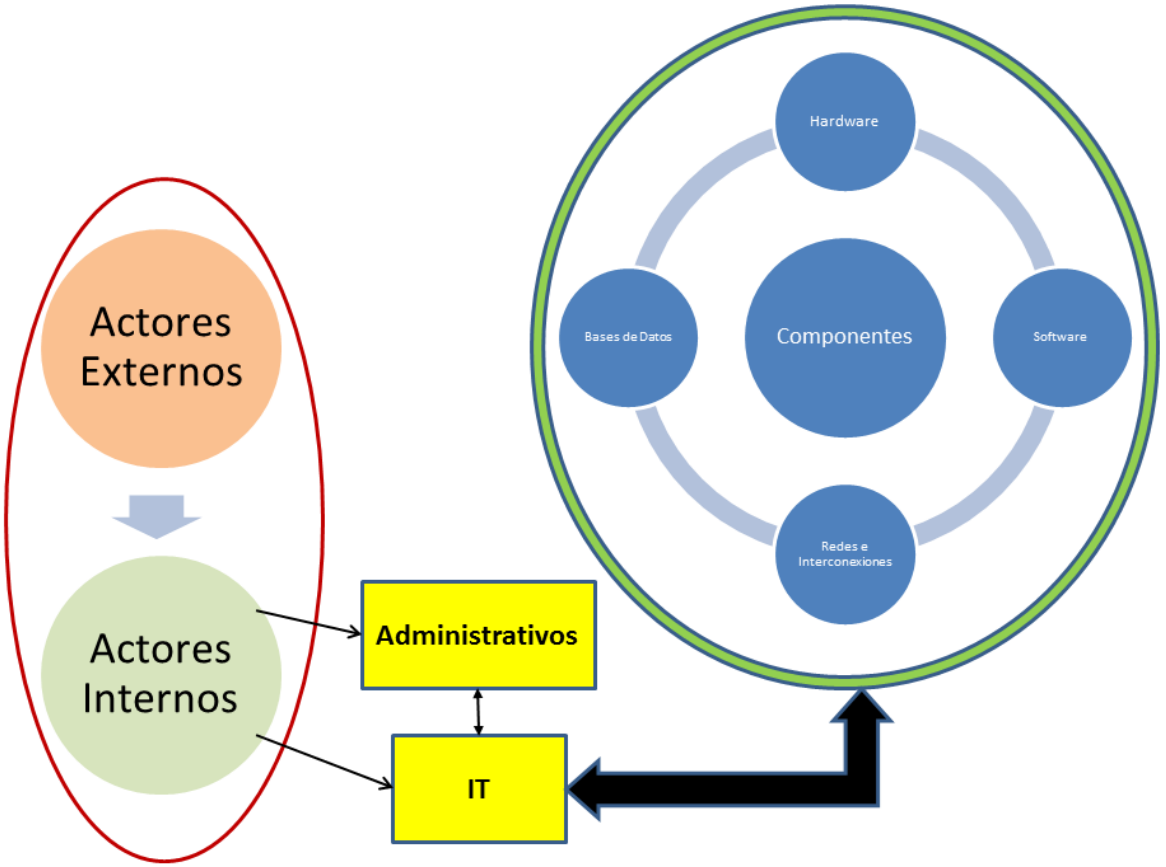


Figura 3. Interacción entre componentes y actores

Los actores, su relación con el problema y sus intereses se presentan en la siguiente matriz de análisis de involucrados:

Tabla 7. Matriz de análisis de involucrados

	Involucrados	Roles	Intereses	Posición	Capacidad de acción	Poder relativo
Beneficiarios directos	Administrativos	Aprobación de propuesta y plan Orden de implantación de cambios en plan Aprobación de adquisiciones Uso de componentes (apoyar las políticas de TI)	Cumplir los objetivos estratégicos de la compañía.	Gerencial – Administrativa	Media	Alto
	Usuarios	Uso de los componentes (apoyar las políticas de TI)	Realizar las operaciones a su cargo	Operativa	Media	Bajo
	Departamento de TI	Planeación de TI Gestión de riesgos de TI Adquisición, instalación, uso mantenimiento y cambios o mejoras de componentes.	Acciones de desarrollo, mantenimiento y mejora de TI para apoyar los objetivos de la empresa	Técnica - operativa	Alta	Alto
Beneficiarios indirectos	Clientes	Adquisición de productos de ROCHE	Recibir productos y servicios de calidad a precios adecuados	Evaluativa	Baja	Bajo
	Accionistas	Inversión de capitales Supervisión general de operaciones (a través de Junta General)	Incrementar las ganancias de la compañía	Directiva	Baja	Medio
Interesados	Proponente	Analizar y determinar el problema. Plantear soluciones alternativas Elegir la alternativa óptima Proponer soluciones	Identificar el problema y plantear la solución óptima	Técnica	Alta	Medio

Como se puede observar en la matriz presentada, la solución presenta una cantidad significativa de beneficiarios directos e indirectos entre los que se encuentran los clientes y accionistas, hacia quienes se deben las decisiones administrativas de toda empresa.

3.4 ÁRBOL DE PROBLEMAS

A través de la investigación se ha determinado la presencia de varios problemas en el uso de los componentes por parte de los usuarios que desconocen cómo dar un buen trato a los mismos y las normas y políticas de uso de dichos componentes. A lo anterior se suma que hay un inadecuado plan de mantenimiento preventivo. Los elementos señalados implican que se incremente sustancialmente la frecuencia de las acciones de mantenimiento correctivo. Adicionalmente se ha verificado que se procede a la implementación de cambios y mejoras de manera desordenada, sin contar con un plan adecuado de estas actividades.

Los problemas señalados implican un inadecuado Plan de Gestión de Riesgos de Información y comunicación que puede producir la presencia de software malintencionado, comunicación tardía de los problemas, desactualización de los componentes, daños y, en última instancia, paralización de las operaciones.

Con el fin de señalar los efectos producidos por los problemas determinados en la descripción anterior, se presenta esta relación en el siguiente Figura de causas – efectos:

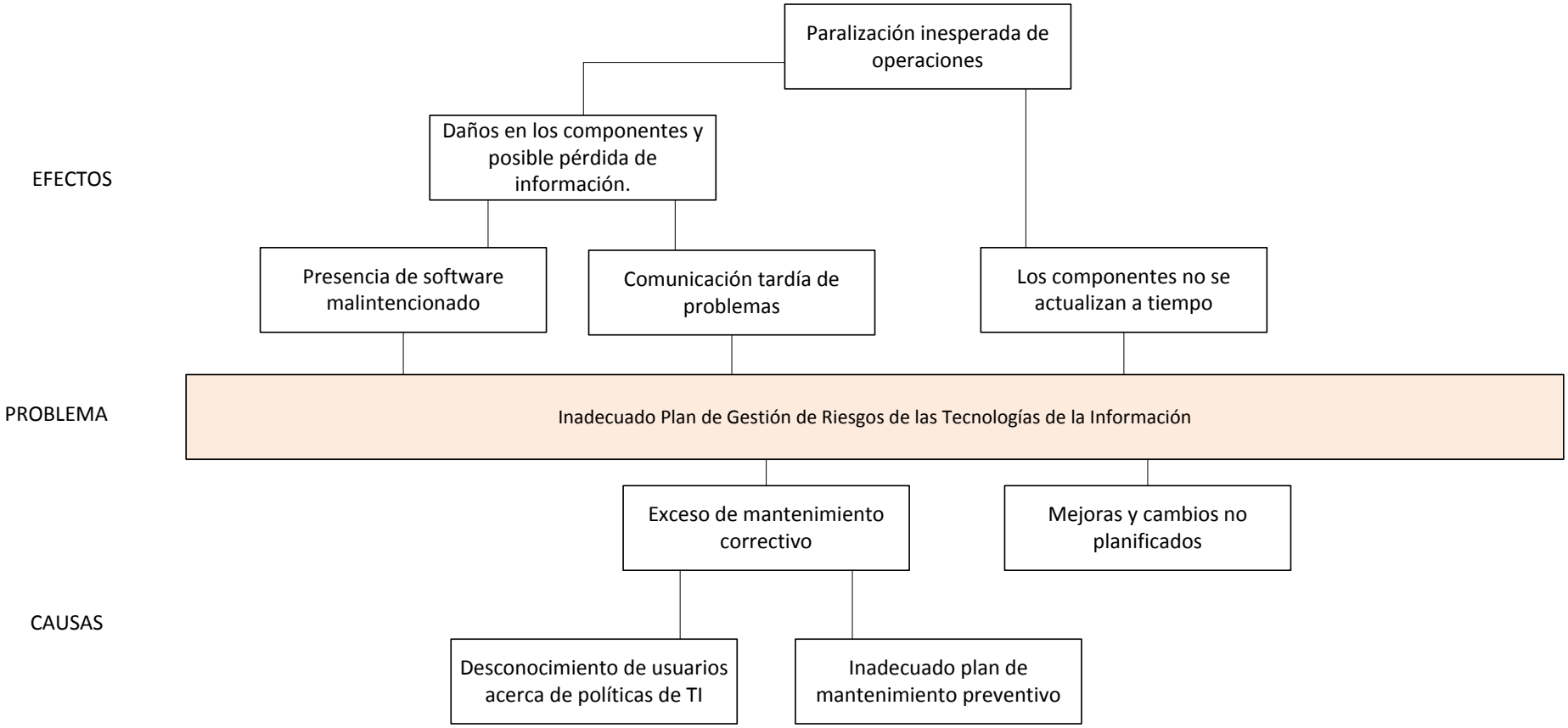


Figura 4. Árbol de problemas

3.5 CONCLUSIONES PARCIALES DEL CAPÍTULO

Durante el desarrollo del presente capítulo, se han logrado determinar las siguientes conclusiones:

- Las principales vulnerabilidades que se han identificado son desconocimiento de los usuarios acerca del uso de componentes y políticas de TI; inadecuado mantenimiento preventivo, paralización de operaciones por mantenimiento correctivo; y, cambios y mejoras de manera desordenada.
- Las causas indicadas han provocado que exista software malintencionado, comunicación lenta para informar acerca de problemas, desactualización de los componentes, daños en los componentes que provocan pérdida de información valiosa para la empresa y, de manera general, paralizaciones inesperadas de las operaciones.

CAPÍTULO IV

INTEGRACIÓN SISTÉMICA PROBLEMA - SOLUCIÓN

4.1 ÁRBOL DE OBJETIVOS

Dentro del sistema de gestión de riesgos de TI propuesto y en base al árbol de problemas definido para el presente estudio, se ha determinado que es imprescindible que los usuarios conozcan normas y políticas de uso de los componentes para evitar la necesidad de mantenimiento correctivo y el aumento de la vida útil de los equipos y software. De manera adicional, se debe implementar un plan de mantenimiento preventivo para permitir el mejor flujo de las actividades sin la necesidad de paralizaciones por mantenimiento correctivo inesperado. Finalmente, la implementación de un plan de cambios y mejoras permitirá una permanente actualización de los componentes con la correspondiente mejora de la eficiencia de las acciones.

Los efectos previstos al implementar las acciones anotadas son la implementación de un adecuado Plan de Gestión de Riesgos de Información y Comunicación que permitirá que se reduzca el riesgo de tener software malintencionado, además de una comunicación pronta de los problemas, para reducir los costos atados a las acciones de mantenimiento correctivo.

Según lo descrito en los párrafos anteriores, se propone el siguiente árbol de objetivos.

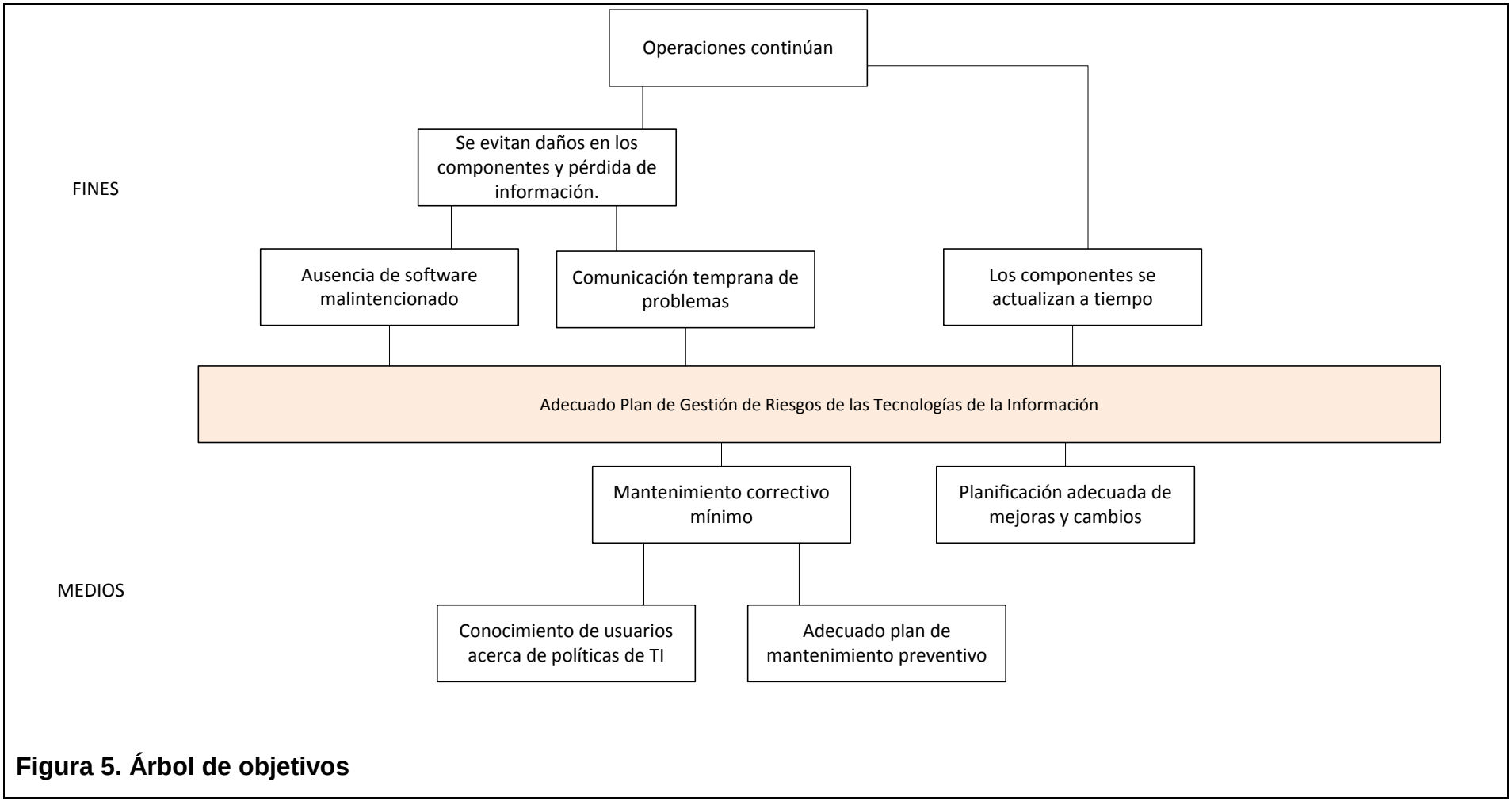


Figura 5. Árbol de objetivos

4.2 IDENTIFICAR ALTERNATIVAS DE SOLUCIÓN

Conforme a lo establecido en el árbol de objetivos, se pueden identificar las siguientes alternativas de solución:

1) Conocimiento de usuarios acerca de políticas de TI

Alternativas: a) Publicación de políticas de TI de ROCHE y difusión entre usuarios.

b) Programa de capacitación a usuarios, de parte de miembros del departamento de TI.

De entre las dos alternativas, se escoge la opción b. Esto debido a que de esta manera se garantiza el nivel de comprensión de los usuarios y se los compromete a que participen en el mantenimiento prospectivo, lo que reduce la necesidad de mantenimientos correctivos.

2) Adecuado plan de mantenimiento preventivo de TI

Alternativas: a) Contratar servicio externo que realice una auditoría de TI y genere recomendaciones de cambio en el plan de mantenimiento preventivo actual.

b) Replantear el plan actual de mantenimiento preventivo por parte del departamento de TI de la empresa.

Como alternativa óptima, se elige a la segunda opción debido a que esto permite el pleno empleo de los recursos existentes en la organización y, aún más importante, se considera que los

miembros del departamento de TI de ROCHE ya conocen con profundidad los problemas y limitaciones del actual plan, por lo que se reducirían los costos en estas acciones, en comparación con la externalización.

3) Mantenimiento correctivo mínimo

Alternativas: a) Mantenimiento correctivo por parte de los miembros de la oficina de TI de ROCHE.

b) Contratación de servicio profesional externo para realizar mantenimiento correctivo.

Se selecciona a la primera opción como la alternativa óptima, ya que el departamento de TI tiene todos los recursos necesarios, tanto humanos como materiales, para realizar las acciones de mantenimiento correctivo y la contratación de un servicio externo implicaría un gasto adicional innecesario.

4) Planificación de mejoras y cambios

Alternativas: a) Realizar mejoras y cambios solamente según la planificación anual.

b) Implementar cambios y mejoras conforme se requieran en la empresa.

Se selecciona la opción b como alternativa óptima, debido a que muchos de los cambios y mejoras son imprescindibles para la normal operación de la empresa. Sin embargo, se especifica que cuando se detecte la necesidad de un cambio o mejora, deberá

planificarse la fecha, tiempo de trabajo y otras especificaciones para reducir la paralización de operaciones al mínimo.

4.3 SELECCIÓN DE LA ALTERNATIVA ÓPTIMA

Según las alternativas seleccionadas en el acápite anterior, se consideran tres alternativas de solución:

1. Desarrollar un plan anual de mantenimiento preventivo para todos los componentes: Esta alternativa puede beneficiar a la compañía al solucionar los problemas de falta de plan de mantenimiento preventivo; exceso de mantenimiento correctivo; y, mejoras y cambios no planificados.

2. Elaborar un plan de gestión de riesgos de TI integral: Esta alternativa busca solucionar los problemas de Falta de plan de mantenimiento preventivo; exceso de mantenimiento correctivo; mejoras y cambios no planificados; y la falta de conocimiento de usuarios sobre políticas de TI.

3. Involucrar a los usuarios para hacer más eficiente el mantenimiento correctivo: Esta última alternativa permitiría la solución de los problemas de exceso de mantenimiento correctivo y la falta de conocimiento de los usuarios.

Una descripción gráfica de las alternativas planteadas se encuentra en el anexo 1 al final del presente trabajo.

4.3.1 Evaluación de las ideas

A continuación, se explicarán las principales ventajas y desventajas de la aplicación de cada una de las ideas de solución planteadas:

- **Plan anual de mantenimiento preventivo:**

- **Ventajas:**
  - Fácil aplicación y coordinación
  - Costos bajos
  - Reduce la ocurrencia de mantenimiento correctivo y, por ende, las paralizaciones inesperadas
  - Permite a los miembros del departamento de TI tener mejor conocimiento de la situación de los componentes y aplicar mejoras o cambios a tiempo , con lo que se logra mayor eficiencia
  - Aumenta la eficiencia de la compañía
- **Desventajas:**
  - Si se realiza con demasiada frecuencia, implicaría paralizaciones por más tiempo que en el mantenimiento correctivo
  - El plan de mantenimiento preventivo no implica el involucramiento de los usuarios en el proceso.

- **Plan integral de gestión de riesgos de TI:**
  - **Ventajas:**
    - Genera soluciones para todos los componentes del problema
    - Desarrolla ventaja competitiva para la empresa
    - Proporciona políticas claras a ser observadas por todos los actores internos (usuarios de TI)
    - Permite el involucramiento de los usuarios, lo que genera motivación y una revisión constante de los componentes
  - **Desventajas:**
    - Costos elevados de implementación
    - Requiere de tiempo y recursos para su difusión en toda la compañía

- **Involucramiento de los usuarios:**
  - **Ventajas:**
    - Hace más efectivo el mantenimiento correctivo ya que no requiere esperar hasta el último momento y una paralización más larga

        - La participación de los usuarios permite que se sientan más motivados al hacérseles notar que son importantes para el desarrollo de la solución
        - Su costo de implementación es relativamente bajo
    - **Desventajas:**
        - No atiende a los problemas de falta de mantenimiento preventivo
        - No beneficia a la falta de planificación en mejoras y cambios de los componentes

Con base en las tres ideas presentadas, se desarrollan las definiciones de sistemas integrados.

4.3.2 Definiciones de los sistemas integrados

4.3.2.1 Definición de sistema integrado 1

Roche Ecuador S. A. presenta problemas en el mantenimiento de sus componentes relacionados a las tecnologías de información que maneja. Estos problemas se traducen en deficiente mantenimiento preventivo que produce daños y mal funcionamiento de hardware, software, redes e interconexión, y bases de datos que deben solucionarse con mantenimientos correctivos al momento en que se producen los problemas; esto deriva en paralización de actividades de manera inesperada y gastos innecesarios de recursos.

Esta situación puede resolverse con la implementación de un plan de mantenimiento preventivo anual desarrollado por el departamento de TI de la empresa. Este plan deberá ser diseñado en base a datos históricos (ocurrencia de problemas en hardware, software, redes y bases de datos), personal disponible, complementos a someter a mantenimiento y requerimientos de la compañía.

El mantenimiento preventivo permitirá extender la vida útil de los componentes, reducir la incidencia de mantenimiento correctivo y mantener una revisión permanente de los componentes con el fin de identificar si se requiere realizar mejoras o cambios.

El costo de implementación se compone aproximadamente de salarios para 5 horas/hombre entre los miembros del departamento de TI para determinar las fechas, horas, departamentos y componentes a mantener, el costo de paralización para las acciones de mantenimiento preventivo y los costos relacionados a la comunicación con los usuarios.

4.3.2.2 Definición de sistema integrado 2

Roche Ecuador S. A. presenta problemas en el mantenimiento de sus componentes relacionados a las tecnologías de información que maneja. Estos problemas se traducen en deficiente mantenimiento preventivo que produce daños y mal funcionamiento de hardware, software, redes e interconexión, y bases de datos que deben solucionarse con mantenimientos correctivos al momento que se producen los problemas; esto deriva en paralización de actividades de manera inesperada y gastos innecesarios de recursos. Adicionalmente, existe un desconocimiento de las políticas de la empresa relativas a sus componentes de TI que provocan que el tiempo de respuesta ante presencia de problemas no sea el adecuado y que sea vulnerable la empresa ante software malintencionado, entre otros riesgos.

Este escenario puede resolverse con el desarrollo de un plan de gestión de riesgos de TI que permita un conocimiento y un orden en las actividades que permitan la identificación, mitigación y el control de los riesgos relativos a TI. Esto ayudará de manera efectiva al mejoramiento de la Organización a través del alineamiento del departamento de TI con los objetivos estratégicos de la Organización.

El plan se desarrollará en base a las normas ISO 27001 y otros elementos que puedan adaptarse a las necesidades de la empresa para la gestión de riesgos de hardware, software, redes y bases de datos. Se tomará en cuenta el personal disponible, complementos a someter a mantenimiento y requerimientos de la compañía.

A través de la aplicación del plan de gestión de riesgos se busca reducir al mínimo la vulnerabilidad de los sistemas de TI de la empresa, extender la vida útil de los componentes y lograr que toda la estructura de TI aporte al logro de los objetivos de la empresa.

El costo de implementación se compondría de salarios para 120 horas/hombre entre los miembros del departamento de TI para ejecución y control de las actividades, costos relativos a la comunicación y capacitación de los usuarios, y los de paralización para las acciones de mantenimiento.

4.3.2.3 Definición de sistema integrado 3

Roche Ecuador S. A. presenta problemas en el mantenimiento de sus componentes relacionados a las tecnologías de información que maneja. Estos problemas se traducen en un ineficiente mantenimiento correctivo, por falta de conocimiento de los usuarios respecto a daños y mal funcionamiento de hardware, software, redes e interconexión, y bases de datos; esto deriva en paralización de actividades de manera inesperada y gastos innecesarios de recursos.

Adicionalmente, el uso de computadoras para actividades diferentes a las relacionadas al trabajo o la descarga de archivos o programas puede ocasionar el ingreso al sistema de la compañía de software malicioso que puede acarrear graves problemas a la empresa.

La comunicación de las políticas de TI a los usuarios (actores internos) permitirá corregir los problemas señalados.

El costo de implementación estaría compuesto por lo relativo al diseño y difusión de políticas claras de TI dirigidas a los usuarios y reuniones para dar a conocer dichas políticas de manera más detallada.

4.3.3 Análisis de las alternativas

Con la finalidad de seleccionar una de las alternativas propuestas para solucionar los problemas analizados en Roche Ecuador S. A., se realiza una matriz de ponderación, que toma como elementos de análisis los tres parámetros:

- Tiempo: con un valor de ponderación de 0,2 y cinco niveles de selección, siendo 1 un tiempo alto y 5 un tiempo bajo.
- Uso de recursos: que se refiere tanto a trabajo como a recursos materiales, tiene un valor de ponderación de 0,3 y cinco niveles de selección, con 1 como uso alto de recursos y 5 uso bajo.
- Solución de los problemas: tiene un valor de ponderación de 0,5 y con cinco niveles de selección, 1 para atención baja a los problemas y 5 para atención alta.

Con estos criterios, se seleccionará la opción que ofrezca mayor valor ponderado. La **matriz de ponderación** se presenta a continuación:

Tabla 8. Matriz de ponderación

Opción	Tiempo (0,2)	Uso recursos (0,3)	Solución de problemas (0,5)	Valor ponderado	Desviación estándar
Factor de Ponderacion	**0,2**	**0,3**	**0,5**		
Sistema integrado 1	1	1,2	1	3,2	0,09
Sistema integrado 2	0,6	0,6	2,5	3,7	0,90
Sistema integrado 3	0,8	0,9	1,5	3,2	0,31
Promedios				3,4	0,43

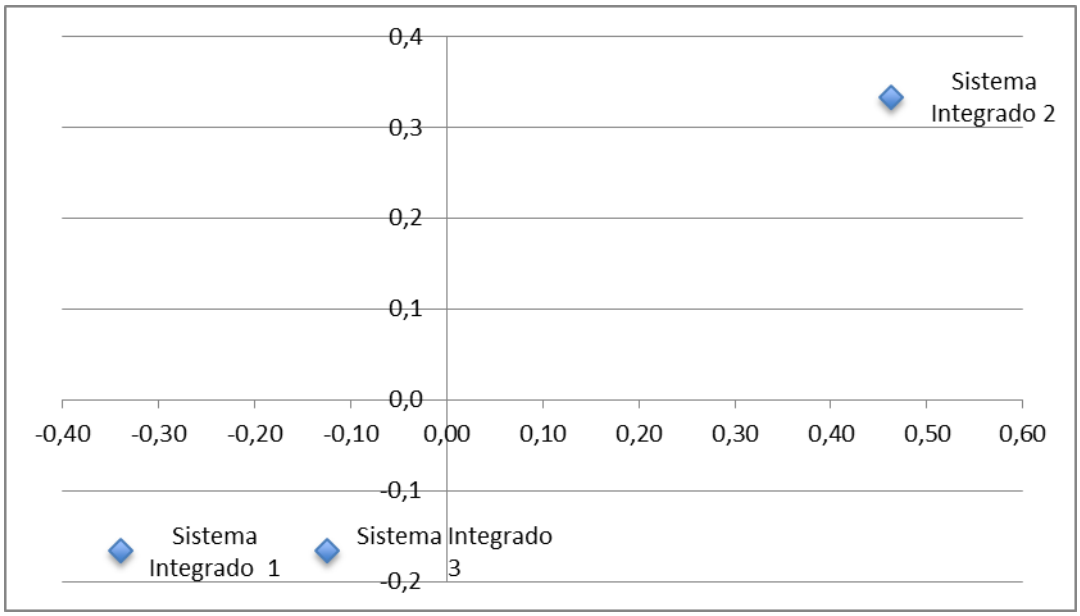


Figura 6. Figura de dispersión

A pesar de que el sistema integrado 2 requiere de una inversión mayor tanto en tiempo como en recursos (por lo que tiene bajas calificaciones ponderadas en esos criterios), el elemento de mayor peso es la capacidad de solucionar el problema descrito dentro de Roche Ecuador S. A.

Por lo fundamentado en el presente análisis, se selecciona el sistema integrado 2 para ser aplicado para la solución del problema de la empresa.

4.4 CONCLUSIONES PARCIALES DEL CAPÍTULO

En el presente capítulo se ha tratado la integración sistémica con el fin de determinar la alternativa más adecuada de solución al problema identificado. Las conclusiones más importantes a las que se ha llegado son:

- Se han identificado como posibles soluciones para el problema de la empresa Roche Ecuador S. A. la planificación de mantenimiento preventivo y de cambios y mejoras, la implementación de un modelo de gestión de riesgos; y la capacitación de los usuarios.
- Tras un proceso de evaluación, se ha establecido que la alternativa óptima de solución para los problemas señalados es la implementación de un modelo general de gestión de riesgos de TI.

CAPÍTULO V

ANÁLISIS DEL DOMINIO DE LA SOLUCIÓN

5.1 USOS DEL SISTEMA

Tal como se describió, el sistema a ser implementado como para dar solución al problema estudiado es un plan de gestión de riesgos para IT dentro de Roche Ecuador S.A.

En primera instancia, es necesario aclarar que determinar el uso del sistema sirve para “determinar la forma en que los actores interactúan con la solución” (Banda, 2013); es decir, señalar la forma en que los usuarios de todos los departamentos de la empresa y los miembros del departamento de IT dan uso a los elementos señalados dentro del dominio del problema. Según lo descrito, los usos del sistema serán los siguientes:

Tabla 9. Usos de mantenimiento preventivo

Uso:	Aplicación de mantenimiento preventivo
Usuarios:	Actores internos administrativos Actores internos IT
Componentes:	Hardware Software Redes e interconexión Bases de datos
Descripción:	El mantenimiento preventivo se realizará mediante una adecuada planificación que incluirá objetivos, acciones, cronograma de actividades y responsabilidades. Para la implementación del plan de mantenimiento preventivo, se requerirá la participación de los actores internos administrativos en dos niveles: por una parte, acomodar sus actividades para que las acciones de mantenimiento preventivo no interfieran con su trabajo; y, por otra parte, conocer elementos básicos de vulneración y errores en los componentes y líneas de comunicación con el departamento de IT para desarrollar acciones de mantenimiento preventivo antes de que los componentes sufran problemas más graves.

Tabla 10. Usos de reducción de mantenimiento correctivo

Uso:	Reducción de mantenimiento correctivo
Usuarios:	Actores internos administrativos Actores internos IT
Componentes:	Hardware Software Redes e interconexión Bases de datos
Descripción:	El uso del sistema para la reducción de mantenimiento correctivo trabaja en dos formas: reducción de ocurrencia de mantenimiento correctivo y reducción de tiempo de mantenimiento correctivo. Con el fin de reducir la ocurrencia de mantenimiento correctivo, se fortalecerá el mantenimiento preventivo y la capacitación de los usuarios internos administrativos sobre el buen uso de los componentes. Para reducir el tiempo de mantenimiento correctivo, se socializarán los procesos de comunicación con los miembros de departamento de IT de la compañía para agilitar el proceso y, adicionalmente, se desarrollará un modelo de mantenimiento correctivo para el departamento de IT con el fin de mejorar la eficiencia de las acciones concretas.

Tabla 11. Usos de mejoras y cambios no planificados

Uso:	Mejoras y cambios no planificados
Usuarios:	Actores internos administrativos Actores internos IT
Componentes:	Hardware Software Redes e interconexión Bases de datos
Descripción:	Los actores internos IT, atendiendo a las autoridades y considerando los requerimientos de la empresa, implementarán mejoras y cambios en los componentes. Dichos cambios se realizarán considerando la relación calidad precio y atendiendo a las necesidades reales de tecnología. Posterior a la instalación y programación de los componentes, se realizará una inducción a los usuarios de los componentes instalados y se incluirán en los procesos de mantenimiento preventivo.

Tabla 12. Uso de capacitaciones a usuarios

Uso:	Mejorar el conocimiento de usuarios administrativos sobre políticas de IT
Usuarios:	Actores internos administrativos Actores internos IT
Componentes:	Hardware Software Redes e interconexión Bases de datos
Descripción:	El departamento de IT realizará acciones de capacitación para los usuarios administrativos de ROCHE Ecuador S. A. Dicha capacitación se concentrará, por una parte, en el conocimiento de las políticas de IT de la compañía especialmente para reducir el mantenimiento correctivo; y, por otro lado, capacitación en el uso de los componentes con el fin de optimizar el mantenimiento preventivo.

Otros usos de la implementación del modelo de gestión de riesgos serán:

- Fortalecer el uso responsable de los componentes por parte de los usuarios internos tanto administrativos como de IT.
- Optimizar la comunicación y el tiempo de reacción del departamento regional de IT ubicado en Colombia para atender problemas en los componentes determinados.
- Implementar un proceso de registro de mantenimiento para determinar necesidades de capacitación, mejora de componentes o procesos de mantenimiento preventivo especiales.
- Realizar acciones de inducción tecnológica en nuevas contrataciones de usuarios administrativos.

5.2 FUNCIONES

A continuación, se hace un recuento de las funciones de los usuarios, realizando una breve descripción en caso de funciones complejas:

5.2.1 Usuarios administrativos

Se consideran como usuarios administrativos a todos los usuarios de tecnologías de información y comunicación; es decir, de uno o varios de los componentes del sistema, que no son parte del departamento de IT de la empresa. Las funciones que llevarán a cabo dentro del sistema propuesto son:

- Usar los componentes con el cuidado y la responsabilidad correspondiente.
- Hacer uso de los componentes de manera exclusiva para sus actividades laborales. Está prohibido el uso de componentes para actividades personales que no tengan relación con el trabajo excepto con expresa autorización de autoridades de la empresa.
- Anticipar su trabajo para que las acciones de mantenimiento preventivo no interfieran en sus actividades. Conociendo el cronograma de mantenimiento preventivo, el usuario deberá haber terminado sus actividades urgentes y, en la medida de las posibilidades, todas las demás actividades de ese día; además, deberá tener su área de trabajo ordenada y con espacio suficiente para que el técnico de IT pueda iniciar sus actividades de manera inmediata.
- Identificar errores o problemas leves y comunicar al departamento de IT para reducir la probabilidad de daños mayores.
- Los usuarios administrativos deberán asistir de manera obligatoria a las actividades de capacitación sobre uso de componentes y procesos de comunicación organizadas por departamento de IT, excepto si cuenta con autorización de autoridad correspondiente.
- Comunicar, de manera inmediata y según los procesos determinados por el modelo de gestión de riesgos de IT, sobre problemas en cualquiera de los componentes de uso: hardware, software, redes / comunicaciones y bases de datos.
- Organizar el área de trabajo y dejar espacio suficiente para el trabajo del técnico de IT en caso de requerimiento de mantenimiento correctivo.

- Atender a las instrucciones y capacitación brindada por el departamento de IT en caso de implementación de mejoras y cambios de los componentes.
- Para usuarios recientemente contratados, asistir a una inducción completa sobre uso de componentes tecnológicos.
- Aplicar los procesos y atender a las políticas de IT implementadas por el departamento correspondiente.

5.2.2 Coordinador de TI

- Autorizar, socializar y garantizar la implementación del sistema de gestión de riesgos de TI de la empresa.
- Coordinar, autorizar, evaluar y ordenar cambios en la planificación anual de mantenimiento preventivo. Para esto se considerarán criterios como registro de mantenimiento, importancia de los componentes, atención a vulnerabilidad de bases de datos e impacto del mantenimiento en la continuidad de las operaciones.
- Disponer, junto con los coordinadores de los demás departamentos de la empresa, las acciones de capacitación para los miembros de los departamentos.
- Ordenar, con la autorización del área financiera y las demás que correspondan a los procesos de adquisiciones de la empresa, la compra en instalación de componentes para cambios o mejoras.
- Realizar informes semestrales sobre la implementación del sistema de gestión de riesgos y presentación a la administración de la compañía para la evaluación del modelo.
- Informar sobre la implementación del sistema al departamento regional para coordinar acciones y garantizar el compromiso de asistencia inmediata a los requerimientos del departamento de Ecuador.
- Coordinar el trabajo de los miembros del Equipo de IT para lograr el pleno empleo del talento humano y los recursos del departamento.

5.2.3 Analistas e ingenieros

- Atender a la planificación de mantenimiento preventivo.
- Realizar capacitación sobre uso de componentes tecnológicos según cronograma desarrollado por la coordinación del departamento.
- Realizar las acciones de mantenimiento preventivo y correctivo de manera eficiente, buscando la optimización de tiempo y recursos.
- Llenar la hoja de registro de mantenimiento preventivo y correctivo para, posteriormente, archivarlo de manera adecuada.
- Proponer, en caso de ser necesario y de manera fundamentada, la aplicación de cambios o mejoras en los componentes.
- Instalar los componentes nuevos y dar una capacitación, en caso de ser necesaria, a los usuarios de los componentes.

5.2.4 Contact Center

- Gestionar la comunicación desde y hacia el departamento de IT, atendiendo al sistema de gestión de riesgos implementado, para la máxima eficiencia en la respuesta del departamento.

5.3 INTERFACES

Los actores involucrados en el proceso han sido identificados en cuatro clases que son usuarios/administrativos, coordinador de TI, analistas y contact center. Estos actores tienen responsabilidades comunes en todas las funciones determinadas (mantenimiento preventivo, correctivo, mejoras y cambios y capacitaciones). Las funciones, de manera general, son:

Usuarios/administrativos: las actividades de estos actores en las funciones descritas se relacionan con el rol de favorecer y facilitar la labor a los analistas

en sistemas por medio de un ambiente ordenado de trabajo, con información oportuna sobre problemas y dudas que tengan y la asistencia puntual y responsable a las actividades de capacitación.

Analistas e ingenieros: son los encargados de llevar a cabo las acciones de mantenimiento tanto correctivo como preventivo, además de los cambios y mejoras, de acuerdo a las órdenes de trabajo entregadas por el coordinador de TI. Adicionalmente, están a cargo de despejar las dudas de los usuarios.

Coordinador de TI: es la persona que está a cargo de la definición de las acciones a través de la generación de un plan tanto de mantenimiento preventivo como de cambios y mejoras. Además es el responsable de los resultados de la implementación del plan.

Contact Center: su actividad principal es la gestión de la comunicación entre los diversos actores en las diferentes funciones.

De manera específica, se presenta en el anexo 2 del presente trabajo un resumen de las actividades de los diversos actores.

INTERACCIÓN ENTRE LOS ACTORES

Los involucrados en el sistema de gestión de riesgos de TI en ROCHE se interrelacionan de tal como se presenta en el siguiente Figura:

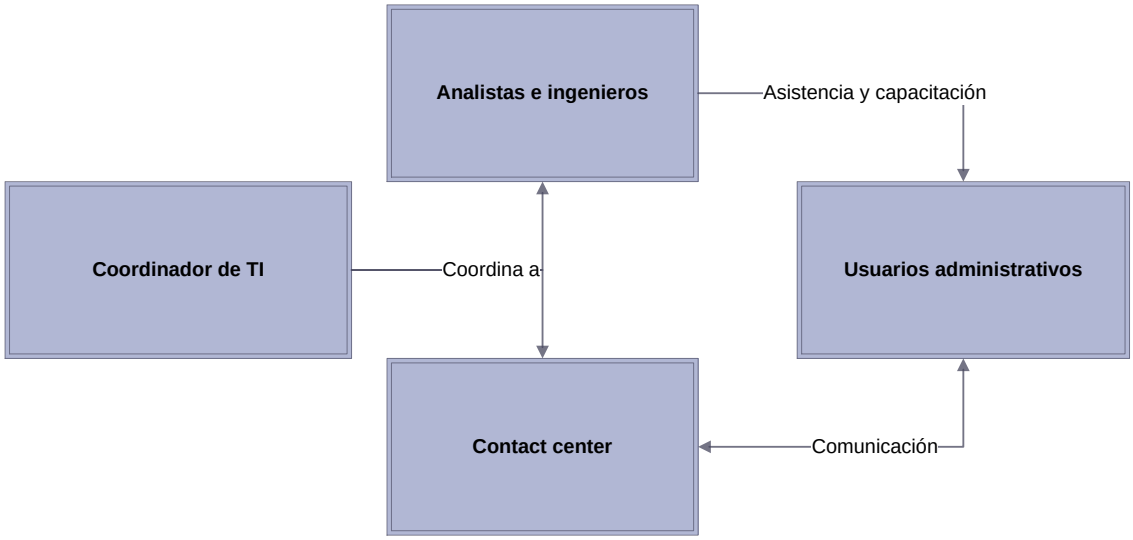


Figura 7. Interacción entre actores

Por lo señalado en este acápite, se puede observar cuáles son las actividades y responsabilidades de los diferentes actores: el coordinador del área de TI señala las actividades a realizar, el contact center informa, el analista desarrolla las acciones y el usuario facilita las acciones.

5.4 CONCLUSIONES PARCIALES DEL CAPÍTULO

En el presente capítulo se han logrado determinar las siguientes conclusiones:

- Se han identificado cuatro tipos de involucrados directos para la aplicación del modelo: usuarios/administrativos, coordinador de TI, analistas e ingenieros; y, contact center del departamento de TI.
- Los usuarios participarán facilitando el trabajo operativo de mantenimiento y cambios al ordenar las estaciones de trabajo y planificar la forma de no interrumpir las labores por las acciones señaladas. Además deberán participar de manera activa en las actividades de capacitación.

- Los analistas e ingenieros tienen como responsabilidad realizar las acciones de mantenimiento, cambios y capacitación de los usuarios.
- El coordinador de TI realiza la planificación y articula las acciones. Además, es el responsable de la implementación del modelo.
- El Contact Center se encarga de la gestión de la comunicación entre los demás actores.

CAPÍTULO VI

DISEÑO LÓGICO Y FÍSICO

6.1 CRITERIOS

Para la implementación de las actividades de gestión de riesgos, se tomarán en cuenta los siguientes criterios:

- Norma ISO-20000: dirigida a la gestión de los servicios de TI.
- Norma ISO 27001: marco de gestión por la seguridad de la información.
- Norma ISO/IEC-38500: marco de principios para que la dirección de las organizaciones al evaluar, dirigir y monitorear el uso de las TI.
- MOF: se considerará el manual interno de la empresa como criterio para la implementación del diseño propuesto para ROCHE Ecuador.

6.2 ARQUITECTURA DE LOS COMPONENTES

Con el fin de sintetizar la estructura y las funciones de los usuarios y componentes del sistema, se presenta de forma gráfica la arquitectura de componentes:

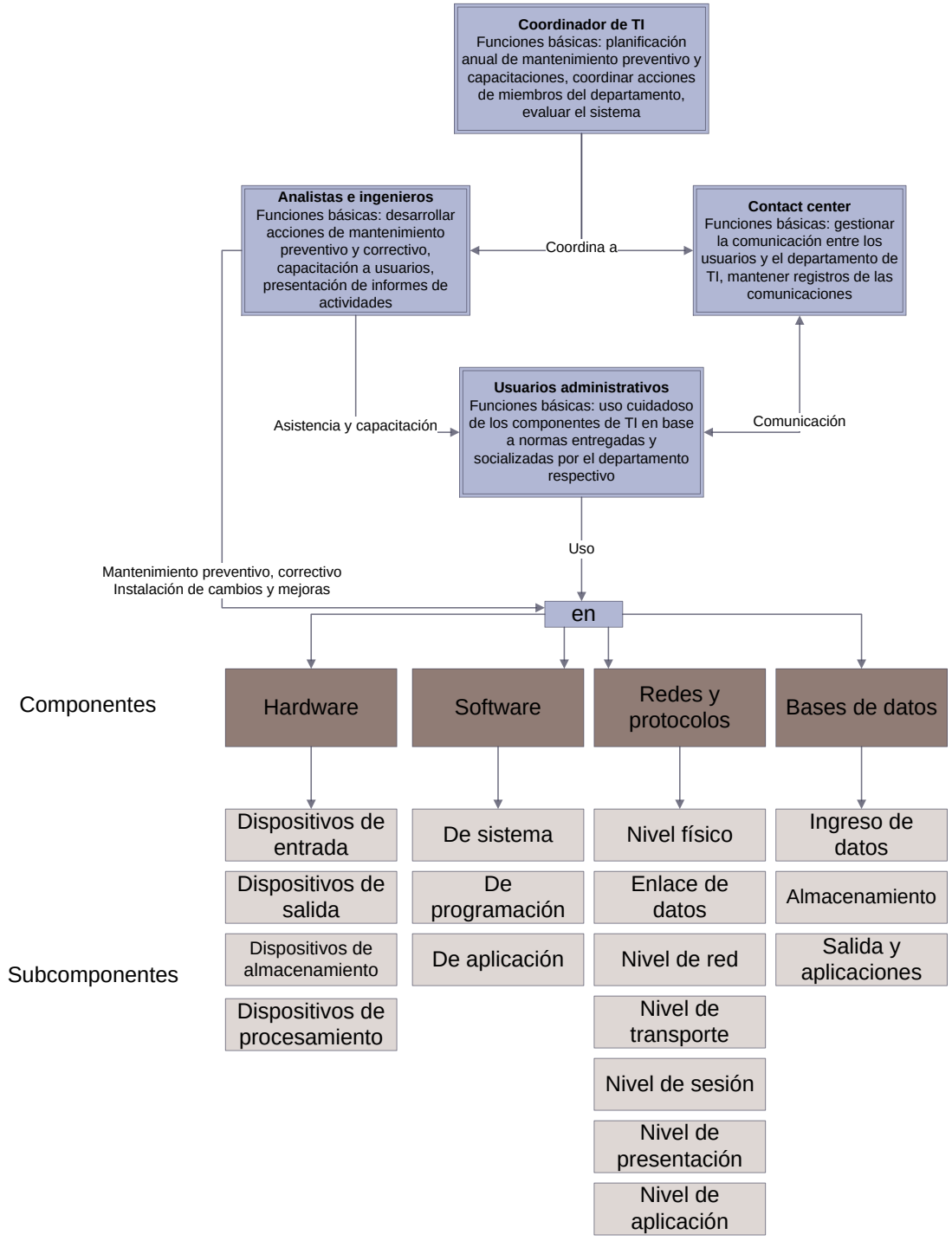


Figura 8. Arquitectura de los componentes

6.3 ARQUITECTURA DE PROCESOS

Se ha establecido, mediante ponderación de beneficios esperados, que la alternativa óptima para solución del problema es la implementación de un plan de gestión de riesgos de TI que permita un conocimiento y un orden en las actividades que permitan la identificación, mitigación y el control de los riesgos relativos a TI.

La implementación del plan propuesto permitirá:

- Diseñar de un plan anual de mantenimiento preventivo: elaborado por el coordinador de TI y socializado con el equipo de trabajo de analistas y el contact center. Luego, el plan anual será comunicado a los usuarios para su conocimiento. El plan anual de mantenimiento atiende los riesgos sobre los componentes de TI como lo estipula la norma ISO 21002: 2005 que indica que se debe contar con un documento que determine la política de seguridad y su gestión; además de su apartado “Evaluación y tratamiento del riesgo” (International Organization for Standardization, 2005).
- Determinar procesos de mantenimiento correctivo: los que serán comunicados a todo el equipo de TI de ROCHE y también a los usuarios con el fin de optimizar las acciones de mantenimiento correctivo. Estos procesos se enmarcan dentro de la norma ISO 27002: 2005 en los artículos relacionados al mantenimiento de los sistemas de información (International Organization for Standardization, 2005).
- Establecer políticas y procesos para mejora o cambio de componentes: comunicados al departamento de TI y a usuarios, con el fin de identificar de manera temprana los cambios o mejoras requeridos para la continuación óptima de las operaciones y la planificación de las actividades. Este elemento atiende a la norma ISO 27002: 2005 que señala (International Organization for Standardization, 2005).

- Desarrollar un cronograma de capacitaciones a usuarios: que será comunicado oportunamente a los mismos y permitirá la difusión de las políticas y procesos implementados, así como información acerca de los componentes y su uso. Esto atiende a la norma internacional ISO 27002:2005 relacionada a “Aspectos organizativos de la seguridad de la información” (International Organization for Standardization, 2005).

6.4 COMPONENTES DEL MODELO

El modelo de plan de gestión de riesgos que se propone como alternativa óptima de solución tiene componentes que se estructurarán de la siguiente manera:

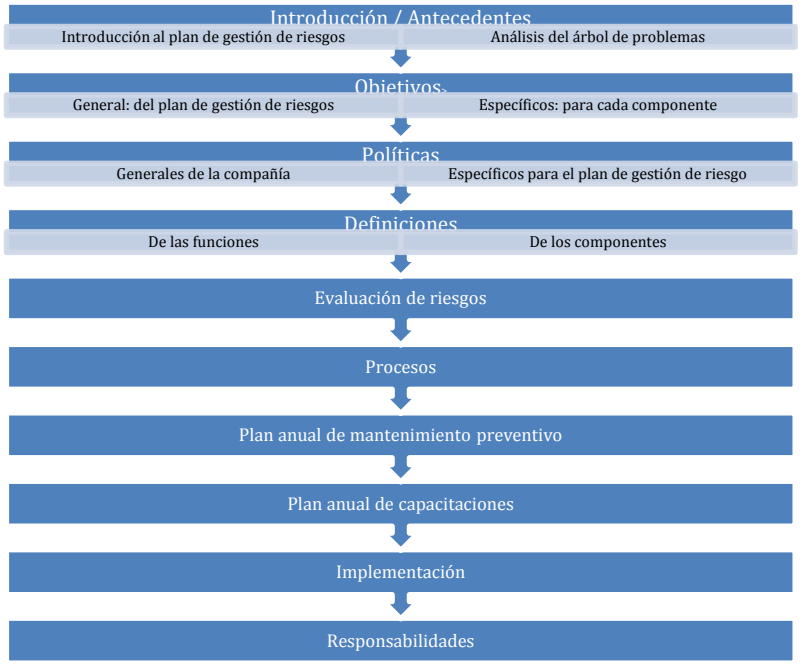


Figura 9. Componentes del modelo

En la introducción y antecedentes del modelo se deberán incluir las conclusiones y recomendaciones del presente trabajo además de otros

elementos que permitan comprender la naturaleza del problema y justificar el desarrollo del modelo.

Los objetivos de la propuesta deberán ser medibles, claros, prácticos y suficientemente difundidos entre todos los involucrados. Se recomienda el establecimiento de un objetivo general y objetivos específicos para cada una de las funciones del modelo. En el presente trabajo se propone un modelo de establecimiento de objetivos en el anexo 4.

Las políticas son normas superiores implementadas en una organización para guiar las acciones y decisiones de la empresa y sus empleados. En el documento del plan deberán especificarse de manera clara las políticas de TI de Roche Ecuador S. A. En el anexo 5 se proponen políticas que pueden ser utilizadas en el modelo propuesto.

Las definiciones se refieren a un glosario de términos a ser utilizado en el modelo propuesto, de manera especial de los componentes. Para delimitar estos componentes y los actores dentro de la etapa de definiciones, en el anexo 6 se muestra un Figura con una visión resumida de dichas definiciones.

La evaluación de riesgos permite determinar el impacto y la probabilidad de un evento específico, relacionado con los componentes del modelo. En el anexo 7 se presenta una matriz de evaluación de riesgos de Roche desarrollada en base a los resultados de entrevistas en la organización.

La determinación de los proceso por medio de mapas facilita enormemente las acciones ya que indica de manera clara la secuencia de acciones a seguir para cada función. En el anexo 8 se proponen mapas de procesos para las actividades determinadas en la investigación.

Plan anual de mantenimiento preventivo y de capacitaciones es un cronograma suficientemente flexible para involucrar a la mayor cantidad de personas y no interrumpir las actividades normales de la compañía.

Finalmente debe indicarse la forma de implementación del modelo y las responsabilidades en esa acción. Estos elementos deben indicar, de manera clara, la forma en que se controlará y evaluará la implementación de las funciones.

Con los elementos señalados, tanto del plan de gestión de riesgos como de funciones, se determina de manera general la conexión entre ellos.

Tabla 13. Detalle de actividades a desarrollar

Componente del plan	Componente				Detalle
	CTI	A&I	CC	U	
Introducción / antecedentes	X	X			1. Se evalúa el análisis del problema y la alternativa de solución propuesta. 1.1. Se redacta el componente.
Objetivos	X				2. Se definen objetivos generales y específicos del plan.
	X	X	X		2.1. Se socializa con el departamento para recopilar sugerencias e implementar cambios. 2.2. Se redactan objetivos.
Políticas	X				3. Se definen políticas específicas para el plan.
	X	X	X		3.1. Se socializa con el departamento para recopilar sugerencias e implementar cambios. 3.2. Se redactan políticas.
Definiciones	X				4. Se definen los componentes del problema y de la solución.

					4.1. Se redactan las definiciones.
Evaluación de riesgos		X			5. Definen riesgos y valoración para cada componente. 5.1. Presentan informe de evaluación de riesgos
	X				5.2. Se aprueban informes y se redacta matriz de evaluación.
Procesos	X				6. Define procesos
	X	X	X		6.1. Se socializa con el departamento para recopilar sugerencias e implementar cambios. 6.2. Se redactan procesos.
Plan Anual de Mantenimiento preventivo	X				7. Define cronograma tentativo
	X	X	X		7.1. Se socializa con el departamento para recopilar sugerencias e implementar cambios. 7.2. Se redacta plan anual.
Plan Anual de Capacitaciones	X				8. Define cronograma tentativo
	X	X	X		8.1. Se socializa con el departamento para recopilar sugerencias e implementar cambios. 8.2. Se redacta plan anual.
Implementación	X				9. Se presenta plan a autoridades para su aprobación. 9.1. Se redacta cronograma de implementación, presupuesto, actividades y responsabilidades.
Responsabilidades	X				10. Se suscribe el documento y se difunde para iniciar su implementación

6.5 FUNCIONES DE LOS ACTORES

Para desarrollar las funciones anotadas dentro del sistema de gestión de riesgos, se contemplan los siguientes elementos y su interacción:

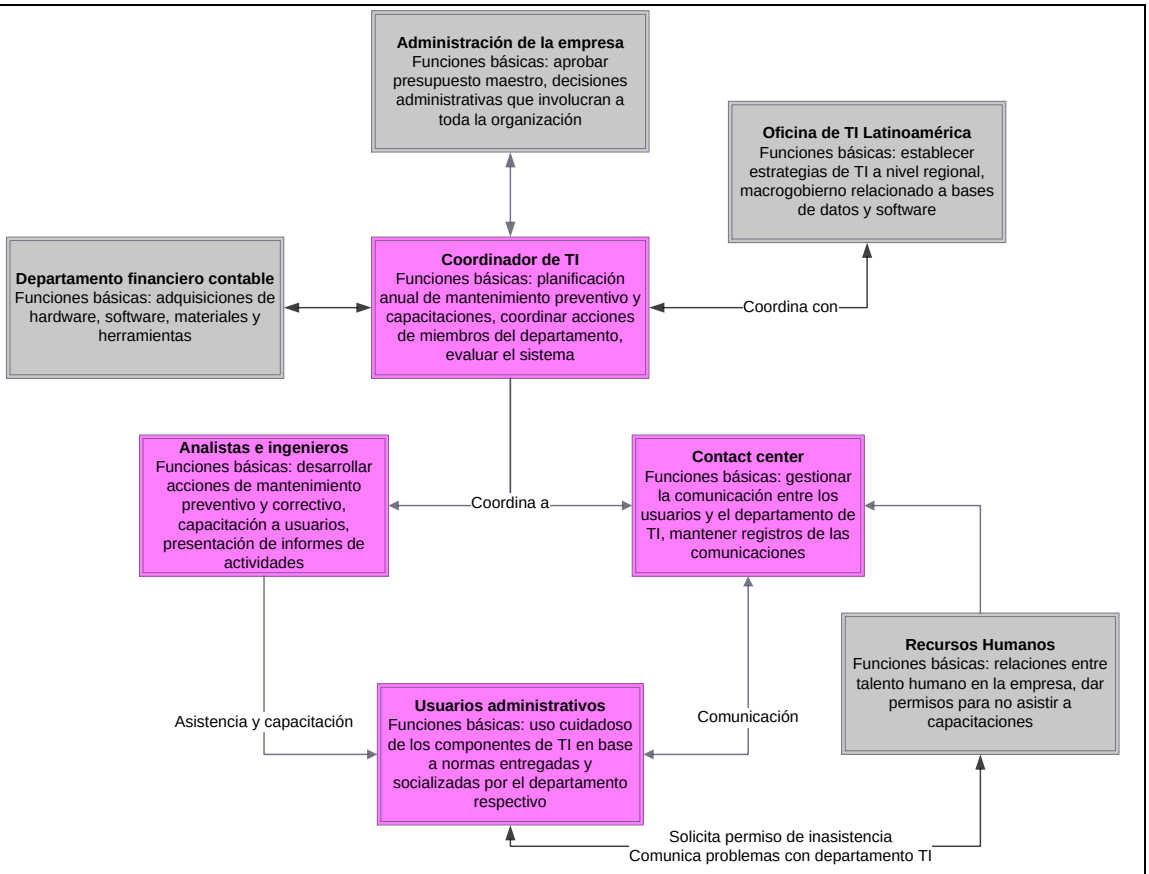


Figura 10. Funciones e interrelación de los actores

Se debe tomar en cuenta que el personal de la administración de la empresa, del departamento financiero y de recursos humanos también son parte del grupo de usuarios administrativos por cuanto dan uso a componentes de TI.

De la manera señalada en las funciones extendidas de los actores, se observa que se requiere de la venia y apoyo de la administración de la empresa para la

aplicación del modelo; así como también es necesaria la coordinación con la oficina para Latinoamérica de Ti, con la finalidad de que no se contrapongan los objetivos generales a nivel regional con los específicos de la empresa en Ecuador.

De manera adicional, se puede identificar que un elemento importante para el desarrollo del modelo es contar con los recursos financieros suficientes, particularmente para las actividades de cambios y mejoras. En este sentido, se involucra al departamento financiero con el fin de que se desarrollen las actividades de adquisición y valoración de los componentes, según requerimientos del coordinador de TI.

Finalmente, para lograr una participación más extensa de los usuarios en las actividades descritas en el modelo, se hace necesaria la participación del departamento de Talento Humano de la organización.

6.6 CONCLUSIONES PARCIALES DEL CAPÍTULO

Tras la presentación del capítulo, se han determinado las siguientes conclusiones:

- El modelo de gestión de riesgos de TI cuenta con criterios de aplicación basados en las normas ISO y el manual de operaciones y funciones.
- Las principales acciones del modelo son: capacitación de los usuarios sobre las políticas de TI de la empresa y manejo de componentes; mejora del plan de mantenimiento preventivo de la entidad, reducción de acciones de mantenimiento correctivo; y, acciones ordenadas de mejoras y cambios no planificados.

CAPÍTULO VII

DEMOSTRACIÓN Y EVALUACIÓN

Una vez que se cuenta con el diseño físico de la propuesta de solución, se lo pone a consideración de los involucrados con capacidad administrativa definidos previamente con el fin de contar con una evaluación que, en caso de ser positiva, posibilite contar con el apoyo gerencial requerido para la puesta en marcha de la propuesta.

7.1 DEMOSTRACIÓN

En la semana comprendida entre el 24 y 28 de febrero de 2014, en las oficinas del departamento de TI de la empresa ROCHE del Ecuador, se realizaron reuniones de información, demostración y evaluación del modelo propuesto a los siguientes personeros del área:

- Ing. Liceth Benavides. Coordinadora de TI y miembro del Management Team de la empresa.
- Ing. Andrés Garzón. Responsable de Infraestructura de tecnologías de Información
- Ing. María Eugenia Paguay. Coordinadora de Servicios de Usuario Final.

Las reuniones incluyeron los siguientes pasos:

- Presentación de antecedentes
- Delimitación del problema
- Integración sistémica del dominio y la solución
- Análisis del dominio de la solución
- Diseño lógico

En las reuniones se atendieron las preguntas de los miembros del área de TI y luego se pasó a la etapa de demostración.

Durante la demostración, se consideraron los procesos definidos en el presente trabajo investigativo para mantenimiento preventivo, mantenimiento correctivo, cambios y mejoras y capacitación de usuarios, considerando la experiencia de los miembros del área de TI en esos aspectos. Los modelos presentados se sometieron a discusión entre los miembros, quienes consideraron que no había nudos críticos en dichos procesos. Además, los entrevistados consideraron que se habían utilizado adecuadamente los datos provistos por los miembros al investigador en las visitas previas.

7.2 EVALUACIÓN

Tras las etapas de información y demostración del modelo desarrollado, el viernes 28 de febrero de 2014 se aplicó una encuesta de evaluación a los participantes. El modelo de cuestionario entregado a los miembros de TI se presenta en el Anexo 9 y evaluó el modelo presentado en cinco aspectos:

- Funcionalidad entendida como la capacidad de solución del problema determinado en el estudio.
- Aplicabilidad legal que consideraba si el modelo requiere poco o ningún cambio en la normativa interna vigente de ROCHE Ecuador.
- Aplicabilidad operativa que se refería a si se cuenta con los recursos humanos y materiales para la implementación del modelo
- Aplicabilidad financiera entendida como si se cuenta con recursos financieros para los costes de implementación
- Resistencia de los involucrados que se refiere a la dificultad para persuadir a los miembros de la compañía considerados como involucrados para adoptar el modelo

Los resultados de las encuestas aplicadas se muestran a continuación:

Tabla 14. Evaluación al modelo por Ing. Liceth Benavides

Parámetro evaluado	**1**	**2**	**3**	**4**	**5**
Funcionalidad					X
Aplicabilidad legal					X
Aplicabilidad operativa					X
Aplicabilidad financiera					X
Resistencia de los involucrados		X			

Tabla 15. Evaluación del modelo por Ing. Andrés Garzón

Parámetro evaluado	**1**	**2**	**3**	**4**	**5**
Funcionalidad				X	
Aplicabilidad legal					X
Aplicabilidad operativa					X
Aplicabilidad financiera					X
Resistencia de los involucrados			X		

Tabla 16. Evaluación del modelo por Ing. María Eugenia Paguay

Parámetro evaluado	**1**	**2**	**3**	**4**	**5**
Funcionalidad					X
Aplicabilidad legal					X
Aplicabilidad operativa				X	
Aplicabilidad financiera					X
Resistencia de los involucrados			X		

Se debe advertir que la pregunta relacionada a la resistencia de los involucrados tiene como valor positivo una menor calificación, al contrario de lo que ocurre con las otras preguntas. Esto quiere decir que si una persona encuentra que habrá poca resistencia, calificará con un valor bajo mientras que se incrementará según su percepción acerca de la resistencia de los

involucrados; una menor resistencia implica una implementación más fácil del modelo.

Con los resultados obtenidos, se desarrolla una matriz de ponderación:

Tabla 17. Matriz de ponderación de las evaluaciones

Parámetro evaluado	Enc. 1	Enc. 2	Enc. 3	Ponderado
Funcionalidad	5	4	5	14/15
Aplicabilidad legal	5	5	5	15/15
Aplicabilidad operativa	5	5	4	14/15
Aplicabilidad financiera	5	5	5	15/15
Resistencia de los involucrados	2	3	3	8/15

De la ponderación desarrollada, se desprende que el modelo propuesto es funcional para mejorar las condiciones actuales de riesgo de TI y, de manera general, el problema planteado en el presente estudio. Este elemento es fundamental para que se considere su aplicación dentro de la empresa.

A lo anterior se suma que el modelo es aplicable en lo legal, operativo y financiero, de donde se desprende la factibilidad del diseño propuesto por parte de ROCHE Ecuador S. A.

Finalmente, como elemento a tener en cuenta es el moderado nivel de resistencia de los involucrados según los criterios de los miembros del área de TI de la empresa a quienes se demostró el modelo y lo evaluaron. La resistencia se reducirá con la aplicación de las siguientes medidas:

- Aprobación y apoyo a la implementación del modelo por parte de la esfera administrativa de la empresa.

- Información completa, oportuna y contextualizada del inicio de la aplicación del modelo, que haga realce a la importancia de la solución del problema establecido.
- Publicación extensa y en varios medios (correo electrónico, carteleras, manuales) de las políticas de TI definidas por el modelo y de los procesos a llevarse a cabo.
- Información permanente a los involucrados, en los procesos de capacitación determinados por el modelo, acerca de sus beneficios tanto para la empresa como para los trabajadores.

Considerando que el primer elemento, el apoyo del nivel administrativo de la empresa a la aplicación del modelo, es el de mayor trascendencia para la implementación, la ingeniera Benavides, como miembro del Management Team de la empresa, diseñó y presentó informe favorable sobre el modelo al grupo de administración de ROCHE.

Tras la deliberación correspondiente, el Management Team de la empresa envió carta de validación de la propuesta en la que se indica que el modelo se ha considerado de utilidad para las operaciones de la compañía y se señala el interés de la administración de ROCHE ECUADOR S. A. para proceder a su implementación en el futuro. Dicha carta se presenta en el Anexo 2 del presente documento.

7.3 CONCLUSIONES PARCIALES DEL CAPÍTULO

Se han establecido las siguientes conclusiones del presente capítulo:

- El modelo es funcional para los requerimientos de la compañía, además de que su implementación es factible en los ámbitos legal, operativo y financiero.

- Se ha identificado como limitación un nivel moderado de resistencia al cambio que implicaría el nuevo modelo. Para reducir este inconveniente se ha identificado la necesidad del apoyo de la administración de la entidad para la implementación; la información efectiva y constante a los involucrados acerca de los beneficios del modelo y publicación en varios medios de las políticas y procesos de TI diseñados en el modelo propuesto.

CAPÍTULO VIII

CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

Tras la elaboración del presente estudio, se han podido determinar las siguientes conclusiones.

- Las tecnologías de la información y comunicación forman una parte de gran importancia en la vida actual por ser parte extendida en actividades sociales, académicas, económicas y profesionales.
- Los componentes de TI son: Hardware, Software, Redes e interconexión; y, bases de datos.
- La gestión de riesgos de TI permite a una empresa conocer sus vulnerabilidades que pueden convertirse en amenazas; sirve para identificar y evaluar el riesgo, determinar la alternativa óptima de solución y realizar controles de resultados.
- Existen varios criterios o normas de gestión de riesgos de TI como ISO-27000, ISO/IEC-38500, MOF, entre otros, que ofrecen lineamientos para evitar amenazas en los componentes de TI.
- ROCHE Ecuador presenta varias vulnerabilidades que se han traducido en problemas en lo que respecta a TI, entre ellas: desconocimiento de los usuarios acerca del uso de componentes y políticas de TI; inadecuado mantenimiento preventivo, paralización de operaciones por exceso de mantenimiento correctivo, cambios y mejoras de manera desordenada, entre otros.
- Los problemas señalados han provocado que exista software malintencionado, comunicación tardía de problemas, desactualización de los componentes, daños en los componentes que provocan pérdida

de información valiosa para la empresa y, de manera general, paralizaciones inesperadas de las operaciones.

- Las ideas que se han identificado como posibles soluciones son la planificación de mantenimiento preventivo y de cambios y mejoras, la implementación de un modelo de gestión de riesgos; y la capacitación de los usuarios.
- Se ha evaluado que la alternativa óptima de solución para los problemas señalados es la implementación de un modelo general de gestión de riesgos de TI.
- Se han podido identificar cuatro involucrados directos para la aplicación del modelo: usuarios/administrativos, coordinador de TI, analistas e ingenieros; y, contact center del departamento de TI.
- Los usuarios participarán facilitando el trabajo operativo de mantenimiento y cambios al ordenar las estaciones de trabajo y planificar la forma de no interrumpir las labores por las acciones señaladas. Además deberán participar de manera activa en las actividades de capacitación. Los analistas e ingenieros tienen como responsabilidad realizar las acciones de mantenimiento, cambios y capacitación de los usuarios. El coordinador de TI realiza la planificación y articula las acciones. Además, es el responsable de la implementación del modelo. El Contact Center se encarga de la gestión de la comunicación entre los demás actores.
- El modelo de gestión de riesgos de TI cuenta con criterios de aplicación basados en las normas ISO y el manual de operaciones y funciones.
- Las principales acciones del modelo de gestión son: capacitación de los usuarios sobre las políticas de TI de la empresa y manejo de componentes; mejora del plan de mantenimiento preventivo de la entidad, reducción de acciones de mantenimiento correctivo; y, acciones ordenadas de mejoras y cambios no planificados.
- Tras etapas de información, demostración y evaluación, se concluye que el modelo es funcional para los requerimientos de la compañía, además

de que su implementación es factible en los ámbitos legal, operativo y financiero.

- Para la implementación, se concluye que podrá existir un nivel moderado de resistencia al cambio que implicaría el nuevo modelo. Entre las acciones previstas para reducir este inconveniente están: el apoyo de la administración de la entidad para la implementación; la información efectiva y constante a los involucrados acerca de los beneficios del modelo y publicación en varios medios de las políticas y procesos de TI diseñados en el modelo propuesto.

8.2 RECOMENDACIONES

- Se recomienda a estudiantes, docentes y profesionales de carreras de gestión de riesgos de TI, ingeniería en sistemas y carreras afines, el estudio y análisis del presente trabajo investigativo como elemento de desarrollo académico.
- Se sugiere a la empresa ROCHE ampliar el estudio propuesto a varias áreas de la empresa para la auditoría de la gestión actual y la propuesta de procesos para todos los departamentos, lo que se considera que beneficiará a la empresa de manera integral.
- Finalmente, se recomienda a la organización la adopción del modelo propuesto en la presente investigación con el fin de reducir las vulnerabilidades de TI que actualmente presenta. Esta recomendación se basa, adicionalmente, en la carta de validación entregada al proponente en la que se señala la utilidad del modelo y se indica que será aplicado por la empresa en el futuro.

Referencias

Alonso, R. C. (2010). *Tecnologías de la información y la comunicación: introducción a los sistemas de información y de telecomunicación.* España: IdeasPropias.

Amador, J. (2005). *Proceso administrativo*. Recuperado el 28 de noviembre de 2012, de Prisma: http://www.elprisma.com

Anderson, D., Sweeney, D., & Williams, T. (2012). *Estadística para negocios y economía, 11ava ed.* México: Cengage learning.

Andrade, H. (2005). *Comunicación organizacional interna: proceso, disciplina y técnica.* España: Netbiblo.

Banda, H. (2013). *Análisis de problemas y diseño de soluciones.* Quito: Propia.

Bernal, C. (2006). *Metodología de la investigación.* México: Pearson Educación.

Bernal, C. (2006). *Metodología de la Investigación .* México: Pearson Educación.

Calder, A. (2008). *ISO/IEC 38500: The IT Governance Standard.* Cambridgeshire, Reino Unido: IT Governance.

Cebrián, V. (18 de Enero de 2013). *Importancia de la Comunicación Organizacional*. Recuperado el 2 de Septiembre de 2013, de Ciclus Group: http://ciclusgroup.wordpress.com/2013/01/18/importancia-de-la-comunicacion-organizacional/

De Gasperín, R. (2005). *Comunicación y Relaciones Humanas.* México: Universidad Veracruzana.

Eyssautier de la Mora, M. (2006). *Metodología de la investigación: desarrollo de la inteligencia.* México: Cengage Learning.

FERRANDO, M., & GRANERO, J. (2005). *Calidad total: modelo EFQM de excelencia.* Madrid: FC.

Gmipc. (28 de 03 de 2011). *Grupo mi pc*. Recuperado el 01 de 12 de 2013, de Conoce la primera computadora que existió: http://gmipc3.blogspot.com/2011/03/conoce-la-primera-computadora-que.html

González, P. (17 de mayo de 2012). *Introducción al proceso de gestión de riesgos de TI*. Obtenido de http://www.seinhe.com/

Hurtado Cuartas, D. (2008). *Principios de Administración.* Medellín, Colombia: Fondo Editorial ITM.

Informática-hoy. (02 de 04 de 2010). *Informática-hoy.com.ar*. Recuperado el 01 de 12 de 2013, de Qué es Hardware y Software: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php

International Organization for Standardization. (2005). *ISO 27000.* Ginebra: ISO.

ISO 27000.es. (2013). *DestacaDos Certificación*. Obtenido de http://www.iso27000.es/

IT Gobernance Institute. (2007). *CobiT Quickstart. 2da ed.* Rolling Meadows, Estados Unidos: ITGI.

ITSMF. (2007). *Fundamentos de gestión de servicios TI.* Amersfoort, Holanda: Van Haren Publishing.

Jesus, M. (18 de 05 de 2009). *Mónica-jesús83.blogspot.com*. Recuperado el 02 de 12 de 2013, de Sistemas de Información a ejecutivos: http://monica-jesus83.blogspot.com/2009/05/sistemas-de-soporte-ejecutivos-ess.html

Laudon, K., & Laudon, J. (2004). *Sistemas de Información Gerencial. 8ava ed.* México: Pearson Educación.

Maass, M. (1998). La Comunicación como Factor de Cambio en una Organización. En J. Esteinou, *Espacios de Comunicación.* México: Universidad Iberoamericana.

Maeztu, I. (13 de enero de 2011). *Certificación ISO/IEC 20000 para la gestión de servicios TIC*. Obtenido de http://www.tic-euskadi.com/

Melinkoff, R. (2007). *Los Procesos Administrativos.* Caracas: Contexto.

Microsoft. (2007). *Office.com*. Recuperado el 29 de 11 de 2013, de Qué es una base de datos? Access: http://office.microsoft.com/es-mx/access-help/conceptos-basicos-sobre-bases-de-datos-HA010064450.aspx

Ministerio de Tecnologías de la información y Comunicaciones. (2013). *Glosario*. Obtenido de http://www.mintic.gov.co/

Navidad, G. N. (11 de 10 de 2011). *Slideshare.net.* Recuperado el 02 de 12 de 2013, de Tipos de sistemas de información.:

http://www.slideshare.net/GiancarloNebioloNavidad/tipos-sistemas-de-informacion-tpsmisdssess

Neira, A. L., & Spohr, J. R. (2005). *iso27000*. Recuperado el 01 de 12 de 2013, de ISO27000: http://www.iso27000.es/iso27000.html

Observatel.ac. (2010). *Observatel.org*. Recuperado el 01 de 12 de 2013, de Qué es interconexión?: http://www.observatel.org/telecomunicaciones/Qu_es_interconexi_n.php

overti.es. (2008). *overti.es*. Recuperado el 02 de 12 de 2013, de ISO 20000: http://www.overti.es/iso-20000/

Robbins, S. (2004). *Fundamentos de comportamiento organizacional.* México: Prentice Hall.

ROBBINS, S. (2005). *Administración.* México: Pearson Educación.

ROCHE. (17 de marzo de 2010). *ROCHE Ecuador*. Obtenido de http://www.roche.com.ec/

Rodriguez, J. M., & Uran, C. C. (02 de 06 de 2011). *Gestión grupo 1*. Recuperado el 29 de 11 de 2013, de sistema de información KWS: http://gestiongrupo1.blogspot.com/

Rosas, G. (29 de mayo de 2012). *Sistema de Procesamiento de Transacciones*. Obtenido de http://2ammmm.blogspot.com/

San., m. (13 de 05 de 2013). *sanmiranda.weebly.com*. Recuperado el 29 de 11 de 2013, de OAS: http://sanmiranda.weebly.com/1/archives/05-2013/1.html

Tecnología al Instante. (30 de 12 de 2006). *Tecnología al Instante*. Recuperado el 01 de 12 de 2013, de El primer teléfono celular de la historia: http://www.tecnologiahechapalabra.com/tecnologia/genesis/articulo.asp?i=443

Van Bon, J., De Jong, A., Kolthof, A., & otros. (2008). *Gestion de Servicios TI basado en ITIL.* Amersfoort, Holanda: Van Haren.

Van Bon, J., Polter, S., Verheijen, T., & Pieper, M. (2008). *ISO/IEC 20000: Una introducción.* Amersfoort, Holanda: Van Haren Publishing.

wikispaces.com. (2013). *wikispaces.com.* Recuperado el 02 de 12 de 2013, de Sistema de Apoyo a las Decisiones: http://sistemadeapoyoadecisiones.wikispaces.com/4.Sistema+de+Apoyo+a+Decisiones+(DSS)

GLOSARIO DE TÉRMINOS Y ABREVIATURAS

CAU: Centro de atención al usuario

CSF: Factores Críticos de Éxito.

DSS Sistemas de soporte de decisión

ESS: Sistema de apoyo a ejecutivos

Hardware: componentes físicos de un sistema informático

ISO: International Organization for Standardization; Organización Internacional para la Estandarización.

KPI: Indicadores Clave de Rendimiento.

KWS: Sistemas de trabajo de conocimiento

MIS: Sistemas de información gerencial

MOF: Manual de operaciones y funciones

OLA: Acuerdo de nivel operativo

SLA: Acuerdo de nivel de servicio

Software: componentes intangibles o conjunto de normas para el funcionamiento de un sistema informático.

TI: Tecnologías de información

TPS: Sistema de procesamiento de transacciones

UC: Contrato de soporte

ANEXOS

Anexo 1. Detalle de las alternativas de solución

El Figura y el cuadro siguientes permiten observar algunas ideas que surgen para procurar la solución de las causas citadas previamente:

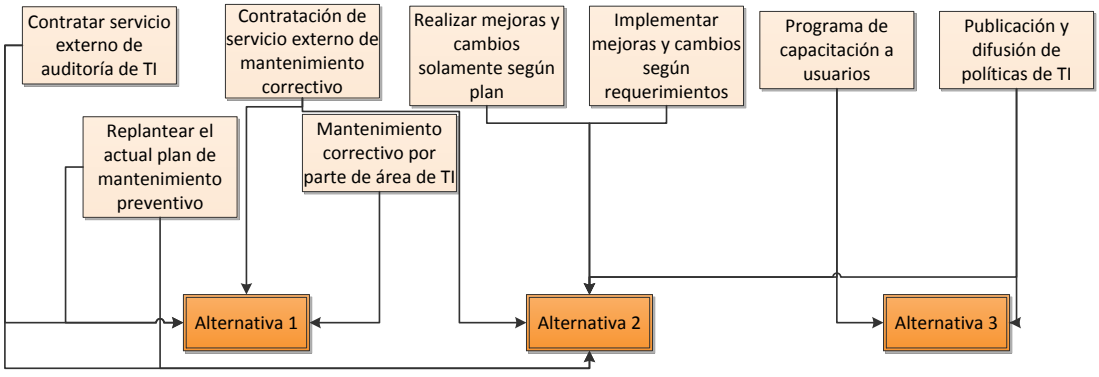


Figura 11. Alternativas de solución

Tabla 18. Análisis de las alternativas

Ideas generadas	**Problema que se soluciona**			
	Falta de plan de mantenimiento preventivo	Exceso de mantenimiento correctivo	Mejoras y cambios no planificados	Falta de conocimiento de usuarios sobre políticas de TI
1. Desarrollar un plan anual de mantenimiento preventivo para todos los componentes				
2. Elaborar un plan de gestión de riesgos de TI integral				
3. Involucrar a los usuarios para hacer más eficiente el mantenimiento correctivo				

Anexo 2. Interfaces de los involucrados

Con el objeto de facilitar la aplicación del sistema para cada uno de los usuarios, se presentan diagramas que serán públicos (enviados de manera individual a todos los usuarios de la empresa).

Cabe indicar que los diagramas, que siguen el ciclo de calidad de Deming, recogen los usos del sistema y el papel de cada usuario en dichas actividades:

Usuarios administrativos

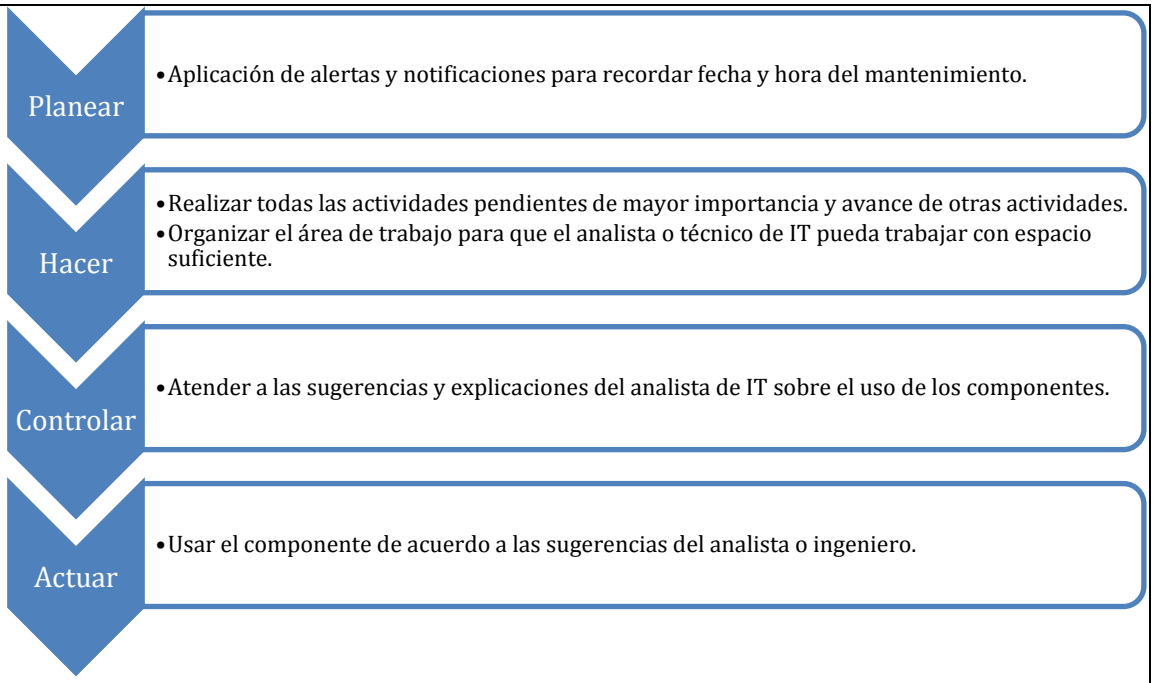


Figura 12. Aplicación de mantenimiento preventivo

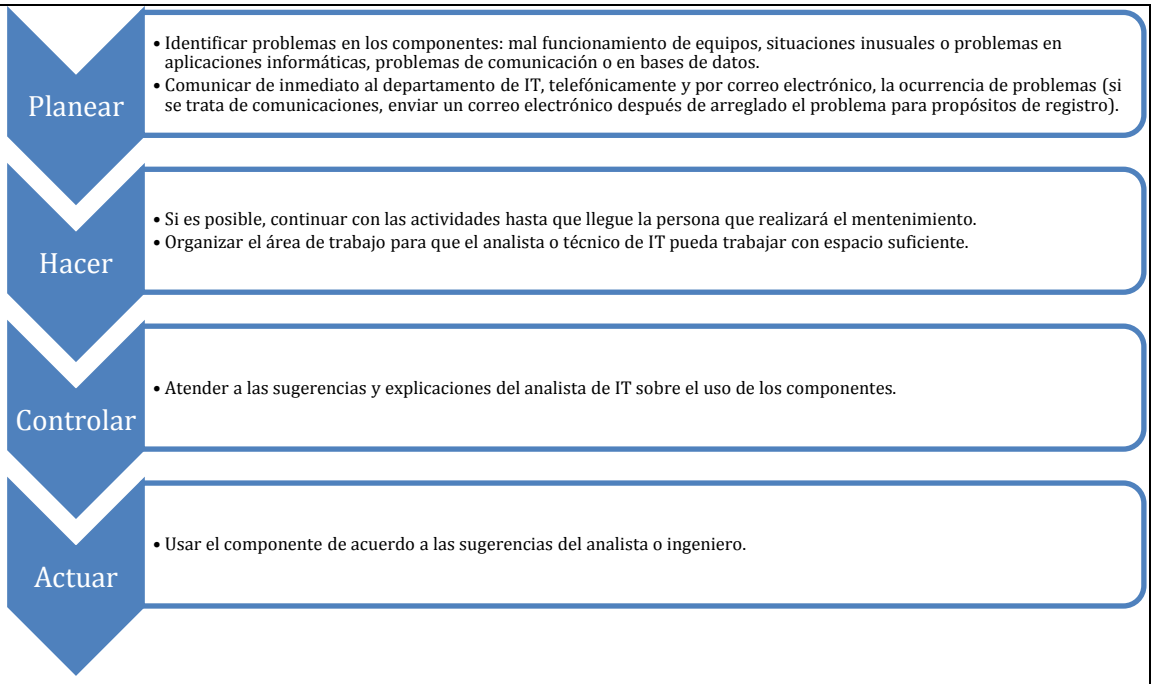


Figura 13. Mantenimiento correctivo

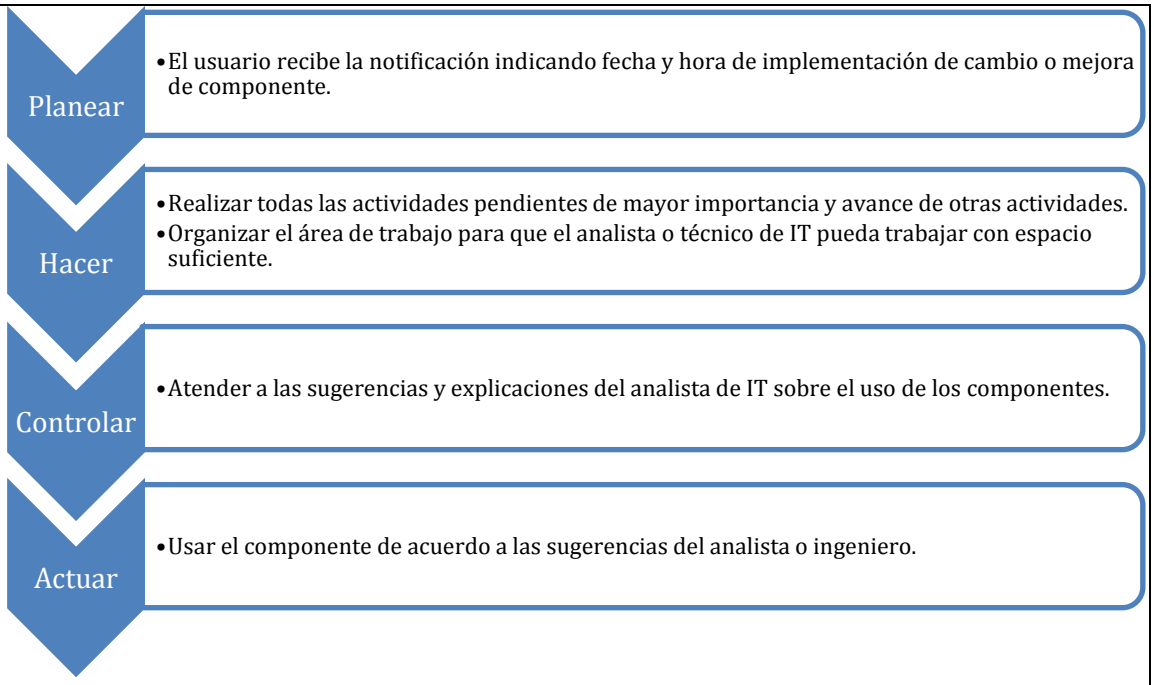


Figura 14. Mejoras y cambios no planificados

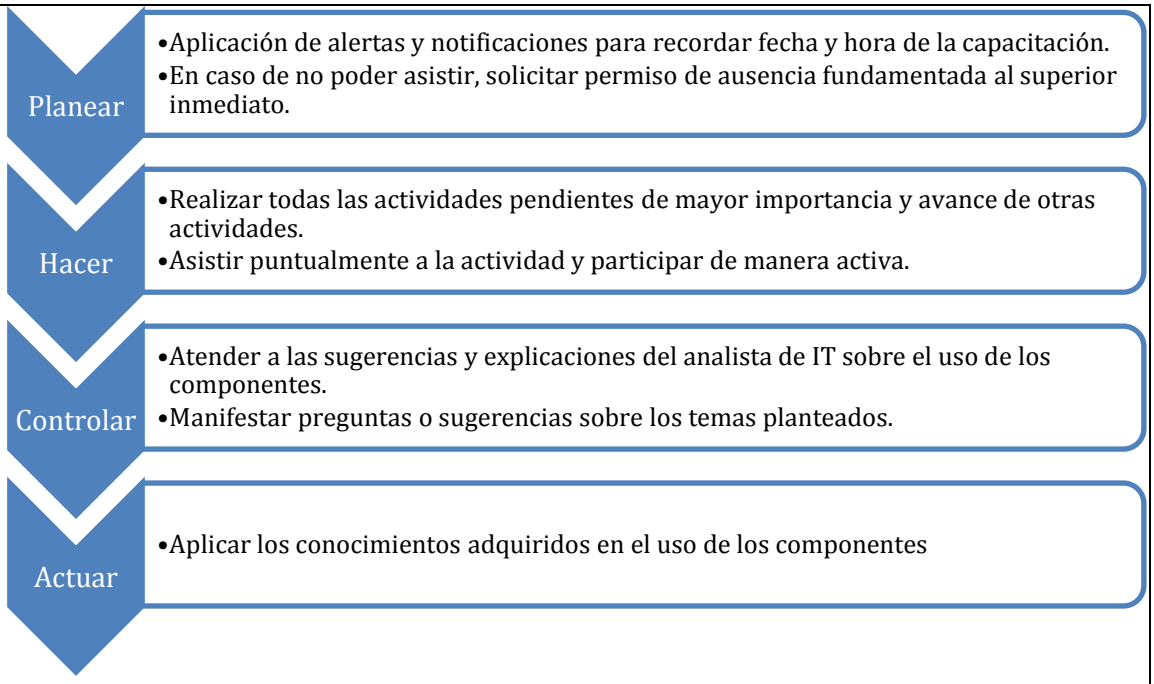


Figura 15. Capacitaciones a usuarios

Coordinador de IT:

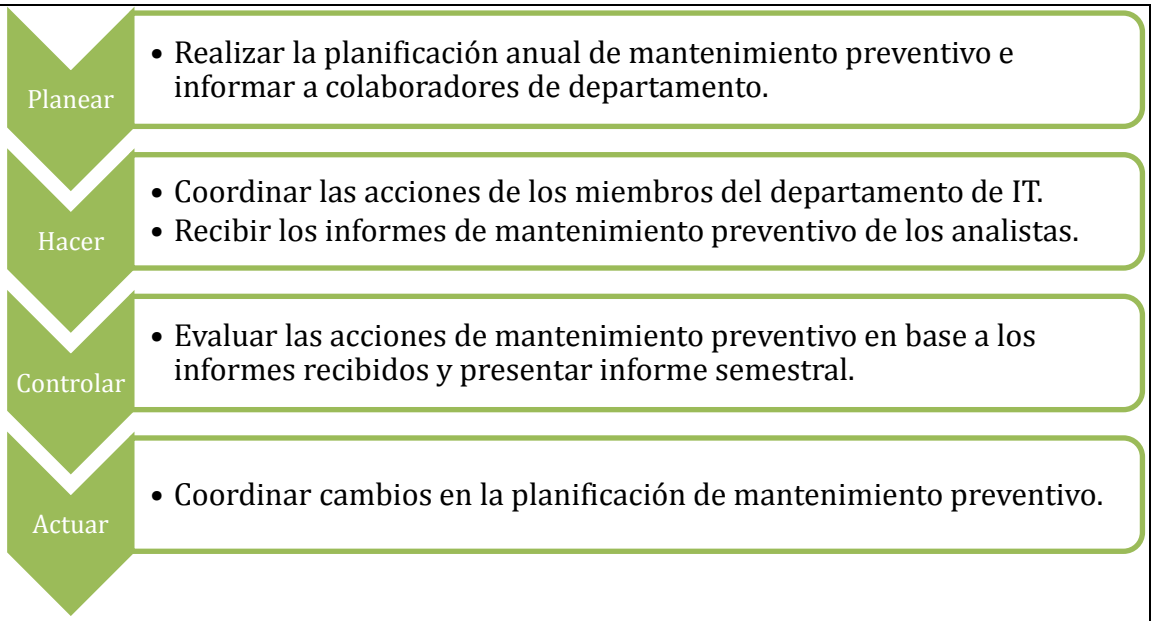


Figura 16. Aplicación de mantenimiento preventivo

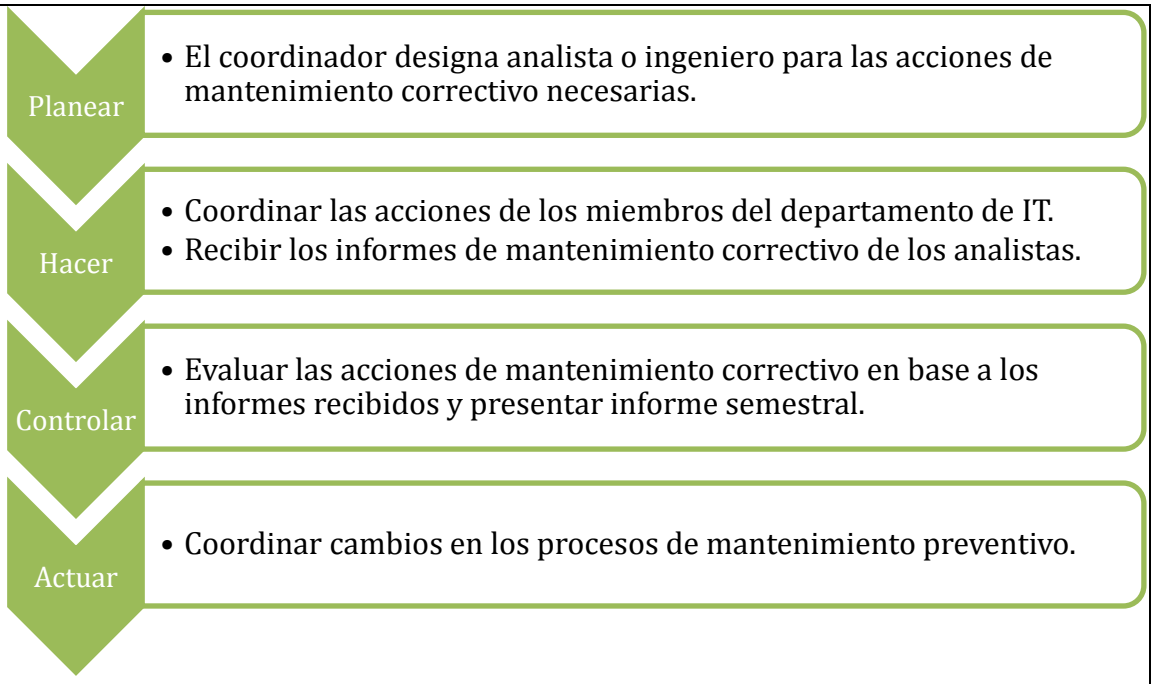


Figura 17. Mantenimiento correctivo

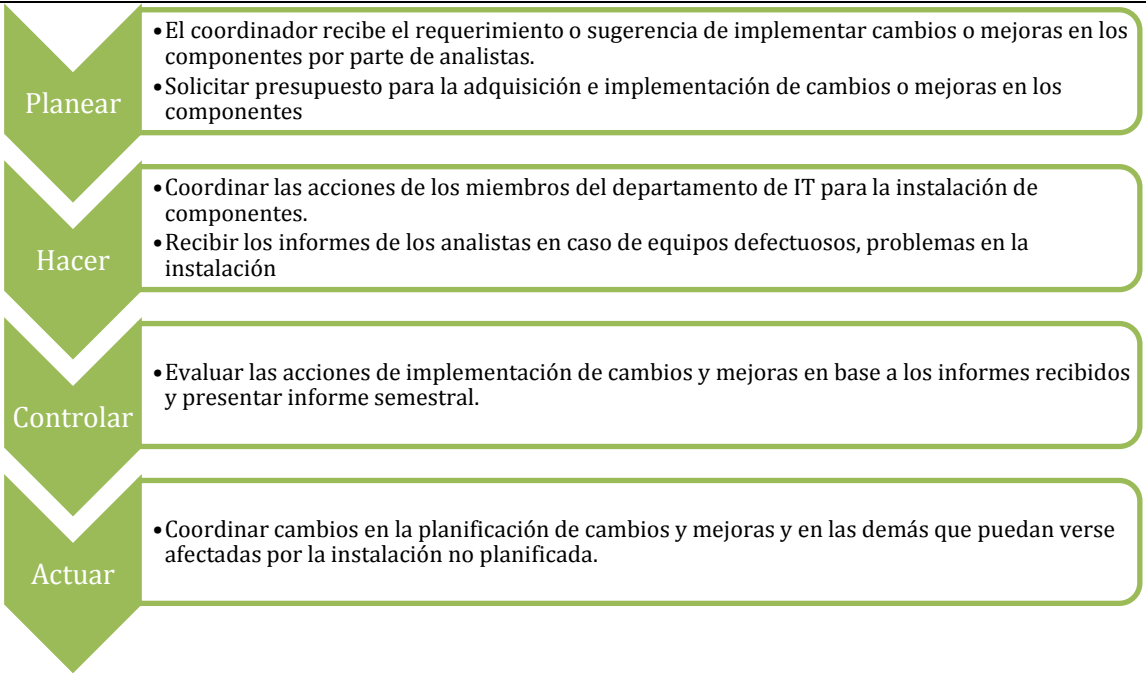


Figura 18. Mejoras y cambios no planificados

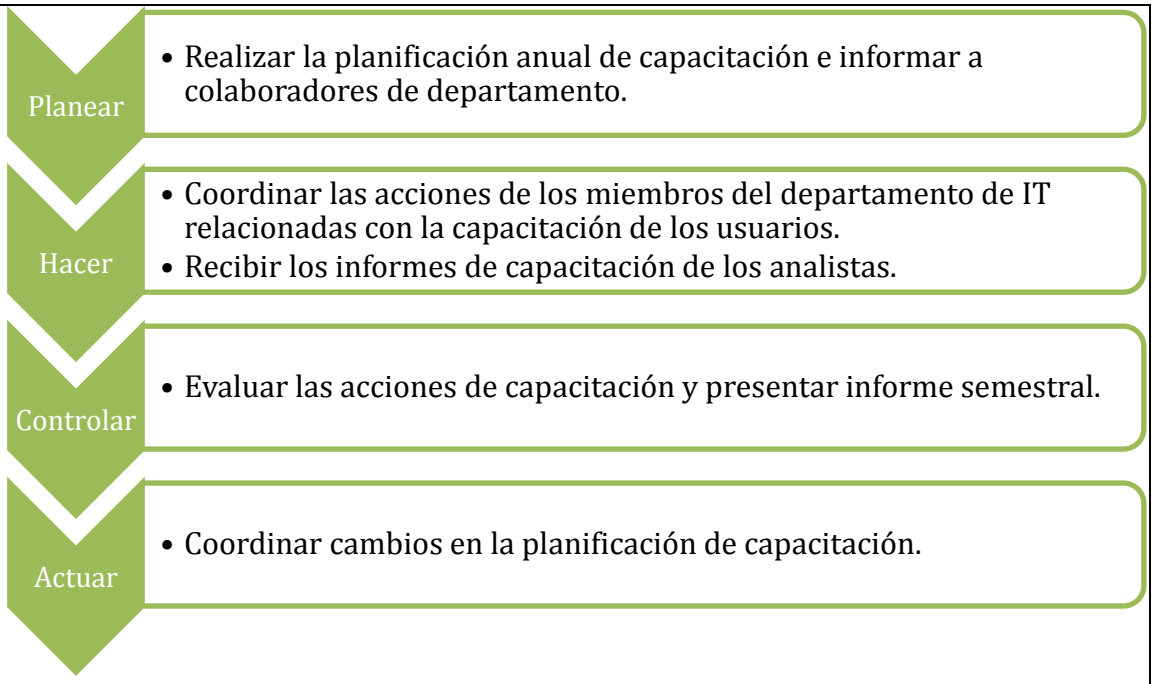


Figura 19. Capacitaciones a los usuarios

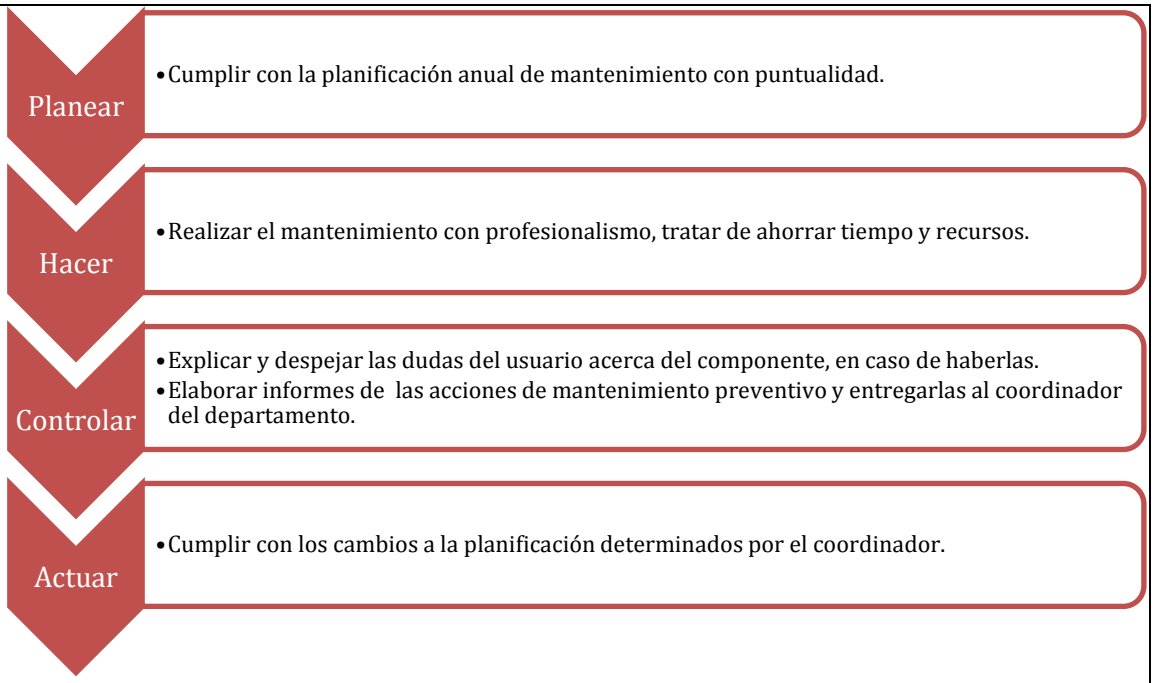


Figura 20. Mantenimiento preventivo

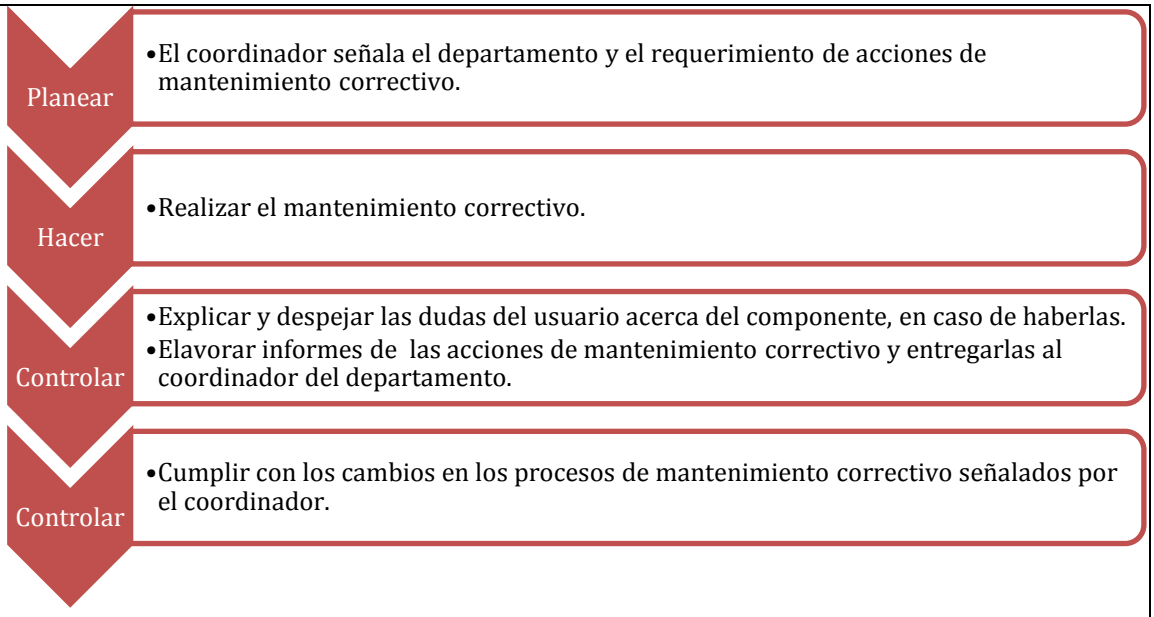


Figura 21. Mantenimiento correctivo

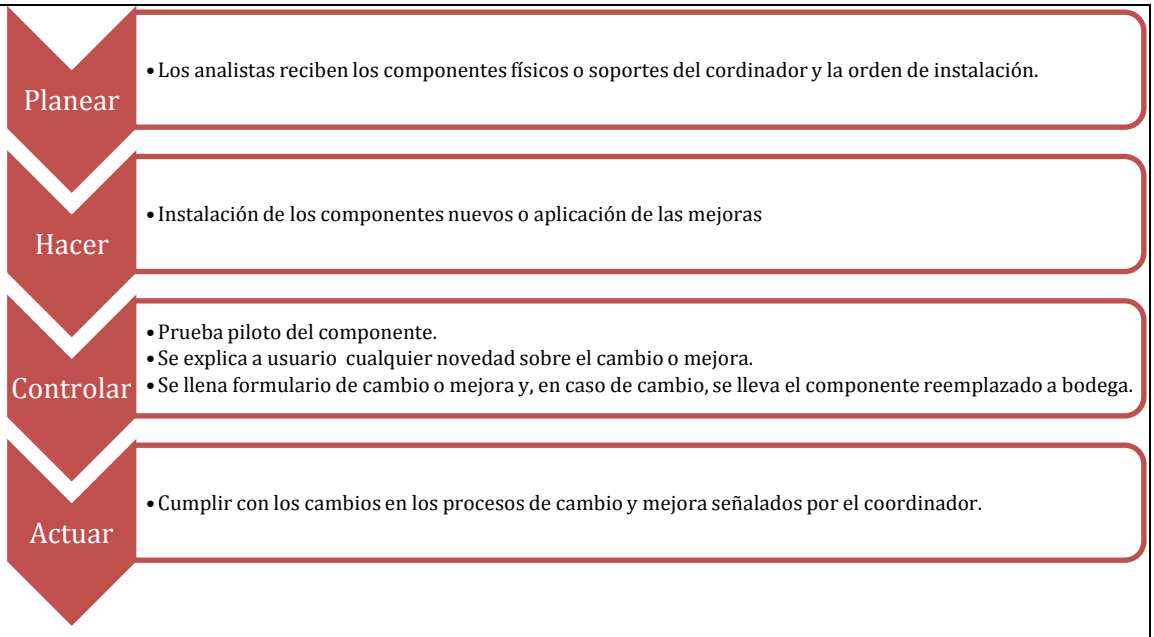


Figura 22. Mejoras y cambios no planificados

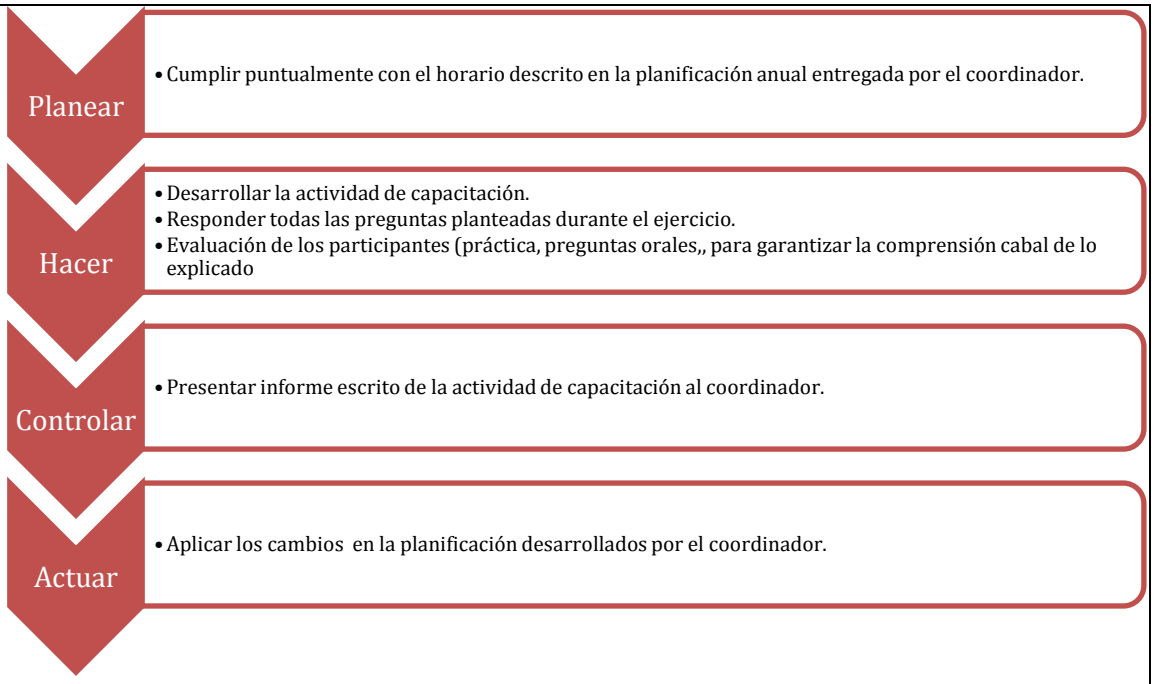


Figura 23. Capacitación a usuarios

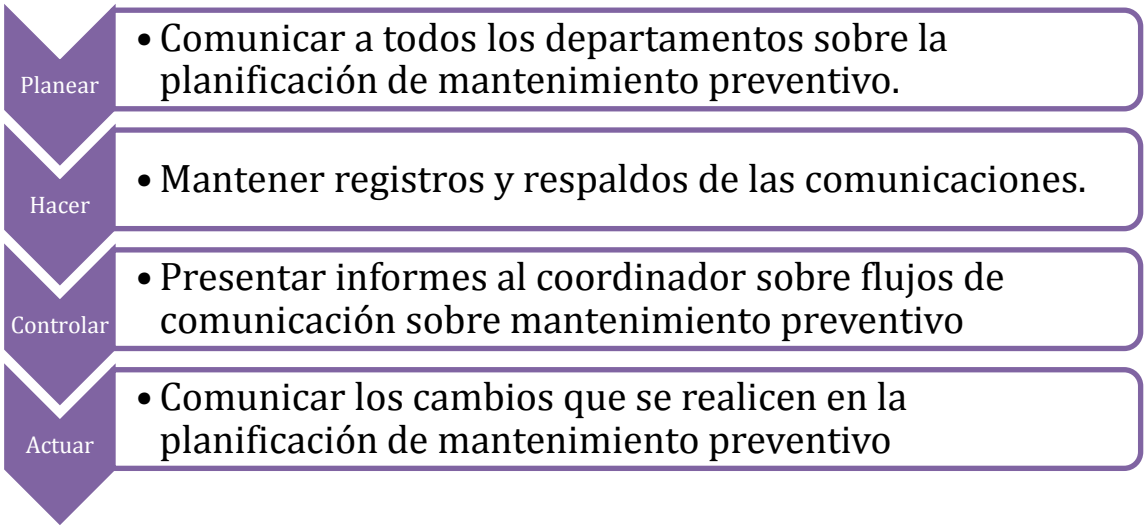


Figura 24. Planificación de mantenimiento preventivo

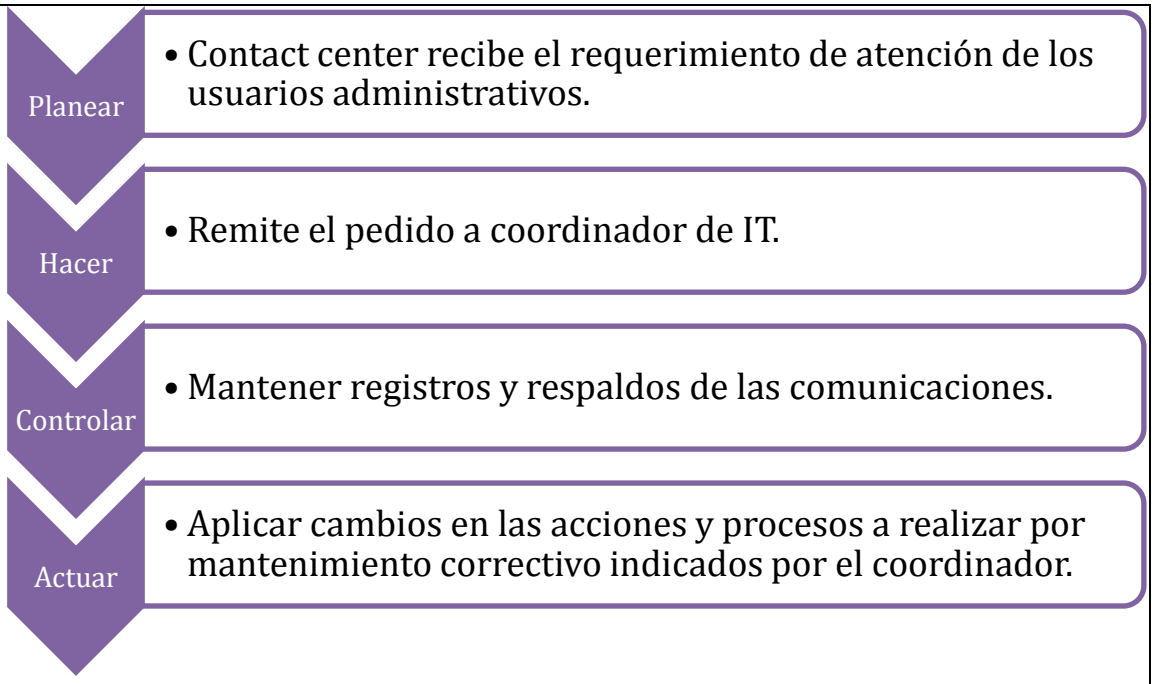


Figura 25. Mantenimiento correctivo

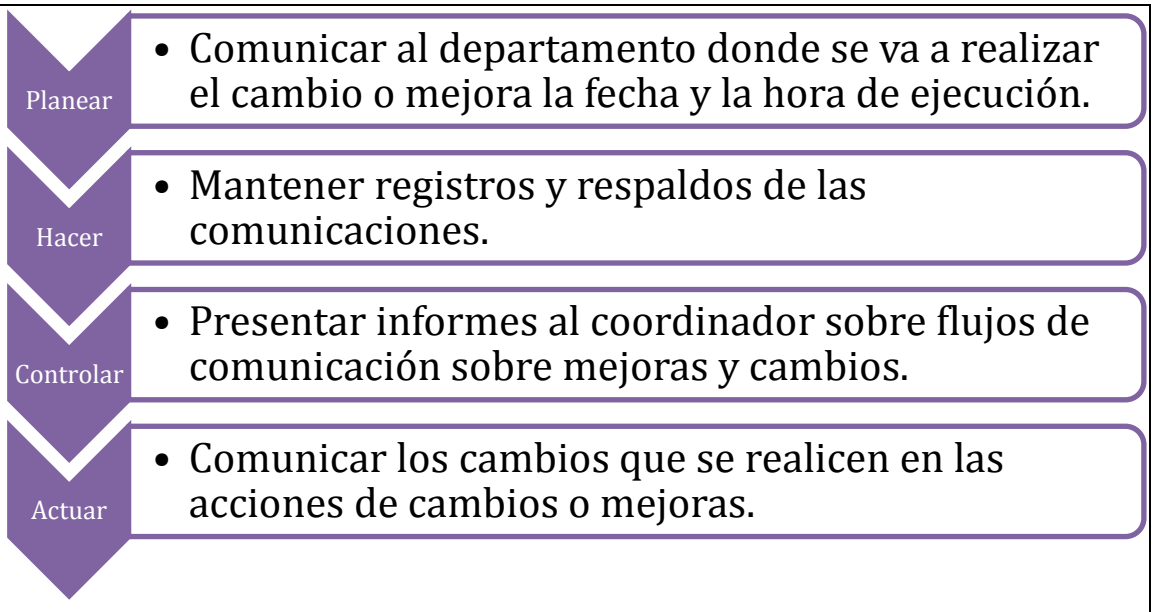


Figura 26. Mejoras y cambios no planificados

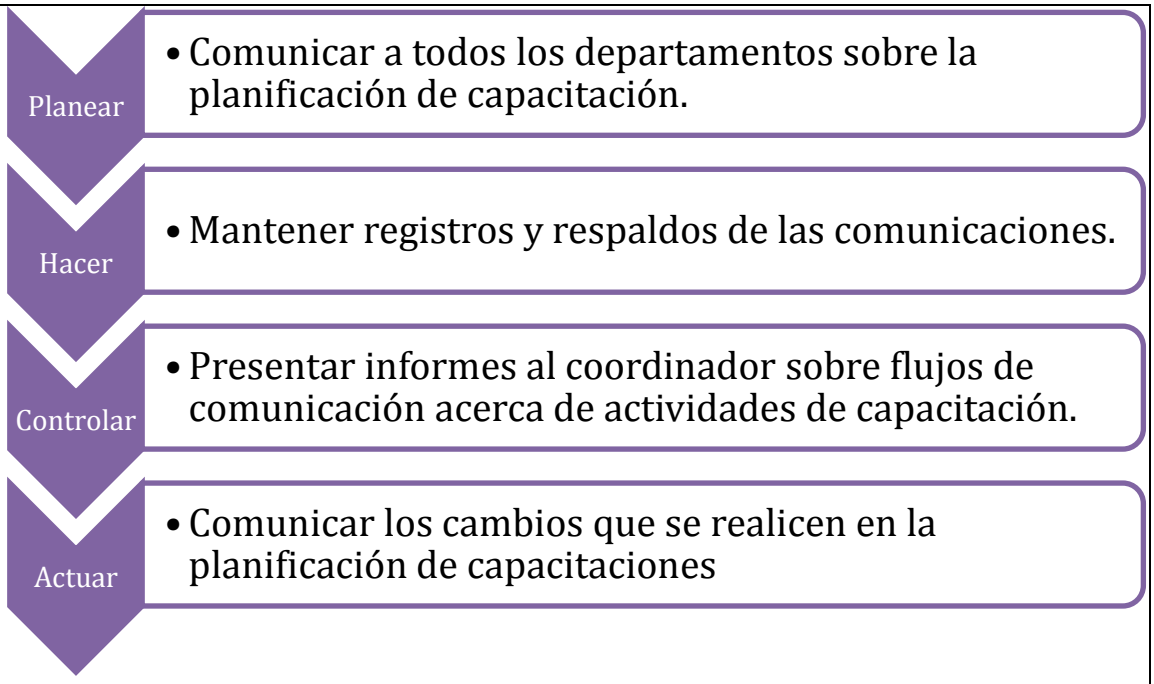


Figura 27. Capacitación de usuarios

Anexo 3. Resumen de criterios considerados en el diseño lógico

- Norma ISO-20000: desarrollada en diciembre de 2005 y está específicamente dirigida a la gestión de los servicios de TI. Fue desarrollada en respuesta a la necesidad de establecer procesos y procedimientos para minimizar los riesgos en los negocios provenientes de un colapso técnico del sistema de TI de las organizaciones. ISO-20000 describe un conjunto integrado de procesos que permiten prestar en forma eficaz servicios de TI a las organizaciones y a sus clientes. Particularmente, se considerará el apartado “Gestión de servicios de TI” que se describe a continuación:

Figura 28. Gestión de servicios de TI

Tomado de: UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

- ISO 27002: Es un conjunto de estándares desarrollados por ISO, la cual proporciona un marco de gestión por la seguridad de la información que

se puede utilizar por cualquier tipo de organización, ya sea esta pública o privada. El número de certificaciones ha aumentado considerablemente en los últimos años como demostración de la relevancia que tiene la protección de la información para el desarrollo de las actividades de las organizaciones y para mantener y desarrollar el tejido industrial en todo el mundo.

Los contenidos de la norma ISO 27002:2005, se detallan a continuación:

- Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de seguridad: documento de política de seguridad y su gestión.
- Aspectos organizativos de la seguridad de la información: organización interna; terceros.
- Gestión de activos: responsabilidad sobre los activos; clasificación de la información.
- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.
- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptoFiguras; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

- ISO/IEC-38500: Su objetivo es el de proporcionar un marco de principios para que la dirección de las organizaciones los usen al evaluar, dirigir y monitorear el uso de las TI. La norma se emplea al gobierno de los procesos de gestión de las TI en todo tipo de empresas que utilicen las tecnologías de la información, proporcionando unas bases para la evaluación objetiva del gobierno de TI. Entre los beneficios de un buen gobierno de TI estaría la conformidad de la organización con:
  - los estándares de seguridad
  - legislación de privacidad
  - legislación sobre el spam
  - legislación sobre prácticas comerciales
  - estándares de responsabilidad social
  - Búsqueda de un buen rendimiento de la TI mediante:
    - apropiada implementación y operación de los activos de TI
    - clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización
    - continuidad y sostenibilidad del negocio
    - alineamiento de las TI's con las necesidades del negocio

- asignación eficiente de los recursos
- innovación en servicios, mercados y negocios
- buenas prácticas en las relaciones con los interesados
- reducción de costes
- materialización efectiva de los beneficios esperados de cada inversión en TI

- MOF: El manual de operaciones y funciones es un documento que las empresas llevan a cabo para implementar parte de la forma de la organización que han adoptado, y que sirve como guía para todo el personal. Se considerará, entonces, el manual interno de la empresa como criterio para la implementación del diseño propuesto para ROCHE Ecuador.

Anexo 4. Objetivos propuestos para el modelo

Objetivo General:

Diseñar, implementar y evaluar un plan de gestión de riesgos de tecnologías de la información y comunicación en Roche Ecuador S. A.

Objetivos Específicos:

Promover el desarrollo de mantenimiento preventivo de componentes de una manera técnica y eficaz que involucre a los usuarios como facilitadores y aportadores de información permanente.

Reducir la frecuencia de mantenimiento correctivo con respecto a años anteriores, al igual que su tiempo de desarrollo.

Implementar un programa permanente de capacitaciones a los usuarios de tecnologías de Información y comunicación desarrollado por el talento humano del departamento de TI de la empresa.

Diseñar, aplicar y controlar un plan para las acciones de cambios y mejoras de los componentes de tecnologías de información y comunicación.

Anexo 5. Políticas propuestas para plan de gestión de riesgos

Las políticas que gobiernan el plan de gestión de riesgos de TI son las siguientes:

- Optimización del talento humano de IT: Se procurará el pleno empleo de los recursos humanos del departamento de TI; en tal virtud, se planificará el mantenimiento preventivo y la capacitación de usuarios administrativos de tal forma que se cubra el 75% de horas hombre, durante el primer año y 85% en los años subsiguientes; dejando el tiempo restante a actividades de mantenimiento correctivo, mejoras y cambios.
- Reducción de paralizaciones de actividades: Es un objetivo importante del sistema planteado el evitar la paralización de las operaciones dentro de ROCHE Ecuador S. A., por lo que el mantenimiento preventivo y la capacitación son fundamentales para reducir al mínimo el mantenimiento correctivo. El mantenimiento correctivo se realizará de forma temprana y eficaz, con el fin de evitar que los usuarios paralicen su trabajo. Cuando sea posible y como política del departamento de IT, se brindarán opciones a los usuarios para que continúe la operación mientras se realizan las acciones señaladas.
- Considerar que las bases de datos son activos de la compañía: Sobre todos los demás componentes, garantizar la estabilidad, seguridad y acceso a las bases de datos por los usuarios competentes, es de suma importancia para el modelo propuesto. En tal virtud, se aplicarán todas las acciones tendientes a esta garantía como respaldos periódicos, protección de bases de datos ante acciones informáticas de daño o espionaje.

- Normas de cuidado de los componentes: El departamento de IT deberá comunicar a todos los usuarios las normas de custodia y uso de los componentes físicos y digitales de la empresa; además, el seguimiento que se dé en las actividades del departamento permitirán evaluar la aplicación de las normas.
- Comunicación efectiva y eficiente: Se buscará que la comunicación entre el departamento de IT y los departamentos, usuarios y otros actores de la empresa, sea rápida, con ahorro de recursos, que permita la atención pronta a los requerimientos y sea controlada a través de registros cuidadosamente administrados.
- Implementación de actividades de evaluación y control del sistema: Se presentarán informes sobre las actividades de mantenimiento preventivo, correctivo, mejoras y cambios y actividades de capacitación por parte de los analistas e ingenieros del departamento de TI; adicionalmente, cada seis meses el coordinador del departamento desarrollará un informe para la gerencia, en base a los resultados obtenidos.

Anexo 6. Definición de componentes

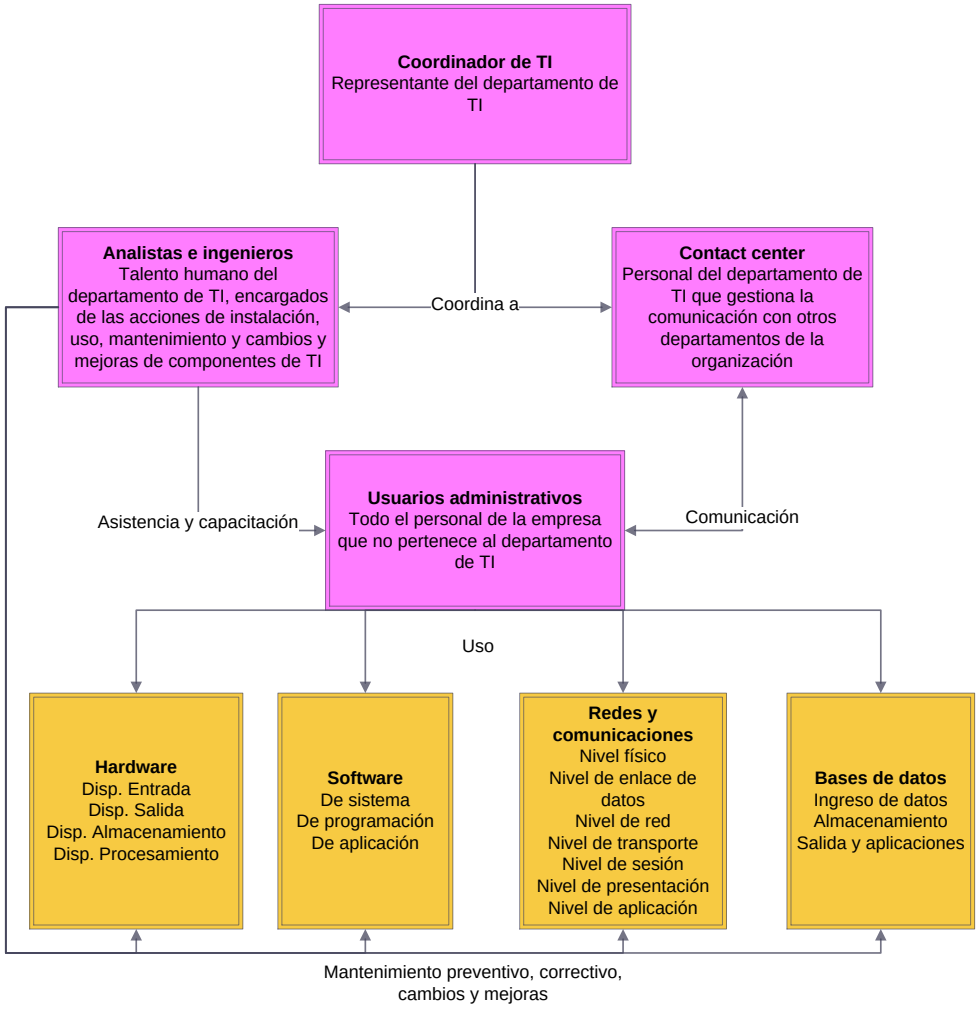


Figura 29. Definición de los componentes

Anexo 7. Evaluación de riesgos

Los riesgos asociados a los componentes se determinan en la siguiente tabla:

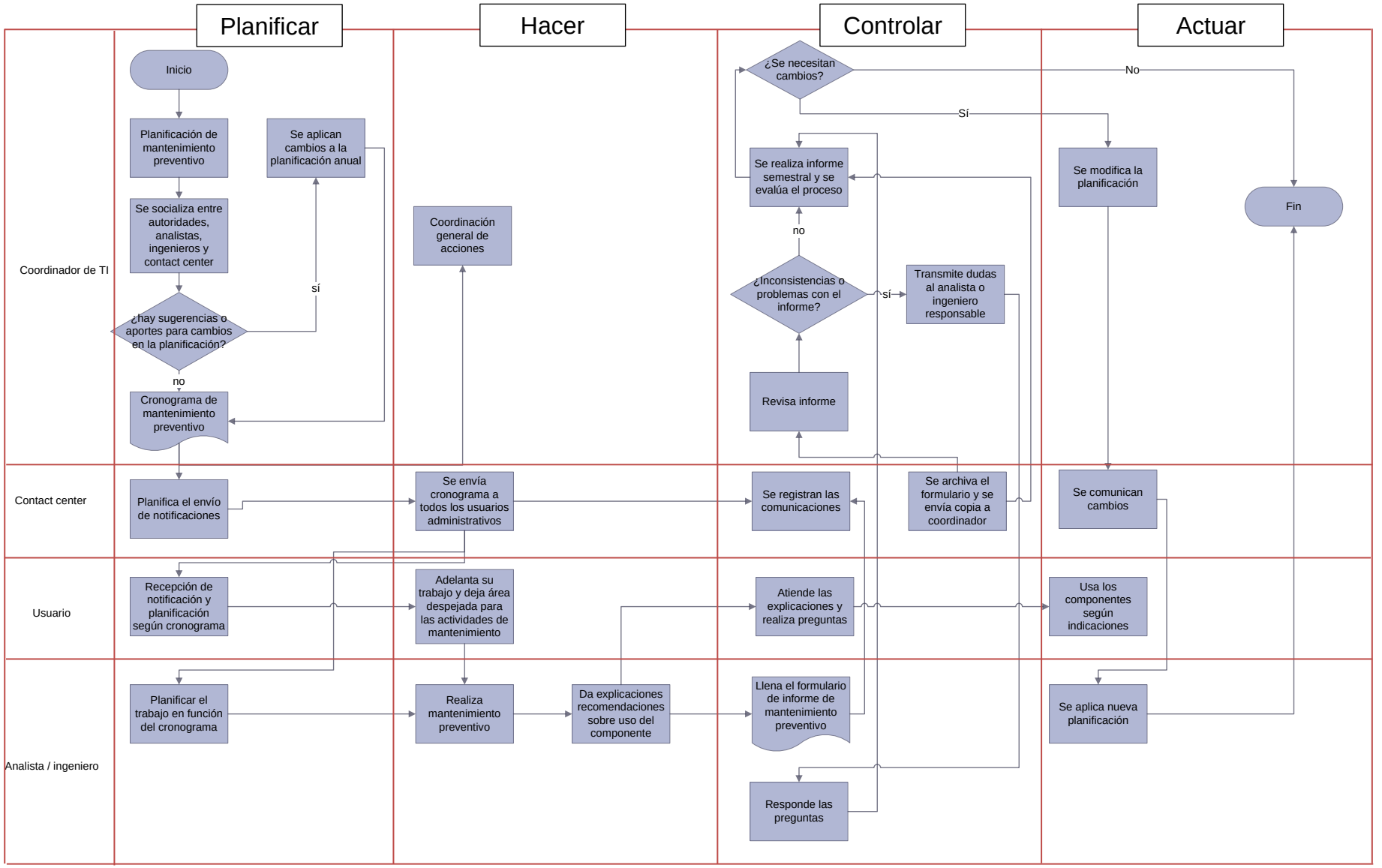
Tabla 19. Riesgos asociados a los componentes

			Mal Uso		Criminalidad		Daños físicos		
			Negligencia	Impericia	Robo	Virus	Incendio	Inestabilidad de corriente	Término de vida útil
Componentes	Impacto	Probabilidad	2	3	2	3	1	2	3
Hardware									
Disp. Entrada	1		2	3	2	3	1	2	3
Disp. Salida	1		2	3	2	3	1	2	3
Disp. Almacenamiento	3		6	9	6	9	3	6	9
Disp. Procesamiento	2		4	6	4	6	2	4	6
Software									
De sistema	3		6	9	6	9	3	6	9
De programación	2		4	6	4	6	2	4	6
De aplicación	1		2	3	2	3	1	2	3
Redes y comunicaciones									
Nivel físico	2		4	6	4	6	2	4	6
Nivel de enlace de datos	2		4	6	4	6	2	4	6
Nivel de red	3		6	9	6	9	3	6	9
Nivel de transporte	3		6	9	6	9	3	6	9
Nivel de sesión	2		4	6	4	6	2	4	6
Nivel de presentación	2		4	6	4	6	2	4	6
Nivel de aplicación	2		4	6	4	6	2	4	6
Bases de datos									
Ingreso de datos	3		6	9	6	9	3	6	9
Almacenamiento	4		8	12	8	12	4	8	12
Salida y aplicaciones	3		6	9	6	9	3	6	9

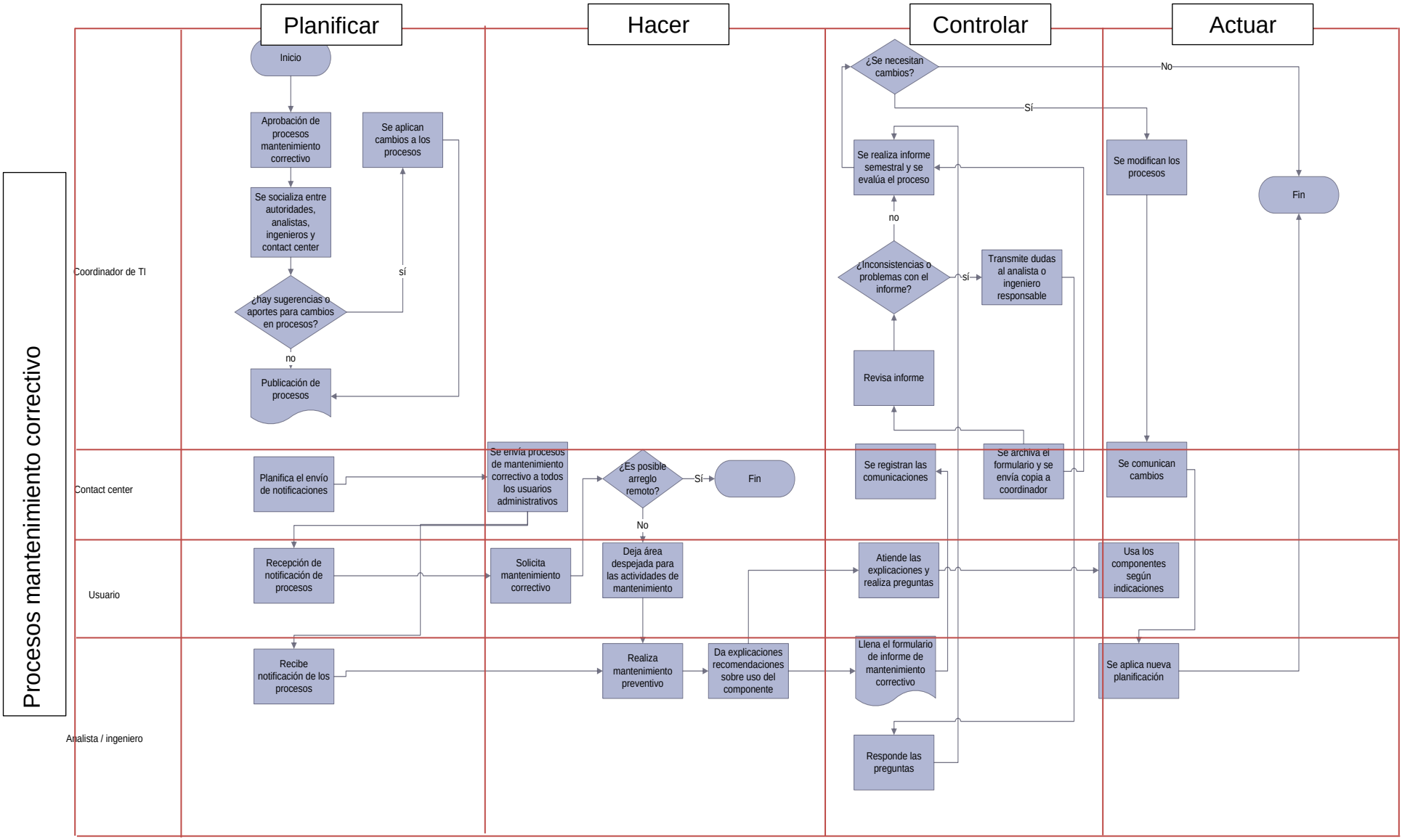
Para encontrar el valor ponderado se multiplica el nivel de impacto por la probabilidad de cada evento.

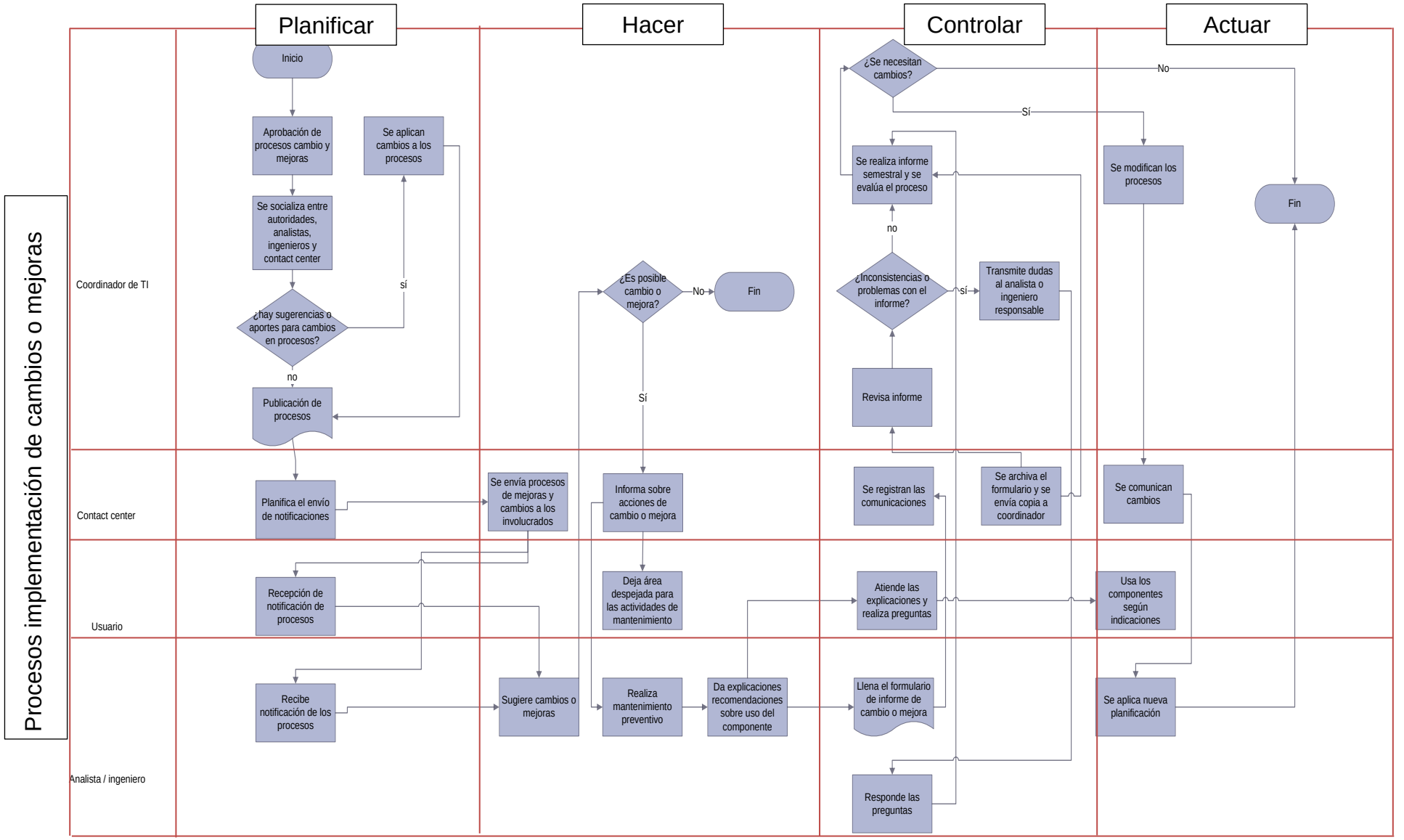
Anexo 8. Procesos

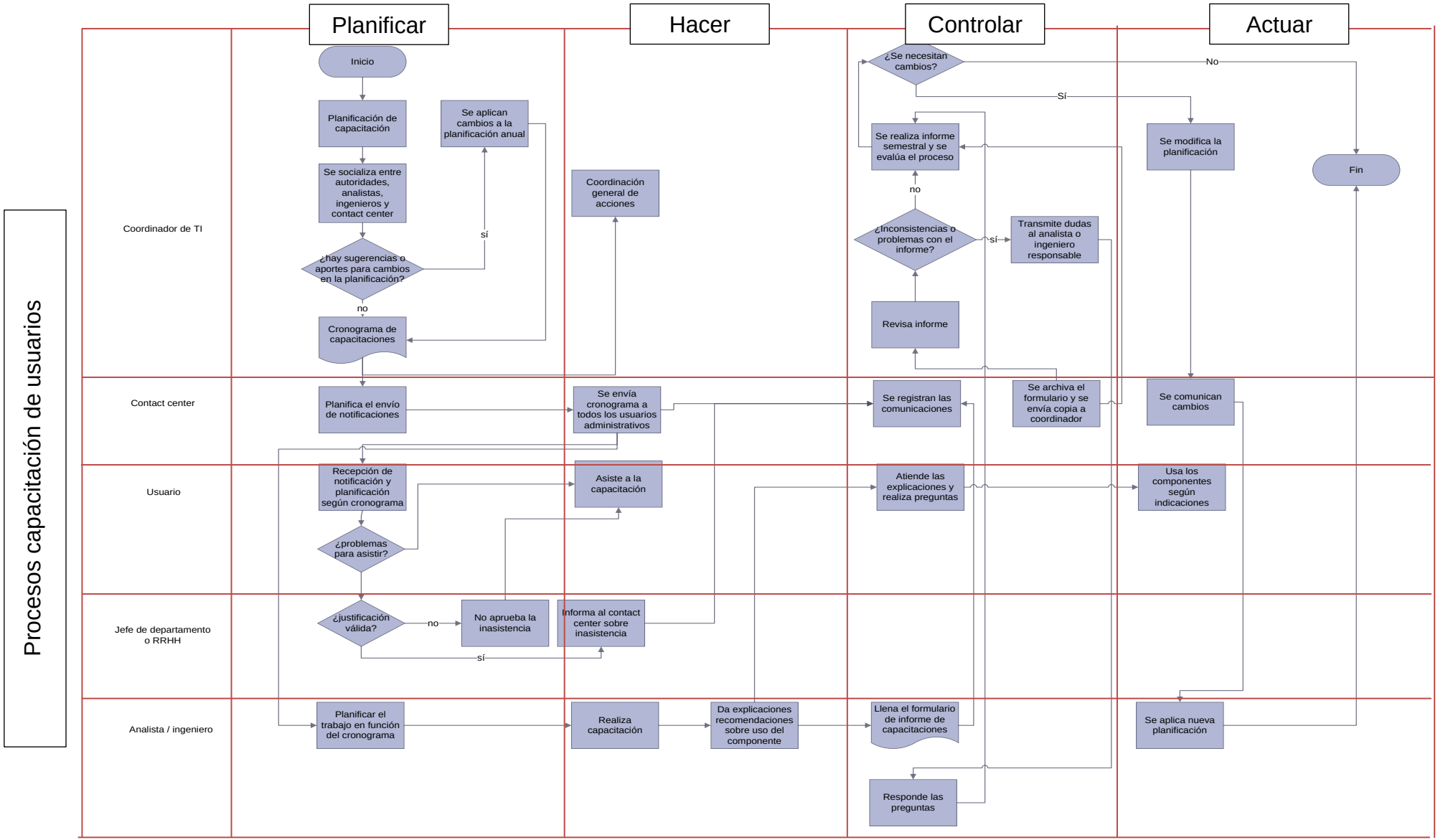
Procesos mantenimiento preventivo



Procesos mantenimiento correctivo




Procesos implementación de cambios o mejoras
Planificar
Hacer
Controlar
Actuar
Coordinador de TI
Contact center
Usuario
Analista / ingeniero
Inicio
Aprobación de procesos cambio y mejoras
Se socializa entre autoridades, analistas, ingenieros y contact center
¿hay sugerencias o aportes para cambios en procesos?
sí
no
Se aplican cambios a los procesos
Publicación de procesos
Planifica el envío de notificaciones
Recepción de notificación de procesos
Recibe notificación de los procesos
¿Es posible cambio o mejora?
No
Fin
Sí
Se envía procesos de mejoras y cambios a los involucrados
Informa sobre acciones de cambio o mejora
Deja área despejada para las actividades de mantenimiento
Sugiere cambios o mejoras
Realiza mantenimiento preventivo
Da explicaciones recomendaciones sobre uso del componente
¿Se necesitan cambios?
No
Sí
Se realiza informe semestral y se evalúa el proceso
no
¿Inconsistencias o problemas con el informe?
sí
Transmite dudas al analista o ingeniero responsable
Revisa informe
Se registran las comunicaciones
Se archiva el formulario y se envía copia a coordinador
Atiende las explicaciones y realiza preguntas
Llena el formulario de informe de cambio o mejora
Responde las preguntas
Se modifican los procesos
Fin
Se comunican cambios
Usa los componentes según indicaciones
Se aplica nueva planificación


Procesos capacitación de usuarios
Planificar
Hacer
Controlar
Actuar
Coordinador de TI
Contact center
Usuario
Jefe de departamento o RRHH
Analista / ingeniero
Inicio
Planificación de capacitación
Se socializa entre autoridades, analistas, ingenieros y contact center
¿hay sugerencias o aportes para cambios en la planificación?
sí
no
Se aplican cambios a la planificación anual
Cronograma de capacitaciones
Coordinación general de acciones
Planifica el envío de notificaciones
Se envía cronograma a todos los usuarios administrativos
Recepción de notificación y planificación según cronograma
Asiste a la capacitación
¿problemas para asistir?
¿justificación válida?
no
No aprueba la inasistencia
Informa al contact center sobre inasistencia
sí
Planificar el trabajo en función del cronograma
Realiza capacitación
Da explicaciones recomendaciones sobre uso del componente
¿Se necesitan cambios?
No
Sí
Se realiza informe semestral y se evalúa el proceso
no
¿Inconsistencias o problemas con el informe?
sí
Transmite dudas al analista o ingeniero responsable
Revisa informe
Se registran las comunicaciones
Se archiva el formulario y se envía copia a coordinador
Atiende las explicaciones y realiza preguntas
Llena el formulario de informe de capacitaciones
Responde las preguntas
Se modifica la planificación
Se comunican cambios
Usa los componentes según indicaciones
Se aplica nueva planificación
Fin

Anexo 9. Modelo de encuesta de evaluación de la propuesta

Nombre: _____

Cargo: _____

Por favor, califique el modelo presentado para la gestión de riesgos de las tecnologías de la información para ROCHE Ecuador S. A., tanto en su capacidad de solución y en su diseño. Marque con una X la calificación que usted asigna a cada uno de los parámetros, siendo 1 la menor y 5 la mayor calificación:

Parámetro evaluado	**1**	**2**	**3**	**4**	**5**
Funcionalidad (capacidad de solución del problema)					
Aplicabilidad legal (el modelo requiere poco o ningún cambio en la normativa interna vigente)					
Aplicabilidad operativa (se cuenta con los recursos humanos y materiales para la implementación del modelo)					
Aplicabilidad financiera (se cuenta con recursos financieros para los costes de implementación)					
Resistencia de los involucrados (dificultad para persuadir a los involucrados para adoptar el modelo)					

Gracias por su colaboración.