# ANÁLISIS DE LA RELACIÓN COSTO – BENEFICIO EN EL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE CALIDAD ISO 27001 EN LA EMPRESA GFI INFORMÁTICA COLOMBIA S.A.S

**Prácticas Empresariales: GFI INFORMÁTICA COLOMBIA S.A.S**

**Dirección Financiera y Administrativa**

**Estudiante:**

**BRAYAN LEONARDO GUERRERO RINCON Código: 319733**

**blguerrero33@ucatoli.edu.co**

**Asesor: Andrés Santana**

**arsantana@ucatolica.edu.co**

**UNIVERSIDAD CATÓLICA DE COLOMBIA**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**

**PROGRAMA ECONOMÍA**

**BOGOTÁ D.C.**

**2018**

**Cesión de derechos**


La presente obra está bajo una licencia:
**Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)**
Para leer el texto completo de la licencia, visita:
http://creativecommons.org/licenses/by-nc/2.5/co/

**Usted es libre de:**

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

**Bajo las condiciones siguientes:**

**Atribución** — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

**No Comercial** — No puede utilizar esta obra para fines comerciales.

# TABLA DE CONTENIDO

## LISTA DE ILUSTRACIONES



## LISTA DE TABLAS

## Resumen

En esta investigación se presenta una descripción de los fundamentos de la norma ISO 27001, como son el identificar el análisis de los procesos en la evaluación del riesgo, la definición de un plan de tratamiento de los riesgos o esquema de mejora, identificar las vulnerabilidades de la seguridad, el buscar una proporción en la mejora de las evaluaciones en los indicadores que midan la ejecución de los proyectos. Y más concretamente se estudia la relación existente entre los costes que para la empresa Gfi informática supone la implementación del sistema de calidad ISO 27001 y su posterior certificación junto con los beneficios esperados.

Para lograrlo fue necesario analizar los procesos actuales, hacer una propuesta de implementación, evaluar el costo de la propuesta analizando tarea a tarea en Microsoft Project para finalmente cruzarlo contra los beneficios esperados.



**Palabras Claves:** ISO 27001, costes, beneficios, calidad, mejora de procesos software.

**JEL:** A12, L24, M21, P11

## Abstract

This research presents a description of the fundamentals of the ISO 27001 standard, such as identifying the analysis of the processes in the risk assessment, the definition of a risk treatment plan or improvement scheme, identifying the vulnerabilities of security, looking for a proportion in the improvement of the evaluations in the indicators that measure the execution of the projects. And more specifically, the relationship between the costs that the Gfi IT Company entails the implementation of the ISO 27001 quality system and its subsequent certification and the expected benefits are studied.

To achieve this, it was necessary to analyze the current processes, make an implementation proposal, evaluate the cost of the proposal, analyzing task to task in Project, and finally cross it against the expected benefits.



**Keywords:** ISO 27001, costs, benefits, quality, improvement of software processes.

# 1. Introducción

A lo largo de la historia de la industria del software se han identificado buenas prácticas y conocimientos disponibles, es por esta razón que el estudio de la certificación ISO 27001, propuesto en esta investigación y sus concernientes objetivos y soluciones, empezaran a desarrollarse a partir de la información suministrada por parte de la empresa Gfi Informática, para con ello conocer el proceso que se ha venido desarrollando para la implementación de esta misma; y de esta manera abrir nuevos espacios para la investigación interna de la empresa como contribución importante del cargo.

Con esta investigación se da a conocer la amplitud del concepto de calidad, partiendo de la certificación ISO 27001 y su principal objetivo es el de analizar el coste – beneficio que conlleva implementar esta certificación dentro de la compañía. Por este motivo se plantea la pregunta, ¿La implementación de la certificación ISO 27001 en la compañía Gfi Informática trae consigo un beneficio progresivo para la empresa? El marco para llevar a cabo este trabajo se refiere al contexto empírico de la empresa Gfi Informática y específicamente el área de PMO (Oficina de Control de Proyectos), el cual es el departamento de calidad, en donde se planifican, controlan y gestionan los proyectos de la compañía

Por lo anterior, en este proyecto se realizó una revisión teórica de los costos y beneficios de la implementación de la norma, además de una medición de los costos del proceso y una proyección de los beneficios esperados; como son mayores oportunidades en el mercado nacional e internacional, asimismo permite aplicar técnicas empresariales más actuales al igual que mejorar continuamente la gestión realizada por la compañía.

# 2. Marco teórico

Un paso clave en la formulación de este trabajo de investigación consiste en identificar cómo se comporta el coste – beneficio en la ejecución de la certificación de calidad ISO 27001 dentro de las empresas de software, además de porque ha habido un creciente aumento de empresas que buscan certificarse en dicha norma. Según Ordás, C. J. V., Sánchez, E. F., & García-Miranda, C. E. (2001) en un mercado globalizado, donde la oferta ha aumentado rápidamente y en el que los competidores se encuentran en cualquier parte del mundo, la calidad se ha convertido en una estrategia vital para competir. Prueba de ello es el crecimiento exponencial del número de empresas certificadas.

## 2.1.Calidad

Uno de los aspectos más complejos del área de calidad, es establecer hasta qué punto el producto o servicio se clasifica como excelente.

*Existen ciertos artículos que se facturan por unidades separadas, las cuales pueden ser; televisores, minicomponentes, etc. en el momento en el que el cliente utilice el televisor y este funcione de manera adecuada, el cliente va a estar satisfecho con el producto, pero hay otros factores que permiten que este televisor funcione de una manera adecuada, como, por ejemplo; el cable de corriente, las tomas eléctricas, etc. Por eso es importante la especificación unitaria sobre la cual se basa la calidad. La cantidad unitaria o unidad de garantía debe estar especificada en las cifras de calidad. Una pregunta clave que utiliza Pablo Valderrey Sanz en su libro "Herramientas para la calidad total" es ¿cuál es la unidad de longitud del cable para la cual se garantiza la calidad?, ¿cuántas pruebas debo hacer para garantizar un software? La cantidad unitaria puede no ser muy viable tanto*

*para los compradores como para los vendedores, por eso la importancia de los controles y métodos para evaluar y cuantificar la calidad. "Existen varias empresas que tienen como resultado productos defectuosos y reciben reclamaciones porque la alta dirección y los supervisores no proporcionan los medios para medir la calidad* (Sanz, 2013)

Una de las formas que menciona Sanz para cuantificar la calidad, es estableciendo límites de tolerancia, esta permite medir la calidad aceptable mediante un intervalo y por ende también se establece la calidad no aceptable.

Establecer medidas de calidad puede ser muy complejo para las empresas, muchas de ellas tienen que depender de interpretaciones sensoriales, como, por ejemplo; calidad de los servicios, olor, sabor, sonido, aquellas medidas dependen de los sentidos humanos y tendrán una valoración muy subjetiva. Para ese tipo de casos es importante que la valoración sea realizada en grupo y no por persona, debido a que en grupo pueden compartir diferentes puntos de vista y llegar a un mutuo acuerdo.

"*La calidad de un software es una preocupación muy importante para la ingeniería de software, especialmente cuando estamos hablando de servicios de desarrollo de programas informáticos en donde deben de estar disponibles las 24 horas del día"* (Paiva, 2016)

### 2.1.1. ISO 27001:2005

Las empresas tienen estándares internacionales y nacionales los cuales requieren para poder cumplir con las especificaciones solicitadas por los clientes. Estos estándares, ayudan a organizar y sistematizar de manera más eficiente los procesos y operaciones que ejecuta la empresa. Una vez la empresa haya cumplido con estos estándares, se puede decir

que tiene implementado un sistema de gestión de calidad. *"Todos los sistemas se encuentran normados bajo un organismo internacional no gubernamental llamado ISO, International Organization for Standardization (Organización Internacional para la Estandarización)"* (Sistemas de la calidad-historia y definición, 2011)

La norma ISO 27001 se concibe al momento de proponer un sistema de gestión de la seguridad de la información (SGSI), el cual se acopla de acuerdo a las necesidades e imparcialidades de los requisitos de seguridad, procesos y estructura de la organización. Por esta es importante implementar un sistema de mejora continua, el cual ayude a que los clientes tengan un mayor grado de satisfacción.

### 2.1.2. Método SGSI

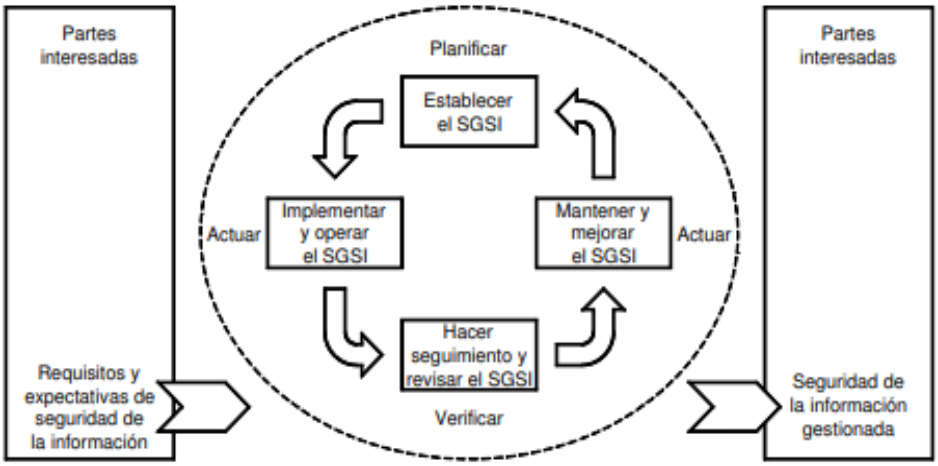
La empresa Gfi informática deberá construir, implementar, aplicar, realizar un acompañamiento, examinar, mantener y optimizar un SGSI argumentado, el cual se establezca en el marco de todas las actividades internas y externas del negocio de la organización, para con ello comprender y minimizar los riesgos que se afronta.

La finalidad que se deben asumir de esta norma, se basan en el modelo PHVA (Planificar-Hacer-Verificar-Actuar), el cual tiene como objetivo brindar soluciones para mantener una competitividad en cuanto a los productos y servicios prestados, para así mejorar la calidad, productividad y con ello maximizar el beneficio, a partir de la reducción de costos y lograr de esta un aumento en la rentabilidad de la empresa.

*"La metodología PHVA nos permitirá solucionar el problema identificado, atacando las causas que lo originan, y además nos permitirá desarrollar un sistema de*

*mejora continua orientado a al incremento de la productividad."* (Gutiérrez Beltrán, I., & Serpa Valdivia, C., 2015)

**ILUSTRACIÓN 1. MODELO PHVA APLICADO A LOS PROCESOS DE SGSI**




Fuente: NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 (2006).

Figura 1. Modelo PHVA aplicado a los procesos de SGSI

2.1.2.1.Establecimiento y gestión

Para establecer el SGSI, la empresa debe definir primero que todo el alcance y limite en cuanto a sus activos, donde quiera implementar dicho sistema; en segundo lugar, debe definir políticas en las cuales deberá incluir (Marco referencias, requisitos legales o reglamentarias, estrategias en cuanto a la gestión de riesgos); en tercer lugar deberá definir un enfoque organizacional en el cual se establezcan las valoraciones del riesgo; en cuarto lugar las identificaciones de los riesgos; en quinto lugar el análisis y posterior evaluación de los riesgos; en sexto lugar, deberá identificar y tranzar un tratamiento para dichos riesgos; y finalmente se deberá declarar la aplicabilidad del sistema, en la cual se proporcione un resumen de las decisiones concernientes al tratamiento de los riesgos de la organización.

La norma ISO 27001 habla de establecer el SGSI en el numeral 1.2; numeral 4.2.1, literal c, e; numeral 5.1, literal f.

Para implementar y operar el SGSI la empresa deberá en primer lugar formular un plan de para el tratamiento de riesgos el cual asemeje (acciones, responsabilidades, prioridades en cuanto a los riesgos de seguridad de la información); en segundo lugar deberá implementar controles con el fin de lograr cumplir los objetivos establecidos; en tercer lugar, deberá definir controles para la eficacia y eficiencia de los procesos; en cuarto lugar, convendrá la implementación para la programación de formación y toma de conciencia, y finalmente deberá gestionar operación y recursos para la puesta en marcha del SGSI dentro de la organización.

La norma ISO 27001 habla de implementar y operar el SGSI en el numeral 5; numeral 4.2.1, literal g; numeral 5.1, literal f; numeral 4.2.3 literal c; numeral 5.2.2.

2.1.2.2.Seguimiento y revisión

Para realizar un seguimiento y revisión del SGSI la empresa deberá en primer lugar ejecutar procedimiento para detectar (rápidamente los errores, los incidentes e intentos de violaciones de la seguridad, divisar sobre los futuros eventos de seguridad y posteriores acciones a tomar); en segundo lugar revisar las valoraciones de los riesgos en cuanto a la misma organizaciones, activos, objetivos y procesos del negocio; en tercer lugar, deberá realizar auditorías internas; en cuarto lugar, convendrá revisiones periódicas de los procesos de la compañía; en cuarto lugar, se actualizará los planes de seguridad; y finalmente deberá registrar las respectivas acciones y eventos tomados sobre el trabajo del SGSI dentro de la organización.

La norma ISO 27001 habla sobre el seguimiento y revisión del SGSI el numeral 6; el numeral 7.1 y numeral 4.3.3

2.1.2.3.Mantenimiento y mejora

Para realizar el mantenimiento y mejora del SGSI la empresa deberá en primer lugar identificar las mejoras propuesta por la norma; en segundo lugar, emprenderá acciones correctivas y preventivas con el fin de asegurar los procesos de seguridad de la información; en tercer lugar, deberá comunicar las acciones pertinentes para ver cómo llegar a los acuerdos de cómo se debe proceder y finalmente la organización asegurar las mejoras en cuanto a los objetivos previstos por el SGSI dentro de la organización.

La norma ISO 27001 habla sobre el mantenimiento y mejora del SGSI el numeral 8.2 y 8.3.

2.1.2.4.Estructura para la continuidad del negocio

Se deben identificar los futuros acontecimientos que puedan producir complicaciones en los procesos del negocio junto con la contingencia y el impacto de dichas complicaciones, así como sus derivaciones en cuanto a la seguridad de la información.

Para consentir una estructura de continuidad del negocio se debe designar un jefe de pruebas al igual que pruebas de desarrollo; en las cuales establezca una revisión periódica para asegurar la actualización y eficacia de la continuidad del negocio.

La norma ISO 27001 habla sobre la estructura para la continuidad del negocio del SGSI en la tabla A.1. (Continuación)

2.1.2.4.1. Jefe de pruebas

Las asignaciones de las actividades siempre van a estar guiadas por un superior, en este caso, guiar la realización de las pruebas pertinentes a cada proyecto, pero guiar no es su única función. Debe estar ahí para la gestión y los recursos necesarios de las pruebas. De esta manera, puede planificar un proyecto, teniendo en cuenta el contexto, los objetivos y los riesgos que debe correr. Se entiende por planificar, tener en cuenta los enfoques de la prueba, calcular el tiempo, esfuerzo y coste de las pruebas. Pero además debe coordinar y contribuir con una estrategia de pruebas para la organización.

2.1.2.4.2. Pruebas de desarrollo

Las pruebas de desarrollo que se adelantan en cada proyecto tienen como objetivo la identificación de defectos, facilitar la información para la toma de decisiones y aumentar la confianza en el nivel de calidad. Como estamos hablando de la realización de las pruebas en diferentes ambientes, es muy importante la verificación del componente o sistema.

## 2.2. Diagnóstico de calidad: diagrama de Pareto

El principio de Pareto establece que debe haber una clasificación de los factores según su peso o importancia dentro de un proceso. Según esa clasificación, el 20% de los factores más determinantes, permite que el otro 80% sea una consecuencia. Por eso es de vital importancia determinar las causas o defectos que más influyen en un proceso. *"Los que tienen sobrecarga de la información también encuentran que el 80% de la información recibida no es de vital importancia, solo el otro 20% es de importancia crítica al trabajo, proceso, cliente o una toma de decisión"*. (Denton, 2003)

### 2.3. Diagnóstico de calidad: ciclo PHVA (Planear, Hacer, Verificar, Actuar)

Es un ciclo de mejora continua propuesto por Shewhart en donde es posible gestionar cualquier tipo de proceso eficientemente. *"Así, el ciclo: Planificar-Hacer-Verificar-Actuar desarrollado inicialmente en la década de 1930 por Walter Shewhart y popularizado luego por W. Edwards Deming en Japón, es un concepto básico y sencillo para dinamizar la gerencia del día a día.* (Paipa, 2012)

### 2.4. Análisis Coste – beneficio en la implementación de ISO/IEC 27001

*La característica que distingue al análisis de costo beneficio es el intento de llevar al máximo posible la cuantificación los beneficios y costos en términos monetarios. Sin embargo, el análisis muy pocas veces logra ese ideal de medir todos los beneficios y costos en términos monetarios…*[1] (Martínez, J. A, 2014, p.3).

Dentro de lo planteado por Martínez para el análisis del coste beneficio, señala que su utilización se demuestra en el momento de tomar decisiones, y de esta manera no se encuentra limitado a una disciplina académica o campo en particular, o en proyectos privados o públicos. Además, expresa que el coste – beneficio es un hibrido de diversas técnicas (dirección, gestión, planeación, finanzas y diversos campos de ciencias sociales). Y por lo cual los costes como los beneficios se presentan en unidades de medición estándar (usualmente monetarias), para que se puedan comparar directamente.

De esta forma, Martínez esboza la idea básica del análisis coste – beneficio la cual consiste en que no importa que tan buena sea la solución al problema, o la alternativa o propuesta esta jamás es gratis.

[1] Se le atribuye al economista francés Jules Dupuit su uso formal en el siglo XIX.

Dentro de los principios de la economía propuestos por Gregory Mankiw, se hace mención al costo como ***aquello a lo que se renuncia para conseguirlo***, así las decisiones se basan en un análisis costo – beneficio, en la cual se plantea cómo los individuos deben afrontan disyuntivas, de tal forma que deberán concertar los costes y beneficios que conllevan dichas decisiones.

*"Debido a que al tomar decisiones los individuos enfrentan disyuntivas, es necesario comparar los costos y los beneficios de los diferentes cursos de acción que pueden tomar. Sin embargo, en muchos casos el costo de una acción no es tan evidente como podría parecer al principio."* (Mankiw, G, 2012, p.6)

La empresa Gfi informática Colombia intenta acoger la norma ISO/IEC 27001[2], para de esta manera adoptar los beneficios que conlleva dicha norma. Algunos de ellos son: el suprimir los riesgos de la información, reducir la probabilidad y el impacto de los incidentes de seguridad, certificarse en estándares de alta calidad, estructurar la evaluación de riesgos, focalizar los gastos de seguridad informática donde esto produzca mayor ventaja y retribución.

De igual manera la empresa deberá acoger ciertos costes como son: una mayor gestión de proyectos, lo que conllevará recursos para dichos proyectos; al generarse cambios en la organización deberá asumir recursos de la entidad; diseño, desarrollo, pruebas e implementación de los proyectos; certificación; visitas de seguimiento y la operación y mantenimiento en curso de la operación.

[2] Estándar para la certificación del sistema de gestión de la información.

La norma ISO 27001 que se enuncia dentro de las implicaciones financieras para la compañía, propuesta por Gary Hinson el 15 de febrero de 2008, tiene como finalidad el identificar el modelo genérico de coste – beneficio el cual establece dos parámetros (Costos de la implementación y beneficios de la implementación).

### 2.4.1. Beneficios

#### 2.4.1.1.Reduce los riesgos de seguridad de la información

- Se fortalece la seguridad de la información en para con ello dar importancia a los requisitos en cuanto al control de la seguridad de la información del negocio.
- Actualización de las políticas actuales de la compañía, además de realizar controles periódicos en cuanto a la seguridad de la información.
- Reducir la probabilidad de futuras amenazas o vulnerabilidades no reconocidas a la información de la seguridad del negocio.
- Enfoques en cuanto a la gestión de riesgos profesionales, asimismo generar un sistema de tiempo en el cual se centre en las áreas de mayor riesgo.
- Se acrecienta la capacidad de transferir riesgos de manera selectiva, lo cual conllevara ha ahorros de costes
- Se capacitará al personal para lograr la reducción de riesgos.

#### 2.4.1.2. Beneficios de la estandarización

- Suministrar un "*denominador común*" para conseguir la construcción de un sistema especializado y lograr ahorrar en costes.
- Evitar la revisión por separado de controles de cada sistema del negocio.

- Consentir una metodología común en la cual se evaluarán las necesidades de seguridad de la información del negocio.
- Ahorrar tiempo, dinero y esfuerzo mediante el ajuste de buenas prácticas.

2.4.1.3. Beneficios de disponer de un enfoque estructurado

- Proveer impulsos para la revisión de sistemas, datos, flujos de información para lograr una reducción en la sobrecarga laborar y con ello mejorar la calidad de la información.
- Proporcionar mecanismos para evaluar el rendimiento y acrecentar progresivamente la línea base de referencia de la seguridad de la información.

2.4.1.4.Beneficios de la certificación

A continuación, se muestran los beneficios de la certificación ISO 27001 que se estipulan en el informe financiero del modelo genérico de coste – beneficio planteado por Hinson, G. (2008):

- *Satisfacer las peticiones de partners y proveedores para justificar los controles de seguridad de la información sin necesidad de atender consultas individuales o proporcionar información confidencial* ***- ahorro de costes y reducción de riesgos.***
- *Proporciona un estándar de seguridad de la información racional e independiente con el que evaluar la calidad de los controles en partners y proveedores* ***- ahorro de costes y reducción de riesgos***
- *Potencialmente, ofrece una ventaja de marketing en los primeros en adoptar la certificación ("insignia de honor" similar a la norma ISO 9000 de calidad)* ***– beneficios en marketing/ventas***

- *La resistencia a demostrar el cumplimiento de la norma ISO/IEC 27001 puede ser tomado como un signo de vulnerabilidad. Certificar el cumplimiento puede promover la imagen de la empresa como un socio seguro para los negocios* ***- ventaja competitiva.***
- *Ayuda a garantizar a las partes interesadas, los auditores, los reguladores de la industria, etc. que la organización está activamente minimizando los riesgos de seguridad de la información mediante la demostración del compromiso de la organización en seguridad de la información (gobierno corporativo o aspectos debidos a diligencia que aporten potenciales exposiciones a riesgos de la seguridad de la información)* ***- ahorro de costes y reducción de riesgos*** (p.3)***.***

2.4.1.5.Evitar Costes

- Contiguamente se comprime o limita las quejas por fallos en la seguridad de la información del negocio lo cal contribuirá al ahorro de costes y su posterior reducción en cuanto a los posibles riesgos.

2.4.2. Coste

2.4.2.1.Costes relacionados con los cambios organizacionales

- Necesidad de enaltecer la concienciación de la organización (personal y directivo).
- Ajuste/conciliación de las políticas, ordenamientos, prácticas, etc. vigentes en la seguridad de la información.

2.4.2.2.Costes de diseño & desarrollo

- Escrutinio y reajuste de las políticas, ordenamientos, prácticas, etc., vigentes en la seguridad de la información.

- Se generarán nuevas políticas, ordenamientos, prácticas, etc., vigentes en la seguridad de la información.
- Se diseñará una nueva estructura de la arquitectura de los controles.

2.4.2.3. Costes de la implementación

- Los costos únicos iniciales para reconstruir y/o perfeccionar diversos controles existentes para cometer con la política de la norma
- Costes de en cuanto asumir el conocimiento, formación y especialización de la norma.

2.4.2.4. Costes de certificación

Así mismo, los costes de la certificación ISO 27001 que se estipulan en el informe financiero del modelo genérico de coste – beneficio planteado por Hinson, G. (2008):

- *Visitas de pre-certificación y de certificación iniciales por entidades de certificación acreditadas por la norma ISO/IEC 27001*.
- *Riesgo de no alcanzar la certificación a la primera (cualquiera de los motivos que causó el fracaso representan ellos mismos riesgos inaceptables para seguridad de la información – retraso de la certificación más probable que un fracaso completo).*
- *Tiempo dedicado por el personal/dirección en las visitas anuales de seguimiento*
- *Recertificación trianual (examen más amplio en las áreas de revisión y, por lo tanto, impacto mayor, aunque todavía relativamente menor).*
- *Todos estos costos se reducirán al mínimo todos si logramos una implementación de alta calidad a través de nuestros propios esfuerzos* (p.3).

2.4.2.5. Costes de Mantenimiento del SGSI en curso

- Revisión/mantenimiento anual de las políticas, ordenamientos, prácticas, etc., de seguridad de la información para salvaguardar el desempeño de la norma.

## 2.5.Metodologías de implementación

### 2.5.1. Metodologías tradicionales

Basadas en el desarrollo de las metodologías, aquellas con mayor énfasis en la planificación y control del proyecto, en especificación precisa de requisitos y modelado, son llamadas metodologías tradicionales o pesadas. Estas metodologías imponen una disciplina de trabajo sobre el proceso de desarrollo del software. Se hace énfasis en la planificación total de todo el trabajo a realizar y una vez que está todo detallado, comienza el ciclo de desarrollo del producto software. En estas metodologías se encuentran: RUP (Rational Unified Procces), MSF (Microsoft Solution Framework), Win-Win Spiral Model e Iconix. (Acuña, s.f.)

### 2.5.2. Metodologías ágiles

*"Es una metodología basada en el trabajo incremental e iterativo. Pensada en proyectos con requerimientos cambiantes, predispuestos al cambio, flexibles, cuyo desarrollo y mantenimiento se adapten según las necesidades, depositando una gran confianza en los equipos de trabajo suponiendo que son autosuficientes."* (Moya, 2017). Las metodologías ágiles más usadas según (Garzás) son: Scrum, Programación extrema-XP y KANBAN

La metodología ágil utilizada por la compañía Gfi informática es la Scrum.

### 2.5.3. Metodología Scrum

Es un método de desarrollo iterativo donde el producto se desarrolla en incrementos. El desarrollo ocurre en intervalos de tiempos cortos llamados Sprints que se mapean en las etapas de desarrollo. Cada sprint termina con un entregable, una demostración para el cliente. Después de una demostración, ocurre una nueva asignación de prioridades que implica la creación de nuevas tareas (Linden, 2018).

## 2.6. Microsoft Project

*"Es una herramienta para la planeación y control de proyectos dotado de los elementos que facilitan crear y programar las tareas, administrar recursos, revisar costos y generar reportes para análisis y presentación, con todas las ventajas que caracterizan un agradable ambiente gráfico.*

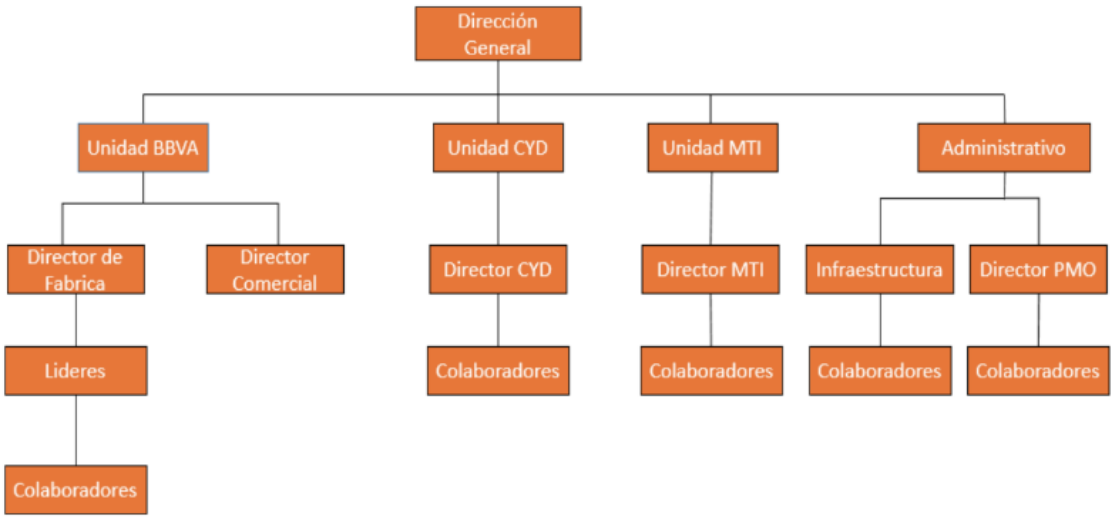
*Además de las características de versiones anteriores que permiten un buen control de proyectos, las mejoras a partir de la versión 2002, facilitan aún más la administración, creación y transmisión de información de proyectos. La forma en que se despliega la información facilita la organización de tareas en un proyecto, la actualización de datos y la supervisión de su desarrollo general, pues permite desplegar la información de distintas maneras para revisar varios aspectos del proyecto al mismo tiempo". (*Pérez Penagos, M. L., & Vargas Gualtero, I. R, 2018, P.43)

# 3. Descripción de la entidad

La información que se presenta en el siguiente epígrafe ha sido construida a partir de la revisión de fuentes primarias (documentos de la compañía, personal encargado) y fuentes secundarias tales como la página web institucional:

Gfi Informática Colombia pertenece al Grupo Internacional Gfi, multinacional de consultoría, outsourcing e integración de sistemas en Tecnologías de la información, con presencia en 20 países y un equipo de trabajo de más de 16.000 colaboradores. En Colombia, Gfi tiene amplio reconocimiento en sectores como Banca y Gobierno, con oficinas en Medellín y Bogotá. Ofrecemos una atractiva carrera profesional en función de la experiencia y potencial personal dentro de una compañía en continua evolución y con un sólido crecimiento, participando en diversidad de proyectos en tecnologías punteras. Incorporación a un equipo de profesionales altamente cualificados, trabajando en un ambiente agradable, innovador y flexible. Adquiriendo una formación en competencias tecnológicas de acuerdo con las exigencias de los proyectos y clientes. Teniendo siempre en cuenta las nuevas ideas que permitan el avance en la industria tecnológica.

**ILUSTRACIÓN 2 ORGANIGRAMA DE GFI INFORMÁTICA COLOMBIA S.A.S.**




Fuente: Gfi informática

Figura 2. Organigrama de Gfi Informática

La compañía cuenta con diferentes departamentos de trabajo, dentro de ellos se encuentra la PMO (Oficina de Control de Proyectos), el cual es el departamento de calidad, en donde se planifican, controlan y gestionan sus proyectos. En la actualidad, Gfi Informática cuenta con tres grandes clientes como lo son BBVA Seguros, Thomas MTI y el Ministerio de Defensa Nacional, para quienes se desarrollan software y aplicaciones. Estos proyectos pasan por el área de calidad, desde allí se analiza un factor crucial que compone el *"concepto de calidad, como por ejemplo: rendimiento, en donde hace referencia a las características primarias del servicio y a los aspectos vinculados a las especificaciones básicas exigidas por los usuarios del servicio"* (María D. Moreno-Luzón, 2001). Según este análisis, la empresa Gfi Informática determina si los proyectos se están llevando a cabo con el rendimiento esperado o no. Si un proyecto no lleva un óptimo rendimiento, se le conoce como un proyecto impactado. Estos proyectos impactados son una gran amenaza para la compañía, por los largos tiempos de ejecución en los que se desarrollan. La relación entre tiempo y costo es directamente proporcional, por lo que a mayor tiempo de ejecución, mayores costos tendrá el proyecto.

# 4. Plataforma Estratégica

## 4.1.Políticas generales:

Gfi Informática Colombia S.A.S., desarrolla sus actividades de consultoría, arquitectura, desarrollo e ingeniería informática promoviendo la protección a la vida y a la salud de sus empleados propios, contratistas, visitantes, practicantes y comunidad en general, por tal razón la Alta Dirección y sus colaboradores se comprometen a cumplir con la siguiente política integral:

- Desarrollar y controlar eficazmente procesos y servicios que satisfagan las necesidades de nuestros clientes y otros grupos de interés.
- Promover y mantener buenos niveles de calidad, seguridad y salud en el trabajo y ambiental, con el fin de la eficaz realización de nuestras operaciones con impacto en la calidad de los servicios suministrados a nuestros clientes.
- Proteger la seguridad y salud de todos los colaboradores mediante la identificación de los peligros, evaluación y valoración de riesgos y establecimiento de controles.
- Cumplir con los requisitos legales vigentes y aplicables en materia de calidad, seguridad y salud en el trabajo y ambiental.
- Asignar los recursos necesarios que permitan la mejora continua del Sistema Integrado de Gestión mediante la implementación de programas y acciones basadas en buenas prácticas organizacionales, que contribuyan al bienestar del colaborador en el desarrollo de su vida laboral, a minimizar el impacto que las actividades e infraestructuras puedan causar sobre el medio ambiente y la calidad del servicio y satisfacción de las partes interesadas.

Esta Política integral debe ser conocida y practicada por todas las personas que conforman la organización, por lo cual será actualizada, divulgada y comunicada de forma permanente y estará disponible para todos nuestros colaboradores y partes interesadas.

### 4.2.Portafolio De Productos y/o Servicios

La empresa Gfi informática cuenta con una amplia gama de productos, y de igual manera se enfoca en diferentes líneas de actividad entre las que se encuentran:

**ILUSTRACIÓN 3 LAS 6 LÍNEAS DE ACTIVIDAD**


Fuente: GFI Marketing

Figura 3. Líneas de actividad

**TABLA 1 PORTAFOLIO DE PRODUCTOS Y/O SERVICIOS**

| PRODUCTO | DEFINICIÓN |
|---|---|
| GFI LanGuard™ | **GFI LanGuard™:** Le permite analizar, detectar, evaluar y rectificar vulnerabilidades de seguridad en su red y en los dispositivos conectados. Proporciona una imagen completa de su red y ayuda a mantener la seguridad con el mínimo esfuerzo. |
| GFI OneGuard™ | **GFI OneGuard™:** Plataforma de administración de TI que permite a los administradores de TI centralizar, simplificar y automatizar el proceso de gestión del estado de seguridad de máquinas, recursos de red y usuarios. |
| GFI OneConnect™ | **GFI OneConnect™:** Plataforma de administración de correo electrónico basada en la nube para su negocio. Protección avanzada contra spam y malware, archivo de correo electrónico y continuidad del correo electrónico para Exchange. |

| | |
|---|---|
|  | **GFI EndPointSecurity™:** Permitiendo mayor tiempo de actividad mediante la recogida, normalización, análisis, clasificación y consolidación de la información de los registros desde múltiples orígenes de toda su red. |
|  | **GFI EventsManagers™:** Permitiendo mayor tiempo de actividad mediante la recogida, normalización, análisis, clasificación y consolidación de la información de los registros desde múltiples orígenes de toda su red. |
|  | **GFI MailEssentials™:** GFI MailEssentials ofrece protección integral, configurable, en múltiples capas, contra las amenazas actuales del correo. |
|  | **GFI WebMonitor™:** Mediante su nuevo modo Proxy Transparente, GFI WebMonitor se integra perfectamente en sus redes cableadas e inalámbricas y no son necesarios cambios en los equipos. |
|  | **GFI Archiver™:** Con GFI Archiver, todo el correo y los archivos de la empresa son archivados automática y centralizadamente en un entorno seguro al que se puede acceder rápidamente y en el que se puede buscar fácilmente. |
|  | **GFI FaxMaker™:** Mejore las comunicaciones por fax, modernice los procesos empresariales y aumente la productividad con faxing automático, seguro y conforme. |
|  | **GFI FaxMaker™ Online:** Servicio de fax por Internet que no requiere ninguna instalación. Libere su negocio de líneas telefónicas, módems, paneles de fax y software adicional. Cambie la forma en que su empresa envía faxes mediante el uso de su correo electrónico para enviar y recibir faxes en línea. |

Fuente: Elaboración Propia

Figura 4. Portafolio de Productos Y/O Servicios

## 5. Objetivos de la práctica

### 5.1.Objetivo General

Analizar la relación costo beneficio de la implementación de la norma ISO 27001 en la empresa Gfi informática Colombia S.A.S.

### 5.2.Objetivos Específicos

- Efectuar un análisis del estado actual de la empresa Gfi Informática Colombia S.A.S con base en la norma ISO 27001.
- Diseñar las bases para la implementación de la norma ISO 27001 en la empresa Gfi informática Colombia S.A.S.
- Evaluar los costos de la implementación de la norma ISO 27001 en la empresa Gfi informática Colombia S.A.S.
- Evaluar los beneficios de la implementación de la norma ISO 27001 de la empresa Gfi informática Colombia S.A.S.

## 6. Funciones desempeñadas

- Las funciones del practicante dentro del área administrativa y financiera de la compañía Gfi Informática Colombia S.A.S, se centran en el análisis del estado de resultados para el posible cumplimiento de los objetivos financieros y así mantener el equilibrio del mismo dentro de la compañía.
- Apoyar en el desarrollo de proyectos e implementaciones integradas, de gran alcance, complejas y de mucho valor para la organización.
- Gestionar en paralelo varios proyectos - tareas asignadas, planificación, administración del tiempo, control y seguimiento, a fin de cumplir con los objetivos y cronogramas planificados.
- Recolectar, procesar y analizar información. Construir, actualizar flujos de procesos y documentos normativos.

- Liderar / participar en la ejecución de proyectos de mejora de la División, respondiendo por los entregables asignados, objetivos y cronogramas.
- Gestionar la preparación y diseminación de los reportes de situación y asistir en su interpretación y aplicación.
- Identificar de forma oportuna las posibles restricciones o riesgos en el proyecto - tareas asignados con impacto en sus entregables, cronograma y objetivos.
- Fortalecer las relaciones con otras áreas de la organización para mejorar la efectividad y éxito de los proyectos tecnológicos.

## 7. Metodología

La comparación costo beneficio se inicia con la consolidación de los costos asociados a la implementación del nuevo proceso de diseño de producto en la compañía Gfi Informática Colombia S.A.S. siguiendo lo dispuesto en la norma ISO 27001:2005 (seguridad de la información). La construcción se hizo por medio de un costeo tarea a tarea mediado por el software Microsoft Project, herramienta que permite la asignación de recursos y la cuantificación de costos que normalmente pasan inadvertidos tales como el uso de equipos, tiempo de trabajo, materiales, etc.

La información fue recolectada utilizando fuentes primarias y secundarias. Las fuentes primarias se relacionan con (de donde se sacaron los costos de computadores, nómina, etc.). Las fuentes secundarias tienen que ver con la revisión suministrada por parte del área comercial y el área de proyectos (informes ejecutivos y demás).

Los beneficios de la puesta en marcha fueron identificados a partir de las expectativas del área PMO y funcionarios encargados, junto con lo identificado en el marco teórico, se analizó que tan viable es para la compañía adoptar dicha certificación dentro de sus proyectos y su estructura interna.

# 8. Desarrollo del Trabajo por Capítulos.

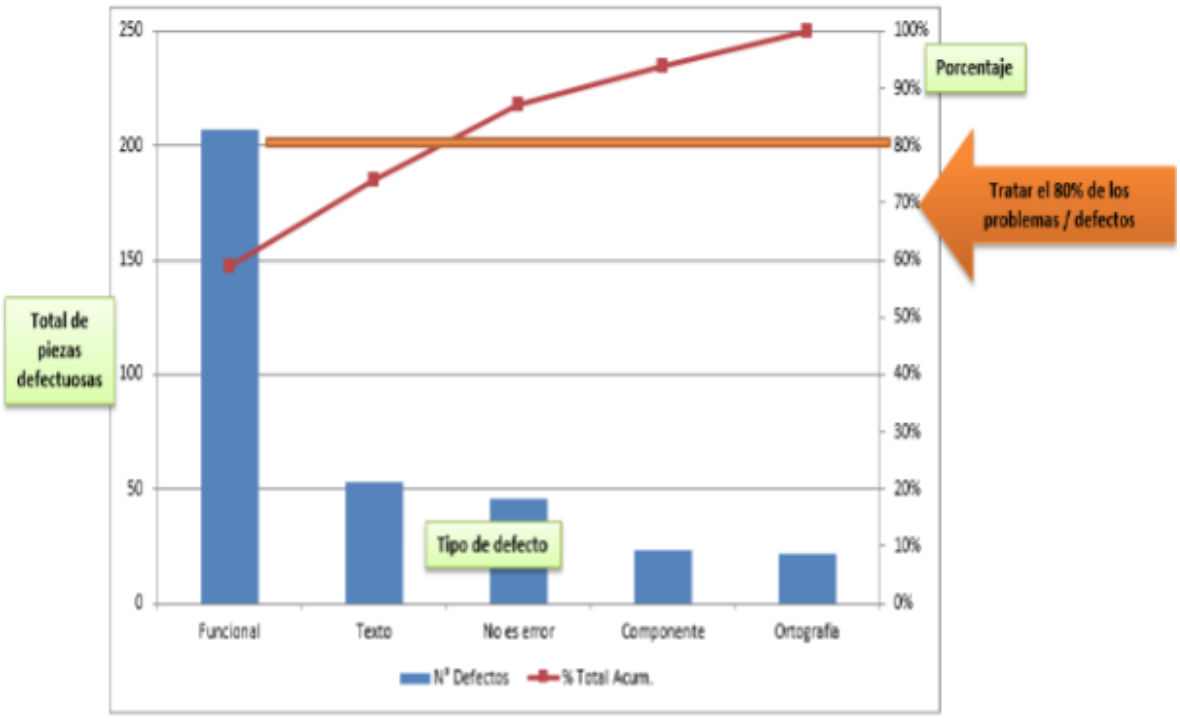
## 8.1. Capítulo I: Diagnostico del estado de la empresa Gfi Informática Colombia S.A.S

La empresa Gfi Informática en el 2017 estuvo realizando la mejora de distintos procesos para obtener una certificación de calidad de la norma ISO 27001:2005, uno de los procesos en el que menos se logró avanzar fue el proceso de realización de pruebas ya que presenta diferentes inconvenientes como: ponerse de acuerdo con las personas encargadas de realizar pruebas y poder hablar en un solo idioma tecnológico, cambiar la forma de trabajar de los empleados para que se adapten al cumplimiento de los requisitos establecidos en la norma y participen activamente en su implementación y la generación de nuevas ideas.

Para identificar la importancia de los errores en las pruebas se realizó el diagrama de Pareto.

**ILUSTRACIÓN 4 DIAGRAMA DE PARETO**

| Tipos de defectos | N° Defectos | N° Defectos Acum. | % Total Defectos | % Total Acum. |
|---|---|---|---|---|
| Funcional | 207 | 207 | 58,97% | 58,97% |
| Texto | 53 | 260 | 15,10% | 74,07% |
| No es error | 46 | 306 | 13,11% | 87,18% |
| Componente | 23 | 329 | 6,55% | 93,73% |
| Ortografía | 22 | 351 | 6,27% | 100,00% |
| Total | 351 | | 100% | |




Fuente: Elaboración Propia

Figura 5. Diagrama de Pareto

En la ilustración 4 se puede observar cada uno de los diferentes fallos y la cantidad de veces que se presentan cuando se están realizando pruebas. Estos fallos son: Funcional, Texto, No es error, Componente y Ortografía[3].

Según el resultado del diagrama hay que analizar la mejor manera para disminuir la cantidad de fallos que se generan de tipo funcional y texto. A pesar de que el diagrama de Pareto propone que identificando y solucionando en este caso los errores más importantes, el resto de los errores se solucionaran casi automáticamente. Pero en este caso no es así, debido a que los errores no son dependientes de los demás.

[3] La descripción de los tipos de fallo puede ser consultada en el glosario del documento.

La importancia del diagrama de Pareto en este estudio es poder identificar cual es el error que más se presenta en el desarrollo del software y poder reducir los tiempos de ejecución.

### 8.2. Capitulo II: bases para la implementación de la norma ISO 27001 en la empresa Gfi Informática Colombia S.A.S

Las bases para la implementación de la norma ISO 27001 en la empresa Gfi Informática, parten de la elaboración del procedimiento de nombre GFI-MSS-003 el cual tiene como fin el trazar un rumbo y dar forma a un proceso de pruebas que estaba sin personas a cargo, sin recursos disponibles y sin un objetivo claro dentro de Gfi Informática Colombia. Este procedimiento muestra la forma de actuar y las responsabilidades que tendría cada una de las personas que hacen parte de este proceso. Además de tener unas etapas dentro del proceso para poder cumplir con los objetivos y así llevar a cabo un proceso de pruebas que funcione de manera adecuada.

| | Nombre | Firma | Fecha |
|---|---|---|---|
| **Elaborado por:** | Juliette Lorena Palta Analista de Calidad y Seguridad y Leonardo Guerrero Practicante PMO | | |
| **Revisado por:** | Edna Liliana Hernández Trujillo Sénior de pruebas | | |
| **Aprobado por:** | Edwin Germán Ortiz Ortiz Director de Operaciones | | |

El objetivo de este formato es establecer lineamientos, alcances, responsabilidades y el paso a paso que permita la implementación de pruebas de software en los proyectos desarrollados por nuestra organización. Adicionalmente, establecer los parámetros de

medición de las características de calidad a través de los resultados alcanzados en las pruebas ejecutadas.

El alcance de este procedimiento debe ser implementado en todos los proyectos ejecutados por Gfi y comienza cuando es aceptado un proyecto, pasando por la obtención de información, preparación del entorno en el que se ejecutarán las pruebas y la instalación, ejecución y desinstalación del producto en cada configuración solicitada y termina con la entrega del Informe de No Conformidades y la evaluación del producto.

Las responsabilidades están dadas por cuatro unidades de trabajo las cuales son:

| | |
|---|---|
| Director de Operaciones | **• Realizar seguimiento al proceso de pruebas de los proyectos en ejecución y terminados.**<br>**• Proponer mejoras a los procesos de pruebas.** |
| Director de unidad | • Realizar el seguimiento a todas las etapas del proceso de pruebas.<br>• Seguimiento a los entregables por parte de los tester o líder de equipo.<br>• Liderar los equipos de pruebas como parte del desarrollo de los proyectos. |
| Jefe o líder de pruebas | • Asignar recursos para el desarrollo de las pruebas<br>• Guiar las pruebas con una planificación y objetivo claro<br>• Proyectar el esfuerzo de los recursos y los costos<br>• Contribuir con una estrategia de pruebas para la organización |
| Tester | Seguir el procedimiento de pruebas de software en todas sus etapas.<br>• Mantener la documentación requerida para el seguimiento y trazabilidad de las pruebas en cada uno de los proyectos de la organización.<br>• Hacer entregas de los defectos, reportes e informes de las pruebas en los tiempos y documentación establecida para ello. |

Así mismo se necesitara una gestión de pruebas las cuales estarán constituidas en primera instancia por una etapa de planificación la cual se define por la obtención de

información vital para ejecutar la prueba y las acciones necesarias para determinar el capital humano más adecuado para ejecutar la evaluación. A continuación, se muestran y describen las actividades definidas en esta primera etapa.

En segunda instancia se deberá realizar reuniones de entendimiento; en estas reuniones se pactan con el cliente los requisitos de la prueba, el tiempo de duración, las particularidades del producto dado que es de vital importancia conocer el producto para realizar de mejor forma la ejecución de la prueba, asimismo la información y acuerdos pactados con el cliente en las reuniones de entendimiento deberán ser registradas en el documento GFI-MSS-003 (Anexo 1) Reuniones de entendimiento, esta información deberá mantenerse actualizada y visible a todas las partes interesadas del proyecto.

En tercera etapa se deberá realizar una obtención de información de interés en la que el cliente deberá entregar toda la información necesaria para la ejecución del plan de pruebas y la documentación de los alcances y requisitos de las pruebas. La información entregada por el cliente se debe dejar relacionada en las reuniones de entendimiento.

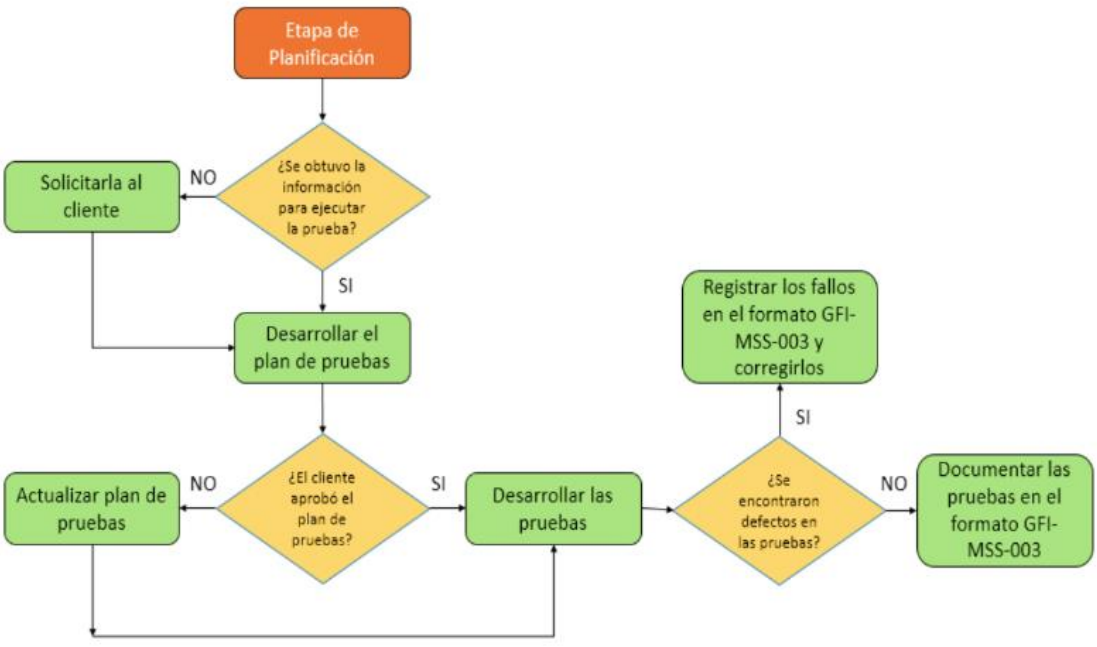
En cuarta instancia se debe generar un plan de pruebas con la información proporcionada por el cliente y los alcances definidos en la reunión de entendimiento, se procede a elaborar la versión inicial del GFI-MSS-003(Anexo 1) Plan de pruebas, para posterior aprobación del cliente.

En quinta instancia se realizarán casos de pruebas. Una vez aprobado el plan de pruebas por el cliente, el tester encargado deberá diseñar los casos de pruebas y enviarlos al responsable para su aprobación y puesta en ejecución; estos deben ser debidamente

documentados por cada uno de los proyectos en el formato GFI-MSS-003(Anexo 1) Casos de prueba.

Posteriormente se realizara la etapa de ejecución; en la que se realiza la ejecución de las pruebas implementadas, con la ayuda de los casos de prueba que se hayan identificado anteriormente. Estas pruebas pueden ser implementadas y ejecutadas desde la línea de comandos o mediante un Entorno de Desarrollo Integrado (IDE). Para ejecutar las pruebas unitarias de forma automática, se hace uso de los casos de prueba diseñados. El Tester ejecuta las pruebas y actualiza la GFI-MSS-003 (Anexo 1) Plantilla de seguimiento casos de prueba con los resultados de éstas y al mismo tiempo va registrando los fallos que puedan surgir en la ejecución de las pruebas. Una vez realizados los ajustes necesarios se vuelven a ejecutar y documentar las pruebas hasta no encontrar fallos.

**ILUSTRACIÓN 5 DIAGRAMA DE FLUJO DE LA ETAPA DE PLANIFICACIÓN**

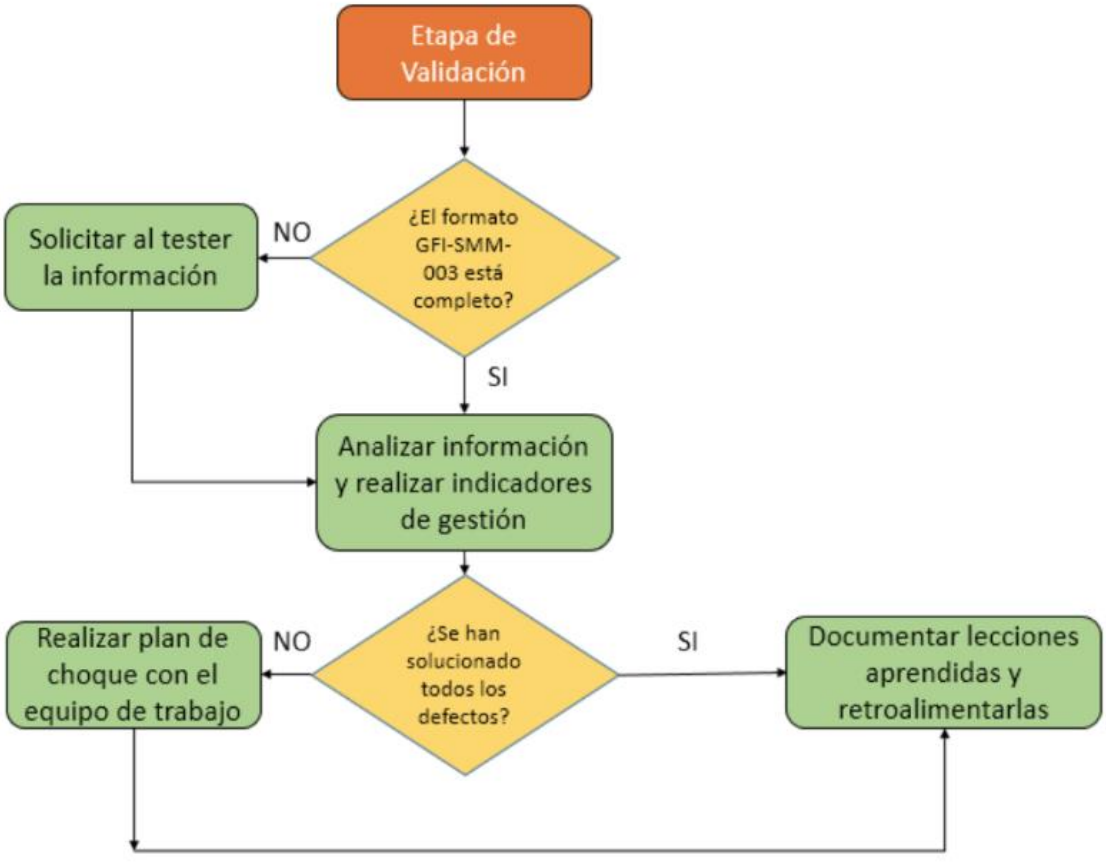



Fuente: Elaboración Propia

Figura 6. Diagrama de flujo de la etapa de planificación

Después de realizar la etapa de ejecución, se deberá realizar la etapa de validación, la cual una vez ejecutadas y registrados todos los casos de prueba por proyecto, se procede a analizar la información y registrar datos para sustentar los indicadores de gestión del proceso, se deben registrar los cierres de los defectos reportados y su plan de acción ejecutado, asimismo se deben documentar las lecciones aprendidas y retroalimentadas con los equipos de trabajo interesados en el proyecto.

**ILUSTRACIÓN 6 DIAGRAMA DE FLUJO DE LA ETAPA DE VALIDACIÓN**

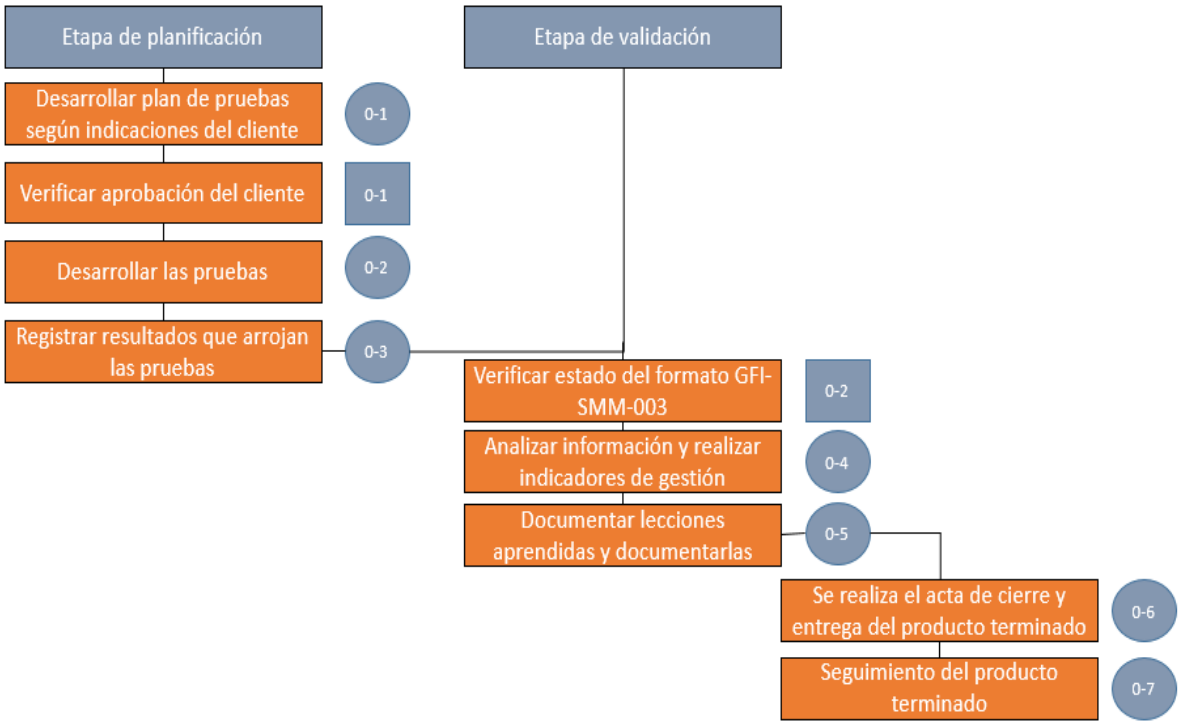



Fuente: Elaboración Propia

Figura 7. Diagrama de flujo de la etapa de validación

Finalmente se debe realizar el formato GFI-MSS-003 (Anexo 1) Acta de cierre y entrega del producto, con los reportes de las pruebas ejecutadas a los clientes; se realizará seguimiento a la puesta en producción del producto para garantizar la certificación de este, dando como cerrado el proyecto o fase del proyecto.

**ILUSTRACIÓN 7 DIAGRAMA DE LA OPERACIÓN DEL PROCESO DE PRUEBAS**

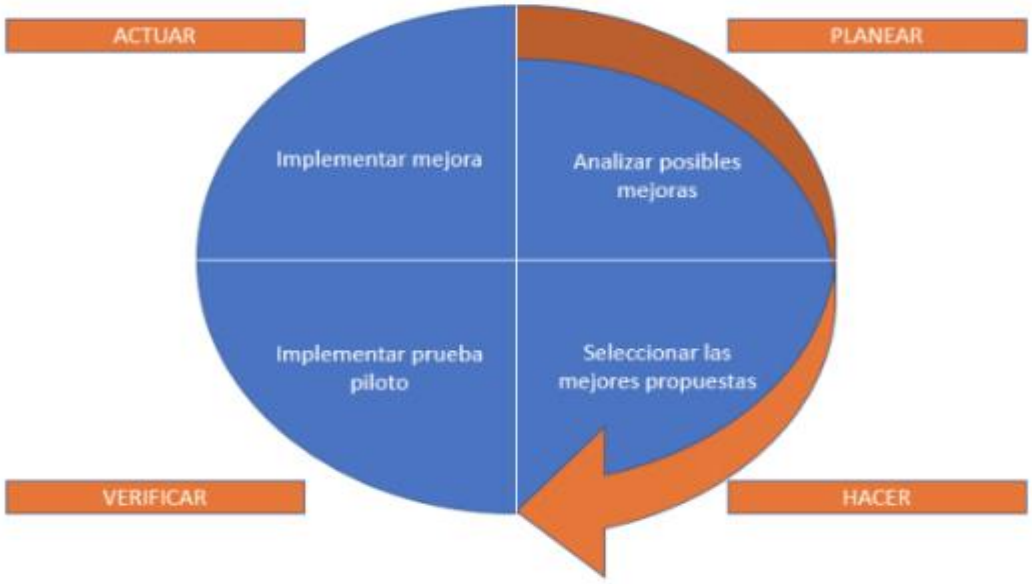



Fuente: Elaboración Propia

Figura 8. Diagrama de la operación del proceso de pruebas

Las propuestas de acciones de mejora se realizan empleando el procedimiento de Mejora Continua, cualquier persona dentro de la organización puede informar a la Dirección de Capital Humano sus propuestas de acciones de mejora a este procedimiento para que sean analizadas y él mismo determine si se implementan o no.

**ILUSTRACIÓN 8 CICLO PHVA (PLANEAR, HACER, VERIFICAR, ACTUAR)**



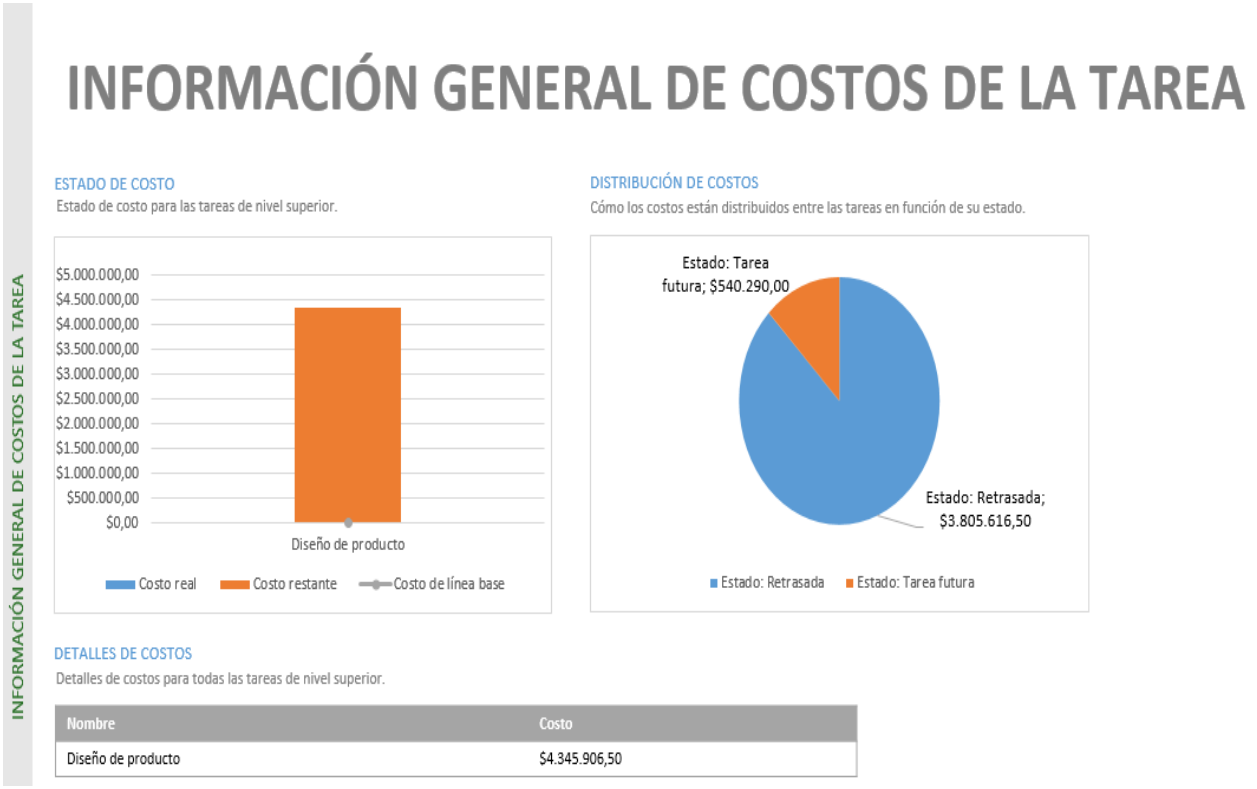

Fuente: Elaboración Propia

Figura 8. Diagrama de la operación del proceso de pruebas

### 8.3.Capitulo III: análisis costo-beneficio de la implementación de la norma ISO 27001 en la empresa Gfi Informática Colombia S.A.S

En esta sección se muestran en detalle los costos asociados a la implementación de la norma ISO 27001:2005 (seguridad en la información) en el área de Gestión de Proyectos de Gfi S.A.S.

El análisis parte de la simulación del proceso en Microsoft Project. En el cual a cada tarea se asignaron recursos y se hizo un costeo basados en datos reales proporcionados por diferentes dependencias de la compañía, en la que se pudo establecer el valor salarial de cada persona, el tiempo utilizado en cada tarea, el material utilizado para cumplir con dicha tarea y demás recursos utilizados para tal fin, como se puede ver continuación:




Resultado de ello se logró establecer que los costos del nuevo proceso ascienden a $4.345.906,50 (gráfico de barras) y que las futuras tareas asignadas a dicho proyecto serán de $540.290 (gráfico de torta). De esta manera se puede observar que el impacto que conlleva la creación de nuevos proyectos llevados a la certificación de calidad ISO 27001, contribuirá a unos mayores costes en las operaciones, de tal modo que dichos valores aumentaran paulatinamente, conforme la compañía acarree nuevos desafíos que se disponen en la norma; la información detallada se presenta en el anexo 5.

Los beneficios esperados por parte de la compañía con la implementación de la norma son en primera instancia el dar a comunicar a sus clientes sobre el interés de la seguridad como pilar de la compañía, asimismo se espera poder identificar los principales riesgos en materia de seguridad y con ello establecer controles, de igual manera se pretende una clasificación de los controles, adaptar y alinear los controles a todas las áreas de la

empresa; además también se espera crear confianza en los clientes y partes interesadas y así como cumplir con los requisitos y demostrar conformidad y compromiso con los mismos; cumplir las leyes y reglamentos pertinentes reduciendo así la posibilidad de enfrentarse a multas y sanciones; ahorrar costes por la reducción de incidentes, conseguir una ventaja competitiva y fortalecer la organización interna y los procesos de mejora continua. Del mismo modo la revisión de literatura dejo ver que los costos y beneficios que normalmente impactan a las organizaciones son la reducción de los riesgos de seguridad de la información; asimismo reducir la probabilidad de futuras amenazas o vulnerabilidades no reconocidas a la información de la seguridad del negocio; y de esta manera se contribuirá al ahorro de tiempo, dinero y esfuerzo mediante el ajuste de buenas prácticas.

## 9. Producto o Valor Agregado

Es común que las empresas implementan normas por obligación, pero pocas veces se detienen a pensar cuáles son las ventajas y desventajas de su puesta en marcha, así como los costos y beneficios asociados. De tal manera que no se evalúa la viabilidad de este tipo de procesos.

Por tal motivo este trabajo dentro de la compañía Gfi informática Colombia S.A.S. contribuirá como punto de partida para absorción de la norma ISO 27001, y sus futuros costes y beneficios que conllevará establecer los lineamientos para la pre-certificación y certificación iniciales de los procesos dentro de la compañía.

La metodología empleada puede ser replicada en procesos de similares características en compañías afines, de manera que se da un aporte a la generación de conocimiento.

## 10. Conclusiones

Con la ayuda de los directores de cada área, se logró recoger información acerca del proceso de pruebas en la compañía Gfi Informática y realizarle un diagnóstico según las normas ISO 27001:2005 del estado actual de sus procedimientos.

Una vez obtenida la información de este proceso, los directores y colaboradores plantearon cual sería la información más relevante para generar un análisis. Como resultado de este diagnóstico, surgió el formato de trazabilidad (GFI-MSS-003) anexo 1, teniendo como referencia los formatos de calidad de pruebas de MTI y BBVA anexos 2 y 3 respectivamente.

El resultado que se obtuvo con la implementación del formato (GFI-MSS-003) es la debida documentación del ciclo de vida que tienen las pruebas en la compañía. Esta documentación debe estar disponible tanto para los tester como para los clientes en el momento en que deseen realizar más pruebas al software o quieran saber acerca de la eficiencia de este. En el momento en que las mesas del BBVA empezaron a recibir un soporte (GFI-MSS-003) bien estructurado de las pruebas, se sintieron más conformes con los proyectos entregados ya que les brindaba información útil del desempeño del software.

La importancia que se destaca en que la empresa se certifique en alta calidad, será que acreditara a la compañía en el cumplimiento de la normatividad vigente, en la elaboración o ejecución de los procesos y esto será a su vez un distintivo de garantía y seguridad ante los clientes y un mayor prestigio ante el mercado.

Los costos de implementación del sistema de calidad ISO 27001:2005 (seguridad de la información) en el área seleccionada ascienden a 4.345.906 y los beneficios que traerá a la compañía Gfi Informática se resumen en un ahorro de costes y reducción de riesgos, beneficios en marketing/ventas y ventaja competitiva frente a los competidores.

## Glosario

**Ambiente:** Fallo al acceder a la aplicación.

**Componente:** Fallo relacionado con pruebas unitarias.

**Defecto:** Una definición de datos o un paso de procesamiento incorrectos en un programa.

**Error:** Una acción humana que conduce a un resultado incorrecto.

**Fallo:** Incapacidad de un sistema o de alguno de sus componentes para realizar las funciones requeridas dentro de los requisitos de rendimiento especificados.

**Funcionales:** Pruebas basadas en el análisis de las especificaciones y funcionalidades de un componente o sistema, es decir, en aquello que hace.

**No es error:** Falla que el cliente reporta como error, pero dentro de la compañía Gfi Informática el software funciona.

**No funcionales:** Pruebas que se ocupan de como el sistema se comporta en su interacción con el usuario y su entorno.

**Proceso de Pruebas:** Identifican aquellos fallos que han sido provocados por defectos.

**Prueba:** Es el conjunto de herramientas, técnicas y métodos que hacen la calidad de desempeño de un desarrollo.

**Regresión:** Garantizar que la corrección llevada a cabo realmente elimina el fallo.

**Texto:** Fallo que no cumple con el texto definido en el requerimiento, fallo de tildes y de ortografía.

**Validación:** Proceso de evaluación de un sistema o de sus componentes durante o al final del proceso de desarrollo, para determinar que satisface los requisitos especificados y que funciona para lo que fue diseñado.

**Verificación:** Es el proceso a través del cual se confirma que el software satisface sus objetivos.

## Bibliografía


- Acuña, K. B. (s.f.). Eumed.net. Obtenido de Biblioteca Virtual de Derecho, Economía y Ciencias Sociales: http://www.eumed.net/librosgratis/2009c/584/Metodologias%20tradicionales%20y%20metodologias%20 agiles.htm
- Calder, A., & Watkins, S. (2008). IT governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd...
- DE, T. D. S. S. (2006). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001.
- Garzás, J. (s.f.). Conectart. Obtenido de https://blog.conectart.com/metodologias-agiles/.
- GUTIERREZ BELTRAN, I., & SERPA VALDIVIA, C. (2015). ANÁLISIS Y DISEÑO DE UN PLAN DE MEJORA EN EL ÁREA DE PRODUCCIÓN DE LA EMPRESA ALBALUZ SRL UTILIZANDO LA METODOLOGÍA PHVA.
- Hinson, G. (2008). Implicaciones financieras de la implantación deISO/IEC 27001 & 27002: modelo genérico de coste-beneficio. ISO 27001 SEGURITY. Recuperado de: http://www.iso27000.es/download/ISO27k%20Generic%20business%20case_ES.pdf
- Linden, T. (2018). Entorno de aprendizaje basado en Scrum. Educación de sistemas de información, 65.
- Manikiw, G. (2012). Principios de economía. Cengage Learning Editores SA de CV.
- Martínez, J. A. (2014). ANÁLISIS DE COSTO BENEFICIO Ejemplos de análisis sector privado.

- Moya, J. (20 de Febrero de 2017). PMI. Obtenido de https://pmi-mad.org/index.php/socios/articulos-direccion-proyectos/1288-metodologia-agil-vs-metodologia-tradicional
- Navarro, J. M., & Garzás, J. (2010). Experiencia en la implantación de CMMI-DEV v1. 2 en una micropyme con metodologías ágiles y software libre. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software, 6(1).
- Paiva, J. E. (2016). Un requisito puesto en práctica que traza la herramienta para la rastreabilidad de los requisitos. Journal of Software, 193.
- Pérez Penagos, M. L., & Vargas Gualtero, I. R. (2018). Evaluación de las aplicaciones Project libre versus Microsoft Project en la programación de un proyecto de edificación.
- Rodríguez, M., Pedreira, Ó., & Fernández, C. M. (2015). Certificación de la mantenibilidad del producto software: Un caso práctico. Revista Latinoamericana de Ingeniería de Software, 3(3), 127-134.
- Sanz, P. V. (2013). Herramientas para la calidad total. Bogotá: Ediciones de la U.

# Anexos

## Anexo 1. Formato de trazabilidad de pruebas GFI-MSS-003

| | CASOS DE PRUEBA | | | | | | GFI-MSS-003<br>Versión:1.0 |
|---|---|---|---|---|---|---|---|
| Proyecto/GP | | | | | | | Fecha: |
| Caso De Prueba | especificaciones | Asignación | Resultado Obtenido | T. Estimado | T. Real Ejecutado | Fallo | Observación |
| Evento a probar | | | | | | | |
| 1 | | | | | | | |
| 2 | | | | | | | |

| | CASOS DE PRUEBA | | GFI-MSS-003<br>Versión:1.0 |
|---|---|---|---|
| | | | Fecha: |
| **Nombre** | | **Complejidad** | |
| **Descripción** | | **Prioridad** | |
| **Asignación** | | **Tiempo Estimado** | |
| **Precondición** | | **Tiempo Real** | |
| **Paso** | | **Resultado Esperado** | |
| **1.** | | | |
| **2.** | | | |
| **3.** | | | |
| **4.** | | | |
| Fallo Asociado | | Resultado Obtenido | |

## Anexo 2. Formato de trazabilidad de pruebas MTI

| | PLANTILLA DE SEGUIMIENTO CASOS DE PRUEBAS | | | | | GFI-MSS-003.03<br>Versión:1.0 | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Fecha: | | |
| Caso | Escenario | Caso de Prueba | Resultado Esperado | Asignación | Resultado Obtenido | T. Real Ejecutado | T. Estimado | Complejidad |
| 1. | | | | | | | | Simple |
| 2. | | | | | | | | Medio |
| 3. | | | | | | | | Complejo |

| | CASOS DE PRUEBAS ESTADO ACTUAL | GFI-MSS-003.03<br>Versión:1.0 |
|---|---|---|
| | | Fecha: |

| Escenario | Cantidad de casos | Casos ejecutados | % Casos ejecutados | Casos exitosos | % Casos exitosos | Casos fallidos | % Casos fallidos |
|---|---|---|---|---|---|---|---|
| | | | | | | | Simple |
| | | | | | | | Medio |
| | | | | | | | Complejo |

| Complejidad de la prueba | Cantidad Casos | Cantidad Fallos |
|---|---|---|
| Simple | | |
| Medio | | |
| Complejo | | |

**Anexo 3. Formato que utiliza BBVA para el control de las pruebas**

BBVA **Resumen Informe de Avance**

Datos del Proyecto

Resumen Ejecutivo

| | | | | |
|---|---|---|---|---|
| Cliente | | % Avance | | % Avance Esperado |
| Nombre del proyecto | | 0% | | 0% |
| Solicitud | | | | |
| Tipo Proyecto | | | | |
| Testing Project Leader | | Casos Diseñados | Casos OK | Casos no OK |
| Service Manager | | 0 | 0 | 0 |
| Responsable en el cliente | | | | |
| Proveedor Desarrollo | | Total Errores Efectivos | | Total Horas Desfase |
| Estado del proyecto | | 0 | | 0 |
| Área o División o Gerencia | | | | |

## Anexo 4. Diagrama de GANTT Microsoft Project

DIAGRAMA DE GANTT

| | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Predecesora | Nombres de los recursos |
|---|---|---|---|---|---|---|---|
| 1 | | **Diseño de producto** | **64 horas** | **lun 22/10/18** | **mié 31/10/18** | | |
| 2 | | **Gestión de Pruebas** | **56 horas** | **lun 22/10/18** | **mar 30/10/18** | | |
| 3 | | **Etapa de Planificación** | **32 horas** | **lun 22/10/18** | **jue 25/10/18** | | |
| 4 | | Reuniones de entendimiento | 8 horas | lun 22/10/18 | lun 22/10/18 | | Comercial[4];Computador[4];Transporte[2] |
| 5 | | Obtención de información de interés | 8 horas | mar 23/10/18 | mar 23/10/18 | 4 | Comercial[1,5];Computador[1,5] |
| 6 | | Plan de pruebas | 8 horas | mié 24/10/18 | mié 24/10/18 | 4;5 | Lider de área 1[16];Lider de área 2[16];Lider de área 3[16];Computador[16] |
| 7 | | Casos de pruebas | 8 horas | jue 25/10/18 | jue 25/10/18 | 6 | Tester Encargado 1[32];Tester Encargado 2[32];Tester Encargado 3[32];Tester Encargado 4[ |
| 8 | | **Etapa de ejecución** | **8 horas** | **vie 26/10/18** | **vie 26/10/18** | **3** | |
| 9 | | Ejecución de las pruebas implementadas | 8 horas | vie 26/10/18 | vie 26/10/18 | | Lider de área 1[4];Lider de área 2[4];Lider de área 3[4];Computador[4];<br>Tester Encargado 1[4];<br>Tester Encargado 2[4];Tester Encargado 3[4];Tester Encargado 4[4];Tester Encargado 5[4] |
| 10 | | **Etapa de validación** | **16 horas** | **lun 29/10/18** | **mar 30/10/18** | **8** | |
| 11 | | Retroalimentación | 8 horas | lun 29/10/18 | lun 29/10/18 | | Comercial[2];Lider de área 1[2];Lider de área 2[2];Lider de área 3[2];Director de operacion |
| 12 | | Cierre y certificació | 8 horas | mar 30/10/18 | mar 30/10/18 | 11 | Comercial[2];Director de operaciones[2];Transporte[2] |
| 13 | | **Mejora Continua** | **8 horas** | **mié 31/10/18** | **mié 31/10/18** | **3;8;10;2** | |
| 14 | | Retroalimentación | 8 horas | mié 31/10/18 | mié 31/10/18 | | Lider de área 1[0,5];Lider de área 2[0,5];Lider de área 3[0,5];Tester Encargado 1[0,5];Tester |