UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

IMPLEMENTACIÓN DE ÁREA DE PROCESO DE GESTIÓN DE RIESGOS DE CMMI v1.3 UTILIZANDO METODOLOGÍAS ÁGILES

TESIS PARA OPTAR AL GRADO DE
MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

ANDRÉS EDUARDO PAOLINI NOGUERA

PROFESORA GUÍA:
MARÍA CECILIA BASTARRICA PIÑEYRO

MIEMBROS DE LA COMISION
SERGIO OCHOA DELORENZI
ÉRIC TANTER
GONZALO ROJAS DURÁN

SANTIAGO DE CHILE

AGOSTO 2013

Resumen

La naturaleza de la competitividad de los mercados, la evolución y continuo crecimiento de las tecnologías de la información, así como una sociedad que se vuelve más demandante cada día exigiendo productos de mayor calidad y planteando nuevos desafíos a la industria, generan distintos tipos de eventos, lo que posiciona a la gestión de riesgos en un lugar de extrema importancia.

Evaluar el alcance y rango de respuestas disponibles que se pueden dar a los riesgos y decidir cuál es la acción más apropiada en un contexto determinado es el corazón de la gestión de riesgos. Responder a los riesgos de forma eficiente se debe traducir en beneficios para los individuos tanto a nivel personal como laboral y para las organizaciones donde trabajan.

Las empresas enfrentan una gran variedad de riesgos que pueden alterar el curso o resultado de sus operaciones. Sus resultados esperados pueden estar descritos por medio de una misión o conjunto de objetivos. Los riesgos que impactan una organización pueden interponerse en el camino de lograr sus metas, pueden representar una oportunidad, o bien pueden crear incertidumbre en el futuro cercano.

La gestión de riesgos debe ofrecer una solución que se aproxime a la evaluación, control y monitoreo de los distintos tipos de riesgos que pueden ocurrir a nivel organizacional. En el mundo del aseguramiento de la calidad del software los riesgos ocurren de forma permanente y es por ello que la identificación y control de estos es una tarea fundamental.

McAfee es una compañía de software relacionada con la seguridad informática. Se encarga de entregar y proveer soluciones y servicios que ayudan a asegurar sistemas, redes y dispositivos móviles alrededor del mundo. En McAfee Labs las prácticas de desarrollo de software están orientadas hacia las metodologías ágiles y los equipos de trabajo han considerado que la aplicación de prácticas ágiles ha sido suficiente para minimizar la ocurrencia de riesgos. Sin embargo, los riesgos existen y se han hecho evidentes, lo que refleja que una adecuada gestión de riesgos no puede omitirse.

Los métodos ágiles no plantean lineamientos formales para identificar problemas potenciales o una manera sistemática para identificar los riesgos así como su posible control o resolución y es aquí donde CMMI v1.3 juega un rol importante.

CMMI v1.3 es un modelo de madurez de mejora de procesos para el desarrollo de productos y servicios. Básicamente propone un conjunto de mejores prácticas para cubrir el ciclo de vida de un proceso de desarrollo de software.

A pesar de que se ha catalogado como un modelo riguroso con respecto a las metodologías ágiles, CMMI define un área de proceso dedicada a la gestión de riesgos, cuyas prácticas proveen un marco formal para institucionalizar la gestión de riesgos en un área específica de la organización. Pero esta nueva versión 1.3 de CMMI incluye además sugerencias para llevar a cabo una gestión de riesgos de la mano con el uso de métodos ágiles, aunque sin indicar específicamente cómo hacerlo.

El propósito de este trabajo de tesis es formular, diseñar y poner en marcha una estrategia de gestión de riesgos adoptando prácticas ágiles en la unidad de aseguramiento de la calidad de contenido de la división de gestión de riesgos y cumplimiento de McAfee Labs de modo que se pueda cumplir con el nivel de capacidad 2 de CMMI v1.3.

Abstract

The nature of competitive markets, the evolution of information technologies and its continuous growth and an emerging society that demands more quality in delivered products as well as the raise of new challenges in the industry, leads to a whole new group of events which requires the adoption of a risk management strategy.

The evaluation and analysis of different choices in order to provide the best answers about how risks could be mitigated or minimized is the core purpose of adopting a risk management process. Such answers should result in benefits for individuals and the organization for which they work for.

Companies face several risks that could have an impact on the business operations. Risks might represent a business opportunity or even increase the uncertainty levels and fall into unpredictable results.

The risk management process must provide a way to evaluate, control and monitor the potential risks that could take place in any organization. In the software quality assurance field, risks occur frequently which means it is mandatory to identify and mitigate them.

McAfee is a software security company that provides solutions and services to help customers to be more protected against cyber threats, such as malware, software vulnerabilities, identity theft, information leakage and so on.

In McAfee Labs, software development practices are based in agile methodologies. Development teams have considered that through the use of such practices, the risk exposure has been minimal. However, there is evidence that risks still exist which means that a proper risk management process should not be discarded.

Agile methodologies don't address risk management in a formal way. Despite of providing some practices that could reduce certain risks within the software development process, there is little consensus in the agile community regarding the adoption of a risk management process and about having a systematic guideline to identify, evaluate and control risks. This is where CMMI v1.3 plays a major role.

CMMI v1.3 is a capacity and maturity model to improve processes to develop software products and services. It provides a set of best practices that are helpful for the software development lifecycle.

CMMI has been considered as a heavy model and bureaucratic compared against agile methodologies, however, it includes a risk management process area which helps the organization to tackle risks down and promote a managed risk driven approach. CMMI v1.3 also contains a section that

mentions some suggestions about how to own a risk management process along with agile methodologies.

The main purpose of this thesis document is to propose, design and execute a risk management strategy adopting agile practices within the content quality assurance unit as part of the risk and compliance division in McAfee Labs in order to achieve the CMMI capacity level 2.

Tabla de Contenido

Lista de Tablas

Lista de Gráficos

1. Introducción

McAfee, como empresa global de desarrollo de soluciones de software en el mercado de la seguridad informática, tiene entre sus objetivos:

- Diseñar soluciones de seguridad informática que permitan minimizar la pérdida de datos y reducir las vulnerabilidades de los sistemas de millones de usuarios y corporaciones a nivel mundial.
- Gestionar la calidad del desarrollo de los productos que permita mantener una alta tasa de detección de vulnerabilidades, una baja tasa de falsos positivos y maximizar el promedio de detección de amenazas en tiempo real.

McAfee está dividida en tres grandes áreas:

- **McAfee Corporation:** Compuesta por las unidades que representan la cara del negocio como ventas, marketing, soporte a clientes y servicios profesionales, así como la unidades transversales, como recursos humanos, finanzas y tecnologías de información.
- **Ingeniería:** Comprende las unidades que desarrollan y construyen los productos que se ofrecen al mercado. Estos productos abarcan desde soluciones anti-malware y de encriptación de datos hasta productos para gestionar riesgos y cumplimiento de políticas de seguridad.
- **McAfee Labs:** Comprende las unidades que investigan las nuevas vulnerabilidades y amenazas que surgen mundialmente, el análisis para su mitigación y la entrega de la solución que elimina la amenaza o bien minimiza la posibilidad de que esta ocurra por medio de los distintos productos que ofrece la compañía. Dentro de esta área se encuentra la división de gestión de riesgos y cumplimiento.

El propósito de la división de gestión de riesgos y cumplimiento es desarrollar contenido de forma permanente que detecte vulnerabilidades en productos de terceros (Microsoft, Oracle, Google, Firefox, Apple) además de ayudar a los clientes en el cumplimiento de mejores prácticas de seguridad y requisitos legales exigidos por gobiernos u otra instituciones. El contenido que se desarrolla es posteriormente incluido en los distintos productos para la gestión de riesgos y cumplimiento que ofrece McAfee.

La Tabla 1 lista algunos de los productos de gestión de riesgos y cumplimiento de McAfee Labs[1].

[1] McAfee Policy Auditor - http://www.mcafee.com/mx/products/policy-auditor.aspx,

Tabla 1 Productos de gestión de riesgo y cumplimiento de políticas de seguridad de McAfee Labs

Producto	Características
McAfee Policy Auditor	• Es un producto que ayuda a reportar de manera consistente y acertada los resultados de auditorías basadas en legislaciones obligatorias (**SOX – Sarbanes Oaxley**, **PCI – Payment Card Industry**, **DISA - Defense Information Systems Agency**, **HIPAA** - **Health Insurance Portability and Accountability Act**) y mejores prácticas de seguridad (**CIS – Center for Internet Security**) sobre sistemas computacionales. • Es una solución que funciona con la instalación de un agente en los sistemas que son auditados y que permite la comunicación bidireccional. • El producto implementa SCAP (**Security Content Automation Protocol o Protocolo de automatización de contenido de seguridad**).
McAfee Vulnerability Manager	• Es una solución de gestión de riesgos que permite detectar vulnerabilidades en los sistemas computacionales y violaciones de políticas de seguridad, asignando prioridades a los activos de tecnologías de información de la organización. • Permite identificar vulnerabilidades en sitios web, bases de datos, sistemas operativos y una variedad de aplicaciones. • Adicionalmente, tiene la capacidad de poder utilizar el contenido que se encuentra en McAfee Policy Auditor y lo complementa con otra diversidad de regulaciones de la industria.
Remediation Manager	• Es una solución que se encarga de identificar la ausencia de actualizaciones y parches de seguridad en sistemas operativos y aplicaciones. Una vez que detecta que la actualización o el parche están ausentes en el sistema objetivo, lo instala y minimiza las probabilidades de que el mismo sea vulnerado.
McAfee Network Access Control	• Es una solución que restringe el acceso a la red para los sistemas de riesgo, como por ejemplo, los portátiles de visitantes y contratistas dentro de una organización. Adicionalmente, verifica si los equipos que se tratan de conectar a la red cumplen con las políticas de seguridad de la empresa en cuanto a su configuración.

A pesar de que McAfee no dispone de una política de desarrollo explicita que se cumpla de forma general en la organización, sí cuenta con un proceso denominado PLF (Product Lifecycle Framework o Marco de trabajo del ciclo de vida del producto). Dicho marco de trabajo comprende un conjunto de fases descritas en el Gráfico 1.

Gráfico 1 PLF - Marco de Trabajo del ciclo de vida del producto en McAfee.

A continuación en la Tabla 2 se detalla cada una de las etapas del ciclo de vida del producto en McAfee[2].

McAfee Vulnerability Manager http://www.mcafee.com/mx/products/vulnerability-manager.aspx,
McAfee Network Access Control http://www.mcafee.com/mx/products/network-access-control.aspx

[2] McAfee Product Lifecycle Framework – Documento interno de McAfee Labs (Uso restringido y confidencial).

Tabla 2 Etapas del ciclo de vida del producto en McAfee (PLF)

Etapa	Definición
Concepto	• Se define el caso de negocio. • Se genera la propuesta del producto para el negocio. • Se desarrolla el alcance del trabajo.
Planificación	• Se establece las políticas que rigen el tiempo en que puede permanecer activo el producto o servicio a ofrecer. • Se evalúan los temas legales relacionados con el producto, patentes, licenciamiento. • Se desarrolla el plan maestro del proyecto relacionado a la propuesta. Este plan incluye los planes de desarrollo del software, los planes de aseguramiento de la calidad del software, desarrollo de la documentación funcional y técnica del producto, traducción o localización del producto, planes de desarrollo de contenido y aseguramiento de la calidad del contenido, etc..
Diseño y Desarrollo	• Se diseña y desarrolla la solución enmarcada en el proyecto. • Se realizan las pruebas del producto. • Se desarrolla el contenido inicial del producto y se realizan las pruebas del contenido. • Se coordinan las áreas de soporte y los canales de venta sobre el ingreso del nuevo producto al mercado. • Se definen los procedimientos operacionales en McAfee Labs para dar continuidad a la operación del producto y cambios requeridos ya sea por defectos o bien para incluir nuevas características al producto.
Preparación	• Se genera la documentación de usuario final. • Se desarrollan los entrenamientos para los usuarios del producto. • Se generan productos de muestra y evaluación a ser utilizados por un conjunto de clientes previamente seleccionados por la empresa. • Se entrega una versión beta a algunos clientes. • Se obtiene una retroalimentación de parte de los clientes.
Liberación	• Se planifica la liberación al mundo del producto (mercadeo, medios de comunicación, socios negocio) y su respectiva realización. • Se empieza a obtener una retroalimentación masiva del uso del producto.
Soporte	• Se obtienen los casos reportados por los clientes, errores, fallas, mejoras al producto.

El presente proyecto se va a desarrollar en la etapa del ciclo de vida del producto correspondiente a “Diseño y Desarrollo”.

1.1 Situación Actual

Área de trabajo

El área de trabajo dentro de McAfee Labs que se encuentra bajo estudio es el área de aseguramiento de la calidad de contenido de la división de productos de gestión de riesgos y cumplimiento de políticas de seguridad.

Grupo de trabajo

El grupo de trabajo cuenta con 12 personas e incluye: 3 ingenieros de aseguramiento de la calidad (Bangalore, India), 7 ingenieros de aseguramiento de la calidad (Santiago, Chile), 1 ingeniero de automatización (Santiago, Chile) y el jefe de todo el grupo (Santiago, Chile).

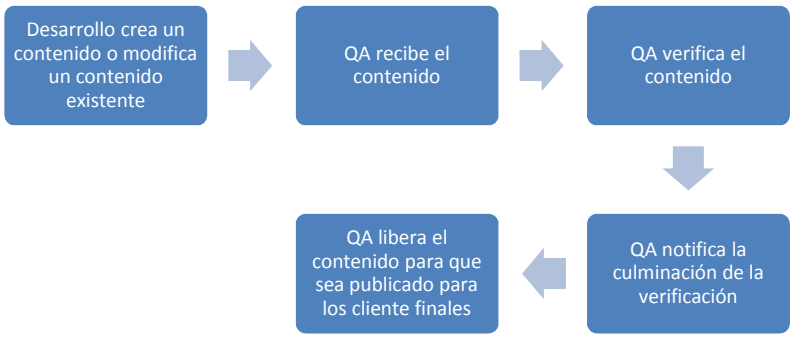
Dentro del grupo hay una división de equipos por producto: 4 ingenieros de aseguramiento de la calidad para el producto Policy Auditor, 2 ingenieros de aseguramiento de la calidad para el producto Remediation Manager y McAfee Network Access Control, 3 ingenieros de aseguramiento de la calidad para el producto McAfee Vulnerability Manager y el ingeniero de automatización que trabaja de forma transversal con todos los equipos.

Cada equipo (por producto) trabaja en conjunto con un equipo de desarrollo. El equipo de desarrollo es el que crea el contenido que va asociado a cada producto y que luego es verificado por el área de aseguramiento de la calidad. Los equipos de desarrollo están distribuidos entre India, Estados Unidos, Chile y China.

Descripción del Proceso de QA

Por cada producto cuyo contenido es revisado por un Ingeniero de aseguramiento de la calidad, existe un proceso diferente, aunque hay pasos similares. De forma general el proceso se describe en el Gráfico 2.

Gráfico 2 Proceso general seguido por el área de aseguramiento de la calidad en McAfee Labs



A continuación en la Tabla 3 se detallan las etapas del proceso general de aseguramiento de la calidad en McAfee Labs.

Tabla 3 Etapas del proceso general de aseguramiento de la calidad en McAfee Labs

Etapa	Definición
Desarrollo crea un contenido o modifica un contenido existente	• Se investiga sobre la vulnerabilidad o política de seguridad a revisar por parte del producto. • El equipo de desarrollo genera el script correspondiente. • Se genera un paquete de contenido que incluye los scripts generados y se envía a QA.
QA recibe el contenido	• Se descarga el paquete generado por el área de desarrollo y se verifica que se puede instalar correctamente.
QA verifica el contenido	• Se diseñan los casos de prueba. • Se preparan los ambientes de las pruebas. • Se ejecutan las pruebas.
QA notifica la culminación de la verificación	• Se reportan los defectos encontrados. • Se notifica que las pruebas han culminado.
QA libera el contenido para que sea publicado para los clientes finales	• Se ejecuta un conjunto de pasos necesarios para liberar el contenido a los clientes finales. • Se generan las notas relacionadas con la liberación.

1.2 Descripción del Problema

Hoy en día es conocido que muchas organizaciones que desarrollan productos de software se encuentran con eventos que afectan la calidad del producto que venden, el presupuesto asignado para un proyecto en particular, el proceso utilizado para la creación del producto y un impacto sobre los compromisos adquiridos con sus clientes. Estos eventos se conocen como riesgos y si ocurren pueden influir negativamente dentro de un proyecto si no son identificados y controlados apropiadamente.

En el área de aseguramiento de la calidad de contenido de McAfee se ha logrado evidenciar la falta de un proceso riguroso de gestión de riesgos que permita identificar los riesgos, priorizarlos y crear los planes de contingencia necesarios para mitigarlos o minimizar su impacto en caso de ocurrencia. En la Tabla 4 se pueden apreciar algunos tipos de riesgos[3] que han ocurrido en distintas oportunidades dentro de la unidad.

[3] Software Testing Help. Types of Risks in Software Projects. http://www.softwaretestinghelp.com/types-of-risks-in-software-projects/
Luckey, Teresa y Phillips, Joseph (2006). Software Project Management for Dummies. John Wiley & Sons, ISBN-10: 0-471-74934-6. Capitulo 5 – Planning for Software Project Risks.

Tabla 4 Tipos de riesgos que se han presentado en el área de aseguramiento de la calidad de contenido de la división de gestión de riesgo y cumplimiento en McAfee Labs

Tipo de Riesgo	Descripción
Riesgos sobre la planificación	Se han llevado a cabo estimaciones sin conocer la complejidad de un proyecto o contenido en específico y el tiempo requerido para probar dichas funcionalidades. Esto ha comprometido en algunas ocasiones los tiempos de entrega y los plazos para las liberaciones a producción.
Riesgos sobre los requisitos	En ocasiones se ha recibido un contenido a ser verificado sin que las personas tengan un entrenamiento adecuado con respecto a lo que se debe verificar, esto incluye: el producto, conocimiento de los sistemas operativos requeridos para realizar las pruebas, ambientes que se deben virtualizar, conceptos básicos de seguridad y cuál es la finalidad de lo que se debe verificar. Esto trae como resultado que se verifique lo que no se está pidiendo verificar y se asuma que se está verificando lo correcto.
Riesgos Operacionales	Cuando ha faltado un recurso humano dentro de los equipos para llevar a cabo alguna tarea, se tarda en tomar una decisión acerca de las acciones a seguir para cubrir esa carencia generando incertidumbre, molestias dentro del equipo y esfuerzo adicional comprometiendo los plazos de entrega. Cuando se acepta realizar las pruebas de un proyecto nuevo o de un contenido específico no se realiza una evaluación formal de los recursos de software y hardware disponibles, lo que lleva a tener que preguntar a otras personas si pueden facilitar los recursos o crear las configuraciones requeridas, sin que dichas personas se comprometan necesariamente porque no forman parte del proyecto o bien porque no han sido asignadas a realizar estas tareas. Si ocurre alguna falla general dentro de la oficina no existe un plan asociado para poder dar continuidad a las operaciones de la unidad lo que puede impactar los plazos de entrega.
Riesgos en la comunicación	Al encontrarse los equipos de desarrollo y de aseguramiento de la calidad dispersos globalmente, cuando se detecta un defecto y este a su vez debe ser corregido por el equipo de desarrollo, se generan discusiones y confusión sobre lo que se tiene que corregir ya que no se dispone de las herramientas necesarias para que se puedan reproducir los defectos apropiadamente y que los individuos puedan acceder al mismo recurso de forma simultánea. En ciertas ocasiones cuando un cliente reporta un defecto en el producto, se le notifica prácticamente al área de aseguramiento de la calidad que verifique si el defecto existe, sin seguir los canales correspondientes de la organización para atender problemas de clientes, como contactar el nivel de soporte respectivo que pueda verificar inicialmente el incidente y al responsable de la cuenta del cliente para que actúe como intermediario en dicha situación. El resultado de esto es que el área de aseguramiento de la calidad pierde tiempo y recursos investigando el incidente cuando el cliente reporta de forma errónea un incidente.

La ocurrencia de estos riegos ha impactado de forma negativa el desempeño de la unidad, a pesar de que ya en ocasiones se han realizado discusiones y conversaciones dentro del equipo de aseguramiento de la calidad al momento de recibir asignaciones y nuevas tareas con la finalidad de que estos riesgos no se presenten. Sin embargo, por lo general se actúa de forma reactiva y de manera informal sin que se institucionalice la gestión de los riesgos dentro de la unidad.

1.3 Oportunidad

Con la existencia de un mercado global altamente competitivo donde las organizaciones e instituciones gubernamentales demandan soluciones de seguridad que puedan garantizar de alguna

forma la protección de sus datos y activos de información más importantes, es primordial que las empresas que construyen y proveen dichas soluciones demuestren que cuentan con procesos capaces de entregar productos de calidad.

McAfee compite globalmente con otros proveedores de soluciones de seguridad como es el caso de firmas como Symantec y Kaspersky, entre otros. En conjunto todas estas organizaciones participan en procesos de licitaciones tanto en el sector privado como el sector público de tal forma de buscar posicionarse y ubicar alguno de sus productos con la idea de fortalecer su negocio.

Actualmente no basta con vender un producto, sino también se debe vender los procesos que respaldan ese producto. Por lo tanto, como resultado de esto, se ha evaluado la posibilidad de que el área de aseguramiento de la calidad de la división de gestión de riesgos y cumplimiento de McAfee pueda desarrollar una estrategia de gestión de riesgos basándose en la adopción de CMMI v1.3.

CMMI (Capacity Maturity Model Integration o Integración de modelos de capacidad y madurez) es un modelo reconocido mundialmente por distintas organizaciones y entes gubernamentales y es soportado por el SEI (Software Engineering Institute) o Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon en los Estados Unidos.

Debido a que posee un gran prestigio en la industria de desarrollo de software, la mayoría de las organizaciones que han enfocado sus esfuerzos en adaptar el modelo a sus necesidades han obtenido resultados positivos, optimizando sus procesos, mejorando el empleo de los recursos, disminuyendo costos y asegurando mayor rentabilidad en la ejecución de sus proyectos.

Muchas organizaciones y en especial del sector gobierno de los Estados Unidos, algunos países de la Unión Europea como es el caso de España, Francia y Alemania, e incluso con un reciente auge Chile y Argentina, exigen a sus proveedores encontrarse en un determinado nivel de madurez o tener algunas áreas de proceso en un cierto nivel de capacidad para poder concursar en un proceso de licitación.

McAfee como organización utiliza y continúa adoptando SCRUM como su marco de trabajo principal para el área de desarrollo de software. Se ha demostrado que CMMI puede integrarse con entornos ágiles como por ejemplo SCRUM o RUP y los resultados han sido beneficiosos[4].

[4] V. Uttangi, Roshan, Rizwan Azeem, Rizwan Syed Abdul (2007) Fast track to CMMI implementation: Integrating the CMMI and RUP process frameworks http://www.ibm.com/developerworks/ rational/library/oct07/uttangi_rizwan/.
Gallagher, Brian, Brownsword, Lisa (2001) The Rational Unified Process and the Capability Maturity Model - Integrated Systems/Software Engineering - http://www.sei.cmu.edu/library/assets/rup.pdf.
Software Engineering Institute (SEI) (2013) CMMI and SCRUM http://cmmiinstitute.com/cmmi-getting-started/cmmi-compatibility/cmmi-and-agile/cmmi-and-scrum/.

CMMI sirve de enfoque para dar a entender el funcionamiento de una organización de manera eficiente y eficaz. Como modelo permite plantear el "qué" y no el "cómo" debe hacerse las cosas. El cómo va asociado a los principios de negocios de cada organización y viene de la mano con las necesidades de cada área y su metodología de desarrollo.

La gestión de riesgos en SCRUM sigue sin tener un consenso en la comunidad de desarrollo de software, no está cubierta de forma explícita[5] y CMMI provee una guía sobre que es la gestión de riesgos y que debe considerarse.

CMMI propone un conjunto de prácticas y ejemplos comunes de un proceso general de gestión de riesgos, declarando que no solo se deben gestionar los riesgos dentro del proyecto de desarrollo de software sino también los relacionados a factores externos al proyecto.

En McAfee no existe ningún área que haya adoptado CMMI y se considera que podría representar una buena oportunidad para el área de aseguramiento de la calidad de contenido de la división de productos de gestión de riesgos y cumplimiento de políticas satisfacer las metas que propone el área de proceso de gestión de riesgos para el nivel de capacidad 2.

Una vez puestas en marcha todas las prácticas necesarias para alcanzar el nivel de capacidad 2 del área de proceso de gestión de riesgos de CMMI se realizará una evaluación SCAMPI[6] por medio de una organización autorizada por el SEI.

Esto podría mencionarse a los clientes dentro de las propuestas realizadas por el área de ventas acerca de los productos de gestión de riesgos y cumplimiento, siendo esto un elemento positivo a considerar por el cliente durante la negociación.

Cabe destacar que CMMI v1.3 es promisorio como estrategia para proponer una gestión de riesgos dentro del área de aseguramiento de la calidad de contenido y que ayuda con un mejor posicionamiento de los productos de McAfee en el mercado global, porque trata la gestión de riesgos como una disciplina técnica y organizada, donde se identifican los riesgos, se cuantifican y se siguen a lo largo del ciclo de vida de los productos.

---

[5] Neil Potter, Mary Sakry (2011) Implementing Scrum (Agile) and CMMI together http://www.scrumalliance.org/community/articles/2011/february/implementing-scrum-(agile)-and-cmmi®-together.
Satheesh Thekku Veethil (2013) Risk Management in Agile http://www.scrumalliance.org/community/articles/2013/2013-may/risk-management-in-agile.

[6] SCAMPI - Standard CMMI Appraisal Method for Process Improvement.

1.4 Propuesta

Para plantear una respuesta a la situación actual, se propone diseñar e implantar un proceso de gestión de riesgos en McAfee orientado a satisfacer la meta genérica y las prácticas genéricas del nivel de capacidad 2 para el área de proceso de gestión de riesgos de CMMI v1.3 adoptando prácticas ágiles.

Se busca poder demostrar de esta forma que se puede identificar, monitorear, controlar y minimizar la probabilidad de ocurrencia de ciertos riesgos y dejar en evidencia que existe una estrategia de gestión de riesgos institucionalizada dentro de la unidad de aseguramiento de calidad de contenido de la división de productos de gestión de riesgo y cumplimiento de McAfee Labs.

Esta solución se puede utilizar como ejemplo para adoptarla en otras áreas de la organización, considerando que el desarrollo de productos de seguridad informática es crítico hoy en día y un impacto negativo en el mercado puede afectar considerablemente la imagen de la empresa y los resultados económicos.

1.5 Objetivos

Objetivo General

Diseñar e implantar un proceso de gestión de riesgos dirigido a satisfacer la meta genérica y prácticas genéricas del nivel de capacidad 2 del área de proceso de gestión de riesgos de CMMI v1.3 con el uso de métodos ágiles en el área de aseguramiento de la calidad de contenido de la división de productos de gestión de riesgo y cumplimiento de McAfee Labs.

Objetivos Específicos

- Identificar los riesgos más críticos que impacten la unidad de aseguramiento de la calidad y categorizarlos.
- Implantar un proceso piloto para la gestión de riesgos identificados dentro de la unidad de aseguramiento de la calidad.
- Recabar datos por medio del proceso piloto que ayuden a identificar nuevos riesgos, a determinar la probabilidad de ocurrencia de los riesgos y al desarrollo de planes de contingencia.
- Validar tanto la pertinencia de los riesgos identificados como del proceso piloto para la gestión de riesgos mediante mediciones y monitoreo.
- Ajustar la lista de riesgos y el proceso piloto para la gestión de riesgos de acuerdo a las necesidades reales de la unidad de aseguramiento de la calidad.

1.6 Metodología

Para lograr la implantación de un proceso de gestión de riesgos orientado a satisfacer la meta genérica y las prácticas genéricas del nivel de capacidad 2 para el área de proceso de gestión de riesgos de CMMI v1.3 adoptando prácticas ágiles se deben seguir los siguientes pasos:

- Analizar cada una de las prácticas genéricas del nivel de capacidad 2 de CMMI v1.3 en términos de comprender lo exigido por cada una así como las prácticas específicas del área de proceso de gestión de riesgos.
- Comparar las prácticas existentes de gestión de riesgos a través de metodologías ágiles con respecto a las prácticas genéricas y específicas que se deben satisfacer en el área de proceso de gestión de riesgos de CMMI v1.3.
- Evaluar las prácticas genéricas del nivel de capacidad 2 y las prácticas específicas del área de proceso de gestión de riesgos de CMMI v1.3 para las que no existan prácticas ágiles específicas que permitan satisfacerlas y proponer métodos alternativos que sí lo permitan.
- Seleccionar las prácticas ágiles y métodos alternativos a utilizar y definir cuándo, dónde y en qué orden deben ser utilizados.
- Implantar las prácticas ágiles seleccionadas y los métodos alternativos a través de un proyecto piloto.
- Medir el resultado de la aplicación de las prácticas ágiles para la gestión de riesgos evaluando si se ha logrado cumplir con las prácticas genéricas del nivel de capacidad 2 de CMMI v1.3 y las prácticas específicas del área de proceso de gestión de riesgos.
- Medir y comparar contra el estado inicial del área de aseguramiento de la calidad, en términos de riesgos no detectados o desviaciones en la probabilidad de ocurrencia de los riesgos.
- Tomar acciones correctivas en los casos que sea necesario para garantizar el cumplimiento de las metas del área de proceso de gestión de riesgos y mantener la unidad en conformidad con el nivel de capacidad 2.

2. Marco Teórico

2.1 Metodologías Ágiles

El desarrollo de software, según Martin Fowler en su artículo "La Nueva Metodología (The New Methodology)" [7] escrito en Diciembre del 2005, "se conoce como una actividad caótica caracterizada por la frase codificar y corregir. El software muchas veces se escribe sin seguir un plan y el diseño del mismo depende de decisiones de corto plazo. Esto puede funcionar cuando se trata de un sistema pequeño, pero en la medida que el tamaño del software es mayor resulta más complejo añadir nuevas funcionalidades, aumenta la cantidad de errores y la dificultad para corregirlos. Una típica señal de esto son largas fases de pruebas una vez que las características principales del sistema hayan sido desarrolladas".

El movimiento original que trató de cambiar esta forma de trabajar, introdujo la noción de metodología. Estas metodologías exigen un proceso disciplinado con la finalidad de tener un proceso de desarrollo más eficiente y predecible. La idea principal consiste en disponer de un proceso detallado con un fuerte énfasis en la "planificación" inspirado por otras disciplinas de la ingeniería.

La presencia y uso de estas metodologías ha estado vigente por muchos años. No han sido notorias necesariamente por proveer excelentes resultados o incluso por ser populares en su uso. Tal vez la crítica más frecuente con respecto a éstas es que son "burocráticas", ya que se considera que demandan tantos requisitos que se disminuye el rendimiento y la velocidad del proceso de desarrollo de software. Como reacción a este movimiento surgieron las metodologías ágiles.

Para muchos la aparición de las metodologías ágiles es la reacción a la demandante burocracia exigida por las metodologías con énfasis en la planificación y basadas en otras disciplinas de la ingeniería. Estas buscan proveer una alternativa entre no tener algún proceso o disponer de muchos procesos, y que se alcancen los objetivos de manera razonable.

El resultado de todo esto es que las metodologías ágiles tienen algunos cambios significativos en comparación con las metodologías tradicionales. Tal vez los cambios más significativos son considerados los siguientes:

- **Los métodos ágiles son adaptativos y no predictivos.** Las metodologías tradicionales buscan crear un plan a largo plazo y en gran detalle con respecto al proceso de desarrollo de software de un proyecto particular, lo que funciona bien hasta que el proyecto comienza a sufrir variaciones en su alcance. Por lo tanto, su naturaleza no contempla el cambio constante. Por

[7] Martin Fowler's blog. The New Methodology. http://martinfowler.com/articles/newMethodology.html.

otra parte, los métodos ágiles contemplan el cambio como algo normal, adaptándose a estos con frecuencia.

- **Los métodos ágiles están orientados a las personas y no orientados a los procesos.** Las metodologías tradicionales definen un proceso que busque satisfacer las necesidades de un proyecto, independientemente de qué individuo lo utilice. Las metodologías ágiles se basan en que no hay proceso que supere las habilidades del equipo de desarrollo. Por lo tanto, el rol del proceso es servir de soporte al equipo de desarrollo y no viceversa.
- **Los métodos ágiles son menos orientados a la documentación.** Las metodologías tradicionales promueven el desarrollo de planes y distintos tipos de documentos dependiendo de la fase del proceso en que se encuentre el proyecto. En cambio, las metodologías ágiles promueven la idea de que el código del software en desarrollo por sí mismo debería ser la documentación existente.
- **Los métodos ágiles consideran la participación del cliente durante el desarrollo como esencial.** La mayor parte del tiempo las características del sistema con mayor valor agregado para el negocio no son tan obvias en un principio, sino una vez que el cliente empieza a utilizar el mismo. Por eso las metodologías ágiles buscan tomar ventaja con esto, ya que permiten a los clientes aprender de sus necesidades de negocio en la medida que se construye el software y así ir desarrollando este de tal forma que los cambios puedan ser incorporados rápidamente.

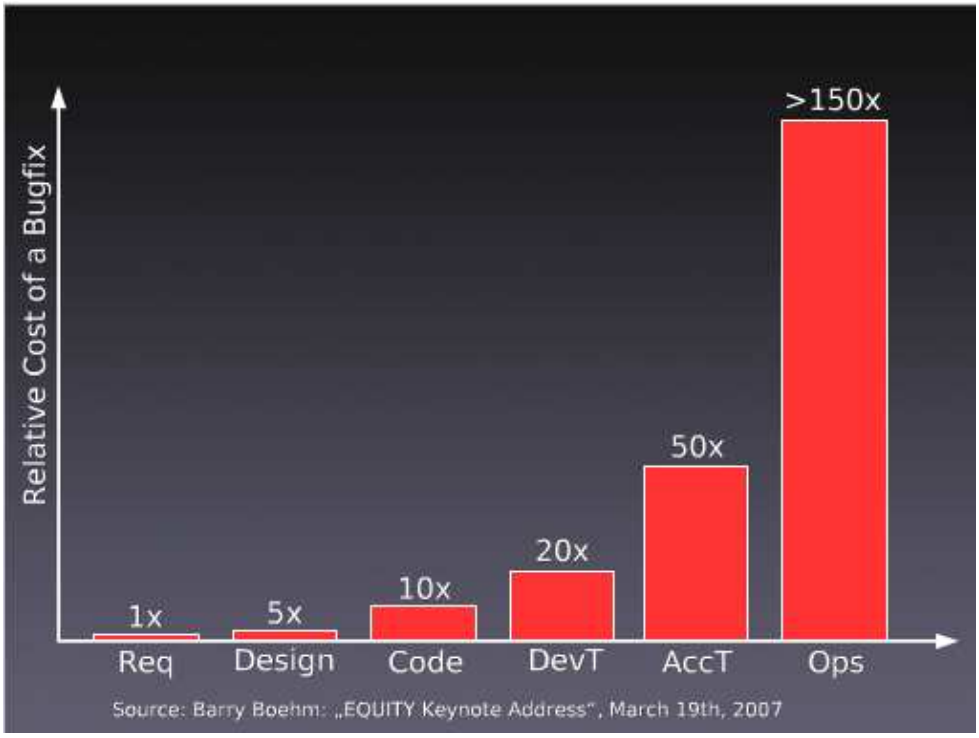
Una característica de las metodologías ágiles es el hecho de que son iterativas. La clave del desarrollo iterativo es proveer partes funcionales y operativas de un conjunto de funcionalidades del software que se encuentra en construcción y por lo tanto del sistema final.

Cada una de las funcionalidades a proveer debe estar probada y ser integrada bajo las mismas condiciones como si fuese la entrega del sistema final.

El punto de trabajar con iteraciones es que se ha comprobado que es realmente productivo ya que el cliente se puede sentar frente al sistema y empezar a utilizarlo y es cuando nuevos defectos o la mala interpretación que pudo existir de algún requerimiento se manifiesta y es visible para el proyecto, lo que permite tomar acción rápidamente y no esperar hasta la entrega de un producto final, donde el costo de corregir errores se incrementa considerablemente.

A continuación en el Gráfico 3 se puede observar la relación del costo de corregir errores en el software en las distintas fases del ciclo de desarrollo.

Gráfico 3 Costo Relativo de corregir errores en distintas fases de ciclo de desarrollo de software expuesto por el profesor Barry Boehm durante la conferencia de Equity, Holanda, en Marzo del 2007



2.2 Manifiesto Ágil (*Agile Manifesto*)

El 13 de Febrero del 2001 en el alojamiento Snowbird Sky Resort en las montañas Wasatch en Utah, 17 personas se reunieron para conversar, esquiar y relajarse. Entre estas personas se encontraban Kent Beck, Alistair Cockburn y Martin Fowler, entre otros. La idea de la reunión era tratar aspectos y compartir ideas sobre procesos para el desarrollo de software que estaban surgiendo como alternativa a las metodologías de desarrollo de software tradicionales, que consideraban como pesadas, rígidas y altamente dependientes de planificaciones detalladas previas al desarrollo. Como resultado de esta reunión, nace lo que se denomina el "Manifiesto para el desarrollo de software Ágil" [8]. Dentro de este manifiesto, se expone lo siguiente:

"Estamos descubriendo formas mejores de desarrollar software tanto por nuestra propia experiencia como ayudando a terceros. A través de este trabajo hemos aprendido a valorar:

- **Individuos e Interacciones** sobre procesos y herramientas.
- **Software funcionando** sobre documentación extensiva.
- **Colaboración con el cliente** sobre negociación contractual.

[8] AgileManifesto.org. Manifesto for Agile Software Development. http://agilemanifesto.org.

- **Respuesta ante el cambio** sobre seguir un plan.

Esto es, aunque valoramos los elementos de la derecha, valoramos más los elementos de la izquierda."

2.3 Programación Extrema (XP – Extreme Programming)

El origen de la programación extrema proviene de principios de los años 90 cuando Kent Beck trató de encontrar una mejor forma de desarrollar software cuando se encontraba gestionando un proyecto en la empresa automotriz DaimlerChrysler.

La programación extrema buscar mejorar un proyecto de software por medio de 5 dimensiones esenciales:

- **Comunicación:** Los programadores extremos se comunican constantemente con sus clientes y con sus compañeros de trabajo.
- **Simplicidad:** Los programadores extremos mantienen un diseño simple y limpio.
- **Retroalimentación:** Los programadores extremos obtienen retroalimentación probando el software desde el primer día en que se empieza a construir el mismo. Adicionalmente, entregan el software lo más temprano posible a sus clientes e implementan los cambios sugeridos por estos últimos.
- **Respeto:** Cada pequeño éxito depende de cada contribución de los miembros del equipo.
- **Coraje:** Los miembros del equipo tienen como reto responder a los cambios de requisitos y tecnologías durante el proyecto.

A continuación en la Tabla 5 se mencionan las reglas de la programación extrema[9].

Tabla 5 Reglas de la programación extrema

Fase	Regla	Descripción
Planificación	Se escriben Historias de Usuario	Son escritas por los clientes o posibles usuarios del sistema acerca de las cosas que este debe hacer.
	Plan de liberación	Se realiza una reunión con la finalidad de crear un plan por cada iteración de forma individual.
	Realizar pequeñas liberaciones	Se realizan pequeñas liberaciones de manera frecuente a los clientes.
	El proyecto se divide en iteraciones	Se divide el calendario de trabajo con una serie de iteraciones con una duración de 1 a 3 semanas cada una.
	Planificación de iteraciones	Se realiza una reunión al comienzo de cada iteración para determinar qué tareas de programación se necesitan, el esfuerzo y quién lo va a realizar.

[9] Extreme Programming, a gentle introduction http://www.extremeprogramming.org/.

Gestión	Proporcionar un espacio de trabajo abierto al equipo	Facilitar un área de trabajo sin barreras y donde nadie sea dueño del espacio, lo que permite mejorar la comunicación entre los miembros del equipo.
	Crear un camino sustentable	Ayuda a planificar las iteraciones y las liberaciones evitando caer en estimaciones irreales y que sobrecarguen demasiado al equipo de trabajo.
	Reuniones diarias	Se mantienen reuniones diarias con los miembros del equipo estando todos de pie y evitando largas discusiones. Los desarrolladores mencionan: ¿Qué se logró ayer?, ¿Qué se pretende hacer hoy?, ¿Qué problemas generan retrasos?
	Medir la velocidad del proyecto	Se mide cuánto trabajo se ha logrado en el proyecto.
	Rotar el personal	Rotar a los miembros del equipo para que todos conozcan de todo y no se tenga que depender en un solo individuo para realizar ciertas tareas.
	Corregir el proceso cuando falla	Con respecto a estas reglas, no se debe vacilar para cambiar alguna si los resultados no son los esperados.
Diseño	Simplicidad	Si se encuentra algo complejo, cambiarlo por algo simple. Es más rápido y barato remplazar código al principio que perder tiempo después.
	Escoger una metáfora para el sistema	Los nombres de los objetos son importantes para el entendimiento del diseño del sistema sin tener que conocer a profundidad sobre este.
	Usar tarjetas CRC	Las tarjetas de clase, responsabilidad y colaboración contribuyen a que los miembros del equipo puedan aportar un gran número de ideas.
	Programa para explorar soluciones potenciales	Disponer de un explorador de soluciones para cuando se presenten problemas técnicos o de diseño. El programa se debe enfocar en corregir el problema sin tomar en cuenta otras posibles preocupaciones.
	Nunca agregar funcionalidad tempranamente	Mantener el código listo para cambios inesperados requiere de un diseño simple. Agregar funcionalidad extra exige un diseño más complejo.
	Refactorizar	Eliminar redundancia de código, eliminar funcionalidades sin utilizar y actualizar diseños obsoletos significa refactorizar. Esto ahorra tiempo y mejora la calidad.
Codificar	El cliente siempre está disponible	Todas las fases de XP requieren comunicación con el cliente, cara a cara, en el lugar de trabajo.
	Codificar con estándares	Codificar con estándares mantiene la consistencia en el código y lo hace más fácil de leer y entender por el equipo de trabajo.
	Codificar las pruebas unitarias primero	Cuando se crean las pruebas unitarias primero es más rápido y fácil crear el código.
	Programación de a pares	Todo el código a ser liberado a producción es creado por dos personas trabajando juntas en una sola computadora.
	Sólo un par integra código al mismo tiempo	Las integraciones de código se deben realizar de forma secuencial y no en paralelo.
	Integrar regularmente	Los desarrolladores deben integrar y colocar el código en el repositorio de código cada pocas horas cuando sea posible.
	Dedicar un computador para la integración	Una computadora dedicada para liberaciones de forma secuencial cuando los desarrolladores se encuentran en un mismo lugar.
	Propiedad colectiva	Cualquier desarrollador puede cambiar una línea de código, corregir un defecto o refactorizar. Nadie es dueño del código, lo que evita cuellos de botella.
Pruebas	Pruebas unitarias	Todo el código debe tener pruebas unitarias. Si se descubre código sin pruebas unitarias, se deben crear en ese preciso momento.
	El código debe pasar las pruebas unitarias	Todo el código debe pasar las pruebas unitarias antes de ser liberado.
	Defectos	Cuando se encuentra un defecto se crean nuevos escenarios de pruebas para asegurar que el defecto no siga presente en el código.
	Pruebas de aceptación	Las pruebas de aceptación se crean a partir de las historias de usuarios. Una historia de usuario puede tener varias pruebas de aceptación.

2.4 Crystal

Crystal se conoce como una familia de metodologías de desarrollo de software propuestas por Alistair Cockburn a partir de 1991. Las metodologías Crystal se basan en el hecho de que hay que tener en cuenta las características del proyecto para aplicar una metodología. No es lo mismo un proyecto en el que intervienen pocas personas que otros en donde intervienen muchas. Creer que todos los proyectos son iguales independientemente de su tamaño es un error que puede derivar desde pérdidas económicas hasta el fracaso completo.

El nombre Crystal deriva de la caracterización de los proyectos según 2 dimensiones, tamaño y complejidad (como en los minerales, color y dureza). Las metodologías Crystal van, en función del tamaño del equipo de proyecto, denominándose con colores más oscuros y en función de la criticidad por la dureza del cristal (en alusión al mineral), de manera que se tiene:

- Metodología Crystal Clear (equipos hasta seis personas).
- Metodología Crystal Amarillo (equipos entre seis y veinte personas).
- Metodología Crystal Anaranjado (equipos entre veinte y cuarenta personas).
- Metodología Crystal Rojo (equipos entre cuarenta y ochenta personas).
- Crystal Marrón (equipos entre ochenta y doscientas personas).
- Metodología Diamond y Sapphire en función de si del sistema depende la vida de las personas o la subsistencia de la organización.

La Tabla 6 resume las características principales de la familia de metodologías Crystal[10].

[10] Cockburn, Alistair (2004). Crystal Clear: A Human-Powered Methodology for Small Teams. Addison-Wesley Professional, ISBN-10: 0-201-69947-8.

Tabla 6 Características comunes del conjunto de metodologías de Crystal Clear

Característica	Descripción
Entregas Frecuentes	• Se basan en una estrategia de desarrollo iterativa e incremental. En función de las características del proyecto se pueden establecer entregas desde semanales hasta trimestrales. • Va en consonancia con la naturaleza adaptativa del proceso de desarrollo de software, permitiendo ajustar progresivamente el sistema a las necesidades de los usuarios.
Mejora Reflexiva	• La existencia de un desarrollo iterativo e incremental, favorece la mejora del sistema y de los procesos a través del feedback que se obtiene tanto de los usuarios como del propio equipo de proyecto. Si algo no funciona saldrá a la luz más pronto que tarde. • No es necesario esperar al resultado de las entregas para pensar en posibles mejoras en los procesos. Por eso, es frecuente encontrarse con reuniones cada dos o tres semanas del equipo de proyecto específicas para detectar e intentar corregir aspectos de la dinámica del proyecto y del proceso de desarrollo que no están funcionando como debieran.
Comunicación Cerrada	• El equipo de proyecto debe encontrarse en una misma ubicación física, si es posible compartiendo la misma habitación. De esta forma se reducen las distracciones, se mejora la concentración, la información fluye más rápidamente dentro del equipo de proyecto, las dudas se resuelven más rápido y se favorece la colaboración entre los miembros del equipo de proyecto. • Por otro lado se disminuyen las limitaciones inherentes a la comunicación a distancia, es decir, se reduce la comunicación por correo electrónico y la necesidad de documentación extra, entre otros.
Seguridad Personal	• En el equipo de proyectos todos tienen derecho a expresar sus ideas y opiniones (dentro de un orden). Cada integrante debe tener la seguridad de que no va a ser ridiculizado o no tenido en cuenta.
Enfoque	El enfoque en las metodologías Crystal tiene dos vertientes: Por un lado el enfoque busca conseguir que se pueda dedicar tiempo suficiente sin interrupciones en las diferentes tareas de un proyecto para que progrese adecuadamente y por otro el enfoque en la dirección del proyecto. En el primer caso se establecen períodos de no interrupción a los desarrolladores (por regla general dos horas) y por otro garantizar la continuidad en el desarrollo de las tareas superponiendo desarrolladores con antelación al cambio de proyecto de uno de ellos. En el segundo caso, para conseguir que la dirección del proyecto sea adecuada es necesario que los desarrolladores tengan totalmente claros los objetivos del mismo y que el responsable del proyecto priorice en cada momento los objetivos para permitir al equipo de proyecto centrarse en tareas concretas.
Fácil acceso a usuarios expertos	• La participación e implicación de usuarios expertos en el proyecto resulta esencial. • Estas metodologías no exigen que los usuarios expertos tengan presencia continua en el equipo de proyecto (se es consciente de que no todas las organizaciones pueden poner personal de estas características al servicio del proyecto), pero sí que como mínimo semanalmente se deben mantener encuentros de al menos un par de horas con ellos y existir accesibilidad para tener comunicaciones telefónicas si fuera necesario.
Entorno técnico	Generar pruebas automatizadas, gestionar la configuración y la integración continua.

2.5 Desarrollo "Lean"

La metodología de desarrollo "Lean" tiene sus raíces en el sistema de producción de la empresa automotriz Toyota y busca ayudar a las organizaciones que desarrollan software a optimizar sus procesos y métodos de producción con la finalidad de entregar productos más rápidamente y de mejor calidad. Los pioneros en la implementación de esta metodología en el mundo del desarrollo de software son Mary y Tom Poppendieck.

Con el desarrollo "Lean", el foco se encuentra sobre las personas y la comunicación, lo que quiere decir que si las personas que producen el software son respetadas y se comunican eficientemente, existe una mayor probabilidad que se entregue un producto que logre satisfacer las necesidades de los clientes.

La Tabla 7 resume los principios básicos de la metodología de desarrollo "Lean" [11].

[11] AgileSoftwareDevelopment.com. Lean Principles. http://agilesoftwaredevelopment.com/leanprinciples.

Tabla 7 Los 7 Principios básicos de la metodología de Desarrollo "Lean"

Principios	Características
Eliminar el desperdicio	• Se basa en proveer un liderazgo técnico y de mercado. • Que los procesos generen valor. • Escribir menos código.
Crear conocimiento	• Crear equipos que puedan dar respuestas a problemas y aportar soluciones rápidamente. • Mantener una cultura de mejoramiento continuo. • Enseñar métodos para resolver problemas.
Construir con calidad	• Empezar a pensar en la calidad del software antes de colocar la primera línea de código. • Automatizar las pruebas, desarrollo e instalaciones del software y hacerlo sin que los demás piensen que el software va a dejar de funcionar. • Refactorizar para eliminar la duplicidad de código y la complejidad.
Compromiso diferido	• Tomar las decisiones cuando se dispone de suficiente información para tomar la dirección correcta. • Romper las dependencias entre los componentes del software. Mientras menos dependencias existan, es mejor. • Hacer un código que sea abierto a los cambios y no vacilar en cambiarlo si es necesario.
Optimizar el todo	• Enfocarse en el flujo de valor. Ver el todo y optimizar toda la organización. • Entregar un producto completo.
Entregar rápido	• Reducir el tamaño de los proyectos, acortar los ciclos de entrega, estabilizar el ambiente de trabajo y erradicar las malas prácticas. • Limitar el trabajo en base a la capacidad. No abordar más de lo que realmente se puede. • No enfocarse en cómo utilizar los recursos en un 100%, sino más bien en los tiempos para salir al mercado y los tiempos de respuesta para los clientes.
Respetar las personas	• Entrenar a los supervisores y promover el desarrollo del liderazgo. • Mover la responsabilidad de la toma de decisiones al nivel más bajo. Dejar que el equipo lleve a cabo sus estimaciones ya que al final el equipo es el que desarrolla el software y los que tienen mayor conocimiento sobre cómo hacerlo y cuánto les puede tomar. • Promover que los miembros del equipo se involucren con pasión en las cosas que hacen.

2.6 Scrum

Scrum se ha utilizado para desarrollar productos complejos desde principios de los '90. Scrum no es un proceso o una técnica para desarrollar o crear productos de software, sino que es un marco en el que se pueden emplear diversos procesos y técnicas, a la vez que proporciona un marco dentro del cual se pueden desarrollar productos complejos.

La historia y existencia de Scrum son el resultado de los esfuerzos en conjunto de Jeff Sutherland trabajando con Jeff McKenna y por otra parte de Ken Schwaber con Mike Smith y Chris Martin y fue presentado formalmente por primera vez y publicado en OOPSLA (Conferencia anual de aplicaciones, sistemas, lenguajes y programación orientada a objetos) en 1995.

Scrum, que se basa en la teoría del control empírico de procesos, emplea un enfoque iterativo e incremental para optimizar la previsibilidad y controlar los riesgos.

La tabla 8 muestra los pilares fundamentales del control empírico de procesos.

Tabla 8 Pilares que sostienen toda implementación del control empírico de procesos

Pilar	Definición
Transparencia	• La transparencia garantiza que los aspectos del proceso que afectan al resultado, son visibles para aquellos que administran dicho resultado. Estos aspectos no sólo deben ser transparentes, sino también conocidos. Es decir, cuando alguien que inspecciona un proceso cree que algo está hecho, esto debe ser equivalente a su definición de "hecho".
Inspección	• Se deben inspeccionar con la frecuencia suficiente los diversos aspectos del proceso para que puedan detectarse variaciones inaceptables en el mismo. • La frecuencia de inspección debe tener en cuenta que todos los procesos se cambian por el propio acto de inspección. El dilema se presenta cuando la frecuencia de inspección requerida excede la tolerancia del proceso a ser inspeccionado. Afortunadamente, esto parece no aplicar al desarrollo de software. El otro factor es la habilidad y la diligencia de la gente que inspecciona los resultados del trabajo.
Adaptación	• Si el inspector determina, a través de la inspección, que uno o más aspectos del proceso están fuera de los límites aceptables, y que el producto resultante será inaceptable, debe ajustar el proceso o el material procesado. El ajuste debe realizarse lo más rápidamente posible para minimizar una desviación mayor.

El marco de Scrum se compone de un conjunto de equipos de Scrum y sus roles asociados; así como de bloques de tiempo, artefactos y reglas.

Los equipos Scrum están diseñados para optimizar la flexibilidad y la productividad, para lo cual, son auto-gestionados, multifuncionales, y trabajan en iteraciones. Cada equipo Scrum tiene tres roles:

- El ScrumMaster (Facilitador).
- El Propietario del Producto.
- El Equipo Scrum.

Scrum emplea bloques de tiempo para crear regularidad. Los elementos de Scrum basados en bloques de tiempo son:

- La Reunión de Planificación de la Entrega.
- El Sprint.
- La Reunión de Planificación del Sprint.
- La Revisión del Sprint.
- La Retrospectiva del Sprint.
- El Scrum Diario.

Scrum emplea 3 artefactos principales, los cuales se mencionan a continuación:

- El Product Backlog.
- El Sprint Backlog.
- El Burndown de la entrega.

En cuanto a las “reglas” en Scrum, estas sirven de unión para los bloques de tiempo, los roles y los artefactos de Scrum. Por ejemplo, una regla de Scrum es que sólo los miembros del equipo - la gente comprometida en convertir el Product Backlog en un incremento - pueden hablar durante un Scrum Diario.

La Tabla 9 muestra las características de los roles de Scrum. También la Tabla 10 muestra las características de los bloques de tiempo de Scrum y en cuanto a la Tabla 11 muestra las características de los artefactos de Scrum.

Tabla 9 Características de los roles de Scrum

Rol	Características
Scrum Master	• Es responsable de asegurar que el equipo Scrum adhiere a los valores, prácticas y normas Scrum. • Ayuda a que el equipo Scrum y la organización adopten Scrum. • Enseña al equipo Scrum mediante entrenamiento y liderándolo para que sea más productivo y a que construya productos de mayor calidad. Ayuda a que el equipo Scrum comprenda y utilice la auto-gestión y a ser multidisciplinario.
Propietario del Producto	• Es la única persona responsable de gestionar el Product Backlog y asegurar el valor del trabajo que el equipo lleva a cabo. • Mantiene el Product Backlog y asegura la visibilidad del mismo para todos. Contribuye a que todo el mundo conozca qué elementos tienen la máxima prioridad y en qué se va a trabajar. • Es una persona, no un comité. Si existe un comité, este debe ser capaz de convencerle para cambiar la prioridad de un elemento. • Para que tenga éxito, todos en la organización deben respetar sus decisiones. Nadie está autorizado a obligar al equipo a trabajar bajo un conjunto diferente de prioridades, y a los equipos no se les permite prestar atención a nadie que diga lo contrario.
El Equipo Scrum	• Convierte el Product Backlog en incrementos de funcionalidad potencialmente entregables en cada Sprint. • Debe ser multifuncional. Los miembros del equipo deben tener todas las habilidades necesarias para crear un incremento de trabajo. • Los miembros deben tener habilidades especializadas, como la programación, el control de calidad, el análisis de negocio, la arquitectura, el diseño de la interfaz de usuario, bases de datos, entre otros. • Todo el mundo interviene, incluso si eso requiere aprender nuevas habilidades o recordar las antiguas. Las personas que se niegan a escribir código, ya que son arquitectos o diseñadores, no se ajustan bien al equipo. • No existen sub-equipos dedicados a áreas particulares. • Debe ser capaz de auto-organizarse. Nadie - ni siquiera el Scrum Master - dice al equipo cómo convertir el Product Backlog en incrementos de funcionalidad entregable. El equipo busca por su cuenta la mejor forma de hacerlo. • El tamaño óptimo para un equipo es de siete personas, más o menos dos. Si hay más de nueve miembros, el problema simplemente es que se necesita demasiada coordinación.

Tabla 10 Características de los bloques de tiempo de Scrum

Bloque de Tiempo	Características
Reunión de Planificación de la Entrega	• El propósito de la planificación de la entrega es establecer un plan y unas metas que los equipos Scrum y el resto de las organizaciones puedan entender y comunicar. • Responde a las preguntas: "¿Cómo podemos convertir la visión en un producto ganador, de la mejor manera posible? ¿Cómo podemos alcanzar o mejorar la satisfacción del cliente deseada y el Retorno de la Inversión?". • Establece el objetivo de la entrega, el Product Backlog de mayor prioridad, los principales riesgos, y las características generales y la funcionalidad que va a contener la entrega. • Establece una fecha probable de entrega, y el coste, que debería mantenerse si no cambia nada.
Sprint	• Representa una iteración. • No se realizan cambios que afecten al objetivo del Sprint. • La composición del equipo se mantiene constante durante todo el Sprint. • Se componen de: la Reunión de Planificación de Sprint, el trabajo de desarrollo, la Revisión del Sprint, y la Retrospectiva del Sprint. • Ocurren uno tras otro, sin tiempo entre ellos. • Puede ser cancelado antes de que el bloque de tiempo del Sprint se haya terminado. Sólo el Propietario del Producto tiene la autoridad para cancelar el Sprint, aunque puede hacerlo bajo la influencia de los interesados, del equipo, o del Scrum Master. ¿Bajo qué tipo de circunstancias puede un Sprint ser cancelado? La gerencia puede necesitar cancelar un Sprint si el objetivo del Sprint queda obsoleto. Esto podría ocurrir si la empresa cambia de dirección, o si cambia el mercado o las condiciones de la tecnología. Las cancelaciones de Sprints son a menudo traumáticas para el equipo, y muy poco frecuentes.
Reunión de Planificación del Sprint	• Durante la reunión la iteración del Sprint es planificada. • La reunión se restringe a un bloque de tiempo de ocho horas para un Sprint de un mes. Para Sprints más cortos, se debería reservar para esta reunión un tiempo proporcionalmente menor, aproximadamente el 5% de la longitud total del Sprint (por ejemplo, para un Sprint de dos semanas sería una Reunión de Planificación de cuatro horas). • La Reunión consta de dos partes. La primera parte, que representa el "¿Qué?", es cuando se decide qué se hará durante el Sprint. La segunda parte, que representa el ¿Cómo?, es cuando el equipo determina cómo se va convertir una funcionalidad en un incremento del producto durante el Sprint. • El equipo de Scrum trabaja en conjunto con el Propietario del Producto para determinar qué funciones se van a desarrollar durante el próximo Sprint. • La información de entrada para esta reunión es el Product Backlog, el último incremento del producto, la capacidad del equipo y el rendimiento anterior del equipo. • Sólo el equipo puede evaluar lo que puede lograr en el próximo Sprint. Es decisión de este.
Revisión del Sprint	• Se lleva a cabo al final del Sprint. Tiene una duración aproximada de 4 horas para un Sprint de un mes. • Es una reunión informal en la que el Equipo Scrum y las partes interesadas debaten sobre lo que se acaba de hacer. En base a eso, y a los cambios en el Product Backlog que se hayan hecho durante el Sprint, colaboran para determinar las próximas cosas que se podrían hacer. • El Propietario del Producto identifica lo que se ha hecho y lo que no se ha hecho. El equipo analiza lo que salió bien durante el Sprint y cuáles son los problemas que encontró, y cómo resolvió estos problemas. • El Equipo Scrum muestra el trabajo que ha sido completado y responde preguntas. El Propietario del Producto analiza el Product Backlog en su estado actual y proyecta las fechas probables de finalización con distintos supuestos de velocidad para la siguiente reunión de Planificación del Sprint.

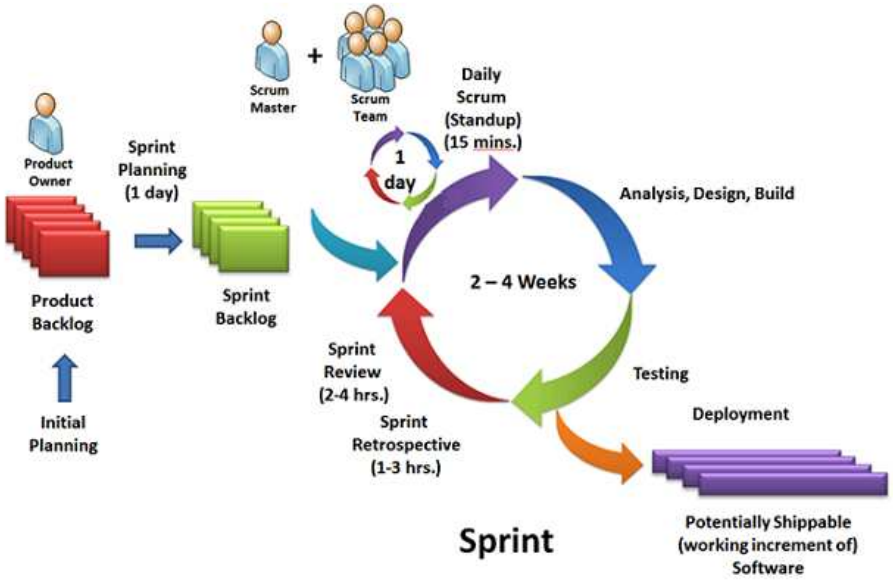
Retrospectiva del Sprint	• Se realiza después de la Revisión del Sprint y antes de la Reunión de Planificación del Sprint y tiene una duración aproximada de 3 horas para un Sprint de un mes. • El Scrum Master alienta al Equipo Scrum a revisar, en el marco de proceso y prácticas de Scrum, su proceso de desarrollo, para que sea más eficaz y agradable para el próximo Sprint. • Tiene como propósito inspeccionar cómo fue el último Sprint en lo que respecta a las personas, relaciones, procesos y herramientas. Por ejemplo, identificar y priorizar los elementos que si se hiciesen de forma diferente podrían producir mejoras, tales como las reuniones, herramientas, métodos de comunicación, la definición de lo "hecho", entre otros. • La salida resultante son acciones de mejora a implementar durante el próximo Sprint.
Scrum Diario	• Todos los días el Equipo Scrum se reúne 15 minutos en una reunión de inspección y adaptación. • Se lleva a cabo a la misma hora y en el mismo lugar durante todos los Sprints. • Durante la reunión, cada miembro del equipo, explica: lo que ha conseguido hacer desde la última reunión; lo que va a hacer hasta la próxima reunión, y qué obstáculos tiene en su camino. • Mejora las comunicaciones, elimina otras reuniones, identifica y elimina los impedimentos al desarrollo, destaca y promueve la rápida toma de decisiones y mejora el nivel de conocimiento de los proyectos. • El Scrum Master se asegura de que el Equipo mantiene la reunión. • El Equipo es responsable de conducir el Scrum Diario. • No es una reunión de seguimiento del proyecto, sino sólo para la gente que trabaja en transformar los elementos del Product Backlog en un incremento.

Tabla 11 Características de los artefactos de Scrum

Artefacto	Características
Product Backlog	• Es una lista de los requisitos del producto que se está desarrollando. • Nunca está completo, cambia constantemente ya que se incluyen correcciones, nuevas funciones, tecnologías, entre otros y evoluciona en la medida que el producto evoluciona. • Los elementos del Product Backlog deben tener los siguientes atributos: una descripción, una prioridad, y una estimación. • Está ordenado por prioridad. La parte más prioritaria determina las actividades de desarrollo que se llevarán a cabo de forma inmediata. • Sólo los elementos de mayor prioridad se encuentran de forma detallada, en especial los que el equipo de Scrum ocupará durante el próximo Sprint. • El equipo Scrum es responsable de la estimación de todos los elementos, a pesar de que pueden contar con la ayuda del propietario del producto.
Sprint Backlog	• Se compone de las tareas que el equipo realiza para convertir los elementos del Product Backlog en un incremento "hecho". • Constituyen todo el trabajo que el equipo identifica como necesario para cumplir con el Objetivo del Sprint. • Los elementos del Sprint Backlog deben descomponerse para ser entendidos durante el Scrum diario. • El tamaño normal para un elemento del Sprint Backlog en el que se está trabajando es de un día o menos. • El equipo modifica el Sprint Backlog a lo largo de todo el Sprint, así como la parte de Sprint Backlog adicional que surja durante el Sprint.
Burndown de la Entrega	• Es un gráfico que registra la suma del esfuerzo restante estimado del Product Backlog a lo largo del tiempo. • El esfuerzo se estima en cualquier unidad de trabajo que el equipo Scrum y la organización hayan decidido. Generalmente se utiliza el Sprint. • El Propietario del Producto mantiene publicados el Product Backlog y la gráfica de Burndown de Entrega actualizados en todo momento. Se puede trazar una línea de tendencia en la gráfica, basándose en el cambio en el trabajo restante.

El Gráfico 4 muestra la representación de Scrum[12].

Gráfico 4 Representación de Scrum



2.7 CMM y CMMI

Un modelo de capacidad y madurez (CMM – Capacity Maturity Model) es una representación simplificada de un entorno y contiene los elementos de procesos efectivos basados en los conceptos desarrollados por Crosby, Deming, Juran y Humphrey[13].

En 1930, Walter Shewhart comenzó a trabajar en la mejora de procesos con sus principios de control estadístico de calidad. Estos principios fueron refinados por Edward Deming, Phillip Crosby y Joseph Juran. Watts Humphrey, Ron Radice y otros extendieron estos principios[2] y empezaron a aplicarlos al software en trabajos de IBM (International Business Machines) y el SEI (Software Engineering Institute – Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon) para el año de 1989.

Posteriormente, el SEI creó el primer diseño de CMM para organizaciones de desarrollo de software y lo publicó en un libro denominado, "El modelo de capacidad y madurez: Guía para el mejoramiento continuo del proceso de Software" en el año 1995[2].

[12] SCRUM.org. The SCRUM guide, the official rulebook. http://www.scrum.org/scrumguides/
[13] CMMI® for Development, Version 1.3, http://www.sei.cmu.edu/reports/10tr033.pdf, Página 5.

Los modelos de capacidad y madurez (CMMs) se enfocan en la mejora de los procesos de una organización. Contienen elementos esenciales de procesos efectivos para una o más disciplinas describiendo un camino hacia el mejoramiento continuo que va desde procesos inmaduros a procesos disciplinados y maduros mejorando la calidad y efectividad.

Tal como los modelos de capacidad y madurez, CMMI (Modelo de capacidad y madurez integrado) provee una guía de referencia a ser utilizada para el desarrollo de los procesos de una organización. El modelo de capacidad y madurez integrado (CMMI), "no es un proceso o una descripción de procesos". Cada organización dispone de procesos que dependen de distintos factores, bien sea por el dominio en el que se encuentra, su estructura o tamaño. Es por esta razón que no existe una relación de uno a uno entre el modelo y los procesos de una organización.

CMMI busca ayudar a las organizaciones a identificar las fortalezas y debilidades de sus procesos y a promover cambios en dichos procesos con la finalidad de convertir aquellas debilidades en fortalezas. CMMI se aplica a equipos, grupos de trabajo, proyectos, divisiones y organizaciones enteras y está basado en un conjunto de mejores prácticas para mejorar la efectividad, eficiencia y calidad.

El marco de trabajo de CMMI

CMMI ofrece soluciones que ayudan a mejorar el rendimiento de las organizaciones y su habilidad para cumplir con los objetivos de negocio. El marco de trabajo de CMMI provee las personas, los modelos, los cursos de entrenamiento y los métodos de evaluación para medir objetivamente el progreso en las mejoras.

Actualmente se proveen tres tipos o modelos de CMMI. Dichos modelos se basan en mejores prácticas y metas de mejoramiento continuo que las empresas utilizan para evaluarse y tratar de mejorar sus procesos. Estas metas y prácticas están organizadas en grupos intuitivos denominados "áreas de proceso".

La Tabla 12 presenta los distintos tipos de CMMI.

Tabla 12 Tipos de CMMI

Tipo	Descripción
CMMI para adquisiciones	Es un modelo que sirve de guía a las organizaciones en la gestión de la cadena de suministros, para adquirir e integrar productos y servicios y cumplir con las necesidades de los clientes.
CMMI para desarrollo	Es un modelo que sirve de guía para la mejora de procesos en organizaciones que desarrollan productos y servicios.
CMMI para servicios	Es un modelo que sirve de guía para organizaciones que establecen, gestionan y entregan servicios para satisfacer las necesidades de sus clientes y de los usuarios finales.

Hoy en día CMMI se encuentra en su versión oficial 1.3 que fue liberada durante el 2010 (http://www.sei.cmu.edu/reports/10tr033.pdf). La última versión oficial anterior a esta fue la 1.2 la cual fue liberada a partir del 2007.

CMMI v1.3 para desarrollo

El modelo propuesto por CMMI para desarrollo utiliza conceptos de gestión e ingeniería para ayudar en la entrega de productos a tiempo y de alta calidad, especialmente para aquellas organizaciones que dependen fuertemente del desarrollo de software.

Este modelo cubre el ciclo de vida de productos y servicios desde la concepción de estos hasta la entrega y mantenimiento. Las prácticas que ofrece son flexibles para ser aplicadas a diferentes tipos de industrias y a la vez son estables y consistentes lo que a su vez sirve como una referencia contra la que la organización puede evaluarse y compararse a sí misma.

Con la adopción de este modelo como guía de referencia, las organizaciones pueden lograr:

- Mejorar la satisfacción del cliente.
- Aumentar la calidad de los productos desarrollados.
- Realizar las entregas en los tiempos acordados.
- Minimizar los costos de desarrollo.
- Garantizar un retorno de inversión.
- Mejorar las condiciones de trabajo de los empleados.

Categorías de componentes de CMMI v1.3

Los componentes del modelo están agrupados en tres categorías:

- Requeridos.
- Esperados.
- Informativos.

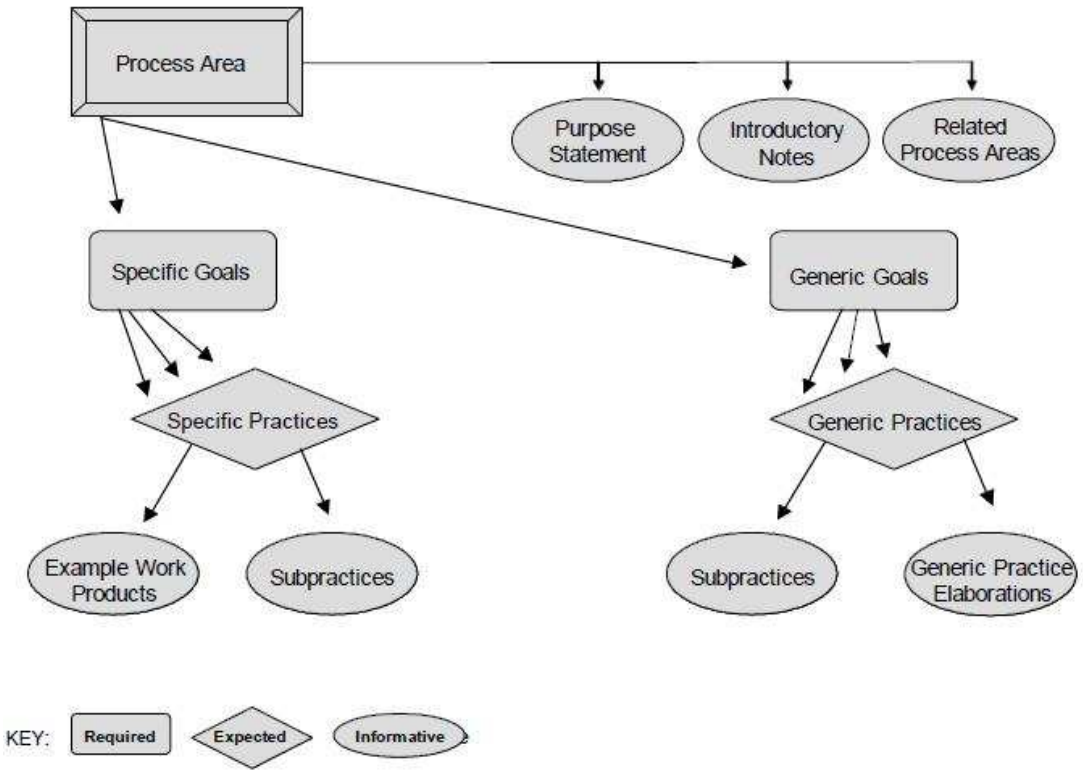
La Tabla 13 lista las categorías de componentes de CMMI v1.3

Tabla 13 Categorías de componentes de CMMI v1.3

Categoría	Interpretación
Componente Requeridos	• Son componentes esenciales para alcanzar la mejora de procesos en una determinada área de proceso. • Esta mejora debe ser visiblemente implementada en los procesos de la organización. • Los componentes requeridos en CMMI son las metas específicas y genéricas. • El cumplimiento de las metas es utilizada en las evaluaciones como la base para decidir cuándo se ha logrado satisfacer un área de proceso.
Componentes Esperados	• Son componentes que describen las actividades que son importantes para lograr satisfacer un componente requerido. • Sirven de guía para aquellos que implementan las mejoras y realizan las evaluaciones sobre los procesos. • Los componentes esperados en CMMI son las prácticas genéricas y específicas. • Antes que las metas específicas y genéricas puedan ser satisfechas, las prácticas específicas y genéricas tal como se describen o alternativas aceptables y aplicables a estas, deben estar presentes en los procesos implementados de la organización.
Componentes Informativos	• Son componentes que ayudan a los usuarios a entender los componentes requeridos y esperados. • Estos componentes pueden ser cajas de ejemplos, explicaciones detalladas u otra información útil. • Las subprácticas, notas, referencias, títulos de metas, títulos de prácticas, fuentes, ejemplos de productos de trabajo y la elaboración de las prácticas genéricas, son ejemplos de componentes informativos.

El Gráfico 5 muestra una representación de los componentes de CMMI v1.3

Gráfico 5 Componentes de CMMI v1.3



La Tabla 14 explica el detalle de cada uno de los componentes de CMMI v1.3

Tabla 14 Detalle de los componentes de CMMI v1.3

Componente	Definición
Áreas de proceso	• Representan un conjunto de prácticas relacionadas en un área, que cuando se implementan de forma colectiva, se satisface un conjunto de metas consideradas importantes en el logro de mejoras de esa área en particular.
Declaraciones de propósito	• Describe la finalidad de un área de proceso y es un componente informativo. • Por ejemplo, la declaración de propósitos del área de proceso Definición de procesos de la organización es "El propósito de la Definición de procesos de la organización (OPD) es establecer y mantener un conjunto utilizable de activos de proceso de la organización y de estándares del entorno de trabajo".
Notas Introductorias	• La sección de "notas introductorias" del área de proceso describe los conceptos principales cubiertos por el área de proceso y es un componente informativo. • Un ejemplo de notas introductorias del área de proceso Planificación de proyecto es "La planificación empieza con los requerimientos que definen el producto y el proyecto".
Áreas de proceso relacionadas	• Lista las referencias a áreas de proceso que están en relación y refleja las relaciones de alto nivel entre las áreas de proceso. • Es un componente informativo. • Un ejemplo de una referencia encontrada en la sección de áreas de proceso relacionadas del área de proceso de Planificación de proyecto es "Para más información sobre la identificación y la gestión de riesgos, se remite al área de proceso de Gestión de riesgos".
Metas Específicas	• Describe las características únicas que deben estar presentes para satisfacer el área de proceso. • Una meta específica es un componente requerido del modelo que se utiliza en las evaluaciones para ayudar a determinar si se satisface un área de proceso. • Por ejemplo, una meta específica del área de proceso Gestión de configuración es "Se establece y se mantiene la integridad de las líneas base".
Metas Genéricas	• Las metas genéricas se denominan "genéricas" porque la misma declaración de la meta se aplica a múltiples áreas de proceso. • Una meta genérica describe las características que deben estar presentes para institucionalizar los procesos que implementan un área de proceso. • Una meta genérica es un componente requerido del modelo y se utiliza en las evaluaciones para determinar si se satisface un área de proceso. • Un ejemplo de una meta genérica es "El proceso se institucionaliza como un proceso definido".
Resúmenes de metas específicas y prácticas específicas	• El resumen de metas específicas y prácticas específicas proporciona un resumen de alto nivel de las metas específicas, que son componentes requeridos, y de las prácticas específicas, que son componentes esperados. • El resumen de metas específicas y prácticas específicas es un componente informativo.
Prácticas Específicas	• Es la descripción de una actividad que se considera importante para alcanzar la meta específica asociada. • Las prácticas específicas describen las actividades que se espera que produzcan la consecución de las metas específicas de un área de proceso. • Una práctica específica es un componente esperado del modelo. • Un ejemplo de una práctica específica del área de proceso de Monitorización y control de proyecto es "Monitorizar los compromisos contraídos frente a los identificados en el plan del proyecto".

Ejemplos de productos de trabajo	• Lista muestras de resultados de una práctica específica. • Estos ejemplos se denominan ejemplos de productos de trabajo porque a menudo hay otros productos de trabajo que son igual de eficaces pero no están en la lista. • Es un componente informativo del modelo. • Por ejemplo, un producto de trabajo típico de la práctica específica "Monitorizar los valores reales de los parámetros de planificación del proyecto frente al plan del proyecto" en el área de proceso de Monitorización y control de proyecto es "Registros de desviaciones significativas".
Subprácticas	• Es una descripción detallada que proporciona una guía para interpretar e implantar una práctica específica o genérica. • Las subprácticas pueden tomar un carácter prescriptivo, pero realmente son un componente informativo indicado sólo para proporcionar ideas que puedan ser útiles para la mejora de proceso. • Por ejemplo, una subpráctica de la práctica específica "Realizar acciones correctivas para los problemas identificados" en el área de proceso de Monitorización y control de proyecto es "Determinar y documentar las acciones apropiadas necesarias para tratar los problemas identificados".
Prácticas Genéricas	• Las prácticas genéricas se denominan "genéricas" porque la misma práctica se aplica a múltiples áreas de proceso. • Una práctica genérica es la descripción de una actividad que se considera importante para el logro de la meta genérica asociada. • Una práctica genérica es un componente esperado del modelo. • Por ejemplo, una práctica genérica de la meta genérica "El proceso se institucionaliza como un proceso gestionado" es "Proporcionar recursos adecuados para llevar a cabo el proceso, para desarrollar los productos de trabajo y para proporcionar los servicios del proceso".
Elaboraciones de las Prácticas Genéricas	• Aparecen después de una práctica genérica en un área de proceso, para proporcionar una guía sobre cómo la práctica genérica debería aplicarse de forma exclusiva al área de proceso. • Una elaboración de práctica genérica es un componente informativo del modelo. • Por ejemplo, una elaboración de la práctica genérica después de la práctica genérica "Establecer y mantener una política organizativa para planificar y ejecutar el proceso de planificación del proyecto" en el área de proceso de Planificación de proyecto es "Esta política establece expectativas de la organización para estimar los parámetros de planificación, para hacer compromisos externos e internos y para desarrollar el plan de gestión del proyecto".

Componentes Informativos de Soporte en CMMI v1.3

En muchos sitios, se necesita más información para describir un concepto. Este material informativo se presenta como uno de los siguientes componentes:

- Notas.
- Ejemplos.
- Referencias.

Cabe destacar que para ayudar a aquellas organizaciones que se desempeñan en entornos ágiles a interpretar las prácticas de CMMI v1.3, se utiliza el componente mencionado arriba denominado "Notas" para especificar el uso de prácticas ágiles.

La Tabla 15 lista los componentes informativos de CMMI v1.3

Tabla 15 Componentes informativos de CMMI v1.3

Componente	Definición
Notas	• Es un texto que puede acompañar casi a cualquier otro componente del modelo. • Puede proporcionar detalles, información previa o de base. • Una nota es un componente informativo del modelo. • Por ejemplo, una nota que acompaña a la práctica específica "Implementar las propuestas de acción seleccionadas que fueron desarrolladas en el análisis causal" del área de proceso "Análisis causal y resolución" es "Sólo deberían considerarse para una implementación más amplia los cambios que muestren ser de valor".
Ejemplos	• Es un componente que comprende texto y, a menudo, una lista de elementos, por lo general en una caja, que puede acompañar a casi cualquier otro componente y proporciona uno o más ejemplos para clarificar un concepto o una actividad descrita. • Un ejemplo es un componente informativo del modelo. • El siguiente es un ejemplo que acompaña a la sub-práctica "Documentar las no conformidades cuando no se pueden resolver dentro del proyecto" bajo la práctica específica "Comunicar problemas de calidad y asegurar la resolución de las no conformidades con el personal y gerentes" en el área de proceso de Aseguramiento de la calidad de proceso y de producto.
Referencias	• Es un enlace a información adicional o más detallada en las áreas de proceso relacionadas y puede acompañar a casi cualquier otro componente del modelo. • Una referencia es un componente informativo del modelo. • Por ejemplo, una referencia que acompaña a la práctica específica "Seleccionar los subprocesos que componen el proceso definido del proyecto según datos de estabilidad histórica y datos de capacidad" en el área de proceso de Gestión cuantitativa de proyecto es "Para más información sobre la biblioteca de activos de proceso de la organización, que podría incluir un elemento de proceso de capacidad conocida y requerida, se remite al área de proceso Definición de proceso de la organización".

Representaciones de CMMI v1.3

CMMI soporta dos caminos de mejora. Un camino permite a las organizaciones mejorar de forma incremental los procesos que corresponden a un área o áreas de proceso individuales seleccionadas por la organización. El otro camino permite a las organizaciones mejorar un conjunto de procesos relacionados, tratando de forma incremental conjuntos sucesivos de áreas de proceso.

Estos dos caminos de mejora se conocen como Representación Continua, que utiliza el término "nivel de capacidad" y la representación por etapas que utiliza el término "nivel de madurez". Independientemente de qué representación se seleccione, el concepto de niveles es el mismo. Los niveles caracterizan a la mejora desde un estado mal definido hasta un estado que utiliza información cuantitativa para determinar y gestionar las mejoras que se necesitan para satisfacer los objetivos de negocio de una organización.

Para alcanzar un nivel particular, una organización debe satisfacer todas las metas apropiadas del área o conjunto de áreas de proceso que son objeto de la mejora, independientemente de si es un nivel de capacidad o de madurez.

Estructura de las representaciones continua y por etapas

Los niveles de capacidad que pertenecen a la representación continua se aplican al logro de mejora de procesos de una organización en áreas de proceso individuales. Estos niveles son un medio para mejorar de forma incremental los procesos que corresponden a un área de proceso dada. En CMMI v1.3 existen 4 niveles de capacidad, numerados de 0 a 3.

Los niveles de madurez, que pertenecen a la representación por etapas, se aplican al logro de mejora de procesos de una organización en múltiples áreas de proceso. Estos niveles son un medio de predecir los resultados generales del siguiente proyecto que se acometa. Existen cinco niveles de madurez, numerados de 1 a 5.

La Tabla 16 muestra la comparación entre los niveles de capacidad y niveles de madures en CMMI v1.3.

Tabla 16 Comparación entre los niveles de capacidad y madurez en CMMI v1.3

Nivel	Representación Continua	Representación por Etapas
Nivel 0	Incompleto	N/A
Nivel 1	Realizado	Inicial
Nivel 2	Gestionado	Gestionado
Nivel 3	Definido	Definido
Nivel 4	N/A	Gestionado Cuantitativamente
Nivel 5	N/A	En Optimización

La Tabla 17 describe en detalle los 4 niveles de capacidad que van desde el nivel 0 hasta el nivel 3 en CMMI v1.3.

Tabla 17 Detalle de los 4 niveles de capacidad que van desde el número 0 hasta el 3 en CMMI v1.3

Nivel de capacidad	Descripción
Incompleto	• Un proceso incompleto es un proceso que, o bien no se ejecuta, o se ejecuta parcialmente. • Al menos una de las metas específicas del área de proceso no se satisface y no existen metas genéricas para ese nivel, ya que no hay ninguna razón para institucionalizar un proceso ejecutado parcialmente.
Realizado	• Un proceso realizado es un proceso que satisface las metas específicas del área de proceso. • Soporta y permite el trabajo necesario para producir los productos del trabajo. • Aunque el nivel de capacidad 1 da como resultado mejoras importantes, esas mejoras pueden perderse en el tiempo si no se institucionalizan.
Gestionado	• Un proceso gestionado es un proceso realizado (nivel de capacidad 1) que tiene la infraestructura básica dispuesta para soportar el proceso. • Se planifica y ejecuta de acuerdo a políticas; emplea personal con habilidades; tiene los recursos adecuados para producir resultados controlados; involucra a las partes interesadas relevantes; se monitoriza, controla y revisa; y se evalúa la adherencia a su descripción de proceso. • La disciplina de proceso reflejada por el nivel de capacidad 2 ayuda a asegurar que las prácticas existentes se mantienen durante tiempos de estrés.

Definido	• Un proceso definido es un proceso gestionado (nivel de capacidad 2) que se adapta a partir del conjunto de procesos estándar de la organización, de acuerdo a las guías de adaptación de la organización, y contribuye a los activos de proceso de la organización con productos del trabajo, medidas e información adicional de mejora de procesos. • La diferencia principal con respecto al nivel de capacidad 2, es que en ese nivel los procesos pueden variar considerablemente por cada instancia o proyecto particular y también porque en el nivel de capacidad 3, los procesos se describen de una manera más rigurosa. • En el nivel de capacidad de 3 los procesos se gestionan más de forma proactiva y no de forma reactiva como ocurre en el nivel de capacidad 2.

La Tabla 18 muestra en detalle los niveles de madurez que van desde el 1 hasta el 5 en CMMI v1.3.

Tabla 18 Detalle de los niveles de madurez que van desde el 1 hasta el 5 en CMMI v1.3

Nivel de madurez	Descripción
Inicial	• En este nivel los procesos son generalmente ad-hoc y caóticos. • La organización generalmente no proporciona un entorno estable para dar soporte a los procesos. • El éxito en estas organizaciones depende de la competencia y heroicidad del personal de la organización y no del uso de procesos probados. • Las organizaciones de nivel de madurez 1 a menudo producen productos y servicios que funcionan; sin embargo, frecuentemente exceden sus presupuestos y no cumplen sus calendarios. • Las organizaciones de nivel de madurez 1 se caracterizan por una tendencia a comprometerse en exceso, a abandonar los procesos en tiempos de crisis y a una incapacidad para repetir sus éxitos.
Gestionado	• En el nivel de madurez 2, los proyectos de la organización han asegurado que los procesos se planifican y realizan de acuerdo a políticas; los proyectos emplean personal con habilidad que dispone de recursos adecuados para producir resultados controlados; involucran a las partes interesadas relevantes; se monitorizan, controlan y revisan; y se evalúan en cuanto a su adherencia a sus descripciones de proceso. • La disciplina de proceso reflejada por el nivel de madurez 2 ayuda a asegurar que las prácticas existentes se mantienen durante tiempos de estrés. • Cuando estas prácticas están en su lugar, los proyectos se realizan y gestionan de acuerdo a sus planes documentados.
Definido	• En el nivel de madurez 3, los procesos son bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos. • El conjunto de procesos estándar de la organización, que es la base del nivel de madurez 3, se establece y mejora a lo largo del tiempo. • Estos procesos estándar se usan para establecer la consistencia en toda la organización. • Los proyectos establecen sus procesos definidos adaptando el conjunto de procesos estándar de la organización de acuerdo a las guías de adaptación. Una distinción crítica entre los niveles de madurez 2 y 3 es el alcance de los estándares, descripciones de proceso y procedimientos. En el nivel de madurez 2, los estándares, descripciones de proceso y procedimientos pueden ser bastante diferentes en cada instancia específica de un proceso (p.ej., en un proyecto particular). En el nivel de madurez 3, los estándares, descripciones de proceso y procedimientos para un proyecto se adaptan para adecuarse a un proyecto particular o unidad organizativa a partir del conjunto de procesos estándar de la organización y, por tanto, son más consistentes, exceptuando las diferencias permitidas por las guías de adaptación.

Gestionado Cuantitativamente	• En el nivel de madurez 4, la organización y los proyectos establecen objetivos cuantitativos en cuanto al rendimiento de calidad y del proceso, y los utilizan como criterios en la gestión de los procesos. • Los objetivos cuantitativos se basan en las necesidades del cliente, usuarios finales, organización e implementadores del proceso. • El rendimiento de calidad y del proceso se comprende en términos estadísticos y se gestiona durante la vida de los procesos. Una distinción crítica entre los niveles de madurez 3 y 4 es la predictibilidad del rendimiento del proceso. En el nivel de madurez 4, el rendimiento de los procesos se controla utilizando técnicas estadísticas y otras técnicas cuantitativas, y es predecible cuantitativamente. En el nivel de madurez 3, los procesos normalmente sólo son predecibles cualitativamente.
En Optimización	• En el nivel de madurez 5, una organización mejora continuamente sus procesos basándose en una comprensión cuantitativa de las causas comunes de variación inherentes a los procesos. • El nivel de madurez 5 se centra en mejorar continuamente el rendimiento de procesos mediante mejoras incrementales e innovadoras de proceso y tecnológicas. • Los objetivos cuantitativos de mejora de procesos para una organización se establecen, se revisan continuamente para reflejar el cambio a los objetivos del negocio, y se utilizan como criterios para gestionar la mejora de procesos. • Los efectos de las mejoras de procesos desplegadas se miden y evalúan frente a los objetivos cuantitativos de mejora de procesos. • Tanto los procesos definidos como el conjunto de procesos estándar de la organización son objeto de las actividades de mejora cuantitativa. En el nivel de 5 las organizaciones buscan tratar las causas comunes de variación en los procesos, mientras que en el nivel 4 se enfocan en las variaciones especiales.

Áreas de proceso en CMMI v1.3

Las áreas de proceso se ven de forma diferente entre las dos representaciones existentes (continua y por etapas). La representación continua permite a la organización elegir el enfoque de sus esfuerzos de mejora de procesos mediante la elección de aquellas áreas de proceso, o conjuntos de áreas de proceso interrelacionadas, que benefician más a la organización y a sus objetivos de negocio. En cambio, la representación por etapas anima a ver siempre áreas de proceso en el contexto del nivel de madurez al cual pertenecen. Las áreas de proceso se organizan en niveles de madurez para reforzar este concepto.

En la Tabla 19 se listan las 22 áreas de proceso de CMMI v1.3[14].

Tabla 19 Áreas de proceso de CMMI v1.3

Área de proceso	Propósito
Análisis Causal y de Resolución (CAR)	Identificar las causas de defectos y de otros problemas, y tomar acción para prevenir que no ocurran en el futuro.
Gestión de la configuración (CM)	Establecer y mantener la integridad de los productos de trabajo utilizando la identificación de configuración, el control de configuración, el registro del estado de configuración y las auditorías de configuración.

[14] CMMI® for Development, Version 1.3, http://www.sei.cmu.edu/reports/10tr033.pdf, Página 127, Part Two: Generic Goals and Generic Practices, and the Process Areas.

Análisis de decisiones y resolución (DAR)	Analizar las decisiones posibles utilizando un proceso de evaluación formal que evalúa alternativas identificadas frente a criterios establecidos.
Gestión Integrada del proyecto (IPM)	Establecer y gestionar el proyecto y la involucración de las partes interesadas relevantes de acuerdo a un proceso integrado y definido que se adapta a partir del conjunto de procesos estándar de la organización.
Medición y Análisis (MA)	Desarrollar y sustentar una capacidad de medición que se utiliza para poder dar soporte a las necesidades de información de la gerencia.
Definición de Procesos de la Organización (OPD)	Establecer y mantener un conjunto usable de activos de proceso de la organización y de estándares del entorno de trabajo.
Enfoque de Procesos de la Organización (OPF)	Planificar, implementar y desplegar las mejoras de procesos de la organización, basadas en una comprensión completa de las fortalezas y debilidades actuales de los procesos y de los activos de proceso de la organización.
Gestión del Rendimiento Organizacional (OPM)	Gestionar proactivamente el rendimiento de la organización para cumplir con los objetivos de negocio.
Rendimiento de los Procesos de la Organización (PPD)	Establecer y mantener una comprensión cuantitativa del rendimiento del conjunto de procesos estándar de la organización en apoyo de los objetivos de calidad y de rendimiento de procesos, y proporcionar datos, líneas base y modelos de rendimiento de los procesos para gestionar cuantitativamente los proyectos de la organización.
Formación Organizativa (OT)	Desarrollar las habilidades y el conocimiento de las personas para que puedan realizar sus roles eficaz y eficientemente.
Integración de Producto (PI)	Ensamblar el producto a partir de sus componentes, asegurar que el producto, una vez integrado, funciona correctamente, y entregar el producto.
Monitorización y Control del Proyecto (PMC)	Proporcionar una comprensión del progreso del proyecto para que se puedan tomar las acciones correctivas apropiadas, cuando el rendimiento del proyecto se desvíe significativamente del plan.
Planificación de Proyecto (PP)	Establecer y mantener planes que definan las actividades del proyecto.
Aseguramiento de la Calidad del Proceso y del Producto (PPQA)	Proporcionar al personal y a la gerencia una visión objetiva de los procesos y de los productos de trabajo asociados.
Gestión Cuantitativa de Proyecto (QPM)	Gestionar cuantitativamente el proceso definido del proyecto para alcanzar los objetivos establecidos de calidad y de rendimiento del proceso del proyecto.
Desarrollo de Requerimientos (RD)	Producir y analizar los requerimientos de cliente, de producto y de componente del producto.
Gestión de Requerimientos (REQM)	Gestionar los requerimientos de los productos y de los componentes del producto del proyecto, e identificar inconsistencias entre esos requerimientos y los planes y productos de trabajo del proyecto.
Gestión de Riesgos (RSKM)	Identificar los problemas potenciales antes de que ocurran para que las actividades de tratamiento de riesgos puedan planificarse e invocarse según sea necesario a lo largo de la vida del producto o del proyecto para mitigar los impactos adversos para alcanzar los objetivos.
Gestión de Acuerdos con Proveedores (SAM)	Gestionar la compra de productos.
Solución Técnica (TS)	Diseñar, desarrollar e implementar soluciones para los requerimientos. Las soluciones, los diseños y las implementaciones engloban productos, componentes de producto y procesos del ciclo de vida asociados al producto, individualmente o en combinación, según sea apropiado.
Validación (VAL)	Demostrar que un producto o componente de producto se ajusta a su uso previsto cuando se sitúa en su entorno previsto.
Verificación (VER)	Asegurar que los productos de trabajo seleccionados cumplen sus requerimientos especificados.

Interpretar CMMI v1.3 para la utilización de metodologías ágiles

Para ayudar a entender a quienes utilizan métodos ágiles a interpretar prácticas de CMMI en sus ambientes de trabajo, se han incluido notas explicativas en esta versión de CMMI para un conjunto de áreas de proceso. Estas notas se muestran usualmente en las notas introductorias de las siguientes áreas de proceso:

- Gestión de la Configuración (CM).
- Integración de Producto (PI).
- Monitorización y Control de Proyecto (PMC).
- Planificación de Proyecto (PP).
- Aseguramiento de la Calidad del Proceso y del Producto (PPQA).
- Desarrollo de Requerimientos (RD).
- Gestión de Requerimientos (REQM).
- Gestión de Riesgos (RSKM).
- Solución Técnica (TS).
- Verificación (VER).

Todas estas notas comienzan con las palabras, "En ambientes ágiles" [15] y están en cajas de ejemplo para ayudar a reconocerlos fácilmente y que sirvan de recordatorio de que dichas notas son ejemplos de cómo interpretar esas prácticas. Sin embargo, los ejemplos de dichas prácticas no son suficientes para satisfacer el área de proceso correspondiente.

En la Tabla 20 se detallan las notas para ambientes ágiles en las áreas de proceso de CMMI v1.3.

Tabla 20 Notas para ambientes ágiles en las áreas de proceso de CMMI v1.3

Área de proceso	Interpretación para ambientes ágiles
Gestión de la configuración (CM)	• En los entornos ágiles es importante la necesidad de soportar cambios frecuentes, múltiples líneas bases y múltiples espacios de trabajo de gestión de configuración para individuos, equipos y programación de a pares. • Los entornos ágiles se pueden ver afectados si no se automatiza y si no se crea gestión de configuración de forma estándar.
Integración de Producto (PI)	• En los entornos ágiles, la Integración de producto es frecuente, mayormente, de forma diaria. La incorporación de nuevo código al código base se le denomina integración continua. • Como parte de la integración continua se debe revisar cómo los componentes proporcionados por algún proveedor serán incorporados y cómo la funcionalidad será construida.

[15] CMMI® for Development, Version 1.3, http://www.sei.cmu.edu/reports/10tr033.pdf, Página 58, Capitulo 5 – Interpreting CMMI When Using Agile Approaches.
Glazer, Hillel, Dalton, Jeff, Anderson, David, Konrad, Michael, Shrum, Sandra (2008). CMMI or Agile, Why Not Embraced Both!. Software Engineering Institute (SEI), http://www.sei.cmu.edu/library/ abstracts/reports /08tn003.cfm.

Monitorización y Control del Proyecto (PMC)	• En los entornos ágiles, la participación continua del cliente y de usuarios potenciales durante el desarrollo del producto del proyecto puede ser crucial para el éxito del proyecto. Por lo tanto la participación activa de ambos debe ser monitoreada.
Planificación de Proyecto (PP)	• Llevar a cabo desarrollo incremental implica planificación, monitoreo y control así como re-planificación constante. • Los equipos no estiman más allá de lo que es conocido del proyecto a excepción de anticiparse a riesgos y eventos mayores. • Los equipos estiman y planifican durante cada iteración. • Los compromisos con los planes son demostrados cuando las tareas son asignadas y aceptadas en cada iteración.
Aseguramiento de la Calidad del Proceso y del Producto (PPQA)	• En entornos ágiles, los equipos tienden a enfocarse en necesidades inmediatas en vez de necesidades a largo plazo. • Para asegurarse que las evaluaciones objetivas tienen valor y son eficientes, se debe discutir lo siguiente de forma temprana: ¿Qué tan objetivas deben ser las evaluaciones a ser realizadas?, ¿Qué productos de trabajo o procesos serán evaluados?, ¿Cómo los resultados de las evaluaciones serán integrados al ritmo del equipo?
Desarrollo de Requerimientos (RD)	• En entornos ágiles las necesidades de los clientes y nuevas ideas son iterativamente elicitadas, elaboradas, analizadas y validadas. • Los requerimientos son documentados en historias de usuario, casos de uso, entre otros. • Los requerimientos que se van a tomar durante una iteración resultan elegidos a partir de un análisis de riesgo y por las prioridades asociadas al producto.
Gestión de Requerimientos (REQM)	• En entornos ágiles los requerimientos son comunicados y seguidos mediante Product Backlogs o tarjetas de historia. • Los compromisos para los requerimientos son realizados de forma colectiva por el equipo o por un líder de equipo. • La asignación de trabajo se hace de forma regular y se ajusta en base al progreso obtenido. • La trazabilidad y consistencia de los requerimientos se mantiene desde el principio de la iteración hasta el fin de la misma.
Gestión de Riesgos (RSKM)	• En entornos ágiles, algunas actividades de gestión de riesgos se encuentran inherentemente embebidas en el método ágil utilizado. • Por ejemplo, una técnica para evaluar el riesgo puede ser una experimentación temprana tipo ensayo y error. Sin embargo, el área de proceso de gestión de riesgos promueve una manera más sistemática para manejar los riesgos, sean técnicos o no técnicos. Esto a su vez se puede integrar al ritmo de las típicas iteraciones ágiles y las reuniones, más específicamente durante la planificación de la iteración, las estimaciones de las tareas y la aceptación de las tareas.
Solución Técnica (TS)	• En entornos ágiles, el foco es una exploración temprana ya que ayuda en la calidad de las decisiones y a lo largo del tiempo. • Las soluciones pueden definirse en términos de funciones, configurar características, liberaciones u otros componentes que faciliten el desarrollo del producto. Si hay bajo riesgo en cuanto a una solución seleccionada, la formalidad para tomar una decisión es significativamente reducida.
Verificación (VER)	• En entornos ágiles, debido a las constantes entregas e involucramiento del cliente, la verificación y la validación van de la mano. Por ejemplo, un defecto puede causar que un prototipo o entrega temprana falle la validación de forma prematura. • De la misma forma, la continua y temprana validación ayuda a asegurar que la verificación se está haciendo sobre el producto correcto.

2.8 Gestión de riesgos

El diseño, desarrollo e implementación de proyectos de software es un proceso complejo que envuelve un gran número de actividades inciertas. Hoy en día pensar sobre los riesgos es una parte fundamental de cualquier proyecto de desarrollo de software y es fundamental para la supervivencia del mismo.

¿Por qué se deben gestionar los riesgos?, la respuesta a esta pregunta es muy simple, si no se hace la empresa pierde dinero, se pierde la confianza de los accionistas y se juega su reputación ante sus clientes. Los siguientes ejemplos muestran que los riesgos en los proyectos de desarrollo de software deben ser considerados como cualquier otro tipo de riesgo de seriedad para el negocio:

- Las ventas de la compañía de chocolates Hersheys durante el tercer cuarto fiscal del año 1999, el cual es el trimestre donde se registran el mayor número de ventas promedio anuales, tuvo una pérdida de alrededor de 150 millones de dólares por un defecto en un software de la empresa que no permitió el envío de caramelos de Halloween, lo que representó una pérdida del 19% con respecto al mismo período del año anterior (1998).
- El distribuidor de productos farmacéuticos FoxMeyer demandó a SAP así como a la empresa Andersen Consulting por las demoras generadas en la distribución de los productos y almacenamiento que supuestamente eran causa del software de planificación de recursos (ERP) vendido por SAP. Las órdenes procesadas bajaron de 420.000 por noche a apenas 10.000 cuando se reemplazó el sistema legado de FoxMeyer por SAP[16].
- Un defecto en una actualización del antivirus de McAfee en Abril de 2010, hizo que el sistema operativo de Windows XP SP3 a nivel mundial se reiniciara continuamente y se perdiera cualquier tipo de acceso a la red tanto en sus clientes corporativos como en los clientes domésticos. La causa fue un falso positivo que identifica el conocido ejecutable de Windows svchost.exe como un virus[17].
- Más 6.46 millones de contraseñas de usuarios de LinkedIn fueron obtenidas después de un supuesto ataque cibernético. El costo de la investigación del incidente fue entre 500.000 y 1.000.000 de dólares aproxidamente[18].

[16] McManus, John (2004) Risk Management in Software Development Projects, ISBN: 9780750658676, Capitulo 1 – Risk Management Process

[17] Ed Bott (2010), Defective McAfee update causes worldwide meltdown of XP PCs http://www.zdnet.com/blog/bott/defective-mcafee-update-causes-worldwide-meltdown-of-xp-pcs/2003

[18] SC Magazine (2010), Data breach costs LinkedIn up to $1 million http://www.scmagazine.com.au/News/310976,data-breach-costs-linkedin-up-to-1-million.aspx

Claramente los errores en el software son costosos y pueden traer graves problemas a una organización. La prevención siempre es mejor que la cura, sin embargo, a pesar de que a primera instancia la gestión de riesgos puede ser vista como agregarle más complejidad al proyecto de desarrollo, más bien lo que hace es reducir la complejidad del proyecto en general, por ejemplo:

- La identificación y priorización de los riesgos permite al gerente del proyecto y a los miembros del proyecto enfocarse en las áreas que tienen mayor impacto dentro del proyecto.
- Las acciones de mitigación de riesgos apropiadas reducen el riesgo del proyecto y en cambio acelera la completitud del mismo.
- Los proyectos que terminan antes cuestan menos y las acciones de mitigación de riesgos pueden reducir el costo del proyecto.
- Los proyectos donde se utiliza la gestión de riesgos son más predecibles y se experimentan menos situaciones sorpresivas porque la mayoría de los problemas se detectan antes de que ocurran.

Paradigma de la gestión de riesgo

Como parte de la gestión de riesgos, un gerente de proyecto trata de responder las siguientes interrogantes:

- ¿Qué puede salir mal?
- ¿Cuál es la probabilidad de que eso salga mal?
- ¿Cuáles son las consecuencias de que eso salga mal?

Como resultado del análisis de los riesgos, un gerente de proyecto debe buscar responder las siguientes interrogantes:

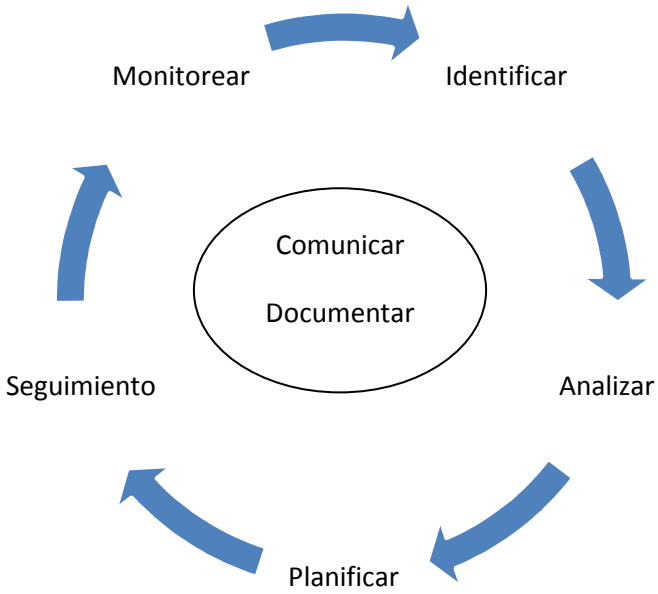
- ¿Qué se puede hacer para que no ocurra eso?
- ¿Cuáles son las opciones disponibles?
- ¿Cuál es el costo o el beneficio asociado a las opciones existentes?
- ¿Cuál es el impacto de las decisiones que se tomen actualmente con respecto a decisiones futuras?

Solo cuando estas preguntas pueden ser contestadas se dice entonces que la gestión de riesgos puede llevarse a cabo. Este es el dominio del paradigma de la gestión de riesgos[19].

[19] Haimes, Yacov Y, 'Total Risk Management', Risk Analysis 11(2) pp. 169–171,

En el gráfico 6 a continuación el paradigma de la gestión de riesgos representa todas las actividades involucradas en la gestión de los riesgos con desarrollo de software. El paradigma está representado por un círculo donde se hace énfasis que la gestión de riesgos es un proceso continuo, mientras que las flechas muestran el flujo lógico de información entre cada una de las actividades. La comunicación se ubica en el centro el paradigma y es a través del cual toda la información fluye y por lo general representa el mayor obstáculo en la gestión de riesgos.

Gráfico 6 Actividades involucradas en la gestión de riesgos con desarrollo de software a partir del paradigma de la gestión de riesgos



A continuación en la tabla 21 se describen cada una de las actividades del paradigma de la gestión de riesgos:

Tabla 21 Actividades del paradigma de gestión de riesgos

Actividad	Descripción
Identificar	• El propósito de la identificación es considerar los riesgos antes de que estos se conviertan en problemas e incorporar esta información en el proceso de gestión del proyecto. • Cualquier miembro del proyecto puede identificar riesgos para el proyecto. Cada individuo tiene un conocimiento particular de distintas partes del proyecto. • Durante esta actividad, los problemas potenciales e incertidumbres se convierten en riesgos tangibles que pueden ser descritos y medidos.

Analizar	• El propósito del análisis es convertir los datos de los riesgos en información para tomar decisiones con respecto a los riesgos. • Esta actividad provee a gerente del proyecto con la base para empezar a trabajar sobre cada riesgo.
Planificar	• Consiste en decidir que se debe hacer con uno o un conjunto de riesgos. • Las decisiones y estrategias de mitigación se desarrollan en base al conocimiento existente sobre cada riesgo del proyecto. • El plan para un riesgo especifico puede tomar múltiples formas, por ejemplo: o Mitigar el impacto del riesgo desarrollando un plan de contingencia para el caso de que el riesgo ocurra. o Evitar el riesgo cambiando el diseño del producto de software o el proceso de desarrollo. o Aceptar el riesgo y aceptar las consecuencias de su posible ocurrencia. o Estudiar el riesgo y obtener más información al respecto con la finalidad de tomar una mejor decisión sobre lo que se debe hacer.
Seguimiento	• Es el proceso mediante el cual los datos relacionados con el estado de los riesgos se recogen, se agrupan y se reportan. • Se debe obtener de forma precisa y en un tiempo permitido toda la información relevante asociada a los riesgos del proyecto y ser presentada de forma clara y fácil de entender a los interesados y personas apropiadas del proyecto. Es realizado por el responsable de monitorear los riesgos observados y mitigados. • Los datos relacionados con las fechas de entrega, presupuesto, cambios en el camino crítico e indicadores de desempeño del proyecto pueden ser utilizados para desencadenar distintas acciones o para tomar medidas específicas.
Control	• Consiste en tomar decisiones efectivas y oportunas con respecto a los riesgos y los planes de mitigación. • En esta actividad se toma la información de seguimiento y se decide que se va a hacer en base a la información reportada. • Controlar los riesgos implica revisar los reportes de estado, decidir cómo se va a proceder y cómo se van a implementar esas decisiones.
Comunicación	• Si la comunicación no es efectiva, la gestión de riesgos no es viable. Mientras que la comunicación facilita la integración de los elementos que propone el paradigma, hay niveles más altos de comunicación que se deben considerar. • Para ser analizados y gestionados correctamente los riesgos deben ser comunicados a los niveles apropiados de la organización. Esto incluye los niveles dentro del desarrollo del proyecto, la organización y el cliente.

Métodos para la identificación de riesgos

Los métodos de identificación de riesgos se pueden clasificar de dos tipos[20]:

1. **Tipo 1:** Son aquellos métodos genéricos que evalúan factores internos y externos de la organización. El alcance de este tipo de métodos va más allá del proyecto en estudio y busca proteger más los intereses globales de la organización.
2. **Tipo 2:** Son métodos que buscan identificar riesgos en un contexto más reducido y se encuentran mayormente vinculados con la entrega del proyecto.

[20] Pandian, C. Ravindranath (2007), Applied Software Risk Management: A Guide for Software Project Managers. Chapter 4 – Risk Identification.

En la tabla 22 a continuación se detallan los métodos de identificación de riesgos de acuerdo a los tipos especificados anteriormente.

Tabla 22 Métodos de identificación de riesgos Tipo 1 y Tipo 2.

Tipos de métodos	Métodos de identificación de riesgos
Tipo 1	• **Métodos Intuitivos:** Mind Mapping, Brainstorming, Out-of-the box thinking y Analogía. • **Métodos basados en historia:** Top Ten Risks, Checklist de riesgos, Taxonomia basada en cuestionarios.
Tipo 2	Se describen en 6 fases: • **Fase I:** Definición del contexto • **Fase II:** Recopilación de datos • **Fase III:** Descubrimiento del riesgo • **Fase IV:** Asignar atributos • **Fase V:** Validación • **Fase VI:** Lista de riesgos

En la tabla 23 a continuación se explican los métodos de identificación de riesgos intuitivos.

Tabla 23 Métodos de identificación de riesgos intuitivos.

Métodos de identificación de riesgos intuitivos	Descripción
Mind Mapping	• Se basa en asociar síntomas de riesgos familiares con otros síntomas que pueden resultar en problemas futuros. En algunas ocasiones, se basa en lecciones aprendidas de situaciones anteriores.
Brainstorming (Tormenta de ideas)	• Consiste en compartir ideas y pensar de formar grupal en conjunto con los demás miembros del proyecto y las partes interesadas de la organización. • Es una técnica útil para identificar riesgos escondidos, que no son obvios y riesgos desconocidos. • Al ser una técnica grupal, por lo general los equipos de trabajo son capaces de encontrar más riesgos que un solo individuo
Out of the Box Thinking	• Consiste en posicionarse fuera del proyecto y tener una perspectiva más amplia sobre las cosas que pueden ocurrir. • Muchas veces los riesgos no son visibles fácilmente y las personas que se acostumbran a un proceso piensan que los riesgos no ocurren o los omiten. La conveniencia enmascara los riesgos y la familiaridad nubla la visión.
Analogía	• Consiste en base a la experiencia en proyectos anteriores, evaluar si en el proyecto bajo estudio se presentan riesgos similares. • Es importante intentar utilizar la analogía y comparar si los riesgos se repiten en el nuevo proyecto. Esto ayuda a eliminar los riesgos más rápidamente o a controlarlos con mayor facilidad.

En la tabla 24 se describen los métodos de identificación de riesgos basados en historia.

Tabla 24 Métodos de identificación de riesgos basados en historia.

Métodos de identificación de riesgos basados en historia	Descripción
Top Ten Risks	• Consiste en listas de riesgos publicadas por distintos autores e investigadores las cuales pueden jugar un papel importante en el proyecto bajo estudio. • Los riesgos que han ocurrido en otras situaciones también pueden estar presentes en la realidad del proyecto actual. • Cada lista de riesgos proporciona una perspectiva distinta, una ventana o punto de partida para examinar el proyecto actual. • Entre algunas de las listas de riesgos conocidas sobre proyectos de desarrollo de software se pueden mencionar: a) Caper Jones's Risk [21] b) SEI Risk Taxonomy[22] c) Dr. Barry W. Boehm's List[23]
Risk Checklist	• Se construye en base a la experiencia del grupo de desarrollo del proyecto o en base a la experiencia de la organización y se coloca un conjunto de riesgos conocidos. • Se pueden crear por fase o etapa del proyecto.

Fase I: Definición del contexto

Se refiere a la identificación de riesgos específicos del proyecto bajo estudio a partir de un proceso de identificación basado en el contexto. El equipo de proyecto define algunos temas para varios ejercicios de identificación de riesgos, por ejemplo:

a) Identificación de los riesgos del producto.

b) Identificación de los riesgos del diseño.

c) Identificación de los riesgos del proyecto.

d) Identificación de los riesgos del negocio.

e) Identificación de los riesgos de las pruebas.

f) Identificación de los riesgos de las correcciones de los defectos.

Fase II: Recopilación de datos

Las personas que se encargan o ayudan en la identificación de riesgos deben estar motivadas, deben tener metas y objetivos a cumplir. Contar con indicadores de riesgos no necesariamente significa que todos los riesgos pueden ser identificados, mitigados o controlados.

[21] Jones, T. Caper (1994) Assessment and Control of Software Risks. ISBN-10: 0137414064.
[22] Carr, Marvin, Konda, Suresh, Monarch, Ira, Walker, Clay F., Ulrich, F. Carol (1993) Software Engineering Institute (SEI) – Risk Taxonomy. http://www.sei.cmu.edu/library/abstracts/reports/93tr006.cfm
[23] Boehm, Barry (1989) Software Risk Management, IEEE. ISBN-10: 0818689064.

Es indispensable realizar un listado de las distintas fuentes o entradas que pueden ayudar a identificar riesgos potenciales, por ejemplo:

Entradas requeridas para identificar riesgos específicos del proyecto:

a) Metas corporativas.
b) Objetivos del proyecto.
c) Requerimientos del cliente.
d) Retroalimentación del cliente.
e) Estudios comparativos (Benchmarking).
f) Métricas.
g) Inspecciones y reportes de pruebas.
h) Listas de riesgos conocidos.
i) Base de datos de riesgos.

Entradas requeridas para identificar riesgos específicos a la organización:

a) Planes de crecimiento.
b) Expectativas de los inversores.
c) Análisis de comportamiento del cliente.
d) Análisis competitivo.
e) Modelar amenazas
f) Inteligencia de negocios.
g) Reportes de auditoría financiera.

Fase III: Descubrir el riesgo

Para tener éxito en el descubrimiento de los riesgos, la organización debe sensibilizarse con la identificación de los riesgos. Tener conciencia sobre los riesgos provee un importante mecanismo de alerta para la organización y maximiza las posibilidades de descubrir nuevos riesgos.

Para descubrir riesgos se necesita gente con visión y niveles de autoridad. Debe de existir el ambiente apropiado y las políticas de gestión de riesgos deben jugar un papel importante dentro de la organización y los proyectos que se lleven a cabo.

El uso de encuestas sobre riesgos presentadas de manera oportuna y con claridad dentro de la organización y el uso de modelos de riesgos son herramientas que ayudan considerablemente en la fase de descubrimiento.

Los modelos de riesgos permiten conectar los parámetros de los riesgos al proceso de la organización, al proyecto bajo estudio y a los parámetros de negocio de la organización proporcionando un valor agregado a la gestión de riesgos. Los modelos de riesgos establecen dicha conexión de una manera científica.

Otra ventaja del descubrimiento de los riesgos mediante el uso de modelos es que se lleva al equipo de proyecto a realizar análisis de las decisiones. Cuando se itera un modelo múltiples veces para descubrir riesgos, el análisis de decisiones se vuelve una rutina donde diversos escenarios son simulados y cada decisión final pasa por un juicio enfocada en el impacto de los riesgos.

A continuación se pueden mencionar algunos modelos cuantitativos de riesgos[24]:

a) **Los modelos de matriz:** En este modelo se relaciona una columna de variables con filas de variables. En la tabla 25 a continuación se describen algunos modelos de matrices empleados para el descubrimiento de los riesgos:

Tabla 25 Modelos de matrices empleados para el descubrimiento de riesgos.

Columna	Fila
Metas	Riesgos
Requerimientos	Riesgos
Riesgos	Causas
Requerimientos	Capacidades

Por ejemplo, en la tabla 26 a continuación se representa una columna donde se establecen un conjunto de metas que pueden ser del proyecto en estudio o de la organización y un conjunto de filas donde se enumeran un conjunto de potenciales riesgos.

Tabla 26 Modelo de matriz tipo Metas-Riesgos.

Metas		Riesgos							
		1	2	3	4	5	6	7	8
1	Meta 1					♦			
2	Meta 2			♦					
3	Meta 3						♦		
4	Meta 4			♦	♦				
5	Meta 5				♦				
6	Meta 6					♦			
7	Meta 7								♦

[24] Pandian, C. Ravindranath (2007), Applied Software Risk Management: A Guide for Software Project Managers. Chapter 8 – Risk Models.

En la tabla xx se logra evidenciar que una meta puede verse influenciada por uno o más riesgos así como también existen riesgos que pueden afectar a una o más metas dentro de la organización o como parte del proyecto bajo estudio.

b) **Modelos de árbol:** Los modelos de árbol y sus variantes (causa y efecto y árbol de decisión) son herramientas extremadamente útiles cuando se quiere realizar una gestión de riesgos.

El diagrama de causa-efecto permite realizar una tormenta de ideas (Brainstorming) y categorizar las variables que pueden estar causando que el proceso, servicio o producto en estudio tenga un bajo desempeño. El diagrama de causa-efecto ayuda a determinar la causa raíz del problema identificando sistemáticamente todas las posibles causas.

Si el proceso de innovación no está resultando como lo esperado o especificado o si se desea anticipar a que cosas podrían salir de manera incorrecta, el diagrama de causa-efecto es de gran utilidad.

Para representar la construcción de un diagrama de causa-efecto, se puede tomar como ejemplo un portal web de alquiler de películas DVD con despacho por correo[25]. A continuación se muestran los pasos para la construcción del diagrama:

I. Declarar el efecto

Se debe dibujar una flecha horizontal de izquierda a derecha. Cerca de la punta de la flecha se debe escribir el "efecto" o el problema que se está buscando resolver.

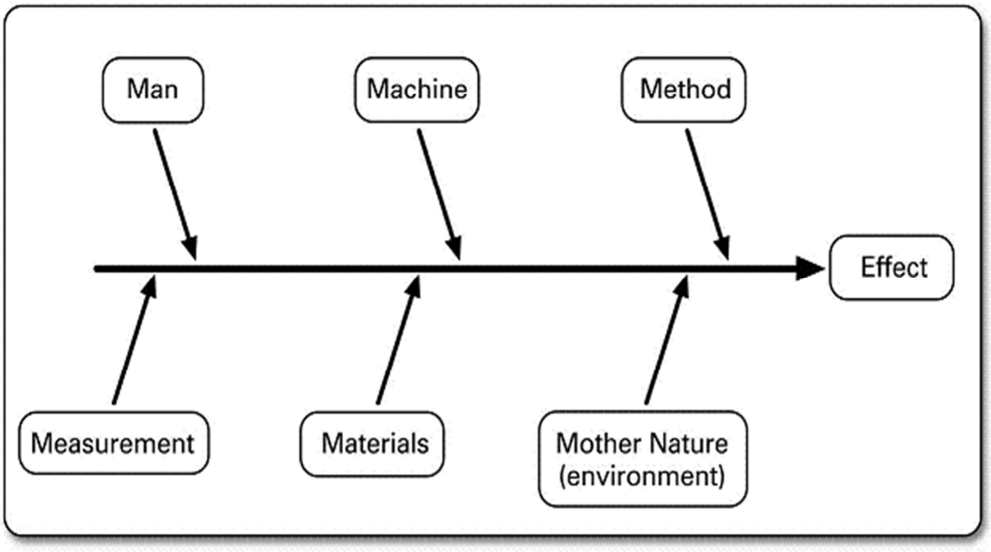
II. Escoger las categorías de las causas

Se debe dibujar líneas diagonales que se conectan con la línea horizontal dibujada anteriormente. Estas líneas representan categorías de las posibles causas del problema a resolver.

Por ejemplo las categorías se pueden representar de la siguiente forma como se muestra en el gráfico 7 a continuación:

[25] Silverstein, David, Samuel, Phillip, Decarlo, Neil (2012) The Innovator's Toolkit: 50+ Techniques for Predictable and Sustainable Organic Growth- Technique 57 - Cause & Effect Matrix—Identify the key input-output relationships in need of attention.

Gráfico 7 Representación de las categorías de las causas en el diagrama de causa-efecto de un portal web de alquiler de películas en formato DVD con despacho por correo



III. Identificar las entradas

Por cada categoría se puede realizar una tormenta de ideas y aportar todas las posibles causas o entradas que pueden contribuir con el problema. Se escribir cada entrada sobre la línea que se extiende por cada categoría.

IV. Preguntar ¿Por qué?

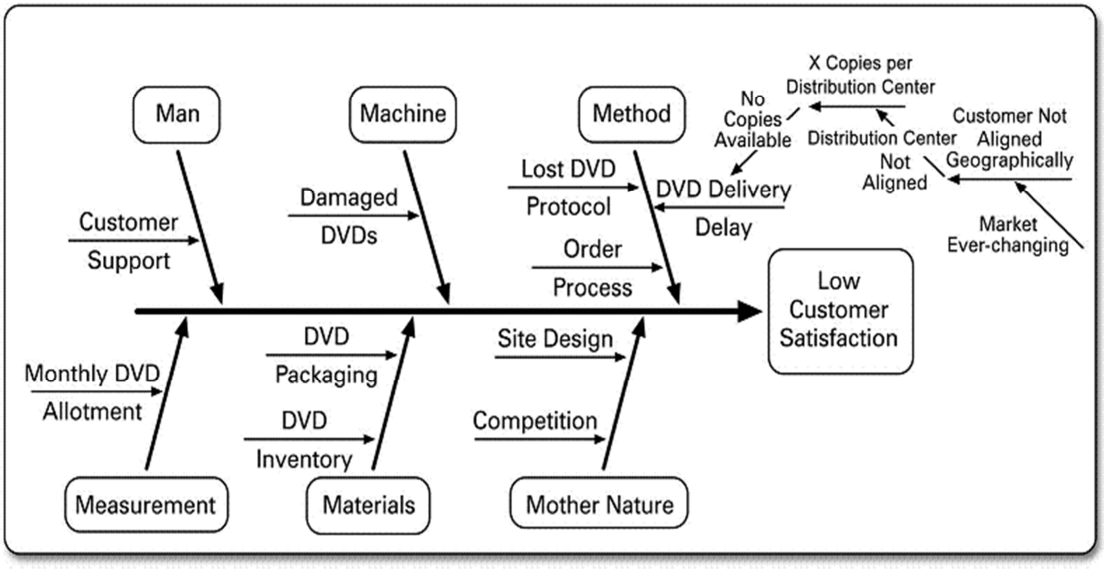
Por cada entrada o causa potencial, se debe formular la siguiente pregunta: ¿Por qué esta entrada causa el efecto declarado en cuestión?. Este proceso se debe repetir continuamente por cada entrada especificada.

V. Descubrir la causa raíz

Una vez que se culmina con el uso del ¿Por qué? sobre cada posible entrada, se puede utilizar una matriz de causa-efecto para determinar cuáles entradas tienen mayor impacto en las salidas esperadas por los clientes de tal manera de actuar con prontitud para mantener las expectativas de los clientes satisfechas.

En el gráfico 8 a continuación se puede visualizar el detalle completo del diagrama de causa-efecto del portal de DVD.

Gráfico 8 Representación en detalle del diagrama de causa-efecto de un portal web de alquiler de películas en formato DVD con despacho por correo



En la matriz causa-efecto representada en el gráfico 9 a continuación se puede visualizar el impacto de cada entrada del proceso sobre cada salida.

Gráfico 9 Representación en detalle de la matriz causa-efecto de un portal web de alquiler de películas en formato DVD con despacho por correo

			Outputs							
			Helpful Support	Quick Delivery	User-Friendly Website	DVD Selection	Affordability	1		
		Customer Priority	3	9	7	9	5			
	Process Step (2)	Process Input	(3x0) + (9x9) + (7x0) + (9x9) + (5x3) = 177							Total
1	Select DVD	Web interface	9	0	9	3	0			117
2		Inventory system	1	5	5	3	0			110
3	Check available inventory	Distribution center locale	0	9	0	9	3	3		177
4		Inventory system	1	5	1	9	0			136 (4)
5	Check customer allotment	Customer database	1	3	1	0	9			82
6	Pick/ship DVD	Customer database	1	9	0	0	0			84
7		Shipping	0	9	0	0	5			106

c) Modelo de análisis de modo y efecto de las fallas (FMEA – Failure Mode Effect Analysis)

Es un método de identificación y prevención de los problemas en procesos y productos antes de que estos ocurran. Es un método enfocado en la prevención de defectos, mejoras de la

seguridad y la satisfacción del cliente y puede ser utilizado en distintas etapas del ciclo de vida del producto, como en la fase de diseño, desarrollo o en productos existentes[26].

Es un método ampliamente utilizado en sus principios en la industria química. También es utilizando en la industria automotriz, aeroespacial y de desarrollo de software critico como por ejemplo en el área de tecnología médica.

El objetivo del FMEA es evaluar todas las posibles fallas que un proceso o un producto puedan tener. La falla de un producto ocurre cuando este no funciona de la forma en que debería. También cabe resaltar que las fallas no solo se limitan a problemas con el producto. Por ejemplo, una falla puede ocurrir porque un usuario comete un error en el uso del producto. Este tipo de fallas también deben ser incluidas en el FMEA.

Las formas en que un producto o proceso pueden fallar se conocen como "modos de falla". Cada modo de falla tiene su "efecto potencial". Cada efecto a su vez tiene un "riesgo" asociado.

De acuerdo con el FMEA, el riesgo relativo de una falla y su potencial efecto está determinado por tres factores:

(O) ¿Con qué frecuencia la falla ocurre?

(S) ¿Qué tan grave es la falla?

(D) ¿Qué tan fácil o difícil es detectar la falla?

La multiplicación de estos tres factores genera el RPN (Risk Priority Number – Número de prioridad del riesgo):

RPN = (O) x (S) x (D)

El RPN, el cual se utiliza con una escala que va de 1 a 1000 por cada modo de falla, es usado para priorizar las acciones correctivas. Los modos de falla que tengan un RPN mayor deberán ser atendidos con mayor prioridad.

También se debe considerar que si la severidad del modo de falla tiene un valor alto, entre 9 y 10, considerando una escala del 1 al 10, se deben atender con prioridad sin importar necesariamente el valor del RPN.

La tabla 27 a continuación muestra un ejemplo de uso de un FMEA para las sucursales de una empresa de venta de materiales para la construcción[27]:

[26] McDermott, Robin E., Mikulak, Raymond J., Beauregard, Michael R. (2009) The Basics of FMEA. Chapter 4 – The FMEA Process

Tabla 27 Ejemplo de uso de un FMEA.

Área en estudio por el FMEA	Modo potencial de falla	Efecto potencial de la falla	S	Causa potencial o mecanismo de falla	O	Control Actual	D	RPN	Acciones recomendadas
Operaciones de la sucursal	Cierre de la sucursal	Pérdida de dinero o bancarrota	9	Un tornado en el lugar	3	Ninguno	10	270	Instalar el canal del tiempo y mantenerlo encendido durante las horas de atención al público
			9	Demanda por parte de un cliente que haya resultado herido durante la visita	3	Seguro para accidentes en la tienda	2	54	Ninguna

En la tabla 27 se puede apreciar que a pesar de que hay dos posibles causas que originen el cierre de la sucursal de la empresa, resultando en una misma severidad y posibilidad de ocurrencia, la detección varía considerablemente. Los tornados no se pueden detectar con anticipación, son impredecibles. Sin embargo, se puede evitar con mayor facilidad que los clientes sufran accidentes dentro de la tienda, demarcando los lugares en donde se puede caminar y con personal de la tienda supervisando las visitas.

d) Modelo de simulación con el método de Monte Carlo

El método de Monte Carlo fue inventado por científicos trabajando en el desarrollo de la bomba atómica en la década de 1940. El método consiste principalmente en utilizar muestras aleatorias de parámetros o entradas para explorar el comportamiento de sistemas o procesos complejos.

La simulación de Monte Carlo[28] se utiliza ante situaciones que ameriten la toma de decisiones, estimaciones o pronósticos con altos niveles de incertidumbre. Si en tales situaciones no se realiza una simulación de Monte Carlo, es probable que los pronósticos y estimaciones se encuentren muy alejados de la realidad y el tratar de convertir la incertidumbre en un simple promedio puede traer graves consecuencias para la organización.

[27] Breyfogle III, Forrester W. (2003) Implementing Six Sigma: Smarter Solutions Using Statistical Methods. Chapter 14 – FMEA.
[28] Breyfogle III, Forrester W. (2003) Implementing Six Sigma: Smarter Solutions Using Statistical Methods. Chapter 14 – FMEA.

Hay situaciones que requieren de uno o dos parámetros para poder proveer una solución simple, sin embargo, en la mayoría de las organizaciones, sus actividades, planes y procesos son bastante complejos, lo que evidencia la incertidumbre en varias dimensiones.

Las variaciones de demanda del mercado, la fluctuación de costos y los cambios en el proceso de manufactura se encuentran bajo ciertos niveles de incertidumbre cuyo impacto de no ser entendido puede representar un riego para el negocio.

La simulación de Monte Carlo propone el uso de rangos de valores para realizar estimaciones. Por ejemplo, en un proyecto de construcción el ingeniero del proyecto puede estimar el mayor tiempo posible para culminar un conjunto de tareas en el peor de los casos y el mínimo tiempo posible en el mejor de los casos.

Utilizando un rango de posibles valores, se puede crear una foto más realista de lo que puede ocurrir en el futuro. Cuando un modelo está basado en un rango de valores estimados, la salida del modelo también será un rango de valores.

El tener un rango de valores como resultado permite empezar a entender el riesgo y la incertidumbre en el modelo. La clave de la simulación de Monte Carlo es indicar que tan probable de ocurrir es cada valor dentro del rango de valores después de ejecutar múltiples iteraciones (entre 100 a 10.000) utilizando valores aleatorios.

Un ejemplo del uso de este método se puede visualizar cuando se requiere estimar el tiempo necesario para completar un proyecto en particular. En este caso es un proyecto de construcción separado en tres partes. Cada parte debe ser completada una después de otra, por lo que el tiempo total del proyecto equivale a la sumatoria de cada parte. En este ejemplo y en la tabla 28 el tiempo se considera en meses.

Tabla 28 Tiempo estimado para completar un proyecto de construcción.

Tarea	Tiempo Estimado
Trabajo 1	5 meses
Trabajo 2	4 meses
Trabajo 3	5 meses
Total	14 meses

Utilizando el caso anterior, se crea una estimación por cada parte del proyecto (Trabajo 1, Trabajo 2, Trabajo 3). Este modelo arroja un valor estimado de 14 meses para completar el proyecto.

Sin embargo, este valor está basado en tres estimaciones, cada una de las cuales es un valor desconocido. Podría representar una buena estimación, pero este modelo no indica algo sobre el posible riesgo o que tan probable es que dicho proyecto sea terminado a tiempo.

Para crear un modelo donde se pueda utilizar la simulación de Monte Carlo, hay que crear tres estimaciones por cada parte del proyecto.

Por cada trabajo se debe estimar un "mínimo" y un "máximo" de tiempo esperado (basándose en la experiencia, conocimiento experto o datos históricos). Luego, se considera como la estimación "más probable", la que se especificó en la tabla anterior.

A continuación en la tabla 29 se representan las nuevas estimaciones:

Tabla 29 Nuevo modelo de estimación utilizando un rango de valores posibles (mínimo, más probable y máximo)

Tarea	Mínimo	Más probable	Máximo
Trabajo 1	4 meses	5 meses	7 meses
Trabajo 2	3 meses	4 meses	6 meses
Trabajo 3	4 meses	5 meses	6 meses
Total	11 meses	14 meses	19 meses

El modelo de la tabla 29 contiene más información que el de la tabla 28. Ahora hay un rango de posibles salidas. Este proyecto podría culminarse entre 11 a 19 meses.

Con el uso de la simulación de Monte Carlo, se pueden generar aleatoriamente valores para cada parte o trabajo del proyecto y posteriormente calcular el tiempo total para completarlo utilizando algún tipo de distribución de probabilidad.

Posteriormente la simulación se debe ejecutar alrededor de 500 veces. Una vez culminada la simulación, se pueden describir algunas características del riesgo en el modelo.

Para conocer la probabilidad de un resultado en particular, se debe contar cuantas veces el modelo retornó ese resultado en la simulación.

En la tabla 30 a continuación se muestra la distribución de la probabilidad generada por la simulación de Monte Carlo:

Tabla 30 Resultados de simulación con Monte Carlo

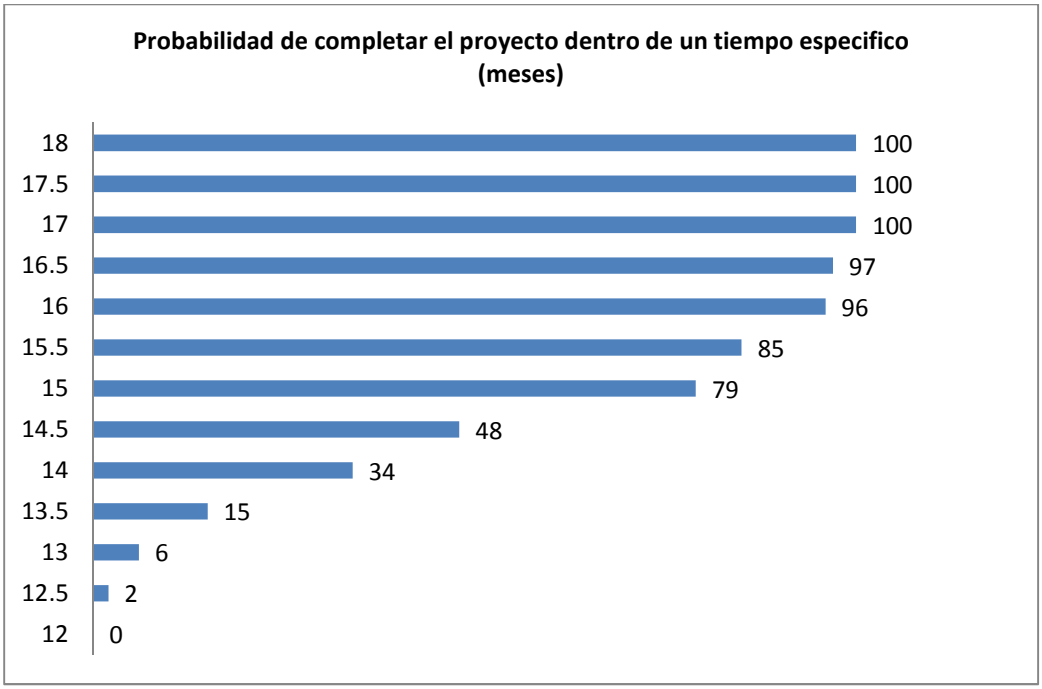
Tiempo	Número de ocurrencias en las 500 iteraciones	Porcentaje del total de ocurrencias
12 meses	1	0%
13 meses	31	6%
14 meses	171	34%
15 meses	394	79%
16 meses	482	96%
17 meses	499	100%
18 meses	500	100%

La estimación original representada en la tabla 29 mostraba que la duración más probable era de 14 meses para culminar el proyecto. Sin embargo, utilizando la simulación de Monte Carlo se refleja que a partir del uso de valores aleatorios en 500 iteraciones, la probabilidad de culminar el proyecto en 14 meses o menos es de solo el 34%.

Por otra parte se demuestra que puede haber un 79% de probabilidad de culminar el proyecto en 15 meses.

En el gráfico 10 a continuación se representa la probabilidad de completar el proyecto en un tiempo específico:

Gráfico 10 Representación de la probabilidad de completar el proyecto en un tiempo específico (meses)



Fase IV: Asignación de atributos

Una vez que se han identificado posibles riesgos, es necesario asignar una identidad a dicho riesgo que permita su seguimiento durante el proceso de gestión de riesgos. Por lo tanto, es importante asociar los siguientes atributos a los riesgos:

a) Unidad estratégica del negocio.

b) Nombre del proyecto.

c) Miembros del equipo de trabajo que identificaron el riesgo.

d) Fecha de identificación del riesgo.
e) Identificador del riesgo o ID del riesgo.
f) Nombre del riesgo.
g) Descripción del evento del riesgo.

Después de definir el riesgo, se debe realizar una evaluación primaria como parte del proceso de identificación. Estos datos de evaluación primaria son:

a) Descripción de la consecuencia del riesgo.
b) Probabilidad de riesgo (p) (Escala 0 al 10)
c) Impacto del riesgo (i) (Escala 0 a 10)
d) Exposición del riesgo (p) x (i).

Después de capturar los aspectos primarios del riesgo, se pueden definir otros atributos catalogados como secundarios y que pueden ser muy útiles para el análisis de los riesgos en etapas posteriores del proyecto:

a) Origen del riesgo (Interno o Externo).
b) Tipo de riesgo (Negocio o técnico).
c) Proceso más afectado (Requerimientos, implementación, pruebas, gestión de la calidad, gestión del proyecto).
d) Evento disparador del riesgo.
e) Tiempo esperado de ocurrencia (existente, próximo mes, trimestre, año)
f) Visibilidad del riesgo.
g) Naturaleza del riesgo
h) Propietario del riesgo (Si el riesgo no tiene un propietario vinculado a la organización, entonces el riesgo no existe y el ejercicio de identificación de riesgos no tiene sentido).

Fase V: Validación

Los riesgos que se acaba de identificar pueden carecer de calidad y claridad. La validación de los riesgos permite remover los siguientes defectos de la lista de riesgos identificados por los miembros de la organización y del proyecto:

h) Descripción del riesgo incorrecta.
i) Nombre del riesgo incorrecto.
j) Clasificación incorrecta del riesgo.
k) Irrelevancia (El riesgo no es relevante para el proyecto o la organización).

l) Ambigüedad.

m) Repetición.

Fase VI: Lista de riesgos

La salida de la identificación de riesgos es una lista con los riesgos validados. Los riesgos serán tabulados en conjunto con los atributos identificados. Esta lista es la base para futuros análisis.

3. Situación actual de la empresa

3.1 Descripción del proyecto a utilizar para implantar el proceso piloto de gestión de riesgos

El propósito del proyecto que se va a utilizar para implantar el proceso de gestión de riesgos piloto dentro del área de aseguramiento de la calidad, es incluir el soporte de contenido de seguridad para dispositivos móviles como parte del producto McAfee Vulnerability Manager. El área de aseguramiento de la calidad debe verificar que el contenido para dispositivos móviles funcione debidamente detectando las vulnerabilidades correspondientes y evitar falsos positivos o negativos.

Es importante destacar que el tipo de proyecto seleccionado tiene características que son comunes en varios de los proyectos que se realizan para incluir nuevo contenido en el producto McAfee Vulnerability Manager. Entre las características más importantes se pueden mencionar:

- Se depende de información sobre vulnerabilidades que los principales proveedores de software ponen a disponibilidad del público general, E.g.(Microsoft, Apple, Adobe, Google, Oracle, Novell, Red Hat).
- La entrega del contenido debe ser lo antes posible ya que permite a los clientes tener información más precisa sobre los riesgos a los que están expuestos y si están protegidos. Se dispone de acuerdos contractuales que definen un tiempo de entrega para cierto contenido que no puede exceder las 72 horas.
- El proceso de desarrollo involucra al área de desarrollo de contenido y aseguramiento de la calidad.

3.2 Descripción del proceso de desarrollo y aseguramiento de la calidad para el proyecto bajo estudio

El proyecto en cuestión es desarrollado por un conjunto de áreas dentro de McAfee Labs. Estas áreas son:

- Área de desarrollo de contenido.
- Área de automatización y herramientas.
- Área de aseguramiento de la calidad.

A continuación se muestra una descripción detallada del proceso que sigue cada una de estas áreas. Cabe destacar que estas descripciones de proceso han sido previamente definidas dentro de McAfee Labs y no son resultado de este proyecto de tesis. Se ha autorizado el uso de dicha

información solamente con fines académicos, puesto que la misma se considera de carácter confidencial.

Descripción del proceso del área de desarrollo de contenido

La Tabla 31 describe los responsables del área, entradas requeridas para iniciar el proceso, actividades del proceso y salidas del proceso.

Tabla 31 Responsables, Entradas, Flujo de actividades y Salidas del proceso del área de desarrollo de contenido para el producto McAfee Vulnerability Manager

Responsables	• Desarrolladores de contenido de McAfee Vulnerability Manager
Entradas	• Nuevas vulnerabilidades a nivel de dispositivos móviles detectadas por clientes, fuentes externas o socios de negocio.
Flujo de actividades	1. **Investigar sobre vulnerabilidades para dispositivos móviles*:*** Consiste en que los desarrolladores de contenido de McAfee Vulnerability Manager deben documentarse leyendo portales de noticias de seguridad informática, blogs, páginas de aplicaciones comerciales para dispositivos móviles, publicaciones de investigadores, entre otras cosas para desarrollar soluciones para detectar nuevas amenazas. 2. **Adaptar contenido del producto:** Los desarrolladores de contenido de McAfee Vulnerability Manager deben trabajar en adaptar parte del contenido existente para que pueda funcionar a nivel de dispositivos móviles. 3. **Desarrollo de scripts para vulnerabilidades nuevas y conocidas:** Los desarrolladores de contenido de McAfee Vulnerability Manager deben desarrollar scripts de detección de vulnerabilidades que ya se encuentren documentadas en línea o bien para vulnerabilidades que apenas fueron descubiertas. 4. **Aplicar cambios a nivel de scripts dentro del producto:** Los desarrolladores de contenido de McAfee Vulnerability Manager deben aplicar cambios en los scripts dentro del producto que vayan a ser soportados tanto a nivel de computadores personales como de dispositivos móviles. 5. **Ejecutar pruebas unitarias y revisión de a pares:** Los scripts nuevos o modificados deben ser sometidos a pruebas unitarias por parte de los desarrolladores de contenido de McAfee Vulnerability Manager para garantizar el funcionamiento de los casos más críticos, por ejemplo, utilizando pruebas unitarias basadas en riesgo. Una vez que se ejecutan las pruebas unitarias, se comparte el código y se llevan a cabo revisiones de a pares. 6. **Evaluar si los cambios se pueden comprometer:** En este paso los desarrolladores de contenido de McAfee Vulnerability Manager determinan si es necesario realizar algún ajuste o prueba adicional antes de comprometer el código respectivamente. 7. **Ejecutar control de cambios:** En este paso el código (scripts), ya es comprometido por parte de los desarrolladores de contenido de McAfee Vulnerability Manager y se registran aquellos scripts modificados e incorporados, para una mayor trazabilidad. 8. **Revisar y corregir defectos:** Los desarrolladores de contenido de McAfee Vulnerability Manager revisan los defectos reportados por el área de automatización y herramientas o el área de aseguramiento de la calidad y deben corregirlos o rechazarlos cuando aplique. Tales defectos pueden ser por ejemplo: falsos positivos o falsos negativos.
Salidas	• Listado de scripts que detectan las vulnerabilidades nuevas o conocidas. • Código comprometido en repositorio de versiones listo para ser integrado y para que se pueda generar un nuevo paquete de contenido. • Solicitud para el área de automatización y herramientas para generar un nuevo paquete de contenido.

Descripción del proceso del área de automatización y herramientas

La Tabla 32 describe los responsables del área, entradas requeridas para iniciar el proceso, actividades del proceso y salidas del proceso.

Tabla 32 Responsables, Entradas, Flujo de actividades y Salidas del proceso del área de desarrollo de automatización y herramientas para el producto McAfee Vulnerability Manager

Responsables	• Equipo de desarrollo para automatización y herramientas
Entradas	• Código comprometido en repositorio de versiones listo por parte de los desarrolladores de contenido de McAfee Vulnerability Manager. • Solicitud para generar un nuevo paquete de contenido por parte del área de desarrollo de contenido.
Flujo de actividades	1. **Generar un nuevo paquete de contenido:** El equipo de desarrollo para automatización y herramientas debe obtener el código comprometido en el repositorio de versiones e integrarlo a un archivo instalador que se origina y distribuye como un archivo ejecutable. Esto se hace con el uso de distintas herramientas a disposición del equipo de automatización. El instalador contiene todos los scripts nuevos, los scripts actualizados y aquellos scripts vigentes que no fueron modificados. 2. **Publicar nuevo paquete de contenido:** El equipo de desarrollo para automatización y herramientas pone el nuevo paquete de contenido generado a disposición del área de aseguramiento de la calidad en un servidor dedicado para esto. Adicionalmente, el equipo de desarrollo para automatización y herramientas notifica a los ingenieros responsables del aseguramiento de la calidad para descargar el nuevo paquete y dar inicio a las actividades de pruebas. 3. **Revisar y corregir defectos:** El equipo de desarrollo para automatización y herramientas revisa los defectos reportados por el área de aseguramiento de la calidad. Estos defectos están asociados a problemas durante la instalación del paquete dentro del McAfee Vulnerability Manager.
Salidas	• Nuevo paquete de contenido listo para ser instalado en el McAfee Vulnerability Manager. • Notificación de la creación de un nuevo paquete de contenido enviada tanto al área de aseguramiento de la calidad como el área de desarrollo de contenido.

Descripción del proceso de aseguramiento de la calidad

La Tabla 33 describe los responsables del área, entradas requeridas para iniciar el proceso, actividades del proceso y salidas del proceso.

Tabla 33 Responsables, Entradas, Flujo de actividades y Salidas del proceso del área de aseguramiento de calidad para el producto McAfee Vulnerability Manager

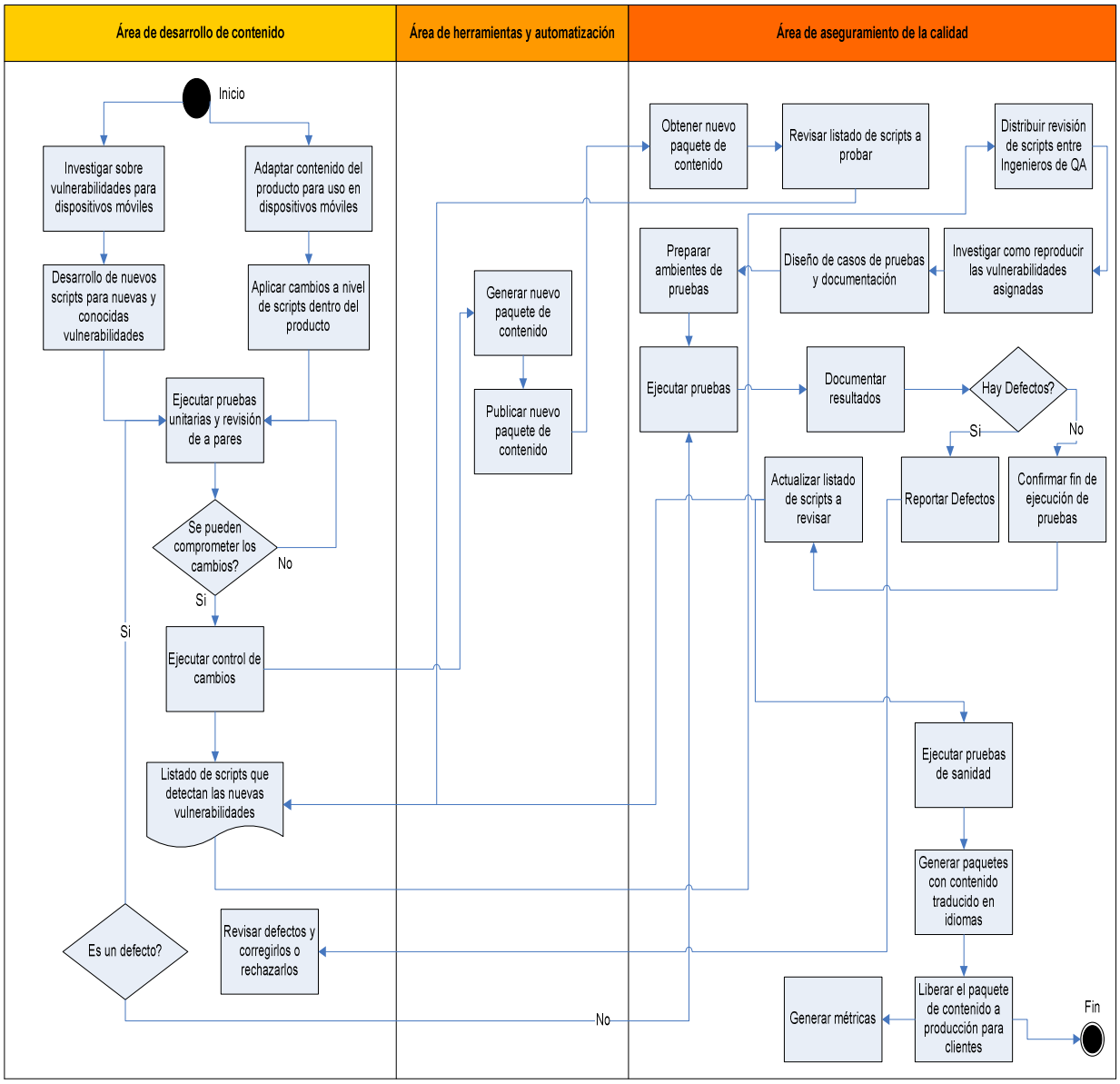
Responsables	• Gerente de aseguramiento de la calidad de contenido • Ingenieros de aseguramiento de la calidad para contenido del producto McAfee Vulnerability Manager.
Entradas	• Nuevo paquete de contenido listo para ser instalado en el McAfee Vulnerability Manager. • Recepción de notificación de la creación de un nuevo paquete de contenido enviada por el equipo de automatización y herramientas. • Listado de scripts que detectan las vulnerabilidades nuevas o conocidas.
Flujo de actividades	1. **Obtener nuevo paquete de contenido:** Los ingenieros de aseguramiento de la calidad descargan el nuevo paquete de contenido liberado por el área de automatización y herramientas. 2. **Revisar listado de scripts a probar:** Los ingenieros de aseguramiento de la calidad revisan el listado de scripts que detectan las vulnerabilidades nuevas o conocidas, actualizado por el área de desarrollo de contenido. Esto permite a los ingenieros de aseguramiento de la calidad conocer qué es lo que se va a probar y si existen dudas preguntar directamente al equipo de desarrolladores de contenido.

3. **Distribución de revisión de scripts:** Debe distribuir la carga de trabajo entre cada uno de los ingenieros de calidad para el producto McAfee Vulnerability Manager. Esto depende de la disponibilidad de cada recurso.
4. **Investigar cómo reproducir las vulnerabilidades:** Cada ingeniero de aseguramiento de la calidad debe hacer una investigación sobre cómo reproducir las vulnerabilidades que le fueron asignadas para verificar si los scripts detectan la vulnerabilidad correspondiente o no. Esta investigación amerita la consulta en línea de foros, blogs, investigaciones de universidades o bien se puede consultar con los desarrolladores de contenido de McAfee Vulnerability Manager sobre cómo reproducirla cuando el tiempo es muy limitado para realizar alguna investigación.
5. **Diseños de casos de prueba y documentación:** Una vez que se conoce cómo se reproduce la vulnerabilidad, los ingenieros de aseguramiento de la calidad diseñan los casos de prueba. Cada caso de prueba tiene un escenario, un resultado esperado y un resultado real. Todo esto se registra en reportes de pruebas.
6. **Preparar ambientes de prueba:** Dependiendo de la vulnerabilidad que se debe reproducir, esto puede variar de plataforma en plataforma, por ejemplo, hay vulnerabilidades que afectan a ciertos productos de Microsoft, o por ejemplo, pueden afectar al sistema operativo Android. Por lo tanto, es indispensable contar con el hardware correspondiente y las aplicaciones necesarias. Si es posible virtualizar entonces se crean las máquinas virtuales correspondientes. También se debe tener actualizada la versión del McAfee Vulnerability Manager cuando corresponda.
7. **Ejecutar pruebas:** Una vez que se tienen los ambientes preparados y los casos de pruebas, los ingenieros de aseguramiento de la calidad empiezan a ejecutar las pruebas necesarias. Esto implica realizar las pruebas del contenido utilizando el producto McAfee Vulnerability Manager.
8. **Documentar resultados:** En la medida que se ejecutan las pruebas los resultados deben ser registrados y almacenados. Información relacionada con el responsable de la ejecución de la prueba, comentarios y otros datos son relevantes.
9. **Reportar defectos:** Si los ingenieros de aseguramiento de la calidad descubren defectos entonces estos deben ser reportados inmediatamente al área que corresponda, por ejemplo, el área de desarrollo de contenido o el área de automatización y herramientas. Dicho defecto debe ser registrado y almacenado para su debido seguimiento.
10. **Confirmar fin de ejecución de pruebas:** En este paso los ingenieros de aseguramiento de la calidad notifican al área de desarrollo de contenido que las pruebas culminaron así como el número de defectos que fueron reportados y el estado en el que se encuentran, por ejemplo, cerrados, pendiente por revisar, asignados, entre otros. Esta actividad se debe realizar al culminar cada listado de scripts enviados por el equipo de desarrollo de contenido de McAfee Vulnerability Manager. Usualmente, cada listado puede representar una iteración con una duración no mayor a dos meses. Ya que las vulnerabilidades en dispositivos móviles aparecen prácticamente de forma diaria hoy en día, los ingenieros de aseguramiento de la calidad van a recibir de forma constante nuevo contenido. Sin embargo, el contenido se debe enviar de forma estructurada y en conjunto, salvo algunas excepciones que representen scripts para detectar vulnerabilidades muy críticas los cuales deben ser probados y liberados a la brevedad posible.
11. **Actualizar listado de scripts a revisar:** Los Ingenieros de aseguramiento de la calidad actualizan el listado de scripts enviado por desarrollo indicando el estado en el que se encuentra cada uno.
12. **Ejecutar pruebas de regresión:** Se realizan un conjunto de revisiones sobre el contenido antiguo en el producto McAfee Vulnerability Manager, así como ciertas opciones generales del producto para estar seguros de que no hay nuevos defectos por parte de los ingenieros de aseguramiento de la calidad.
13. **Generar paquetes de contenido traducidos:** Los ingenieros de aseguramiento de la calidad generan nuevos paquetes de contenido en distintos idiomas. Esto requiere que un equipo de traductores realice las traducciones convenientes.
14. **Liberar el paquete de contenido a producción para clientes:** Los ingenieros de aseguramiento de la calidad publican en un portal para clientes el último paquete de contenido así como los paquetes de otros idiomas listos para ser utilizados
15. **Generar métricas:** Los ingenieros de aseguramiento de la calidad generan métricas asociadas a la cantidad de scripts liberados, cantidad de paquetes de contenido verificados así como esfuerzo realizado durante las pruebas. Estas métricas son analizadas por el Gerente de aseguramiento de la calidad quien se encarga de consolidarlas y enviarlas a otros niveles de la organización semanalmente.

Salidas	• Paquete de contenido publicado para el producto McAfee Vulnerability Manager listo para ser utilizado por los clientes finales. • Reportes de pruebas e informe de métricas.

En el gráfico 9 a continuación se representa el mapa de los procesos de desarrollo de contenido, herramientas y automatización y aseguramiento de la calidad.

Gráfico 11 Mapa de los procesos de desarrollo de contenido, herramientas y automatización y aseguramiento de la calidad



4. Propuesta de nuevo proceso

4.1 Descripción de la propuesta para implantar el proceso de gestión de riesgos.

El proceso de gestión de riesgos piloto a implantar está basado en las metas específicas del área de proceso de gestión de riesgos de CMMI v1.3:

- Preparar la gestión de riesgos
- Identificar y analizar los riesgos
- Mitigación de los riesgos

El alcance del proceso de gestión de riesgos piloto se limita hacia el área de aseguramiento de la calidad.

Cabe destacar así mismo que los artefactos propuestos para satisfacer cada una de las metas específicas y que se mencionan a continuación son contribución del autor de esta tesis de grado.

4.2 Preparar la gestión de riesgos

El propósito de esta meta específica del área de proceso de gestión de riesgos es elaborar un plan de gestión de riesgos para el proyecto piloto. Esta meta específica requiere el cumplimiento de las siguientes prácticas específicas:

- Determinar las posibles fuentes de riesgos y categorizar las fuentes de los riesgos.
- Definir los parámetros de los riesgos (Probabilidad de ocurrencia y severidad del impacto de la ocurrencia del riesgo)
- Elaborar un plan de gestión de riesgos que muestre cada una de las actividades que se deben realizar como parte de la gestión de riesgos, así como los responsables y en qué momento del proyecto pueden suceder.

4.3 Determinar las posibles fuentes de riesgos

Como resultado de la propuesta para implantar un proceso de gestión de riesgos hemos tomado la decisión de crear una plantilla con conocimiento empírico (por parte de los integrantes del proyecto) donde se muestran eventos que han ocurrido en proyectos anteriores y que afectaron el

resultado del proyecto como guía para identificar las posibles fuentes de riesgos[29]. A continuación se muestra el formato de la plantilla en la Tabla 34.

Tabla 34 Listado de fuentes de posibles riesgos elaborado por el área de aseguramiento de la calidad

Categoría	Descripción	SI	NO	Justificar
Planificación	¿Hay algún método para estimar el esfuerzo en horas-hombre para probar el contenido del proyecto solicitado?			
	¿Se conocen los plazos de entrega del proyecto?			
	¿Se sabe quiénes son las personas importantes dentro del proyecto, por ejemplo, gerentes, directores, especialistas técnicos, en caso de ser necesario contactarlos?			
Requisitos	¿Hay alguna especificación disponible para verificar lo que se desea probar como parte del proyecto?, Por ejemplo, algún documento del CIS (Center for Internet Security), PCI (Payment Card Industry), etc..			
	¿Existen casos de prueba documentados para utilizarlos durante la ejecución de las pruebas?			
	¿Se entiende la finalidad del contenido y a qué clientes va dirigido especialmente?			
Operacional	¿Hay el personal suficiente dentro del grupo de trabajo para poder llevar a cabo la fase de pruebas del proyecto?			
	¿Es necesario trasladar personal de una localidad a otra?			
	¿Hay riesgo de que alguien abandone el grupo de trabajo?			
	¿Es posible realizar las pruebas del proyecto en un mismo lugar o es necesario realizarlo en más de una zona horaria?			
	En caso de fallas eléctricas o desastre en el entorno de trabajo, terremoto, incendio; ¿Es posible continuar con la ejecución del proyecto?			
	¿Se debe incurrir en gastos adicionales para la compra de hardware o software?			
Comunicación	¿Hay los medios disponibles para comunicarse con los involucrados en el proyecto, por ejemplo, correo, teléfono, mensajería, etc.?			
	¿Las diferencias culturales son entendidas entre los miembros del proyecto, barreras de idioma, escritura, creencias, etc.?			
	¿Los gerentes y directores se pueden ubicar fácilmente cuando los problemas se presentan, por ejemplo, un proceso de escalamiento?			
	Si un cliente reporta una falla; ¿Existe un proceso formal para atender las quejas de los clientes y resolver las posibles fallas, sin incurrir en pérdidas de esfuerzo o involucrar a áreas que no corresponden?			
Técnico	¿Hay el hardware disponible para poder realizar las pruebas del proyecto?			
	¿Hay el software disponible para poder realizar las pruebas del proyecto, por ejemplo, licencias, productos de terceros, etc.?			
	¿Los ingenieros tienen el conocimiento suficiente para empezar a realizar las pruebas del proyecto lo antes posible?			
	¿Se requiere un período de entrenamiento?			
	¿Los datos de las pruebas se pueden almacenar en algún repositorio?			
	¿Existe algún software para reportar y dar seguimiento a los defectos durante la ejecución de las pruebas?			

[29] McManus, John (2004) Risk Management in Software Development Projects, ISBN: 9780750658676, Capitulo 2 - Discovering Risk in Software Development Projects.
Project Management Institute (2008), A Guide to the Project Management Body Of Knowledge (PMBOK® Guide), Fourth Edition, ISBN: 9781933890517, Capitulo 11, Project Risk Management.

Esta plantilla se puede actualizar en la medida que más proyectos se vayan ejecutando y como resultado de las lecciones aprendidas durante el proceso de gestión de riesgos.

4.4 Definir los parámetros de los riesgos

Los parámetros de los riesgos[30] deben servir para analizar los riesgos, compararlos, conocer la severidad de la ocurrencia del riesgo y priorizar los riesgos. Entre los parámetros mencionados por el modelo CMMI v1.3 se encuentran:

- La probabilidad de ocurrencia de los riesgos.
- Impacto, exposición y prioridad de los riesgos.
- Punto de entrada para aceptar o rechazar la ocurrencia de un riesgo y accionar las actividades de gestión de riesgos correspondientes.

Parámetro 1: Definir la probabilidad de ocurrencia de los riesgos

Este parámetro permite entender con qué frecuencia es posible enfrentarse a un determinado evento dentro del proyecto y si hay que actuar proactivamente a lo largo del proyecto para evitar que este riesgo ocurra[31].

Como parte de la definición del proceso de gestión de riesgos, se ha adoptado dentro del área de aseguramiento de la calidad para el proyecto piloto la siguiente escala que se muestra en la Tabla 35.

Tabla 35 Escala de probabilidad de ocurrencia de riesgos a utilizar por el área de aseguramiento de la calidad

Probabilidad de ocurrencia de riesgos	
Improbable	0.00-0.10
Remoto	0.11-0.40
Ocasional	0.41-0.60
Probable	0.61-0.90
Frecuente	0.91-1.00

Parámetro 2: Impacto, exposición, priorizar de los riesgos

El Impacto[32] se define como la consecuencia para el proyecto si efectivamente llega a ocurrir un determinado riesgo. En el área de aseguramiento de la calidad se ha decido adoptar la siguiente notación que se describe a continuación en la Tabla 36.

[30] CMMI® for Development, Version 1.3, http://www.sei.cmu.edu/reports/10tr033.pdf, Página 362, Part Two: Generic Goals and Generic Practices, and the Process Areas – Risk Management Process Area.
[31] McManus, John (2004) Risk Management in Software Development Projects, ISBN: 9780750658676, Capitulo 3 - Risk Assessment in Software Development Projects.

Tabla 36 Notación utilizada para determinar el impacto de un riesgo dentro del área de aseguramiento de la calidad

Impacto del riesgo	Descripción del Impacto	Valor del impacto	Interpretar el valor del impacto
Insignificante	Puede ser fácilmente mitigado	1	Este riesgo retrasa el progreso de una tarea individual dentro del grupo
Menor	Afecta de forma menor el presupuesto del proyecto y puede tomar unos pocos días para resolver	2	Este riesgo retrasa el progreso del proyecto de forma mínima
Moderado	Afecta de forma moderada el presupuesto del proyecto y puede requerir una re-planificación en el plan del proyecto	3	Este riesgo afecta de alguna manera el progreso del proyecto y al equipo de trabajo
Serio	Afecta la credibilidad e integridad del proyecto. Puede requerir solicitar nuevo financiamiento y adición de recursos. Se debe considerar un importante cambio en la planificación del proyecto	4	Este riesgo afecta el progreso de todo el equipo de trabajo y demanda la atención del gerente del proyecto
Critico	Puede representar el fracaso total o abandono del proyecto	5	Este riesgo afecta a todo el equipo de trabajo y requiere de la atención inmediata del gerente del proyecto

La exposición se define como el valor generado de la probabilidad y el impacto asignado a un riesgo. El valor del impacto puede ser expresado en unidades como días o costo. Exposiciones con alto valor indican que el riesgo es un peligro potencial para el proyecto, sin embargo, exposiciones bajas son relativamente sin importancia. La exposición al riesgo se define de la siguiente forma:

Exposición = Probabilidad de ocurrencia del riesgo * Valor del Impacto del riesgo

A continuación en la Tabla 37 se puede visualizar la relación entre la probabilidad de ocurrencia y el impacto de un riesgo y el nivel de exposición.

Tabla 37 Relación entre la probabilidad de ocurrencia, impacto del riesgo y el nivel de exposición

		Impacto del riesgo				
Probabilidad de ocurrencia		**Insignificante**	**Menor**	**Moderado**	**Serio**	**Critico**
Improbable	0.00-0.10	Bajo	Bajo	Bajo	Medio	Medio
Remoto	0.11-0.40	Bajo	Bajo	Medio	Medio	Alto
Ocasional	0.41-0.60	Bajo	Medio	Medio	Medio	Alto
Probable	0.61-0.90	Medio	Medio	Alto	Medio	Alto
Frecuente	0.91-1.00	Medio	Alto	Alto	Alto	Alto

La prioridad de los riesgos se debe asignar a partir del valor de la exposición. Los riesgos que impliquen la mayor exposición deben ser considerados como los de mayor “prioridad”.

[32] Hopkin, Paul (2010). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, Second Edition. Kogan Page, ISBN-13: 978-0-7494-5942-0, Capitulo 15 - Risk Likelihood and Impact.

Parámetro 3: Punto de entrada para aceptar o rechazar la ocurrencia de un riesgo

Este parámetro permite determinar en qué momento se deben generar las alertas correspondientes antes de que ocurra realmente un riesgo y a quién se debe involucrar. También permite limitar la cantidad de recursos que se pueden asignar para monitorear los riesgos, sin hacer uso excesivo de estos.

En la Tabla 38 se describe una plantilla propuesta para gestionar dichas alertas.

Tabla 38 Puntos de entrada para gestionar aquellas situaciones que pueden representar la ocurrencia de un riesgo

Situación que puede generar un riesgo al proyecto	Acción
Si la cantidad de defectos en la primera iteración es mayor de 30	Se debe notificar al gerente de desarrollo de contenido que revise junto con su grupo de trabajo el proceso de desarrollo que se está siguiendo y si las pruebas unitarias se están ejecutando debidamente.
Si el avance de la ejecución de las pruebas no supera el 60% antes de los dos meses	Se debe contactar a los gerentes del proyecto, así como a los gerentes de aseguramiento de la calidad y de desarrollo de contenido

4.5 Identificar y analizar riesgos

El análisis de riesgos implica la identificación de nuevos riesgos, evaluar y determinar su probabilidad de ocurrencia así como las consecuencias de ocurrir dichos riesgos. Esta meta específica requiere el cumplimiento de las siguientes prácticas específicas:

Identificar los riesgos

La identificación de riesgos potenciales debe ser documentada debidamente. Se debe evitar considerar cualquier evento como un riesgo posible, por lo que la identificación se debe de hacer de manera organizada siendo lo más realista posible.

En la Tabla 39 se describe el artefacto propuesto para documentar los nuevos riesgos.

Tabla 39 Plantilla de registro para la identificación de nuevos riesgos

Nombre del proyecto	Indicar el nombre del proyecto sobre el que se realiza el análisis de riesgos
Descripción del proyecto	Proveer una breve descripción sobre el propósito del proyecto.
Fase del proyecto	Especificar la fase del proyecto donde se determina que el riesgo puede originarse con mayor probabilidad. Por ejemplo, durante el análisis de requisitos, ejecución de pruebas o durante todo el ciclo de vida del proyecto.
Código identificador del riesgo	Proveer de un código de identificación al nuevo riesgo identificado, que sirva para su posterior seguimiento y uso en futuros proyectos.
Descripción del riesgo	Especificar cuál es el riesgo y en qué consiste
Condición para la ocurrencia del riesgo	Indicar las condiciones bajo las que puede existir el riesgo identificado. Por ejemplo, el riesgo actual sólo puede existir dependiendo de la versión del producto que el cliente se encuentre utilizando.
Consecuencias de la ocurrencia del riesgo	Si el riesgo ocurre, entonces se puede afectar la credibilidad de la empresa o el cliente puede prescindir del uso del producto al terminar el contrato.
Gerente del proyecto	Especificar quién es el gerente del proyecto; en este caso sería el gerente del proyecto de calidad.
¿Quién es el responsable por la ocurrencia del riesgo?	Especificar qué personas van a ser las encargadas de evitar que este riesgo ocurra.

Evaluar, categorizar y priorizar riesgos

La evaluación de los riesgos es necesaria para asignar la relevancia que corresponde a cada uno de los riesgos identificados así como determinar cuándo una debida atención durante el proceso de gestión es requerida.

En la Tabla 40 se muestra el artefacto propuesto para representar los distintos parámetros para el análisis de los riesgos.

Tabla 40 Representación de la matriz de riesgos a utilizar en el área de aseguramiento de la calidad

Descripción del riesgo	Probabilidad de ocurrencia	Impacto	Exposición
Riesgo 1	0.70	4	2.8
Riesgo 2	0.90	5	4.5
Riesgo 3	0.50	3	1.5

También en la Tabla 41 se describe la plantilla propuesta para para priorizar los riesgos:

Tabla 41 Plantilla del registro de la prioridad de los riesgos y notas adicionales

Descripción del riesgo	Prioridad	Notas
Riesgo 1	1	Este riesgo requiere atención inmediata una vez se disponga del contenido a probar.
Riesgo 2	2	
Riesgo 3	3	

4.6 Mitigar Riesgos

La mitigación de los riesgos implica la adopción de estrategias para dar respuesta a los riesgos y la implantación de un plan de mitigación de riesgos. Esta meta específica requiere el cumplimiento de las siguientes prácticas específicas:

Desarrollar un plan de mitigación de riesgos

Un componente clave para la implantación de un plan de mitigación de riesgos es el desarrollo de alternativas de acción recomendadas para cada riesgo identificado[33]. En la Tabla 42 se describen las estrategias para dar respuesta a los riesgos negativos o amenazas.

Tabla 42 Estrategias para dar respuesta a los riesgos negativos o amenazas

Estrategia	Descripción
Evitar	Evitar el riesgo implica cambios en el plan del proyecto para eliminar la amenaza completamente. Un ejemplo del uso de esta estrategia es extender el plazo del proyecto o reducir el alcance del proyecto. La estrategia más radical es la de cancelar el proyecto. Algunos riesgos que se pueden presentar en etapas tempranas del proyecto pueden ser evitados clarificando los requerimientos, obteniendo información, mejorando la comunicación o con experiencia técnica.
Transferir	Transferir el riesgo consiste en traspasar la gestión de un grupo o todos los riesgos a una tercera parte incluyendo también la respuesta ante estos riesgos.
Mitigar	Consiste en reducir la probabilidad de ocurrencia y el impacto de un riesgo hacia el negocio dentro de ciertos límites. Tomar acciones tempranas para reducir la probabilidad o el impacto es mucho más efectivo que reparar el daño una vez que el riesgo ha ocurrido.
Aceptar	Esta estrategia se adopta porque por lo general es muy difícil eliminar o reducir los riesgos en todos los proyectos. Esta estrategia implica que el equipo del proyecto ha decidido no realizar ningún cambio al proyecto para poder lidiar con el riesgo en sí o bien porque no ha logrado dar con otra estrategia para dar respuesta al riesgo en cuestión.

En la Tabla 43 se describen las estrategias para dar respuesta a los riesgos positivos u oportunidades.

Tabla 43 Estrategias para dar respuesta a los riesgos positivos u oportunidades

Estrategia	Descripción
Explotar	Esta estrategia puede ser seleccionada para riesgos con impactos positivos donde la organización desea asegurar que la oportunidad es materializada. Un ejemplo de uso de esta estrategia es utilizar a los recursos más talentosos de una organización para reducir los tiempos de entrega del proyecto y reducir los costos planeados inicialmente.
Compartir	Compartir un riesgo positivo implica traspasar parte o toda la oportunidad a terceros quienes se encuentran en mayor capacidad de capturar dicha oportunidad para el beneficio del proyecto.
Mejorar	Esta estrategia se utiliza para incrementar la probabilidad de ocurrencia y el impacto positivo de una oportunidad.

[33] McManus, John (2004) Risk Management in Software Development Projects, ISBN: 9780750658676. Capitulo 4 - Planning Risk Mitigation Strategies in Software Development Projects.
Project Management Institute (2008), A Guide to the Project Management Body Of Knowledge (PMBOK® Guide), Fourth Edition, ISBN: 9781933890517. Capitulo 11 - Project Risk Management - 11.5.2 Plan Risk Responses: Tools and Techniques.

Aceptar	Aceptar una oportunidad consiste en tener disposición a tomar ventaja de esta si se presenta, pero no significa necesariamente perseguirla.

A continuación se describen tres artefactos propuestos como resultado del trabajo de tesis para representar las estrategias de mitigación de riesgos y las acciones de mitigación a ejecutar. En la Tabla 44 se muestra la representación del artefacto para registrar las estrategias de mitigación a seguir para cada riesgo identificado.

Tabla 44 Estrategias de mitigación a seguir para cada riesgo identificado

Riesgos	Estrategia	Justificar adopción de estrategia	Responsables de aplicar la estrategia
No realizar pruebas en todos los sistemas operativos	Aceptar	Para el caso de los sistemas operativos Windows, a pesar de existir distintas versiones, tienen muchas configuraciones similares. Por lo tanto si se limita la cantidad de versiones a probar se ahorra tiempo y esfuerzo.	Ingeniero de aseguramiento de la calidad.

En la Tabla 45 se muestra un ejemplo de cómo registrar las acciones de mitigación para reducir la probabilidad de ocurrencia y el impacto de un riesgo. En la columna “Status del riesgo”, se pueden registrar los siguientes valores:

- Si el riesgo ha sido **controlado**, quiere decir que su probabilidad de ocurrencia ha disminuido considerablemente o bien que si llega a ocurrir, el impacto va a ser menor.
- Si el riesgo ha sido **mitigado**, quiere decir que el riesgo ya no existe y por lo tanto se puede descartar.
- Si el riesgo sigue **abierto**, quiere decir que aún no se han podido aplicar las acciones de mitigación correspondientes o que las acciones de mitigación establecidas previamente no han sido exitosas.
- Si el riesgo está en **contingencia**, quiere decir que el riesgo ha ocurrido y se ha aplicado el plan de contingencia correspondiente.

Tabla 45 Acciones de mitigación de riesgos para reducir la probabilidad de ocurrencia y el impacto

Riesgos	Acciones de mitigación	Responsables de la mitigación	Status del riesgo
Falta de conocimientos sobre virtualización de sistemas operativos Linux	Entrenar a los desarrolladores en crear ambientes virtuales utilizando distribuciones de Linux, como Debian, SuSE, Red Hat. Proveer de los recursos en línea necesarios para agilizar el proceso de aprendizaje.	Gerente de desarrollo y Analista de recursos humanos y capacitación de personal	Controlado

En la Tabla 46 se muestra un ejemplo de cómo registrar las acciones de mitigación en caso de que el riesgo ocurra. Esto representa el plan de contingencia.

Tabla 46 Acciones de mitigación de riesgos en caso de que el riesgo ocurra (Plan de contingencia)

Riesgos	Acciones a seguir en caso de que el riesgo ocurra	Responsables de la mitigación	Status del riesgo
Falta de conocimientos sobre virtualización de sistemas operativos Linux	Conversar con el cliente para extender el plazo de entrega. Ubicar otros desarrolladores internamente dentro de la empresa que puedan ayudar con la creación de los ambientes virtuales en Linux.	Gerente de desarrollo y Analista de recursos humanos y capacitación de personal	Mitigado

Implementar planes de mitigación de riesgos

Los riesgos deben ser monitoreados periódicamente[34] y se debe implementar un plan de mitigación de riesgos cuando sea apropiado. En el área de aseguramiento de la calidad se ha propuesto revisar cada uno de los siguientes artefactos de manera periódica durante el curso del proyecto:

- **Matriz de riesgos.** Ver Tabla 40.
- **Acciones de mitigación de riesgos para reducir la probabilidad de ocurrencia y el impacto.** Ver Tabla 45.
- **Acciones de mitigación de riesgos en caso de que el riesgo ocurra.** Ver Tabla 46.

4.7 Uso de métodos ágiles para dar soporte al proceso de gestión de riesgos

A continuación se listan un conjunto de métodos ágiles que han sido identificadas como valiosos para ayudar en la identificación, control y mitigación de los riesgos:

Reunión de planificación de la entrega y priorizar las tareas más criticas

En esta reunión[35] se discute en términos generales cuál es el contenido que se va probar, se revisan los tiempos de entrega y los plazos, se revisan y discuten los riesgos. En esta reunión se puede partir con la identificación de posibles fuentes de riesgos y revisar los parámetros de la definición de riesgos.

Durante esta reunión se debe empezar a construir un backlog con el conjunto de tareas requeridas por los ingenieros de aseguramiento de la calidad para verificar el contenido a ser enviado

[34] Project Management Institute (2008), A Guide to the Project Management Body Of Knowledge (PMBOK® Guide), Fourth Edition, ISBN: 9781933890517. Capitulo 11 - Project Risk Management - 11.6 Monitor and Control Risks.
[35] SCRUM.org. The SCRUM guide, the official rulebook. http://www.scrum.org/scrumguides/ - Páginas 10 y 18.

por el grupo de desarrollo de contenido. Esta reunión debe ser realizada semanalmente y no debería de exceder una hora y se debe revisar tanto las próximas asignaciones de contenido como las que los ingenieros de aseguramiento de la calidad se encuentran llevando en la actualidad.

En la reunión se debe discutir sobre aquellas tareas que sean consideradas como las más críticas. Durante esta reunión se debe distribuir el contenido a verificar y se debe considerar el nivel de conocimientos que tenga cada miembro del grupo.

Gráfico de exposición pendiente al riesgo (Risk Burndown Chart)

El propósito de este gráfico desarrollado por John Brothers (The Agile Times 2004) y expuesto por Mike Cohn (Mountain Goat Software) [36] es mostrar la tendencia de la exposición al riesgo durante cada iteración. Para esto se realiza una evaluación de riesgos por cada iteración o Sprint donde se determina la probabilidad de ocurrencia y el impacto de dicha ocurrencia representado en cantidad de días perdidos durante el proyecto.

En el caso del proceso actual que sigue tanto el área de aseguramiento de la calidad como el equipo de desarrolladores de contenido de McAfee Vulnerability Manager, el contenido se libera de forma iterativa, sin embargo, no se define un Sprint como tal. Para obtener más detalles sobre esto se puede consultar la tabla 21, específicamente en la actividad 10.

Para entender cómo utilizar esta técnica, se asume que si la probabilidad de ocurrencia de un riesgo es de 0.25 y el impacto de ocurrencia genera una pérdida de 20 días al proyecto, entonces utilizando la fórmula para obtener la exposición al riesgo de probabilidad de ocurrencia por el impacto, la exposición resultante es de 5 días.

A continuación en la Tabla 47 se representa el valor del impacto de un riesgo expresado en días.

Tabla 47 Valor del impacto de un riesgo medido en días perdidos de trabajo durante un proyecto

Impacto del riesgo	Descripción del Impacto	Valor del impacto en días	Interpretar el valor del impacto
Insignificante	Puede ser fácilmente mitigado	1 día	Este riesgo retrasa el progreso de una tarea individual dentro del grupo
Menor	Afecta de forma menor el presupuesto del proyecto y puede tomar unos pocos días para resolver	2 días	Este riesgo retrasa el progreso del proyecto de forma mínima
Moderado	Afecta de forma moderada el presupuesto del proyecto y puede requerir una re-planificación en el plan del proyecto	5 días	Este riesgo afecta de alguna manera el progreso del proyecto y al equipo de trabajo

[36] Mike Cohn's Blog (2010), Managing Risk on Agile Projects with the Risk Burndown Chart http://www.mountaingoatsoftware.com/blog/managing-risk-on-agile-projects-with-the-risk-burndown-chart.

Serio	Afecta la credibilidad e integridad del proyecto. Puede requerir solicitar nuevo financiamiento y adición de recursos. Se debe considerar un importante cambio en la planificación del proyecto	30 días	Este riesgo afecta el progreso de todo el equipo de trabajo y demanda la atención del gerente del proyecto
Critico	Puede representar el fracaso total o abandono del proyecto	90 días	Este riesgo afecta a todo el equipo de trabajo y requiere de la atención inmediata del gerente del proyecto

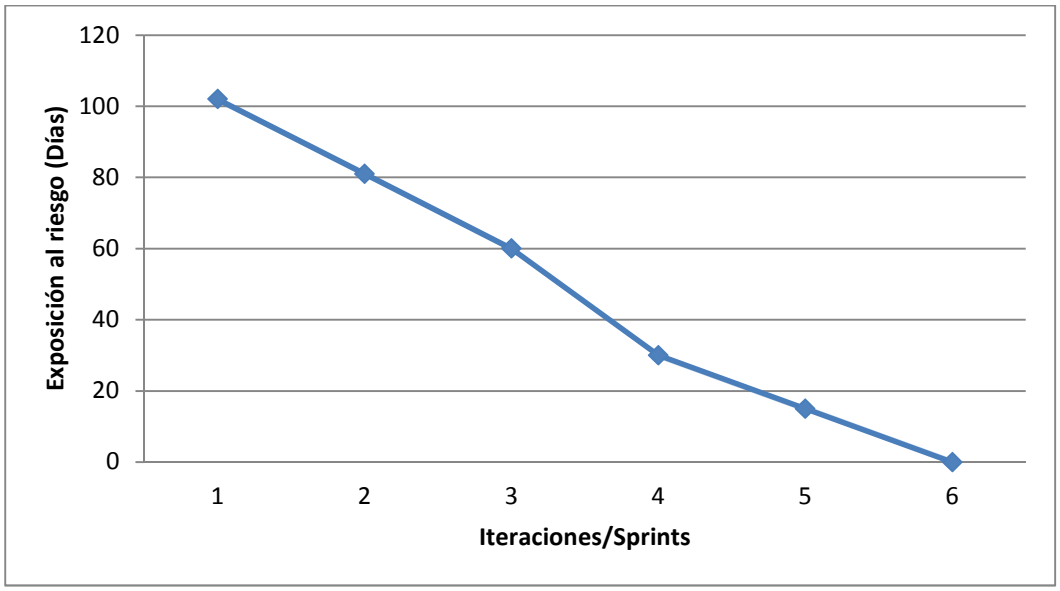
El valor del impacto reflejado en la tabla 47, es un valor que debe ser determinado en conjunto con el grupo de ingenieros de aseguramiento de la calidad. Esto puede variar dependiendo del tipo de proyecto, es decir, es probable que el impacto no solo se refleje en días sino también se puede representar en horas o en costo (dinero).

En la Tabla 48 se representa un conjunto de riesgos identificados durante la primera iteración o Sprint del proyecto, reflejando su probabilidad de ocurrencia, impacto y exposición al riesgo.

Tabla 48 Matriz de evaluación de riesgos por cada iteración o Sprint

Iteración/Sprint	Descripción del riesgo	Probabilidad de ocurrencia	Impacto	Exposición
1	Falta de dispositivo móvil con el sistema operativo iOS (Apple) Instalado para realizar pruebas	0.90	Crítico / 90 días	81
1	Una tasa de defectos igual o superior al 30% por cada 10 scripts liberados para el área de aseguramiento de la calidad.	0.70	Serio / 30 días	21
			Exposición∑=	**102**

Gráfico 12 Gráfico de exposición pendiente al riesgo



En el gráfico anterior, el eje de la exposición al riesgo (días), se obtiene de la sumatoria de todas las exposiciones al riesgo por cada iteración o Sprint a partir de la tabla 48. En este caso se toma como valor esperado 102 días de exposición al riesgo.

Sucesivamente, en la iteración 2 se debe realizar una nueva evaluación y ajustar el valor de la exposición según sea necesario por cada riesgo identificado durante las siguientes iteraciones. Cabe destacar que los datos expuestos tanto el gráfico 10 como en las tablas 47 y 48 son solamente explicativos y no reflejan las mediciones reales del proceso piloto de gestión de riesgos a implantar.

El Scrum diario

Esta técnica consiste en que el equipo de aseguramiento de la calidad se reúne diariamente para discutir:

- Lo que se hizo desde la última reunión, el día anterior.
- Lo que se va a hacer hasta la próxima reunión, es decir, hasta el día siguiente.
- ¿Qué obstáculos tiene en su camino?

En el caso del área de aseguramiento de la calidad, no se desarrolla software, sin embargo, sí se dispone de un backlog donde se coloca cada tarea que requiere pasar por un proceso de pruebas. Estas tareas están asociadas directamente con el contenido que es entregado por parte del equipo de desarrollo.

La realización del Scrum permite identificar posibles riesgos[37], en especial porque se mencionan aquellos obstáculos o factores que alteran el curso normal de las actividades y permiten al Scrum master en el caso particular del área de aseguramiento de la calidad, al gerente del área, tomar las decisiones en consenso con el grupo de trabajo y actuar de forma oportuna.

Rotar el personal

Cada miembro del grupo pueda verificar el mismo tipo de contenido que el resto de los miembros. De esta forma se asegura que el contenido más difícil no es revisado sólo por una persona en particular sino que todos los demás puedan aprender y así estar en capacidad de probar cualquier contenido enviado por el área de desarrollo.

También la rotación de los miembros del grupo de trabajo permite que cada uno pueda llevar a cabo las tareas de gestión de riesgos y dirigir el proceso cuando lo amerite.

4.8 Trazabilidad entre las prácticas ágiles y la gestión de riesgos en CMMI v1.3

En vista de que la propuesta de esta tesis de grado es implantar un proceso de gestión de riesgos basado en CMMI v1.3 utilizando prácticas ágiles, es importante resaltar cuáles son las prácticas ágiles mencionadas a partir del punto 5.7 que ayudan a satisfacer las prácticas especificas del área de proceso de gestión de riesgos.

En la Tabla 49 se representa la trazabilidad entre las prácticas ágiles y las prácticas específicas del área de proceso de gestión de riesgos.

Tabla 49 Relación entre las prácticas especificas del área de procesos de gestión de riesgos de CMMI v1.3 y las prácticas ágiles identificadas a ser utilizadas en el área de aseguramiento de la calidad

Metas Especificas del área de proceso de gestión de riesgos de CMMI v1.3	Prácticas ágiles identificadas que ayudan en la gestión de riesgos para el área de aseguramiento de la calidad
Preparar la gestión de riesgos • Determinar las posibles fuentes de riesgos • Definir los parámetros de los riesgos	Reunión de planificación de la entrega Scrum diario
Identificar y analizar riesgos • Identificar los riesgos • Evaluar, categorizar y priorizar riesgos	Scrum diario Priorizar las tareas más críticas dentro del backlog o plan de proyecto
Mitigar riesgos • Desarrollar un plan de mitigación de riesgos. • Implantar planes de mitigación de riesgos.	Gráfica de exposición pendiente al riesgo Reunión de planificación de la entrega Scrum diario

[37] Agile 101. Agile Risk Management – Identifying Risks. http://agile101.net/2009/07/27/agile-risk-management-identifying-risks-step-1-of-4/.

4.9 Institucionalizar el proceso de gestión de riesgos

En CMMI existe el concepto de "institucionalizar". Institucionalizar se define como la manera de hacer las cosas que una organización sigue rutinariamente como parte de su cultura corporativa. A pesar que el término de institucionalizar en CMMI hace referencia a mantener un nivel de disciplina en múltiples proyectos, en este trabajo se van a sentar las bases de la institucionalización del área de proceso de gestión de riesgos dentro del área de aseguramiento de la calidad.

CMMI v1.3 soporta la institucionalización a través de las prácticas genéricas asociadas con todas las áreas de proceso. Para el propósito de este trabajo se van a tomar en cuenta las prácticas genéricas del nivel de capacidad 1 y nivel de capacidad 2 para el área de proceso de gestión de riesgos.

En la Tabla 50 se describen las guías de elaboración necesarias para dar cumplimiento a las prácticas genéricas de los niveles de capacidad 1 y 2[38].

Tabla 50 Representación de las Guías de elaboración de las prácticas genéricas.

CL	Práctica genérica	Guía de Elaboración
1	GP 1.1 Realizar las prácticas especificas del área de proceso de gestión de riesgos para desarrollar productos de trabajo y proveer servicios para lograr las metas específicas del área de proceso de gestión de riesgos	Se evidencia al ejecutar el proceso piloto utilizando cada uno de los productos de trabajo generados en la sección 4.3 y las prácticas ágiles que se mencionan a partir de la sección 4.4 del presente trabajo.
2	GP 2.1 Establecer y mantener una política organizacional para la planificación y realización del proceso de gestión de riesgos	Con este proyecto, se pretende incluir dentro del área de aseguramiento de la calidad y en especial por cada proyecto de ejecución de pruebas un proceso para identificar, analizar y mitigar los riesgos.
2	GP 2.2 Establecer y mantener el plan para la realización del proceso de gestión de riesgos	Dentro del proceso documentado y definido para la ejecución de pruebas de contenido de seguridad para dispositivos móviles se incluyen los pasos a seguir para llevar a cabo la gestión de riesgos del proyecto. A partir del proceso piloto, esto se debe replicar en el resto de los proyectos de pruebas.
2	GP 2.3 Proveer los recursos adecuados para la realización del proceso de gestión de riesgos	Se dispone de software de escritorio y hojas de cálculo donde se mantienen las plantillas para recopilar y gestionar los datos del proceso de gestión de riesgos. Se dispone de acceso a libros en línea sobre gestión de riesgos por medio de portales especializados en los cuales McAfee posee suscripciones anuales. Por ejemplo, SumTotal Books 24x7.
2	GP 2.4 Asignar responsabilidad y autoridad en la realización del proceso de gestión de riesgos.	En el proceso de aseguramiento de la calidad se definen los responsables del proceso. Sin embargo, en vista de que el grupo de trabajo es pequeño (no más de 4 personas) y el proyecto se desarrolla en un entorno ágil, todos los miembros del equipo se rotan para llevar a cabo la gestión de los riesgos.

[38] CMMI® for Development, Version 1.3, http://www.sei.cmu.edu/reports/10tr033.pdf, Página 68, Part Two: Generic Goals and Generic Practices, Generic Goals and Generic Practices.

2	GP 2.5 Proveer de entrenamiento según sea necesario a las personas que dan soporte al proceso de gestión de riesgos.	El equipo de trabajo tiene a su disposición libros en línea para la consulta de términos asociados a la gestión de riesgos. La empresa dispone de cursos en línea en un portal propio donde los miembros del equipo pueden entrenarse y realizar evaluaciones con respecto a métodos ágiles, aseguramiento de la calidad, entre otros. La empresa ofrece a los miembros del grupo de trabajo la realización de entrenamientos presenciales que pueden estar orientados a la gestión de riesgos y proyectos en general.
2	GP 2.6 Colocar los productos de trabajo seleccionados del proceso de gestión de riesgo bajo los niveles de control apropiados.	Los productos de trabajo del proceso de gestión de riesgos, principalmente, la matriz de gestión de riesgos y las acciones de mitigación en caso de que los riesgos ocurran son almacenadas en un servidor de SharePoint donde se dispone de una estructura por cada proyecto de pruebas.
2	GP 2.7 Identificar e involucrar a personas relevantes dentro del proceso de gestión de riesgos.	Todas las personas del grupo de trabajo del proyecto de pruebas de contenido para dispositivos móviles participan activamente tanto en la identificación, análisis y mitigación de los riesgos. Por lo tanto se consideran relevantes dentro del proceso. La comunicación diaria por medio del Scrum como práctica ágil ayuda a identificar situaciones que afecten el desempeño del proyecto y notificarlas inmediatamente. En algunos productos de trabajo para la gestión de riesgo se define los responsables a contactar en caso de que la exposición a un riesgo sea muy evidente o quienes son las personas responsables para ayudar en la mitigación. Esto puede involucrar no sólo al grupo de trabajo sino otros gerentes o incluso directores.
2	GP 2.8 Monitorear y controlar el proceso de gestión de riesgos contra el plan para la realización del proceso de gestión de riesgos y tomar las acciones correctivas apropiadas	Con la realización del Scrum diario, la revisión periódica de la matriz de riesgos y el plan de mitigación y la gráfica de exposición pendiente al riesgo, se puede visualizar el status de los riesgos y tomar las acciones correspondientes, para minimizar la probabilidad de ocurrencia, comunicarse con los responsables de la mitigación de los riesgos o bien descartar o incluir nuevos riesgos una vez que el proyecto se encuentre en una fase más avanzada. La incorporación de métricas con respecto al proceso de gestión de riesgos permite facilitar el control del mismo.
2	GP 2.9 Evaluar objetivamente la adherencia del proceso de gestión de riesgos y los productos de trabajo seleccionados contra la descripción del proceso de aseguramiento de la calidad y los procedimientos para la gestión de riesgos.	Esto se puede evidenciar actualizando los productos de trabajo como la matriz de gestión de riesgos y de mitigación de riesgos. También se puede evidenciar el uso del correo electrónico para entregar los aportes de los miembros del grupo en cuanto a la gestión de los riesgos.
2	GP 2.10 Revisar las actividades, estado y resultados del proceso con niveles gerenciales que permita la resolución de problemas.	El grupo de trabajo tiene la libertad de consultar distintos niveles gerenciales para atacar problemas potenciales. Adicionalmente, el gerente de aseguramiento de la calidad se reúne semanalmente con otros gerentes y directores para entregar un estado de las actividades de aseguramiento de la calidad y los proyectos en curso.

4.10 Descripción del proceso piloto de aseguramiento de la calidad que incluye las actividades de gestión de riesgos

A continuación se describen las tareas propuestas de gestión de riesgos que van a formar parte del proceso piloto de gestión de riesgos y van a estar incluidas en el proceso general de aseguramiento de la calidad de contenido de seguridad para dispositivos móviles como parte del producto de McAfee Vulnerability Manager.

En la Tabla 51 se describe la tarea relacionada con la determinación de las fuentes de riesgos.

Tabla 51 Tarea del proceso piloto de gestión de riesgos: Determinar fuentes de riesgos

Tarea	Determinar fuentes de riesgos
Descripción de la tarea	Se persigue identificar posibles riesgos que puedan impactar el proceso de aseguramiento de la calidad.
Responsables	• Principales: Ingenieros de aseguramiento de la calidad • Secundarios: Desarrolladores de contenido
Entradas	• Email de notificación de nuevo contenido a desarrollar (Obligatorio) • Listado de fuentes de riesgos (Obligatorio)
Actividades	**1. Notificar el desarrollo de nuevo contenido** El grupo de desarrollo de contenido debe notificar a los ingenieros de aseguramiento de la calidad cuando existe una necesidad de desarrollar nuevo contenido bien sea como resultado de una solicitud de un cliente o bien porque la empresa ha decidido que el producto debe cubrir más vulnerabilidades por razones de competencia o de posicionamiento en el mercado. La salida de esta actividad debe ser la confirmación de los ingenieros de aseguramiento de la calidad de haber revisado el Email de notificación de nuevo contenido a desarrollar. **2. Identificar las posibles fuentes de riesgos** Una vez que los Ingenieros de aseguramiento de la calidad reciben un Email de notificación de nuevo contenido a desarrollar, deben considerar la discusión de esta nueva tarea en la **Reunión de planificación de entrega de contenido** (ver Pag. 56) semanal. En este paso los ingenieros de aseguramiento de la calidad revisan el Listado de Vulnerabilidades y Amenazas a cubrir filtrando las líneas que se encuentran "sin asignación". Entre los ingenieros de aseguramiento de la calidad deciden en la Reunión de planificación de entrega de contenido llevada a cabo en el lugar de trabajo qué líneas cubre cada uno y quién va a ser el responsable de consolidar los resultados que van a enviar los Ingenieros de aseguramiento de la calidad (ver. **Rotar al personal – Pag. 59**). Posteriormente, cada ingeniero de aseguramiento de la calidad debe utilizar una plantilla denominada el **Listado de fuentes de riesgo** (ver Tabla 24). Este listado se ha creado en conjunto con cada uno de los Ingenieros de aseguramiento de la calidad utilizando como base la experiencia de cada uno. De manera individual cada ingeniero debe revisar el listado de fuentes de riesgo y pensar sobre las líneas que le fueron asignadas del Listado de Vulnerabilidades y Amenazas a cubrir y completar el listado de fuentes de riesgo. La salida de este paso es el **Listado de fuentes de riesgo** completado. **3. Recolectar listados de posibles fuentes de riesgos** Cada ingeniero, al completar el Listado de fuentes de riesgo, debe enviarlo a la persona encargada

	de consolidar los resultados. Esta persona debe saber cómo interpretar el Listado de fuentes de riesgo y por lo tanto documentar los posibles riesgos que se deriven de dicho listado utilizando el **Registro de riesgos identificados** (ver Tabla 29). Una vez que se han documentado los posibles riesgos en el archivo de Registro de riesgos identificados, se debe sostener una breve reunión entre los Ingenieros de aseguramiento de la calidad para aclarar cualquier ambigüedad presente en el documento y que dificulte la posibilidad de identificar un determinado riesgo. La salida generada de este paso es el **Registro de riesgos identificados**. **4. Evaluar otros posibles riesgos** Los ingenieros de aseguramiento de la calidad deben estar en capacidad de cuestionar el proceso actual y evaluar la existencia de otros riesgos que puedan no derivarse del Listado de fuentes de riesgo y que puedan tener un impacto dentro del área de aseguramiento de la calidad. En este caso dichos riesgos deben ser notificados a la persona encargada de documentar los riesgos en el Registro de riesgos identificados. Si existen dudas sobre la inclusión del riesgo, esto puede ser discutido en una breve reunión con el grupo o bien durante la Reunión de planificación de entrega de contenido. También una vez que los ingenieros de aseguramiento de la calidad han comenzado a verificar el contenido, se puede mencionar la posible existencia de un riesgo durante el **Scrum Diario** (ver Pág. 58). En caso de que se incluya el nuevo riesgo, se debe considerar actualizar el mismo en el **Listado de fuentes de riesgo**, formulando una pregunta que se encuentre asociada con dicho riesgo.
Salidas	• Listado de fuentes de riesgo (Obligatorio) • Registro de riesgos identificados (Obligatorio)

En la Tabla 52 a continuación se describe la tarea relacionada con analizar los riesgos identificados.

Tabla 52 Tarea del proceso piloto de gestión de riesgos: Analizar los riesgos identificados

Tarea	Analizar los riesgos identificados
Descripción de la tarea	Se analizan y priorizan los riesgos identificados.
Responsables	• Ingenieros de aseguramiento de la calidad
Entradas	• Registro de riesgos identificados (Obligatorio)
Actividades	1. **Desarrollar la matriz de gestión de riesgos** Una vez que se han determinado las posibles fuentes de riesgos y se han documentado en el Registro de riesgos identificados, entonces se debe crear la **Matriz de gestión de riesgos** (ver Tabla 30). El resultado de este paso debe ser la **Matriz de gestión de riesgos** generada. 2. **Priorizar los riesgos** Una vez que se ha creado la Matriz de gestión de riesgos se debe establecer los **Riesgos priorizados** (ver Tabla 31) asignando la prioridad correspondiente para atender cada riesgo identificado y la justificación del nivel de prioridad. El resultado de la realización de este paso son los **Riesgos priorizados.**
Salidas	• Matriz de gestión de riesgos (Obligatorio) • Riesgos priorizados (Obligatorio)

En la Tabla 53 a continuación se describe la tarea relacionada con el desarrollo de un plan de mitigación y contingencia de los riesgos.

Tabla 53 Tarea del proceso piloto de gestión de riesgos: Desarrollar plan de mitigación y contingencia de los riesgos

Tarea	Desarrollar plan de mitigación y contingencia de los riesgos
Descripción de la tarea	Se desarrolla un plan de mitigación de riesgos y contingencia para los riesgos identificados del proyecto.
Responsables	• Ingenieros de aseguramiento de la calidad
Entradas	• Matriz de gestión de riesgos (Obligatorio)
Actividades	**1. Definir la estrategia para dar respuesta a los riesgos** En este paso los Ingenieros de aseguramiento de la calidad deben analizar y decidir sobre la estrategia de mitigación para cada riesgo identificado en la Matriz de gestión de riesgos. Como referencia se pueden consultar **Estrategias de mitigación de riesgos conocidas** (ver Tablas 32 y 33). En la Reunión de planificación de entrega de contenido semanal o bien en el Scrum Diario, se puede discutir sobre la adopción de la mejor estrategia para cada riesgo identificado. También se debe justificar la adopción de dicha estrategia y quien sea el responsable de dicha adopción debe garantizar que efectivamente esta sea la estrategia a utilizar. El resultado de este paso es la **Selección de estrategia de mitigación de riesgos.** **2. Definir las acciones a tomar para mitigar un riesgo** Los ingenieros de aseguramiento de la calidad deben analizar cuál es la acción o conjunto de acciones más recomendables para mitigar un riesgo o disminuir la probabilidad de ocurrencia del mismo. Estas acciones pueden ser discutidas durante la Reunión de planificación de entrega de contenido o en el Scrum Diario. Sin embargo, también cada miembro del equipo de trabajo puede enviar voluntariamente su propuesta para mitigar un determinado riesgo identificado vía e-mail. En este paso se deben identificar las **Acciones para mitigar riesgos** (ver Tabla 35). **3. Definir un plan de contingencia** En este paso los Ingenieros de aseguramiento de la calidad deben diseñar un plan de acción alternativo en caso de que un riesgo no pueda ser controlado (bien sea eliminado o al menos reducir su probabilidad de ocurrencia y que sea aceptado) y que en efecto ocurra. En tal caso, los Ingenieros de aseguramiento de la calidad deben colocarse en la perspectiva de reconocer que un riesgo puede ocurrir y tal vez no sea controlado porque puede depender de factores externos y ajenos al grupo de trabajo. El resultado de la realización de este paso es la elaboración de un **Plan de contingencia** (ver Tabla 36).
Salidas	• Estrategias de mitigación de riesgos seleccionadas (Obligatorio) • Acciones de mitigación de riesgos (Obligatorio) • Plan de contingencia (Obligatorio)

En la Tabla 54 a continuación se describe la tarea relacionada con monitorear los riesgos.

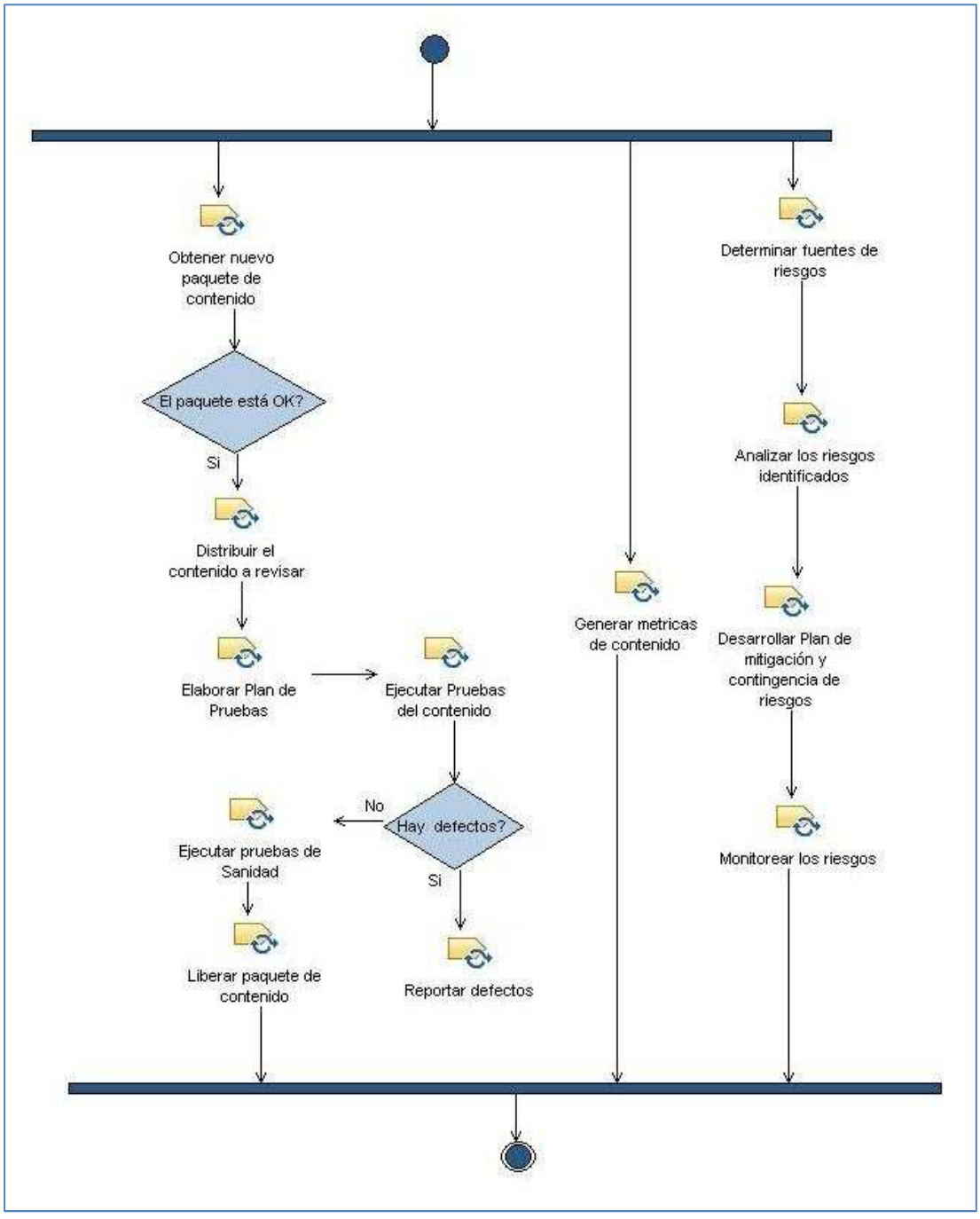
Tabla 54 Tarea del proceso piloto de gestión de riesgos: Monitorear los riesgos

Tarea	Monitorear los riesgos
Descripción de la tarea	Se evalúan los riesgos identificados y si corresponde la aplicación de las acciones de mitigación y contingencia.
Responsables	• Ingenieros de aseguramiento de la calidad
Entradas	• Matriz de gestión de riesgos (Obligatorio) • Acciones de mitigación de riesgos (Obligatorio) • Plan de contingencia (Obligatorio)
Actividades	**1. Implementar las acciones de mitigación de riesgos** Los Ingenieros de aseguramiento de la calidad debe contribuir en el monitoreo periódico de los riesgos y por lo tanto tomar las acciones necesarias cuando sea requerido. Por esta razón los siguientes artefactos deben ser revisados continuamente bien sea en la Reunión de planificación de entrega de contenido o en el Scrum Diario: • La Matriz de gestión de riesgos • Las Acciones para mitigar riesgos • El Plan de contingencia El resultado de este paso es la revisión continua de los tres artefactos mencionados y ejecutar las acciones de mitigación y contingencia en la medida que sea necesario. También cada uno de los artefactos debe ser actualizado según corresponda. **2. Realizar mediciones** Los Ingenieros de aseguramiento de la calidad deben utilizar métricas para evaluar el desempeño del proceso de gestión de riesgos. Para llevar a cabo este paso se deben de realizar tres mediciones: • **Obtener el Indicador de exposición al riesgo** (ver Gráfico 7 y Pág. 56) • **Obtener el Indicador de ocurrencia e impacto de los riesgos** (ver Indicador de ocurrencia e impacto de los riesgos) • **Obtener la trazabilidad de la gestión de riesgos en el área de aseguramiento de la calidad con los objetivos del negocio** (ver Trazabilidad de la gestión de riesgos con los objetivos del negocio) La salida resultante de este paso es la obtención de métricas por cada iteración.
Salidas	• Reporte de métricas que incluye: Indicador de exposición al riesgo Indicador de ocurrencia e impacto de los riesgos Trazabilidad de la gestión de riesgos en el área de aseguramiento de la calidad con los objetivos del negocio.

4.11 Representación gráfica de las tareas de gestión de riesgo en el marco del proceso de aseguramiento de la calidad

En el gráfico 11 se muestran cada una de las tareas de gestión de riesgos propuestas dentro del marco del proceso de aseguramiento de la calidad de contenido.

Gráfico 13 Gráfico desarrollado en el Eclipse Process Framework que muestra las tareas de gestión de riesgos en el marco del proceso de aseguramiento de la calidad



4.12 Descripción de las métricas a recolectar durante la ejecución del proceso piloto de gestión de riesgos

Indicador de exposición al riesgo

Esta métrica permite evaluar el desempeño del proceso piloto de gestión de riesgos, comparando la exposición al riesgo por cada iteración, lo que permite saber si los riesgos se han venido mitigando o si su probabilidad de ocurrencia se ha reducido.

En la medida que la mitigación tenga efecto o la probabilidad de ocurrencia sea menor, el valor de la exposición al riesgo disminuye, lo que se traduce en un desempeño positivo de la gestión de los riesgos.

También se debe considerar que el valor de la exposición al riesgo se puede incrementar entre una iteración y otra debido a la identificación de nuevos riesgos. Sin embargo, esto no quiere decir que el desempeño de la gestión de riesgos ha sido negativa, pero sí se debe determinar por qué los riesgos nuevos no fueron identificados en iteraciones anteriores o si corresponden a factores externos.

Para la obtención de esta métrica se debe utilizar el gráfico de exposición pendiente al riesgo el cual es representado en el gráfico 10.

Indicador de ocurrencia e impacto de los riesgos

Esta métrica permite cuantificar distintos elementos del proceso de gestión de riesgos, por ejemplo:

Tabla 55 Métrica resultante sobre la ocurrencia e impacto de los riesgos

Indicador	Valor	Impacto Positivo o Negativo ¿Cuantos días se ganan o pierden?
Número de riesgos identificados en el proyecto	10	
Número de riesgos identificados y que fueron mitigados antes de ocurrir	6	2 días ganados
Número de riesgos identificados y cuya probabilidad de ocurrencia fue reducida	3	
Número de riesgos que ocurrieron	1	5 días perdidos
Número de riesgos no identificados que ocurrieron	1	3 días perdidos

5. Validación de la propuesta

5.1 Implantación del proceso piloto de gestión de riesgos

Propuesta de desarrollo de contenido nuevo para dispositivos móviles

A partir del proceso de gestión de riesgos piloto propuesto se solicitó al equipo de desarrollo de contenido el envío de una notificación vía correo electrónico donde se indique que hay un contenido tentativo a desarrollar y que va a ser agregado al contenido del producto McAfee Vulnerability Manager.

Una vez que el equipo de desarrollo envió el correo electrónico, se les indicó a los Ingenieros de aseguramiento de la calidad que revisaran el listado de vulnerabilidades y amenazas a cubrir.

El número total de scripts a desarrollar inicialmente era de aproximadamente 40, que cubren distintos tipos de vulnerabilidades en dispositivos móviles tanto para Android como para iOS principalmente.

Revisión del contenido a desarrollar y asignación de contenido

Una vez que se ha recibido la notificación por parte del equipo de desarrollo de contenido, los Ingenieros de aseguramiento de la calidad agendaron la realización de una reunión de planificación de la entrega del contenido durante la semana en que fue recibido el correo de notificación. Esta reunión es parte del proceso de gestión de riesgos piloto.

En la reunión participaron todos los Ingenieros de aseguramiento de la calidad del contenido del producto McAfee Vulnerability Manager, así como el gerente de aseguramiento de la calidad. La reunión se desarrolló en el mismo lugar de trabajo puesto que la ubicación de los puestos de los empleados lo permite. La reunión fue dirigida en parte por el gerente de aseguramiento de la calidad. Durante la reunión de planificación de la entrega de contenido se discutieron los siguientes puntos:

- **¿Cuál es el contenido que se iba a probar?**

Se mencionó que el contenido era orientado exclusivamente a dispositivos móviles, específicamente para los sistemas operativos Android y iOS.

- **¿Cuáles eran los plazos de entrega exigidos por el cliente o por el área de gestión del producto McAfee Vulnerability Manager?**

Los plazos en este caso no pudieron ser sometidos a una estimación más precisa por parte de los ingenieros de aseguramiento de la calidad ya que el plazo lo había definido el área de gestión del producto. Un punto que se mencionó en la reunión era que no necesariamente todo el contenido

debía de funcionar plenamente para el momento de ser liberado, ya que el contenido del producto se libera de forma incremental y el contenido no iba a ser liberado para todos los clientes, sino para un grupo específico.

Por lo tanto se podía utilizar cierta holgura y aprovechar la retroalimentación con el cliente para mejorar el contenido de ser necesario.

- **Se realizó la discusión sobre la identificación de los posibles riesgos.**

En este punto se mencionó que cada ingeniero de aseguramiento de la calidad iba a revisar un grupo de scripts enviados por el grupo de desarrollo de contenido y que se encuentran en el listado de vulnerabilidades y amenazas a cubrir con la finalidad de llevar a cabo la identificación de riesgos para el contenido.

Se solicitó revisar en qué consistía cada vulnerabilidad a cubrir por los 40 scripts y completar el listado de fuentes de riesgos, que es un producto de trabajo incorporado como parte del proceso de gestión de riesgos piloto.

También los 3 ingenieros de aseguramiento de la calidad se comprometieron a distribuir equitativamente la cantidad de scripts a revisar, filtrando el listado de vulnerabilidades y amenazas a cubrir por aquellos scripts que se encuentran "sin asignación". Se designó al Ingeniero de aseguramiento de la calidad encargado de consolidar los resultados enviados por cada uno de los miembros del equipo.

El Ingeniero designado para consolidar los resultados se encargaría de actualizar el listado de vulnerabilidades y amenazas a cubrir con el nombre del ingeniero encargado de revisar cada uno de los 40 scripts tentativos a desarrollar.

- **Se revisó el backlog actual del área de aseguramiento de la calidad.**

Se discutió el estado de cada una de las tareas en curso y pendientes por comenzar así como el nivel de prioridad de cada tarea y la cantidad de recursos necesarios para la realización de cada tarea en específico.

También se incluyó en el backlog la tarea relacionada con la entrega de los 40 scripts para dispositivos móviles.

Identificación de las posibles fuentes de riesgos.

Cada uno de los Ingenieros de aseguramiento de la calidad se encargó de revisar el listado de vulnerabilidades y amenazas a cubrir de acuerdo a lo discutido en la reunión de planificación de la entrega y evaluar el listado de fuentes de riesgos.

Una vez que los Ingenieros de aseguramiento de la calidad revisaron el listado de fuentes de riesgos y lo completaron, procedieron a enviar una copia del mismo vía correo electrónico al Ingeniero que fue asignado inicialmente para consolidar los resultados de la identificación de riesgos. Durante la consolidación de los resultados, el Ingeniero designado para esta tarea tuvo que consultar a los otros 2 Ingenieros cualquier duda relacionada con los datos colocados en el listado de fuentes de riesgos y la justificación proporcionada por cada uno con respecto a cada punto.

Posteriormente, se lograron consolidar los resultados los cuales son representados en la Tabla 56 a continuación:

Tabla 56 Consolidado de fuentes de riesgos obtenido a partir de las evaluaciones realizadas por cada uno de los Ingenieros de aseguramiento de la calidad sobre los 40 scripts tentativos a ser desarrollados para dispositivos móviles

Categoría	Descripción	SI	NO	Justificar
Planificación	¿Hay algún método para estimar el esfuerzo en horas hombre para probar el contenido del proyecto solicitado?		X	Las estimaciones se realizan en base a la experiencia de los Ingenieros de aseguramiento de la calidad. No se dispone de datos estadísticos para las estimaciones.
	¿Se conocen los plazos de entrega del proyecto?	X		Los directores del área colocaron un plazo de entrega y se colocó el proyecto entre las prioridades del cuarto fiscal.
	¿Se sabe quiénes son las personas importantes dentro del proyecto, por ejemplo, gerentes, directores, especialistas técnicos, en caso de ser necesario contactarlos?	X		En el documento de la propuesta de negocio entregado a QA se muestra un detalle de los responsables del proyecto y los grupos técnicos que participan.
Requisitos	¿Hay alguna especificación disponible para verificar lo que se desea probar como parte del proyecto?, por ejemplo, algún documento del CIS (Center for Internet Security), PCI (Payment Card Industry), etc..	X		En el documento de la propuesta de negocio entregado a QA se hace referencia a qué es lo que se debe probar y el alcance.
	¿Existen casos de prueba documentados para utilizarlos durante la ejecución de las pruebas?		X	Se tienen que diseñar los casos de prueba al tener más conocimiento sobre los requerimientos y las tecnologías involucradas.
	¿Se entiende la finalidad del contenido y a qué clientes va dirigido especialmente?	X		En el documento de la propuesta de negocio se menciona cuál es el alcance del contenido y a qué tipo de clientes va dirigido.

Operacional	¿Hay el personal suficiente dentro del grupo de trabajo para poder llevar a cabo la fase de pruebas del proyecto?	X		El recurso humano se debe ir asignando en la medida que las otras tareas con mayor prioridad lo permitan.
	¿Es necesario trasladar personal de una localidad a otra?		X	Tanto el grupo de QA como de desarrollo de contenido está mayoritariamente en Chile.
	¿Hay riesgo de que alguien abandone el grupo de trabajo?		X	El grupo se encuentra estable y no se han presentado inquietudes con respecto a este tema.
	¿Es posible realizar las pruebas del proyecto en un mismo lugar o es necesario realizarlo en más de una zona horaria?	X		Las pruebas se pueden realizar sin problemas en Chile y durante la zona horaria de Chile sin depender de otro lugar.
	¿En caso de fallas eléctricas o desastre en el entorno de trabajo, terremoto, incendio, es posible continuar con la ejecución del proyecto?		X	Todo el hardware para la realización de las pruebas se encuentra en la oficina de McAfee Chile.
	¿Se debe incurrir en gastos adicionales para la compra de hardware o software?	X		Se tienen que comprar teléfonos móviles que soporten Android, iOS y RIM y un servidor dedicado desde donde se pueda instalar el McAfee Vulnerability Manager y lanzar auditorías a los teléfonos móviles o emuladores de los cuales se disponga.
Comunicación	¿Hay los medios disponibles para comunicarse con los involucrados en el proyecto, por ejemplo, correo, teléfono, mensajería, etc.?	X		Las comunicaciones se pueden hacer sin inconvenientes por correo electrónico, teléfono, mensajería, etc..
	¿Las diferencias culturales son entendidas entre los miembros del proyecto, barreras de idioma, escritura, creencias, etc.?	X		Se está acostumbrado a trabajar con personas de distintos países y culturas como China, India y Estados Unidos.
	¿Los gerentes y directores se pueden ubicar fácilmente cuando los problemas se presentan, por ejemplo, un proceso de escalamiento?	X		Se puede hacer de forma directa, no es necesario involucrar a muchas personas para contactar a los niveles más altos de la organización internamente.
	¿Si un cliente reporta una falla, existe un proceso formal para atender las quejas de los clientes y resolver las posibles fallas, sin incurrir en pérdidas de esfuerzo o involucrar a áreas que no corresponden?	X		Hay un proceso de escalamiento de incidentes y defectos que tiene como punto de entrada el área de soporte y servicio al cliente. Este proceso utiliza como herramienta principal Bugzilla.

Técnico	¿Hay el hardware disponible para poder realizar las pruebas del proyecto?		X	Se debe adquirir el hardware necesario, su configuración y puesta en marcha.
	¿Hay el software disponible para poder realizar las pruebas del proyecto, por ejemplo, licencias, productos de terceros, etc..?	X		Se cuenta con la licencia del McAfee Vulnerability Manager que es el software que va a utilizar el contenido a ser desarrollado.
	¿Los ingenieros tienen el conocimiento suficiente para empezar a realizar las pruebas del proyecto lo antes posible?		X	Tienen que entrenarse y documentarse. Se debe coordinar el entrenamiento en línea con personas del área de desarrollo del producto en Estados Unidos. También se debe solicitar la mayor información posible al área de desarrollo de contenido sobre cómo realizar las pruebas.
	¿Se requiere un período de entrenamiento?	X		Se requiere un periodo de al menos una semana para comenzar lo antes posible la ejecución de las pruebas.
	¿Los datos de las pruebas se pueden almacenar en algún repositorio?	X		Los datos de las pruebas se almacenan en planillas de Excel donde se registran los casos de prueba.
	¿Existe algún software para reportar y dar seguimiento a los defectos durante la ejecución de las pruebas?	X		Para los defectos internos, de QA al área de desarrollo de contenido se utilizan planillas de Excel y el correo para hacer seguimiento de los defectos. Cuando son defectos externos y reportados por los clientes se utiliza Bugzilla.

Registro de los riesgos identificados

Una vez consolidados los listados de fuentes de riesgos completados por cada uno de los Ingenieros de aseguramiento de la calidad y cuyo resultado se muestra en la tabla 56, el Ingeniero designado para consolidar los riesgos pudo proceder con el registro de los riesgos identificados. A continuación se muestran los distintos riesgos identificados:

Nombre del proyecto	Mobile Content
Descripción del proyecto	Desarrollo de 40 scripts para dispositivos móviles
Fase del proyecto	Planificación
Código identificador del riesgo	R001
Descripción del riesgo	Falta de presupuesto para armar el laboratorio de dispositivos Mobile
Condición para la ocurrencia del riesgo	Depende del presupuesto que asigne Gerencia.
Consecuencias de la ocurrencia del riesgo	Si el Riesgo ocurre, el equipo de desarrollo y calidad no tendrá los equipos necesario para asegurar la calidad del producto que saldrá a producción.
Gerente del proyecto	Raul Collantes
¿Quién es el responsable por la ocurrencia del riesgo?	Raul Collantes

Nombre del proyecto	Mobile Content
Descripción del proyecto	Desarrollo de 40 scripts para dispositivos móviles
Fase del proyecto	Ejecución de Pruebas
Código identificador del riesgo	R002
Descripción del riesgo	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.
Condición para la ocurrencia del riesgo	Si los Analistas no reciben capacitación acerca del nuevo producto y de tecnologías mobile
Consecuencias de la ocurrencia del riesgo	La calidad del producto se verá impactaba ya que a medida que los analistas tengan más experiencia y conocimiento las pruebas serán de mejor nivel.
Gerente del proyecto	Dorian Guzman
¿Quién es el responsable por la ocurrencia del riesgo?	Dorian Guzman

Nombre del proyecto	Mobile Content
Descripción del proyecto	Desarrollo de 40 scripts para dispositivos móviles
Fase del proyecto	Ejecución de Pruebas
Código identificador del riesgo	R003
Descripción del riesgo	No contar con los ambientes necesarios para la ejecución de pruebas
Condición para la ocurrencia del riesgo	Falta de experiencia de los Analistas de Calidad y Falta de Soporte por parte de los especialistas para la configuración de los ambientes necesarios para las pruebas.
Consecuencias de la ocurrencia del riesgo	Si el riesgo ocurre, las pruebas no podrán ser realizadas simulando los casos reales. La calidad final del producto se verá afectada y por ende la satisfacción del cliente
Gerente del proyecto	Dorian Guzman
¿Quién es el responsable por la ocurrencia del riesgo?	Dorian Guzman

Nombre del proyecto	Mobile Content
Descripción del proyecto	Desarrollo de 40 scripts para dispositivos móviles
Fase del proyecto	Ejecución de Pruebas
Código identificador del riesgo	R004
Descripción del riesgo	Cambios en la prioridad del proyecto (ejecución de pruebas)

Condición para la ocurrencia del riesgo	Los Analistas de Calidad trabajan en diferentes proyectos y con diferentes prioridades; si se presenta un proyecto con mayor prioridad, el proyecto Mobile se verá afectado.
Consecuencias de la ocurrencia del riesgo	Atrasos en las fechas comprometidas.
Gerente del proyecto	Raul Collantes
¿Quién es el responsable por la ocurrencia del riesgo?	Raul Collantes

Nombre del proyecto	Mobile Testing
Descripción del proyecto	Desarrollo de 40 scripts para dispositivos móviles
Fase del proyecto	Planificación, Requerimientos, Desarrollo, Ejecución
Código identificador del riesgo	R005
Descripción del riesgo	Cambio de requerimientos
Condición para la ocurrencia del riesgo	Como es una tecnología nueva y es un nuevo producto podrían cambiar las definiciones de los requerimientos.
Consecuencias de la ocurrencia del riesgo	Afectarán los plazos del proyecto.
Gerente del proyecto	Raul Collantes
¿Quién es el responsable por la ocurrencia del riesgo?	Raul Collantes

Evaluación de otros riesgos

Una vez que los riesgos identificados fueron documentados, se discutió en una nueva reunión de planificación de la entrega sobre estos riesgos junto con el gerente de aseguramiento de la calidad con la finalidad de confirmar si efectivamente los riesgos son realistas y se justifican. Adicionalmente, se evaluó si existían otros riesgos no identificados inicialmente, pero no se logró evidenciar algún otro potencial riesgo.

Analizar los riesgos identificados y definir la prioridad

Luego de haber identificado y registrado los riesgos potenciales presentes en el nuevo contenido a desarrollar para dispositivos móviles desde el punto de vista del área de aseguramiento de la calidad, se tuvo que generar la matriz de riesgos pertinente.

Durante la última reunión de planificación de la entrega, se logró discutir sobre la probabilidad de ocurrencia y el impacto asociado a cada riesgo, siendo este último representado en días de pérdida para el proyecto, utilizando como punto de referencia las tablas 35, 36 y 37 de la sección relacionada con la definición de los parámetros de riesgo.

Para el desarrollo de la matriz de riesgos se generaron los siguientes cálculos que se representan en la Tabla 57:

Tabla 57 Matriz de riesgos para los 40 scripts tentativos a ser desarrollados para dispositivos móviles

Id del Riesgo	Descripción del riesgo	Probabilidad de ocurrencia	Impacto (Días)	Exposición
R001	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	0,5	20	10
R002	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	0,7	15	10.5
R003	No contar con los ambientes necesario para la ejecución de pruebas	0,9	15	13.5
R004	Cambios en la prioridad del proyecto	0,9	5	4.9
R005	Cambio de requerimientos	0,8	10	8

También se tuvo que establecer la prioridad para cada uno de los riesgos de tal forma de tomar las acciones correspondientes cuando lo amerite. Para asignar la prioridad de los riesgos se toma como base el valor de la exposición al riesgo. Aquellos riesgos con mayor exposición deben ser atendidos con prioridad. En la Tabla 58 a continuación se puede visualizar la prioridad asignada a cada riesgo.

Tabla 58 Asignación de prioridad para los riesgos identificados relacionados con los 40 scripts tentativos a ser desarrollados para dispositivos móviles

Id del Riesgo	Descripción del riesgo	Prioridad
R001	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	1
R002	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	1
R003	No contar con los ambientes necesarios para la ejecución de pruebas	1
R005	Cambio de requerimientos	2
R004	Cambios en la prioridad del proyecto	3

Cabe destacar que la recolección de los datos fue una tarea para la que se tuvo que asignar esfuerzo y por lo tanto también se mencionó en varias oportunidades en el Scrum diario.

Desarrollo del plan de mitigación y contingencia de los riesgos

Durante esta etapa los Ingenieros de aseguramiento de la calidad tuvieron que discutir sobre la adopción de las estrategias de mitigación de riesgos que resultaran más convenientes.

Estas estrategias se discutieron en la reunión de planificación de entrega semanal y se mencionaron durante el Scrum diario. En la Tabla 59 se muestran las estrategias de mitigación de riesgos seleccionadas.

Tabla 59 Estrategias de mitigación de riesgos seleccionadas para los 40 scripts tentativos a desarrollar para dispositivos móviles

Id del Riesgo	Riesgos	Estrategia	Justificar adopción de estrategia	Responsables de aplicar la estrategia
R001	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	Evitar	Si es que no hay presupuesto para la compra de los dispositivos mobile, no se podrá tener el ambiente necesario para el desarrollo del contenido ni para el aseguramiento de calidad por lo que se tiene que evitar no obtener el presupuesto para la compra de equipos. Si no se puede asegurar la calidad es preferible la cancelación del proyecto.	Software Manager
R002	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	Mitigar	Se pueden definir acciones de mitigación para reducir el riesgo en etapas tempranas; por ejemplo capacitaciones.	QA Manager
R003	No contar con los ambientes necesarios para la ejecución de pruebas	Mitigar	Se puede mitigar tempranamente empezando con la capacitación y configuración desde el inicio del proyecto.	QA Manager
R004	Cambios en la prioridad del proyecto	Aceptar	Como el equipo de Calidad maneja muchos proyectos a la vez, si aparece un proyecto con p0 o patch Tuesday; el proyecto mobile necesariamente bajará su prioridad.	Software Manager
R005	Cambio de requerimientos	Aceptar	Como es un producto nuevo y nueva tecnología lo más probable es que los requerimientos vayan cambiando en el tiempo a medida que se adquiere más experiencia por lo que se tendrá que lidiar con estos cambios.	Software Manager

En cuanto a las acciones para la mitigación de los riesgos, se adoptaron las siguientes que se encuentran representadas en la Tabla 60:

Tabla 60 Acciones de mitigación para los riesgos identificados relacionados con los 40 scripts tentativos a desarrollar para dispositivos móviles

Id del Riesgo	Riesgos	Acciones de mitigación	Responsables de la mitigación
R001	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	Demostrar tempranamente a los inversionistas/managers la necesidad de tener el laboratorio de Mobile. Elevar la solitud de presupuesto a los niveles que sean necesarios.	Software Manager
R002	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	Organizar sesiones de capacitacion sobre tecnologias mobile y sobre el nuevo producto MAM	QA Manager
R003	No contar con los ambientes necesarios para la ejecución de pruebas	Incluir en el plan de proyecto la tarea de configuracion de ambiente en fases tempranas del proyecto. Organizar sesiones de entrenamiento con los expertos en el producto.	QA Manager
R004	Cambios en la prioridad del proyecto	Si la prioridad aumenta, entonces, asignar un recurso exclusivo para el proyecto e incluir el proyecto como parte de las metas del grupo de trabajo para el cuarto fiscal actual.	Software Manager
R005	Cambio de requerimientos	Coordinar con el equipo de desarrollo de contenido la realización de iteraciones formales y que se incluyan todos los detalles técnicos necesarios para la realización de las pruebas.	Software Manager

Por último se tuvo que definir las acciones como parte de un plan de contingencia en caso de que el riesgo efectivamente ocurra. Tales acciones se encuentran representadas en la Tabla 61 que se muestra a continuación.

Tabla 61 Acciones de mitigación para los riesgos identificados relacionados con los 40 scripts tentativos a desarrollar para dispositivos móviles

Id del Riesgo	Riesgos	Acciones a seguir en caso de que el riesgo ocurra	Responsables de la mitigación
R001	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	Cancelar el proyecto.	Software Manager
R002	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	Solicitar cambio de fecha de entrega por parte de QA para incluir las capacitaciones necesarias para que se asegure la calidad de las pruebas.	QA Manager
R003	No contar con los ambientes necesarios para la ejecución de pruebas	Extender la fecha de fin del proyecto, solicitar ayuda por parte de los expertos del producto.	QA Manager
R004	Cambios en la prioridad del proyecto	Cambiar la fecha de entrega del proyecto.	Software Manager
R005	Cambio de requerimientos	Solicitar el detalle de los cambios de requerimientos y ajustar los casos de prueba a las nuevas definiciones.	Software Manager

5.2 Evaluación de los resultados del proceso piloto de gestión de riesgos en el área de aseguramiento de la calidad

A continuación se describen los resultados obtenidos a partir de la implantación del proceso piloto de gestión de riesgos en el área de aseguramiento de la calidad de contenido. Estos resultados se encuentran representados a través de las métricas que se mencionan en el punto 4.12.

- **Indicador de ocurrencia e impacto de los riesgos**

Como resultado de la revisión de los 40 scripts por parte de los ingenieros de aseguramiento de la calidad en conjunto con la aplicación del proceso piloto que incluye la gestión de riesgos se lograron evidenciar los siguientes datos que se muestran en la Tabla 62.

Tabla 62 Estado de los riesgos identificados durante el proceso piloto y como impactaron al proyecto

Indicador	Valor	Riesgos	Impacto Positivo o Negativo ¿Cuantos días se ganan o pierden?
Número de riesgos identificados en el proyecto	5		
Número de riesgos identificados y que fueron mitigados antes de ocurrir	2	R001, R004	No se ganaron ni perdieron días.
Número de riesgos identificados y cuya probabilidad de ocurrencia fue reducida	2	R002, R003	No se ganaron ni perdieron días.
Número de riesgos que ocurrieron	1	R005	10 días perdidos
Número de riesgos no identificados que ocurrieron	0		

Como resultado de la implantación del proceso piloto de gestión de riesgos en el marco del proceso general de aseguramiento de la calidad de contenido, un 40% de los riesgos identificados durante el proyecto fueron mitigados antes de ocurrir, un 40% de los riesgos identificados tuvieron una reducción en su probabilidad de ocurrencia y un 20% de los riesgos ocurrió.

- **Indicador de exposición al riesgo**

Los 40 scripts desarrollados para dispositivos móviles y que fueron enviados al área de aseguramiento de la calidad para la realización de las pruebas correspondientes pasaron por dos iteraciones. En la primera iteración (Iteración 1), el área de aseguramiento de la calidad empezó con la ejecución de las pruebas. Durante esta iteración 1, se detectaron defectos que fueron reportados para su corrección al grupo de desarrollo de contenido.

Posteriormente, se llevó a cabo la segunda iteración (Iteración 2). En esta Iteración 2, se revisaron los defectos corregidos y se anexaron los 40 scripts para dispositivos móviles al producto McAfee Vulnerability Manager.

Las tareas de gestión de riesgos se realizaron principalmente durante la iteración 1. Sin embargo, durante la Iteración 2 también se revisaron los riesgos identificados en la iteración 1 y se evaluó la posible existencia o inclusión de nuevos riesgos.

Una vez realizada la evaluación de los riesgos durante la iteración 2 se coincidió junto con los ingenieros de aseguramiento de la calidad que no existían las condiciones para incluir algún riesgo adicional.

En la Tabla 63 a continuación se pueden visualizar los riesgos identificados por cada iteración.

Tabla 63 Riesgo identificados durante la iteración 1 para la obtención del indicador de exposición al riesgo

Iteración/Sprint	Descripción del riesgo	Probabilidad de ocurrencia	Impacto	Exposición
1	Falta de presupuesto para armar el laboratorio de dispositivos Mobile	0,5	20	10
1	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología Mobile.	0,7	15	10.5
1	No contar con los ambientes necesario para la ejecución de pruebas	0,9	15	13.5
1	Cambios en la prioridad del proyecto	0,9	5	4.9
1	Cambio de requerimientos	0,8	10	8
			Exposición∑=	**46,9**

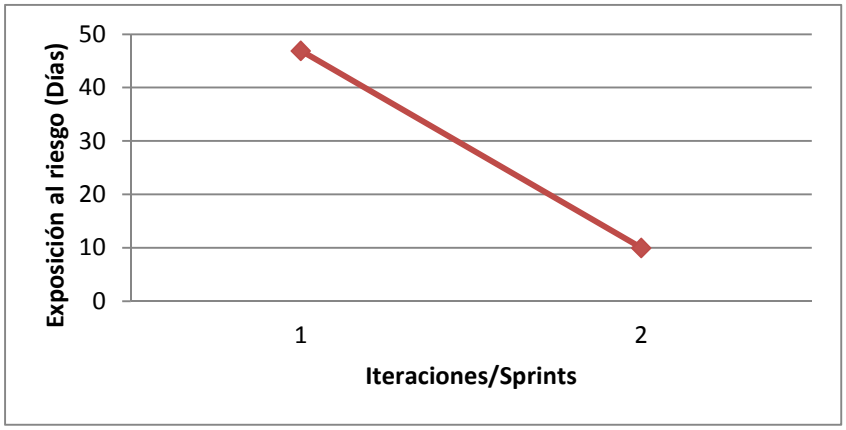
En la Tabla 64 a continuación se pueden visualizar los riesgos identificados por cada iteración.

Tabla 64 Riesgo identificados durante la iteración 2 para la obtención del indicador de exposición al riesgo

Iteración/Sprint	Descripción del riesgo	Probabilidad de ocurrencia	Impacto	Exposición
2	Falta de experiencia de los Analistas de Calidad para realizar las pruebas con tecnología mobile.	0,4	5	2
2	No contar con los ambientes necesario para la ejecución de pruebas	0,2	5	1
2	Cambio de requerimientos	0,8	10	8
			Exposición∑=	**10**

En el Gráfico 12 a continuación se puede visualizar la relación entre la exposición al riesgo y las iteraciones del proyecto.

Gráfico 14 Gráfico que muestra la exposición al riesgo entre las iteraciones del proyecto



Como se muestra en el gráfico 12, la exposición al riesgo disminuyo en 36 días entre la iteración 1 y la iteración 2 del proyecto. Esta reducción en el valor de la exposición se debe a la mitigación de 2 riesgos durante la iteración 1 y a la disminución de la probabilidad de ocurrencia de riesgos durante la iteración 2. Sin embargo, en la iteración 2 aún persiste un riesgo tanto con la probabilidad de ocurrencia y el impacto invariable con respecto a la iteración 1.

6. Conclusiones

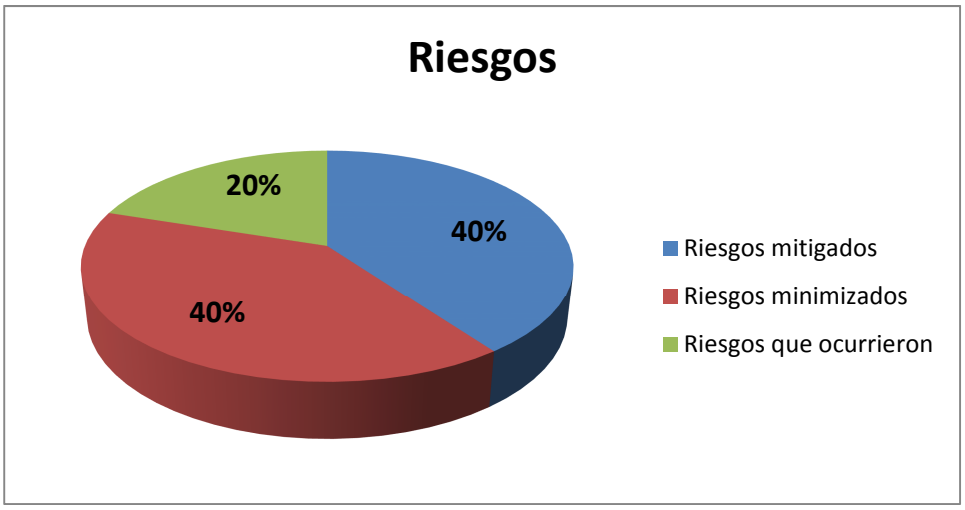
El constante dinamismo que existe en las organizaciones de hoy en día debido a la gran cantidad de operaciones y la necesidad de liberar productos que sean capaces de satisfacer las demandas de los clientes, trae como consecuencia la ocurrencia de eventos inesperados que pueden impactar la calidad del producto y comprometer la imagen de la organización.

La problemática existente en el área de aseguramiento de la calidad de contenido de McAfee Labs debido a la falta de un proceso de gestión de riesgos que permita identificar, analizar, priorizar y mitigar los riesgos que se puedan presentar se ha traducido en liberaciones de productos con contenido de seguridad incompleto, ajustes de última hora en las fechas de entrega de los proyectos o bien falta de conocimiento por parte de los ingenieros de aseguramiento de la calidad para realizar las pruebas asociadas a determinadas plataformas y políticas de seguridad.

En este trabajo de grado se ha presentado una propuesta para resolver la problemática existente y ha consistido en diseñar e implantar un proceso de gestión de riesgos piloto en McAfee orientado a satisfacer la meta genérica y las prácticas genéricas del nivel de capacidad 2 para el área de proceso de gestión de riesgos de CMMI v1.3 adoptando prácticas ágiles.

El proceso piloto de gestión de riesgos se implantó en un proyecto de desarrollo de contenido para dispositivos móviles y los resultados generales de la implantación se pueden visualizar en la gráfica 13 a continuación:

Gráfico 15 Resultados de la gestión de riesgos en el proyecto de desarrollo de contenido para dispositivos móviles



De un total de 5 riesgos identificados, el 80% de los riesgos fueron controlados sin generar un impacto negativo al proyecto. Por otra parte, el 20% restante corresponde a un riesgo que generó la pérdida de 10 días de trabajo generando retrasos. La falta de seguimiento y la poca coordinación con el equipo de desarrollo de contenido en cuanto a estabilizar el conjunto de requerimientos y los cambios en el producto fueron determinantes en la ocurrencia del riesgo. El resultado de esto fue esfuerzo duplicado y retraso de otras tareas no asociadas al proyecto por requerir de un recurso adicional.

Sin embargo, cabe destacar que al haber controlado el 80% de los riesgos del proyecto, se pudo evitar una pérdida de 55 días total aproximadamente tomando como referencia el impacto estimado de los riesgos identificados.

En términos generales los objetivos específicos propuestos para este trabajo de grado se han cumplido en su totalidad:

Tabla 65 Cumplimiento de los objetivos específicos propuestos para el presente trabajo de grado

Cumplimiento	Objetivos específicos
100%	Identificar los riesgos más críticos que impacten la unidad de aseguramiento de la calidad y categorizarlos.
100%	Implantar un proceso piloto para la gestión de riesgos identificados dentro de la unidad de aseguramiento de la calidad.
100%	Recabar datos por medio del proceso piloto que ayuden a identificar nuevos riesgos, a determinar la probabilidad de ocurrencia de los riesgos y al desarrollo de planes de contingencia.
100%	Validar tanto la pertinencia de los riesgos identificados como del proceso piloto para la gestión de riesgos mediante mediciones y monitoreo.
100%	Ajustar la lista de riesgos y el proceso piloto para la gestión de riesgos de acuerdo a las necesidades reales de la unidad de aseguramiento de la calidad.

Por otra parte, en cuanto al cumplimiento del objetivo general relacionado con satisfacer las metas específicas y genéricas del nivel de capacidad 2 del área de proceso de gestión de riesgos de CMMI v1.3, se ha logrado un resultado parcial.

A pesar de satisfacer todas las metas específicas del área de proceso de gestión de riesgos junto con el soporte de prácticas ágiles, aún no se ha logrado institucionalizar el proceso de gestión de riesgos en toda la unidad de aseguramiento de la calidad y en cada uno de los proyectos que se llevan a cabo.

Durante la ejecución del proyecto piloto se presentaron algunas limitaciones dentro del área de aseguramiento de la calidad. Tales limitaciones tienen que ver con la resistencia de algunos miembros del grupo de adoptar el proceso de gestión de riesgos y la asignación de recursos para su

ejecución (tiempo requerido por los ingenieros de aseguramiento de la calidad para la discusión, registro de los datos y el análisis correspondiente de los riesgos). El apoyo por parte de la dirección fue escaso puesto que consideraron que había que enfocarse en otras prioridades por el momento.

Como resultado de la implantación del proceso piloto de gestión de riesgos cabe destacar algunas lecciones aprendidas. Entre estas se puede mencionar que es indispensable contar con el apoyo tanto de la gerencia como de la dirección para poder llevar adelante un proceso piloto.

También es importante dar a entender a los miembros del grupo de trabajo que el proceso piloto de gestión de riesgos se traduce en algo positivo y beneficioso y que no sea visto como trabajo y esfuerzo adicional del cual se obtenga poco valor.

Por otra parte se demostró ante el grupo de trabajo en la organización que es fundamental hacer seguimiento constante de los riesgos ya que es la manera más efectiva para evitar que estos ocurran y afecten negativamente al proyecto.

La implantación de un proceso piloto de gestión de riesgos no solo se debe limitar al área de aseguramiento de la calidad sino también a las áreas de desarrollo de contenido y desarrollo del producto. Por lo tanto para poder llevar a cabo cambios en los procesos para incluir actividades de gestión de riesgos hay que entrenar al personal y buscar institucionalizar la gestión de riesgos a todos los niveles.

Por último, si se logra realizar una evaluación formal con algún tercero sobre la gestión de riesgos en el área de aseguramiento de la calidad y posteriormente en otras áreas de la organización, desde el punto de vista operativo se pueden detectar muchos problemas que van a requerir de la inclusión de actividades de gestión de riesgos en sus procesos.

Desde el punto de vista económico, en caso de que la empresa lograra cumplir con el nivel de capacidad 2 del área de proceso de gestión de riesgos en algunas áreas, el grupo de ventas puede hacer uso de sus destrezas recalcando que McAfee es una organización donde las áreas más críticas satisfacen el área de proceso de gestión de riesgos de CMMI v1.3 considerando que CMMI es un requisito exigido en muchas licitaciones con entidades gubernamentales y empresas.

7. Bibliografía

Software Testing Help. Types of Risks in Software Projects. http://www.softwaretestinghelp.com/types-of-risks-in-software-projects/. Fecha de consulta: Abril 2012

Project Smart. The Top Five Software Project Risks. http://www.projectsmart.co.uk/top-five-software-project-risks.html. Fecha de consulta: Abril 2012.

Luckey, Teresa y Phillips, Joseph (2006). Software Project Management for Dummies. John Wiley & Sons, ISBN-10: 0-471-74934-6. Fecha de consulta: Abril 2012

Hopkin, Paul (2010). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, Second Edition. Kogan Page, ISBN-13: 978-0-7494-5942-0. Fecha de consulta: Abril 2012.

Software Engineering Institute (SEI) (2010). CMMI for Development, Version 1.3. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm. Fecha de consulta: Marzo 2012

Glazer, Hillel, Dalton, Jeff, Anderson, David, Konrad, Michael, Shrum, Sandra (2008). CMMI or Agile, Why Not Embraced Both!. Software Engineering Institute (SEI), http://www.sei.cmu.edu/library/abstracts/reports/08tn003.cfm. Fecha de consulta: Marzo 2012.

Fernández, Javier, De La Fuente, Pablo, Prieto Martínez, Miguel (2009). Succeding in Software Quality: Agile and CMMI working together. Universidad de Valladolid, España. Fecha de consulta: Noviembre 2011.

Agile 101. Agile Risk Management – Identifying Risks. http://agile101.net/2009/07/27/agile-risk-management-identifying-risks-step-1-of-4/. Fecha de consulta: Marzo 2012.

Martin Fowler's blog. The New Methodology. http://martinfowler.com/articles/newMethodology.html. Fecha de consulta: Marzo 2012.

SCRUM.org. The SCRUM guide, the official rulebook. http://www.scrum.org/scrumguides/. Fecha de consulta: Marzo 2012.

Cockburn, Alistair (2004). Crystal Clear: A Human-Powered Methodology for Small Teams. Addison-Wesley Professional, ISBN-10: 0-201-69947-8. Fecha de consulta: Marzo 2012.

Extreme Programming.org. Extreme Programming, a gentle introduction http://www.extremeprogramming.org/. Fecha de consulta: Marzo 2012.

AgileSoftwareDevelopment.com. Lean Principles. http://agilesoftwaredevelopment.com/leanprinciples. Fecha de consulta: Marzo 2012.

AgileManifesto.org. Manifesto for Agile Software Development. http://agilemanifesto.org. Fecha de consulta: Marzo 2012.

McAfee. McAfee Policy Auditor. http://www.mcafee.com/mx/products/policy-auditor.aspx. Fecha de consulta: Marzo 2012.

McAfee. McAfee Vulnerability Manager. http://www.mcafee.com/mx/products/vulnerability-manager.aspx. Fecha de consulta: Marzo 2012

McAfee. McAfee Network Access Control. http://www.mcafee.com/mx/products/network-access-control.aspx. Fecha de consulta: Marzo 2012.

McAfee, Product Lifecycle Framework. Documento interno McAfee Labs (Uso Confidencial). Fecha de consulta: Marzo 2012.

Tamayo, M. (1994). El proceso de la investigación científica. Editorial Limusa, México. Fecha de consulta: Marzo 2012.

Project Management Institute (2008), A Guide to the Project Management Body Of Knowledge (PMBOK® Guide), Fourth Edition, ISBN: 9781933890517. Fecha de consulta: Octubre 2012.

Kulpa, Margaret K. , Johnson , Kent A (2008), Interpreting the CMMI: A Process Improvement Approach, Second Edition, ISBN:9781420060522. Fecha de consulta: Octubre 2012.

McManus, John (2004) Risk Management in Software Development Projects, ISBN: 9780750658676, Fecha de consulta: Octubre 2012.

Cobb, Charles G. (2011) Making Sense of Agile Project Management: Balancing Control and Agility, ISBN: 9780470943366. Fecha de consulta: Noviembre 2012.

Watkins, John (2009), Agile Testing: How to Succeed in an Extreme Testing Environment, ISBN: 9780521191814. Fecha de consulta: Noviembre 2012.

Wideman (ed), R. Max (1992) Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities. ISBN: 9781880410066. Fecha de consulta: Diciembre 2012.

The Eclipse Foundation (2012), Eclipse Process Framework. Fecha de consulta: Noviembre 2012.

Meet Agarwal (2012), http://www.c-sharpcorner.com/UploadFile/953215/risk-analysis-in-software-testing/. Fecha de consulta: Enero 2013.

(The Original and the authentic) Ask the CMMI Appraiser! - We need to get to "Level 2" fast! How long will it take us?. http://askthecmmiappraiser.blogspot.com/2007/02/we-need-to-get-to-level-2-fast-how-long.html. Fecha de consulta: Marzo 2013.

Risk Management Performance Benchmarking. http://riskbenchmarking.blogspot.com/. Fecha de consulta: Febrero 2013.

Risk Management is more than just risk mitigation. http://www.exsecutus.com/haughwout/2010/03/risk-management-is-more-than-just-risk-mitigation. Fecha de consulta: Febrero 2013.

Mike Cohn's Blog (2010), Managing Risk on Agile Projects with the Risk Burndown Chart http://www.mountaingoatsoftware.com/blog/managing-risk-on-agile-projects-with-the-risk-burndown-chart. Fecha de consulta: Febrero 2013.

Ed Bott, ZDNet (2010), Defective McAfee update causes worldwide meltdown of XP PCs http://www.zdnet.com/blog/bott/defective-mcafee-update-causes-worldwide-meltdown-of-xp-pcs/2003. Fecha de consulta: Julio 2013

SC Magazine (2010), Data breach costs LinkedIn up to $1 million http://www.scmagazine.com.au/News/310976,data-breach-costs-linkedin-up-to-1-million.aspx. Fecha de consulta: Julio 2013.

Pandian, C. Ravindranath (2007), Applied Software Risk Management: A Guide for Software Project Managers. ISBN:9780849305245. Fecha de consulta: Julio 2013.

Jones, T. Caper (1994) Assessment and Control of Software Risks. ISBN-10: 0137414064. Fecha de consulta: Julio 2013.

Carr, Marvin, Konda, Suresh, Monarch, Ira, Walker, Clay F., Ulrich, F. Carol (1993) Software Engineering Institute (SEI – Carnegie Mellon) – Risk Taxonomy. http://www.sei.cmu.edu/library/abstracts/reports/93tr006.cfm. Fecha de consulta: Julio 2013.

Boehm, Barry (1989) Software Risk Management, IEEE. ISBN-10: 0818689064. Fecha de consulta: Julio 2013.

Silverstein, David, Samuel, Phillip, Decarlo, Neil (2012) The Innovator's Toolkit: 50+ Techniques for Predictable and Sustainable Organic Growth. ISBN: 9781118298107. Fecha de consulta: Julio 2013.

Breyfogle III, Forrester W. (2003) Implementing Six Sigma: Smarter Solutions Using Statistical Methods. ISBN: 9780471265726. Fecha de consulta: Julio 2013.

McDermott, Robin E., Mikulak, Raymond J., Beauregard, Michael R. (2009) The Basics of FMEA. ISBN: 9781563273773.

RiskAMP 2013 – What is Monte Carlo Simulation. http://www.thumbstacks.com/files/RiskAMP%20-%20Monte%20Carlo%20Simulation.pdf. Fecha de consulta: Julio 2013.

Software Engineering Institute (SEI) (2013) CMMI and SCRUM http://cmmiinstitute.com/cmmi-getting-started/cmmi-compatibility/cmmi-and-agile/cmmi-and-scrum/. Fecha de consulta: Julio 2013.

Satheesh Thekku Veethil (2013) Risk Management in Agile http://www.scrumalliance.org/community/articles/2013/2013-may/risk-management-in-agile. Fecha de consulta: Julio 2013.

Neil Potter, Mary Sakry (2011) Implementing Scrum (Agile) and CMMI together http://www.scrumalliance.org/community/articles/2011/february/implementing-scrum-(agile)-and-cmmi®-together. Fecha de consulta: Julio 2013.

V. Uttangi, Roshan, Rizwan Azeem, Rizwan Syed Abdul (2007) Fast track to CMMI implementation: Integrating the CMMI and RUP process frameworks http://www.ibm.com/developerworks/rational/library/ oct07/uttangi_rizwan/. Fecha de consulta: Julio 2013.

Aked, Mark (2003) Risk reduction with the RUP phase planhttp://www.ibm.com/developerworks/rational/library/1826.html. Fecha de consulta: Julio 2013.

Gallagher, Brian, Brownsword, Lisa (2001) The Rational Unified Process and the Capability Maturity Model - Integrated Systems/Software Engineering - http://www.sei.cmu.edu/library/assets/rup.pdf. Fecha de consulta: 2013