CIMAT

Centro de Investigación en Matemáticas, A.C.

Proceso de Desarrollo de Software Ágil para preservar la Privacidad e Integridad de Datos en la Nube

TESIS

Que para obtener el grado de

Maestro en Ingeniería de Software

P r e s e n t a

I.S.C. Diego Estrada Jiménez

Directores de Tesis

Dr. Hugo Mitre Hernández

M.A. Juan Gabriel Hernández

Zacatecas, Zacatecas., 12 de julio de 2013

Resumen

Actualmente el cómputo en la nube ha cobrado un gran auge y aceptación, presentando grandes ventajas y beneficios, como lo son la elasticidad de recursos, reducción de costos, acceso universal, entre otros más.

A pesar de los grandes beneficios del cómputo en la nube, se presentan grandes preocupaciones a los usuarios con respecto a la privacidad e integridad de los datos alojados en la nube, ya que dicha información alojada aquí puede ser altamente confidencial, y a los usuarios les preocupa que sus datos puedan ser interceptados por terceros, el mal manejo de dichos datos dentro de la nube y sí sus datos han sido realmente eliminados cuando ellos lo hayan solicitado.

Es por las razones anteriores, en la presente tesis se ha realizado un proceso a nivel de prácticas de desarrollo de software ágil basado en MoProSoft (norma mexicana de desarrollo de software, de gran aceptación y uso en México) y en prácticas de las normas y estándares de ITIL V3, MAAGTIC, OWASP y S3M. La creación de este proceso, se realizaron tres filtros para la extracción de prácticas, en donde se seleccionaron todas aquellas prácticas que estuvieran relacionadas con la gestión de riesgos y el mantenimiento de software, posteriormente fueron descartadas todas aquellas que no tuvieran relación alguna con la preservación de la privacidad e integridad de datos y por último fueron adaptadas y mejoradas para su implementación dentro del cómputo en la nube. Finalmente se obtuvo una propuesta para el desarrollo de software ágil que permite reducir las amenazas hacia la privacidad e integridad de datos en servicios del cómputo en la nube.

Para la comprobación de las prácticas seleccionadas en la propuesta se realizó una evaluación de éstas con respecto a las prácticas llevadas a cabo en una empresa real, en donde se encontró que solo tres prácticas no son implementadas dentro de dicha empresa, y por consecuente como parte de trabajo futuro se deberá realizar una validación del proceso en dos o más proyectos de servicios de software.

Dedicatoria

La presente tesis la dedico a la memoria de mi padre, quien en vida siempre creyó en mí, me apoyó, y me impulso siempre a salir adelante, y la culminación de este trabajo es prueba de ello. Gracias Pá, siempre recordaré todo lo que me enseñaste y siempre te llevaré en mi corazón.

A mi madre, por su apoyo incondicional, amor y sacrificio durante estos dos años, gracias a ella y a mi padre, fue posible que yo pudiese iniciar y terminar este trabajo, cumplir una meta más en vida. Gracias.

Agradecimientos

Agradezco al CIMAT Unidad Zacatecas por haberme acogido durante estos dos años y al COZCyT por el apoyo económico que se me brindó a lo largo de mis estudios en la maestría de ingeniería de software.

Del mismo modo mi eterna gratitud a mis dos directores de tesis, el Dr. Hugo Mitre y al Ing. Juan Gabriel Hernández por sus orientaciones y aportaciones brindadas durante el desarrollo de esta tesis.

Índice

Lista de Tablas

Lista de Figuras

Capítulo 1. Introducción

El cómputo en la nube representa un nuevo paradigma de la computación con gran auge en los últimos años, en donde se ofrecen una gran cantidad de beneficios entre los que destacan la reducción de costos de producción, la elasticidad de recursos, servicios bajo demanda, virtualización de recursos, acceso universal, administración simplificada, entre otros más [1], ofrecidos en 3 capas de servicios:

(1) Servicio como infraestructura (IaaS, Infrastructure as a Service): se refiere a recursos computacionales como un servicio. Esto incluye computadoras virtuales con la garantía del poder de procesamiento y ancho de banda reservado para almacenamiento y acceso a internet. Un ejemplo de esto es el Cómputo en la Nube Elástico de Amazon (Amazon Elastic Compute Cloud).
(2) Servicio como plataforma (PaaS, Platform as a Service): es similar a IaaS, pero además incluye un sistema operativo y requiere servicios para una aplicación en particular. En otras palabras PaaS es IaaS con una pila personalizada de software para una aplicación en particular. Ejemplos de PaaS: El motor de aplicaciones de Google (Google App Engine) y Microsoft Azure.
(3) Servicio como software (SaaS, Software as a Service): se refiere a los servicios y aplicaciones que están disponibles en el fundamento bajo demanda. Sales-force.com es un ejemplo de SaaS.

Además el cómputo en la nube es clasificado en tres diferentes tipos:

- Privadas: son una variante genérica del cómputo en la nube, en donde los recursos internos del centro de datos de una organización no están disponibles al público en general.
- Públicas: son una variante genérica del cómputo en la nube, en donde los recursos están disponibles al público en general.
- Híbridas: combinan nubes privadas y públicas. Pueden ser utilizadas en casos donde la capacidad de la nube privada es agotada y necesita ser provista de algún otro lado.

El paradigma del cómputo en la nube presenta problemas importantes en seguridad, especialmente relacionados con la integridad y privacidad de datos [2][3], al igual retos en disponibilidad, interoperabilidad, desempeño [4], definición de Acuerdos de Nivel de Servicios (SLA, Service-Level Agreement) [3], entre otros más. El presente estudio se enfocó solo a la privacidad e integridad de datos, atacando problemas como la falta de comprobación de eliminación de los datos del cliente [3], invasión a la información de cliente en el SLA por otros servicios Cloud [2], y la falta de seguridad ante ataques de competidores en el tráfico de datos del cliente [5].

Así como el cómputo en la nube va a reemplazar los paradigmas de la computación anteriores a él, los métodos agiles están remplazando rápidamente a los métodos tradicionales para el desarrollo de software de las compañías. De acuerdo con

un estudio de 1,000 encuestado en siete países de Europa, Norte América y Asia, el 60% de las personas con experiencia en métodos agiles no desean regresar a la antigua forma de trabajo (el método tradicional) [6]. Por esta razón, este estudio fue enfocado al desarrollo de software ágil.

El presente estudio también ve una gran oportunidad de presentar una solución aplicable en México, porque numerosas compañías han reconocido grandes oportunidades en el sector de Tecnologías de Información (TI) y se refleja en el crecimiento de éstas al pasar de alrededor de 2000 empresas en 2002 a más de 3000 en 2011, lo que representa un incremento promedio anual de 5%. Es importante señalar que, para el sector de TI, el incrementar la eficiencia, productividad así como la innovación es fundamental, por lo que en México ha tenido un crecimiento en gran medida los Centros de Desarrollo Certificados en modelos de calidad, los cuales actualmente son cercanos a 400 [7].

Para adquirir fondos sobre proyectos importantes de desarrollo de software, como el Fondo PROSOFT, es necesario contar con una certificación ya sea en CMMi o en MoProSoft. De acuerdo al registro de la Normalización Y Certificación Electrónica existen 314 empresas certificadas con MoProSoft en México [8]. Entre 2006 y 2011, las inversiones en el sector de TI, a través de los proyectos apoyados por el Fondo PROSOFT, pasaron de 1.4 MDP (Millones de Pesos) de pesos a cerca de 2.1 MDP [7].

Por la importancia que se le ha dado en México al sector de las tecnologías de la información y los aumentos a los apoyos para adquisición de proyectos es necesario que una pyme que desee madurar empresarialmente y además darle una mayor calidad a sus procesos de desarrollo de software conozca mínimamente la norma MoProSoft.

MoProSoft es una norma mexicana para el desarrollo y mantenimiento de software tradicional, basado en CMM 1.1, ISO 9001:2000 e ISO/IEC 15504-2:1998 desarrollada a solicitud de la Secretaría de Economía del Gobierno Federal Mexicano a través de la Facultad de Ciencias de la Universidad Nacional Autónoma de México [9]. Con las tendencias actuales, tal como el Cómputo en la Nube, es necesario que MoProSoft logre ser adaptado para el desarrollo de software en este ambiente, atendiendo los problemas de integridad y privacidad de datos que se presentan en el Cómputo en la Nube, ya que aquí se almacenan datos muy delicados como números de tarjetas de crédito, fechas de nacimiento, estados bancarios entre otros datos personales. Ante dicha necesidad de adquirir fondos y la contradicción del desarrollo de software ágil y el tradicional, el enfoque de esta investigación es el preservar la agilidad del desarrollo de software y cumplir con MoProSoft dentro del paradigma del Cómputo en la Nube.

La propuesta de esta investigación presenta una propuesta basada en MoProSoft, debido a que la norma no integra prácticas de seguridad y servicio, y presenta una gran ambigüedad en cuestión de prácticas de mantenimiento de software. La propuesta de mejora está basada en actividades y procesos de los modelos y normas de la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL, Information Technology Infrastructure Library) V3 [10], el Manual Administrativo de Aplicación General en Materia

de Tecnologías de la Información y Comunicaciones (MAAGTIC) [11], el Proyecto de Seguridad de Aplicaciones Web Libres (OWASP, Open Web Application Security Project) [12], [13], [14], [15] y el Modelo de Madurez para el Mantenimiento de Software (S3M, Software Maintenance Maturity Model) [16] (actividades de los niveles de madurez del 0 al 2) que abordan específicamente la problemática de integridad y privacidad de datos y que pueden ser enfocados al cómputo en la nube preservado la agilidad de desarrollo acorde al manifiesto ágil [17]. Además la propuesta es un pequeño paso para la formalización de procesos de una empresa, ya que la propuesta es a nivel de prácticas.

Finalmente, la presente tesis hace las siguientes aportaciones:

1. Identifica tres problemas de privacidad e integridad de datos dentro del cómputo en la nube.
2. Presenta un proceso para el desarrollo de aplicaciones de cómputo en la nube, a nivel de prácticas, que afronta los problemas de privacidad e integridad de datos.
3. El proceso propuesto puede ser implementado en empresas certificadas en MoProSoft o en vías de certificación en esta norma, al igual que en empresas que implementan metodologías ágiles.
4. Presenta una metodología para la extracción de prácticas de normas y estándares que ayuden a combatir los problemas de privacidad e integridad de datos dentro del cómputo en la nube.

1.1 Contexto

La propuesta aquí presentada ha sido enfocada y adaptada a la empresa Softlogik S.A. de C.V. quien cuenta con 15 trabajadores, y desarrolla software a la medida en los lenguajes de programación de PHP, Java y .Net para los sistemas operativos Linux, Windows y Unix utilizando bases de datos como MySQL, MSSql, PostgreSQL, Sqlte e Informix, al igual la empresa desarrolla aplicaciones SaaS.

Softlogik S.A. de C.V. se constituye en la ciudad de Zacatecas con capital zacatecano el día 15 de febrero del 2011, con el objetivo de incorporarse al mercado local y nacional de desarrollo e implementación de soluciones basadas en procesos y tecnologías de información para el sector público y privado, contratando personal con habilidades especificas en las áreas de Tecnologías de Información y Comucación (TIC), utilizando metodologías congruentes con el contexto del país, de la región y del propio estado de Zacatecas [18].

El consejo administrativo de la empresa está conformado por personal de Compulogic, quien es accionario importante de Softlogik. Se cuenta con un Director de Operaciones quien es encargado de las áreas de Desarrollo y Proyectos e Innovación. Existen dos Ingenieros Senior y ambos tienen a su mando 5 Ingenieros Junior para el desarrollo de proyectos. La gran mayoría de los ingenieros Senior y Junior cuentan con una certificación en Scrum. Dentro de Proyectos e Innovación se desarrollan los proyectos

a realizar en la empresa en donde participan personas que no se encuentran dentro de la nómina. Existe un tercer Ingeniero Senior, quien realiza todas las funciones del área de Subcontratación de Procesos de Negocios y cuando es necesario por algún proyecto en específico desarrolla software en Delphi.

Para el desarrollo de los diversos proyectos, la empresa cuenta con alianzas estratégicas con socios y fabricantes líderes en la materia para el diseño e instalación de ambientes en la nube.

La empresa trabaja bajo una metodología ágil, en donde se hace una combinación de Scrum, Programación Extrema (XP, Extreme Programming) y Kanban para el desarrollo de software.

Softlogik S.A. de C.V. tiene pensado en un futuro próximo certificarse en MoProSoft, ya como mencionado anteriormente, los proyectos importantes ofertados para el desarrollo de software tienen como requisito estar certificados en MoProSoft o CMMi, y además la empresa desea mejorar sus procesos de desarrollo de software con la finalidad de ofertar mayor calidad y rapidez en sus desarrollos. Por las razones mencionadas encaja perfectamente la propuesta trabajada en este documento en la empresa Softlogik S.A de C.V.

1.2 Problemática

El tema de seguridad de la información ha sido un tema de gran interés, y por ello ya se han desarrollado normas, estándares, leyes, herramientas para poder minimizar los riesgos que atentan en contra de la seguridad de la información.

Como ya se ha establecido anteriormente, se busca dar una mejor seguridad dentro del cómputo en la nube específicamente en las áreas de privacidad e integridad de datos, por la razón que los usuarios almacenan gran cantidad de información personal y privada. Como mencionado anteriormente la propuesta aquí presentada, la cual afronta los problemas anteriormente presentados, se encuentra dentro del marco de trabajo de MoProSoft (la cual está enfocada al desarrollo tradicional de software), por los beneficios que ofrece para la licitación de fondos PROSOFT y permite aumentar la calidad de los procesos de una empresa, pero además la propuesta busca conservar la esencia de las metodologías agiles, por la aceptación que presenta con los desarrolladores de software.

Antes de poder abordar el problema de la privacidad dentro de esta investigación fue necesario conocer su definición. La privacidad, también conocida como confidencialidad es definida como *la propiedad de que los datos sean inaccesibles a usuarios no autorizados* [19]. Dentro de [20], se hace mención que para mantener la confidencialidad de los datos, estos deben de ser protegidos contra accesos no autorizados. El grado de confidencialidad en un sistema se mide usualmente en los recursos necesarios para revelar la información de dicho sistema [19].

En la privacidad dentro del contexto del cómputo en la nube, existe la incógnita por parte del usuario si realmente fueron eliminados sus datos de la nube cuando estos lo hayan solicitado [3], y además existe una ambigüedad dentro de la definición SLA sobre el acceso a la información del usuario por parte de proveedores terceros del prestador de servicios Cloud [2]. Ambos problemas son atacados dentro de la propuesta elaborada en este documento.

Al igual que la privacidad, para poder abordar la problemática de la integridad de datos, fue necesario conocer su definición. La integridad es definida como *la propiedad de que los datos sean resistentes hacia una modificación no autorizada* [19]. Para mantener la integridad de los datos, estos deben de ser entregados según lo previsto [20]. La integridad es medida usualmente por el tiempo y recursos necesarios para que un adversario pueda modificar datos o procesos sin autorización [19].

La problemática de la integridad de datos, dentro del punto de vista empresarial, no solo existe el riesgo de que un mensaje o registro con datos confidenciales sea interceptado, sino además que los competidores puedan interferir en las operaciones de negocio desde el tráfico de mensajes [5]. Este es el problema de integridad de datos a atacar dentro de la propuesta del presente documento.

Analizando la norma MoProSoft, presenta un déficit de actividades relacionadas con la conservación de la privacidad e integridad de datos, al igual que una ambigüedad dentro de las actividades de mantenimiento de software. A pesar de este déficit dentro de la norma, MoProSoft ayuda a aumentar la calidad de los procesos dentro de una empresa, lo cual es una razón más por lo que la propuesta expuesta en este documento tomó como base esta norma.

Finalmente el presente estudio busca respetar cada uno de los 12 principios del manifiesto ágil [17] ya que el marco de trabajo de MoProSoft está dentro de las formas tradicionales de desarrollo de software, pero la propuesta presentada en esta tesis busca preservar la agilidad para el desarrollo de software, por su gran aceptación en numerosas empresas de diferentes partes del mundo [6]. Es aquí donde surge problema de contradicción de metodologías de desarrollo de software, al tratar de preservar la agilidad con un método tradicional de desarrollo de software.

1.3 Objetivo

A partir de los problemas mencionados anteriormente, se establece como objetivo el *crear una propuesta de proceso a nivel de prácticas para el desarrollo de software ágil que cumpla con MoProSoft integrando prácticas de mantenimiento, servicio y seguridad, para generar evidencias de que la información del cliente realmente ha sido eliminada, establecer el uso acordado de los datos del cliente y establecer el aseguramiento de la integridad de los datos con el cliente dentro de un ambiente de cómputo en la nube*.

Ya que la propuesta deberá adaptarse a MoProSoft, solo se utilizarán aquellas secciones de la norma que encajen directamente para la solución de los problemas mencionados de integridad y privacidad de datos.

1.4 Importancia del estudio

El cómputo en la nube por la serie de beneficios que ofrece ha tenido una gran aceptación en el mundo de las tecnologías de la información, y de acuerdo a Tendencias de Google (Google Trends) el término 'Cloud Computing', a partir del año 2007 ha ido en aumento dentro del famoso buscador. Dichos resultados pueden ser observados en la Figura 1.1.

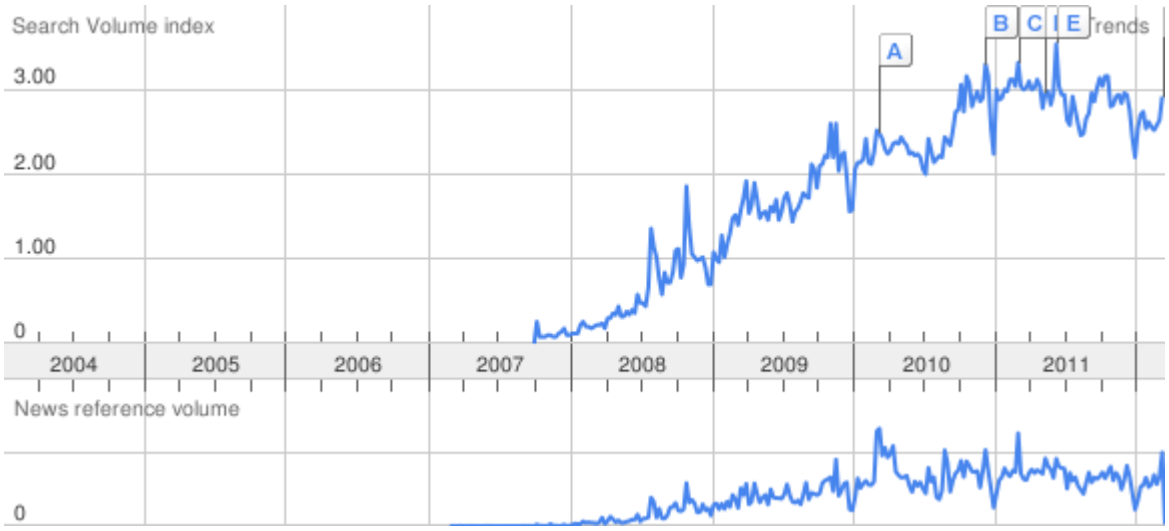


Figura 1.1 – Tendencias del término Cloud Computing en Google [21]

En la Figura 1.1 se muestra el rápido crecimiento de la popularidad del término Cloud Computing, medido por Google. Las etiquetas A, B, C, D y E muestran el comportamiento que se describe a continuación. A: Google busca convertirse en un sembrador de nubes del cómputo en la nube para otras empresas de servicios en línea. B: El cómputo en la nube puede darle un empuje a la Unión Europea por 763 billones de euros. C: La expo tecnología en Alemania aprovecha el cómputo en la nube. D: Empresa local de Tecnologías de la Información da a conocer servicios de cómputo en la nube. E: Una nube doméstica se estima que crezca 53% de acuerdo a un estudio.

Actualmente el cómputo en la nube se está integrando en gran parte de las aplicaciones que utilizamos día a día, y de acuerdo a lo reportado por "World Privacy Forum" los datos alojados en la nube son registros de clientes, datos sobre impuestos, datos financieros, correos electrónicos, registros médicos, documentos de Word, Excel y PowerPoint [2], y todos estos datos son altamente confidenciales y delicados, por lo cual nace la gran preocupación de los usuarios Cloud sobre la privacidad de sus datos.

Las empresas presentan cierto grado de desconfianza para migrar su información hacia la nube, y es por eso que en [4] se realizó una encuesta a 244 empresas, en donde se les pidió que clasificarán de acuerdo a su importancia, los problemas/retos que el modelo del cómputo en la nube presenta. Los resultados obtenidos pueden ser observados en la Figura 1.2, en donde la principal preocupación es la Seguridad, seguido por el Desempeño, la Disponibilidad, la Interoperabilidad y la Personalización.

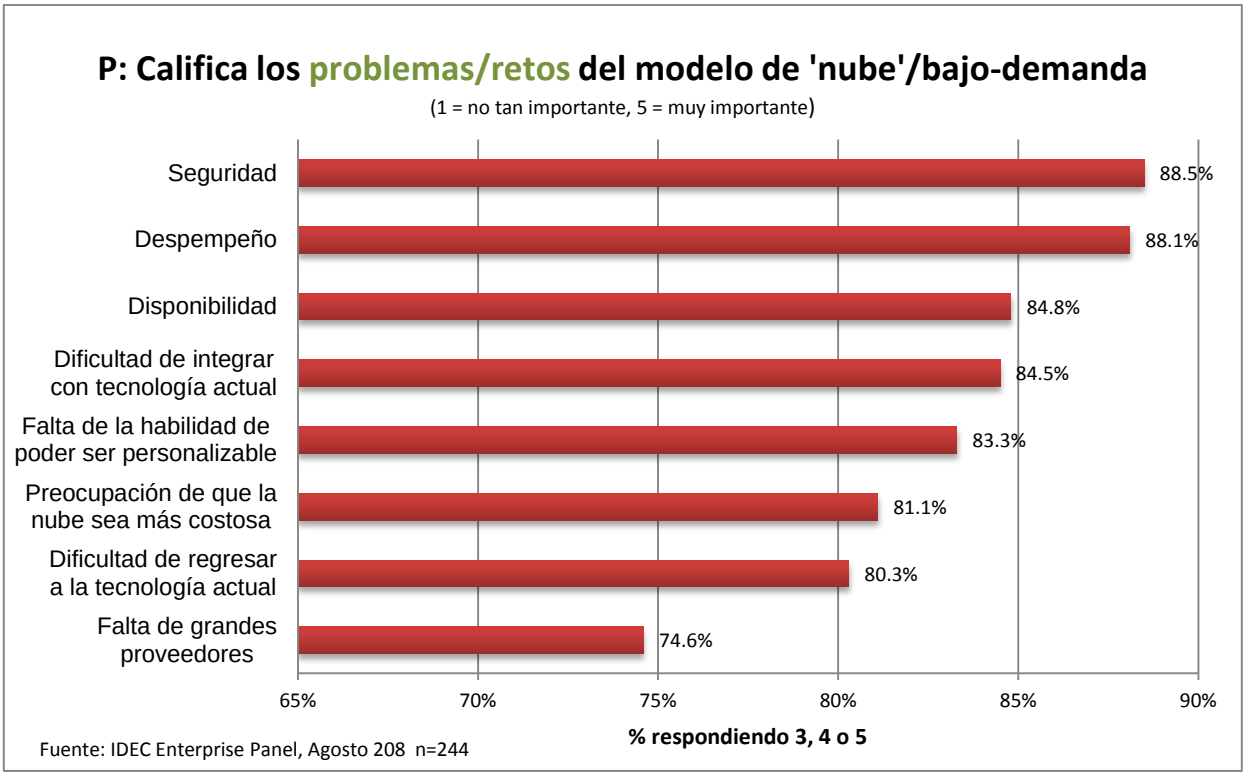


Figura 1.2 – Resultados de la encuesta de los retos del Cómputo en la Nube [4]

La privacidad e integridad de datos son propiedades elementales dentro de la seguridad de información de un sistema de software, y cualquier acceso no deseado por parte de terceros, en donde los datos puedan ser comprometidos, afecta seriamente estas dos propiedades, y por consecuente el sistema de software se vuelve no confiable para el usuario.

Por lo mencionado en los párrafos anteriores y con la popularidad del cómputo en la nube, la gran aceptación de las metodologías ágiles y por lo vital que es MoProSoft en la creciente industria del software en México, se busca abordar los problemas de la privacidad e integridad de datos a partir del desarrollo ágil de servicios de la nube dentro del marco de MoProSoft, y así poderle brindar al usuario de la nube servicios seguros y confiables.

1.5 Metodología

Para realizar la propuesta expuesta en este documento, y como mencionado anteriormente se analizaron y seleccionaron prácticas de las normas ITIL V3, la cual es un conjunto de prácticas para la gestión de servicios de tecnologías de la información y además abarca la norma ISO 20000, MAAGTIG, norma elaborada por el gobierno federal mexicano para la gestión de las tecnologías de la información y comunicación de las dependencias gubernamentales, OWASP, es una organización que ha desarrollado varias normas para el desarrollo y mantenimiento de aplicaciones de software confiables, y S3M,

norma canadiense enfocada principalmente al mantenimiento de aplicaciones de software.

La elaboración de la propuesta fue divida en 3 fases:

1. Extracción de prácticas
2. Mejora de prácticas
3. Evaluación del uso actual de las prácticas.

La Fase 1, se encuentra divida en tres filtros de selección de prácticas:

(1) Se seleccionaron todas aquellas prácticas relacionadas con el mantenimiento de software y la gestión de riesgos.
(2) Se descartaron todas aquellas prácticas que no tengan relación con la preservación de la privacidad e integridad de datos.
(3) Las prácticas fueron mejoradas y adaptadas al ambiente del cómputo en la nube.

Fueron tomadas en cuenta los criterios de prácticas de manteniendo de software por su relación de tener que reparar y adaptar el software por las nuevas amenazas que surgen y puedan afectar al software. El criterio de la gestión de riesgos fue tomado en cuenta porque durante una buena gestión de riesgos, pueden ser identificados las principales amenazas que puedan afectar al software cuando este es puesto en producción.

Continuando con la Fase 2, el listado de prácticas obtenidas durante la Fase 1 debe de ser insertado al marco de MoProSoft. Finalmente en la Fase 3 se realiza una entrevista en una empresa real en donde se cuestiona si realizan o no cada una de las prácticas del proceso, y así poder determinar qué tan factible es la implementación del proceso obtenido dentro de una empresa de desarrollo de software, y además se realiza una adaptación del proceso para que respete el manifiesto ágil.

1.6 Estructura de Tesis

A continuación se muestra la descripción del contenido de los capítulos de la presente tesis de maestría.

En el capítulo 2 se describe toda la fundamentación teórica de cada una de las normas en la que se basó la realización de la propuesta expuesta en el presente documento.

En el capítulo 3 se exponen los problemas encontrados en el cómputo de la nube, especialmente los de privacidad e integridad de datos, ya que la propuesta expuesta aquí trata de resolver dichos problemas.

En el capítulo 4 se relata la metodología a emplear para el desarrollo de la propuesta, justificando el porqué de cada uno de los pasos a realizar para la obtención del

proceso de desarrollo de software que solucionará los problemas de privacidad e integridad de datos dentro del cómputo en la nube.

En el capítulo 5 se dan a conocer los resultados obtenidos de la metodología expuesta en el capítulo 4, dichos resultados permitirán abordar los problemas de privacidad e integridad de datos, para que así el usuario presente una mayor confianza al entorno del cómputo en la nube.

Finalmente, en el capítulo 6 se presentan las conclusiones sobre el proceso de desarrollo de software obtenido, el avance que se tiene conforme al objetivo de la tesis, al igual que el trabajo futuro basado en dichos resultados, para así desarrollar aplicaciones de software más seguras en cuestiones de privacidad e integridad de datos dentro del entorno del cómputo en la nube.

Capítulo 2. Fundamentación Teórica

La propuesta expuesta en este documento, está enfocada a resolver los problemas de privacidad e integridad de datos que presenta el cómputo en la nube dentro de la República Mexicana. Dicha propuesta fue analizada para su posible aplicación en la empresa Softlogik S.A. de C.V. ubicada en la ciudad de Zacatecas, la cual fue un factor muy importante para que la propuesta se adaptara a MoProSoft.

Las normas y estándares de ITIL V3, MAAGTIC, OWASP y S3M, hacen referencia principalmente a la ***gestión de riesgos***, que de acuerdo a la ISO 31000, lo define como: *"La coordinación de actividades para dirigir y controlar una organización con respecto a un riesgo"* y el mismo estándar define ***riesgo*** como: *"efecto de una incertidumbre en los objetivos"* [22]; y el ***mantenimiento de software***, que de acuerdo al ISO 14764, es definido como: *"la modificación de un producto de software después de la entrega, para corregir errores, mejorar el rendimiento, u otros atributos"* [23].

2.1 MoProSoft

La base de la propuesta de este documento es el marco de trabajo de MoProSoft, la cual es una norma desarrollada a solicitud de la Secretaria de Economía del Gobierno Federal Mexicano a través de la Facultad de Ciencias de la Universidad Nacional Autónoma de México, dicha norma está basada en las normas ISO 9001:2000, CMM v1.1 e ISO/IEC 15504-2:1998 [9].

MoProSoft presenta 6 niveles de capacidad que van del 0 al 5, en donde cada uno representa la capacidad de los procesos llevados en la empresa [24] y como se puede observar en la Figura 2.1, están representados los atributos que debe tener el proceso de acuerdo al nivel de capacidad.

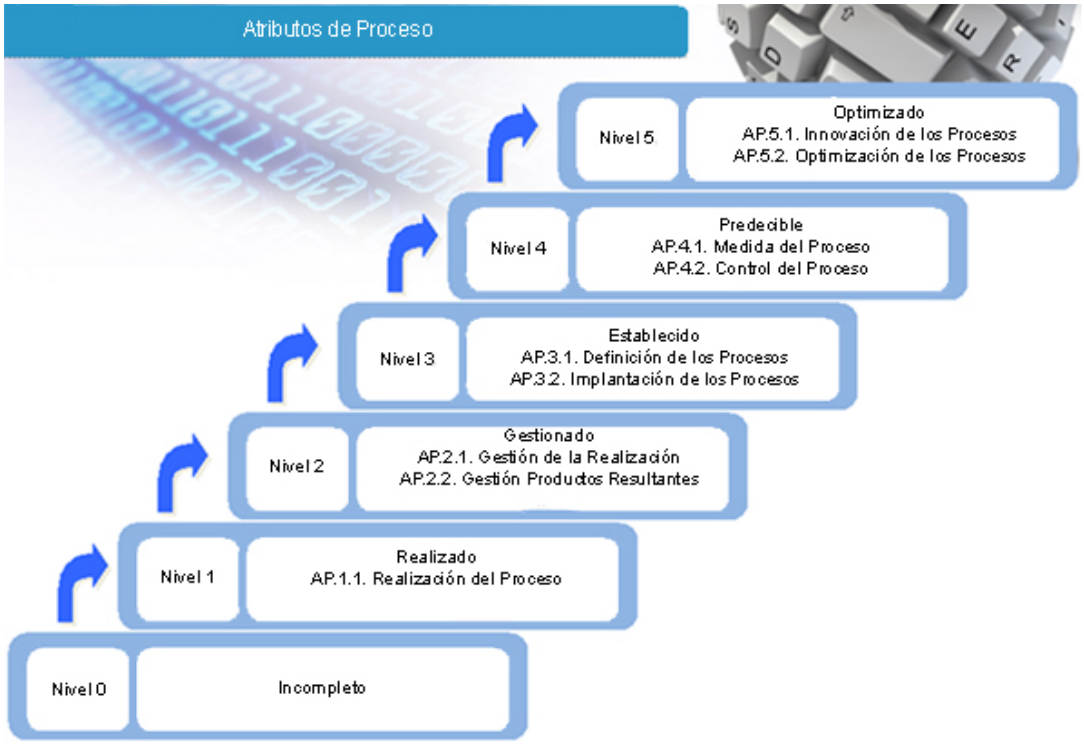


Figura 2.1 – Atributos de Proceso de los Niveles de Capacidad MoProSoft [24]

Dentro de MoProSoft se consideran los tres niveles básicos de la estructura de una organización, los cuales son: la alta dirección, la gestión y la operación. El modelo pretende apoyar a las organizaciones en la estandarización de sus prácticas, en la evaluación de su efectividad y en la integración de la mejora continua [9].

2.2 ITIL V3

Para la elaboración de la propuesta, la primera norma analizada para el desarrollo de ésta fue ITIL, que fue desarrollada a finales de 1980, y se ha convertido en el estándar mundial por de facto en la Gestión de Servicios Informáticos. Inició como una guía para el gobierno de Reino Unido, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. Pertenece a la Oficina de Comercio del Gobierno Británico, pero es de libre utilización [25].

ITIL puede ser definido como un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI. Su objetivo último es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible [26].

Los 5 principios claves para la gestión de servicios de tecnologías de la información que ataca ITIL V3 son: Estrategia de Servicios, Diseño de Servicios, Transición de Servicios, Operación de Servicios y Mejora Continua de Servicios [10], los cuales forman parte del ciclo de vida del servicio, tal como se muestra en la Figura 2.2.

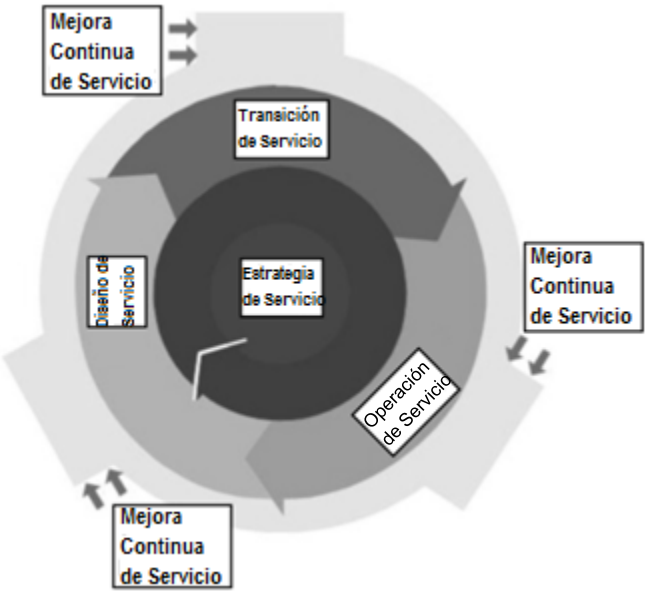


Figura 2.2 – Ciclo del vida del Servicio [10]

Se había considerado incluir dentro de la propuesta la norma ISO/IEC 20000 el cual es un estándar para la gestión de servicios de tecnologías de la información y al ser comparada con ITIL V3, fue descartada ya que ITIL V3 indica el qué y el cómo realizar la gestión de servicios de tecnologías de la información mientras que la norma ISO/IEC 20000 solo indica el qué para realizar la gestión de servicios de tecnologías de la información.

2.3 MAAGTIC

La segunda norma analizada para la propuesta presentada en este documento fue MAAGTIC, la cual es decretada en el mes de septiembre de 2009, cuando el presidente de los Estados Unidos Mexicanos, Felipe de Jesús Calderón Hinojosa, instruyó al C. Titular de la Secretaría de la Función Pública profundizar las acciones en materia de reforma regulatoria y derogar todos aquellos acuerdos, oficios, decretos o reglamentos cuya necesidad no quedara plenamente justificada, con el propósito de mejorar la eficiencia institucional y la calidad de los servicios que brindan las diversas dependencias y entidades de la Administración Pública Federal [11].

MAAGTIC es una normatividad para la eficiencia operativa gubernamental de las operaciones del área de Tecnologías de la Información y Comunicación emitido por la Secretaría de Función Pública en la que se establece el acuerdo por el que se expide el

Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones por decreto presidencial; cuyo ámbito de aplicación y alcance está definido para implementarse en las instituciones a través de sus correspondientes unidades administrativas responsables de proveer infraestructura y servicios de tecnologías de la información y comunicaciones; regulado bajo el marco jurídico aplicable a reglamentos, lineamientos, leyes, decretos y seguridad de la información. MAAGTIC es un conjunto de 31 procesos en el que establece un marco rector para la gestión de las TICs, agrupados en 4 grupos principales para la gestión del gobierno, para la organización estratégica, para la ejecución entrega y soporte de los servicios de TIC. Los procesos se basan en las mejores prácticas internacionales como Six Sigma, COBIT, BSC, normas ISO (como la ISO/IEC 9001, ISO/IEC 27,000, entre otras), Risk IT, CMMI, PMI, ITIL, MoProSoft, Rational Unified Process, etc. [27].

En la Figura 2.3 se muestran los 31 procesos MAAGTIC agrupados en 11 macroprocesos, considerados en 4 niveles de gestión, que integrados forman el "Macro rector de procesos" para las unidades de tecnologías de la información y comunicación de las dependencias y entidades de la Administración Pública Federal.

Figura 2.3 – "Marco rector de procesos" de tecnologías de la información y comunicaciones; 31 procesos en 11 grupos específicos [11]

2.4 OWASP

La tercera norma analizada para la propuesta de este documento fue OWASP. OWASP es una fundación que entró en funcionamiento el 1 de diciembre de 2001 y fue establecida como una organización sin fines de lucro en los Estados Unidos de América el 21 de abril de 2004. OWASP es una comunidad abierta dedicada a habilitar a las organizaciones a concebir, desarrollar, adquirir aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitas y libres a cualquier persona interesada en la mejora de la seguridad de aplicaciones [28].

El propósito principal de OWASP es ser una comunidad mundial próspera que impulse la visibilidad y la evolución en la seguridad y protección dentro del mundo del software [28]. Además OWASP se rige de los siguientes valores [28]:

- **Abierta**: Absolutamente todo en OWASP es radicalmente transparente, desde sus finanzas hasta su código.
- **Innovación**: OWASP promueve y apoya la innovación/experimentos para la solución de los problemas de seguridad de software
- **Global**: Se fomenta que cualquier persona en cualquier parte del mundo participe en la comunidad OWASP.
- **Integración**: OWASP es honesta y veraz, un proveedor neutral, y una comunidad global.

Empresas de renombre mundial como Adobe, Amazon, HP, Firefox, Nokia, Oracle, Twitter, entre otras más utilizan las diferentes herramientas y documentos que OWASP ofrece, además cuenta con apoyo académico de diferentes universidades de todo el mundo, como UCLA, Tecnológico de Monterrey, Instituto Politécnico de Nyu, Universidad de Israel, Facultad de Ingeniería de la Universidad de Buenos Aires, Universidad de Fordham, Universidad de Corea, entre muchas otras más.

De las múltiples herramientas y documentos de OWASP, para esta propuesta se analizó la Guía para Construir Aplicaciones y Servicios Web Seguros, la cual abarca todas las cuestiones de seguridad en aplicaciones web, desde las más antiguas, como la inyección SQL, hasta las modernas tales como la suplantación de identidad, manipulación de tarjetas de crédito, fijación del período de sesiones, falsificación de petición en sitios cruzados, el cumplimiento de las reglas y cuestiones de privacidad [14].

También se consideró la Guía de Pruebas de OWASP, la cual tiene el objetivo de ayudar a las personas entender el qué, porqué, cuándo y cómo realizar pruebas a sus aplicaciones web, y no únicamente proveer un lista de verificación o prescribir los retos que deben ser atacados. El producto final de este proyecto es un marco de referencia de pruebas, para el cual otros puedan construir sus propios programas de pruebas o evaluar los procesos de otras personas. La Guía de Pruebas describe a detalle el marco de referencia general de pruebas y las técnicas requeridas para implementar el marco en la práctica [13].

Además se analizó el Contrato Legal (Legal Project) de OWASP, el cual tiene como objetivo asegurar en cada etapa del ciclo de vida, y que la atención adecuada sea prestada a la seguridad [15]. Y finalmente fue analizado las 10 principales amenazas (Top 10) de OWASP, el cual presenta y describe los 10 principales y más críticos riesgos de seguridad para las aplicaciones web [29].

2.5 S3M

Finalmente, para concretar las normas analizadas para la propuesta presentada, se analizó el modelo S3M, el cual se enfoca primordialmente a los procesos de gestión de manteamiento de software. Dentro de la ISO/IEC TR 19759 dentro del capítulo de mantenimiento de software existe una referencia a S3M [30].

A pesar de que S3M no sea un estándar, se mapea completamente con los procesos de la ISO/IEC 14764 y ofrece información invaluable a las organización que desean cumplir con la ISO 9001:2000. Provee una guía de procesos para cumplir con el estándar de la ISO/IEC en el área de mantenimiento de Software [30].

El dominio S3M reconoce la importancia del recurso humano en el núcleo de las actividades de mantenimiento de software, a través del contacto diario con los clientes y su ejecución con varios procesos [16], tal como se muestra en la Figura 2.4.

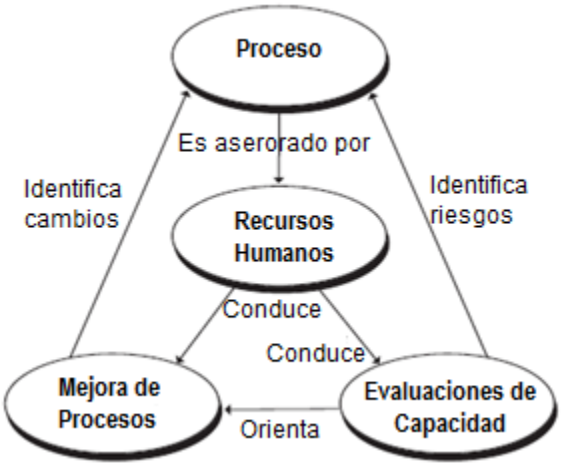


Figura 2.4 – Contexto de Gestión de Procesos de S3M [16]

S3M cuenta con 6 niveles de madurez que van del 0 al 5 y abarca 5 áreas de proceso clave [16]:

1. **Enfoque al proceso de mantenimiento**: Ayuda a mejorar el plan de mantenimiento continuo de la organización, ya que recolecta información de los clientes, el personal, el desempeño actual del proceso de mantenimiento, de las fuerzas/debilidades de las técnicas y herramientas de mantenimiento, el ambiente actual de mantenimiento y la retroalimentación de las interfaces de mantenimiento de software

2. **Definición al proceso/servicio de mantenimiento**: Aquí los procesos, técnicas y herramientas de mantenimiento son asesorados y revisados para mejorar el desempeño de las tareas diarias del ingeniero de mantenimiento
3. **Entrenamiento de mantenimiento**: Identifica las necesidades estratégicas para la educación y el entrenamiento, mientras se enfoca a los procesos y además en los aspectos técnicos.
4. **Desempeño del proceso de mantenimiento**: Establece las metas cuantitativas para los niveles de calidad y desempeño de la ejecución de los procesos de desempeño, los productos de software en operación, y los productos intermedios del mantenimiento de software.
5. **Ejecución e innovación de manteamiento**: Agrupa las actividades para seleccionar e implementar los proyectos de mejora e innovación.

Por cuestiones de la privacidad con la que cuenta S3M en su página oficial, solo fueron analizados los niveles de madurez de 0 al 2, ya que para acceder a la información del resto de los niveles se requiere ser socio y/o miembro de S3M.

Capítulo 3. Teoría de la problemática

El cómputo en la nube es el paradigma de la computación con mayor auge [1], el cual está teniendo mucha aceptación ya que ofrece grandes beneficios para todo tipo de usuarios, desde grandes empresas hasta usuarios individuales. Estos beneficios del cómputo en la nube son la elasticidad de recursos, la prestación de servicios bajo demanda y la modalidad de solo pagar lo que se consumió.

Para las empresas, el computo en la nube es algo que vale la pena considerar y probar para construir sistemas empresariales como una forma de negocio en la que pueden indudablemente bajar costos y dar mayores ganancias, entre otras cosas más [2].

A pesar de los grandes beneficios que el cómputo en la nube ofrece, existen varios problemas y desventajas dentro de este paradigma, pero hay un problema que es de mayor importancia para los usuarios de la nube, ya que acuerdo a [2] la gran mayoría de los datos que se encuentran aquí almacenados son altamente confidenciales y el usuario al no tener físicamente el hardware en donde estos son almacenados y procesados, le surge la gran preocupación a los usuarios en cuestión de la seguridad sobre los datos que tiene almacenados en la nube.

Este problema de seguridad está relacionado principalmente con la integridad y privacidad de los datos en la nube. Ambos problemas se ven a detalle en las siguientes dos secciones.

3.1 Privacidad de Datos

Los proveedores de servicios de cómputo en la nube tienen sus gigantescos centros de datos, los cuales son el corazón de la prestación de los servicios de la nube, localizados en lugares estratégicos para ellos, lo que significa que pueden encontrarse en cualquier parte del mundo.

La gran mayoría de los usuarios del cómputo en la nube desconocen donde están estos centros de datos en donde su información se encuentra almacenada y como se ha mencionado anteriormente, el usuario al desconocer en qué parte del mundo se encuentra el centro de datos y el no tener físicamente el hardware, le nace una gran preocupación de quién pueda ver y tener acceso a su información, y es por eso que la Universidad de Berkeley propuso que para resolver este problema es necesaria la encriptación de datos [2], pero esta solución involucraría un uso mayor de ciclos del procesador y por consecuente aumentaría los tiempos de respuesta al igual que los costos para el usuario, así que esta solución no es viable, por lo que es requerido seguir la búsqueda de nuevas soluciones.

Cabe mencionar que un problema que resalta [3] es que el usuario se queda con la incógnita si realmente sus datos fueron eliminados completamente de la nube cuando este lo solicitó, y así asegurarse que dicha información no pueda ser vista por parte de terceros que pueda perjudicar al usuario.

Aunque en muchos casos el origen del problema de la privacidad de datos proviene desde la contratación de los servicios del cómputo en la nube, ya que el usuario por falta de leer y comprender lo que se encuentra estipulado dentro del SLA y además por una pobre definición de este documento por parte del proveedor, no se estipula claramente que proveedores terceros que interactúan con el proveedor de servicios de computo en la nube, pueden tener acceso a la información que tiene el usuario en la nube [2].

3.2 Integridad de Datos

Como ya se mencionó anteriormente, los centros de datos que dan vida a los servicios del cómputo en la nube se encuentran localizados en puntos estratégicos para el proveedor, entonces, por consecuente dichos servicios son accedidos remotamente.

Al acceder remotamente a la nube, los usuarios, especialmente las empresas, presentan el gran temor que los mensajes entre ellos y los servicios de computo en la nube puedan ser interceptados por algunos de sus competidores y estos puedan ver y hasta alterar dichos mensajes, comprometiendo gravemente la integridad de los mensajes que son enviados y recibidos durante las operaciones de negocio realizadas en la nube [5].

3.3 Carencia de procesos

La calidad de un producto de software depende fuertemente de los procesos utilizados para su creación [31]. Por lo tanto una empresa que carezca de un proceso de desarrollo de software definido difícilmente puede desarrollar software seguro y de calidad.

La propuesta hecha en esta tesis es solo un pequeño paso que permitirá ayudar a todas las empresas que deseen empezar a definir su proceso de desarrollo de software para los servicios en la nube y que además busquen ofrecer una mejor privacidad e integridad de datos dentro de estos servicios.

Pero durante el desarrollo de esta propuesta se ha encontrado que MoProSoft presenta de manera muy superficial prácticas de gestión de riesgos y de mantenimiento de software, las cuales son de gran importancia para asegurar la privacidad e integridad de datos, por tal razón y por la falta de un estándar que ayude a brindar una mejor seguridad dentro del cómputo en la nube, fue necesario desarrollar la propuesta expuesta en este documento.

3.4 Conclusiones

Por los graves problemas del cómputo en la nube presentados en las secciones anteriores, los cuales pueden comprometer gravemente un usuario en especial las

operaciones de negocio de una empresa, se decidió abordar estos problemas desde la raíz, o sea desde el desarrollo de aplicaciones del cómputo en la nube para brindarle al usuario una aplicación del cómputo en la nube más segura.

La solución presentada en este documento, maneja una serie de prácticas implementadas durante el desarrollo de aplicaciones del cómputo en la nube, que permiten llevar un mejor seguimiento de los SLAs e integran mecanismos de seguridad para la transmisión de mensajes, gestión de incidentes y establecimiento de políticas de seguridad, abordando así los problemas identificados de la privacidad e integridad de datos dentro del cómputo en la nube.

Capítulo 4. Diseño y Metodología de la Investigación

La propuesta expuesta en este documento fue elaborada con el propósito de crear un proceso de desarrollo de software, específicamente dentro de un ambiente de cómputo en la nube, que afronte los problemas de privacidad e integridad de datos presentados en dicho ambiente y que pueda ser utilizado por empresas que estén dentro del marco de MoProSoft y/o utilicen metodologías de desarrollo ágil.

Para el desarrollo de la propuesta se consideraron las normas de MoProSoft y MAAGTIC por ser de origen mexicano, ya que se pretende que esta propuesta pueda ser utilizada en empresas mexicanas ubicadas dentro del país, y se decidió que la propuesta estuviera dentro del marco de MoProSoft por los beneficios que presenta en la licitación de proyectos, especialmente para las pymes.

Como se hace mención en [6] se ha visto una gran aceptación por las metodologías de desarrollo de software ágil por parte de las empresas, ya que hace a las pymes más competitivas, los ciclos de desarrollos son más rápidos y cortos, y disminuye los costos de desarrollo, por esta razón es que la propuesta debe de respetar cada uno de los 12 principios del manifiesto ágil.

La propuesta presenta una flexibilidad, ya que permite a empresas certificadas en MoProSoft o en camino a una certificación dentro de esta norma y a empresas que manejan una metodología de desarrollo de software ágil abordando los problemas de privacidad e integridad de datos presentados en el cómputo en la nube.

Se pretende que la propuesta sea analizada dentro de la empresa Softlogik S.A. de C.V., quien cuenta con una metodología de desarrollo de software ágil y además tiene pensado en un futuro próximo certificarse en MoProSoft, haciendo que el entorno de análisis sea perfecto para aplicar esta propuesta, pero además da cabida a la realización de un trabajo futuro, que en base al proceso actual presentado, se realice un proceso que permita certificarse en MoProSoft y que el manifiesto ágil se siga respetando.

4.1 Metodología para la creación de la propuesta

Por los problemas de integridad y privacidad de datos [2][3] que afectan gravemente al cómputo en la nube, es necesario crear un proceso de desarrollo de software que afronte dichos problemas, y que mejor manera de hacerlo que seleccionando prácticas que actualmente se encuentran en normas y estándares nacionales e internacionales.

Las normas y estándares antes de ser establecidos oficialmente por alguna organización como la ISO, deben ser validados por grupos de expertos en el área y pasar por rigurosos filtros, y es por esto que se decidió seleccionar prácticas de normas y estándares.

Se busca abordar los problemas de privacidad e integridad de datos utilizando primordialmente prácticas relacionadas con la gestión de riesgos durante el desarrollo de software del cómputo en la nube y con el mantenimiento del mismo.

Como ya se ha estado mencionando anteriormente, para desarrollar dicho proceso, se toma como base la norma MoProSoft por los beneficios que ofrece, especialmente paras las pymes y además por ser una norma mexicana que facilita la adquisición de fondos federales. La propuesta está enfocada a resolver los problemas antes mencionados del cómputo en la nube en el territorio mexicano. Las normas de MAAGTIC, S3M, ITIL V3 y OWASP fueron seleccionadas por estar completa o parcialmente relacionadas con la gestión de riegos y el mantenimiento de software.

En la Figura 4.1 podemos observar todo el proceso que se llevará a cabo para la realización de la propuesta, la cual deberá atacar los problemas de privacidad e integridad de datos ya mencionados anteriormente.

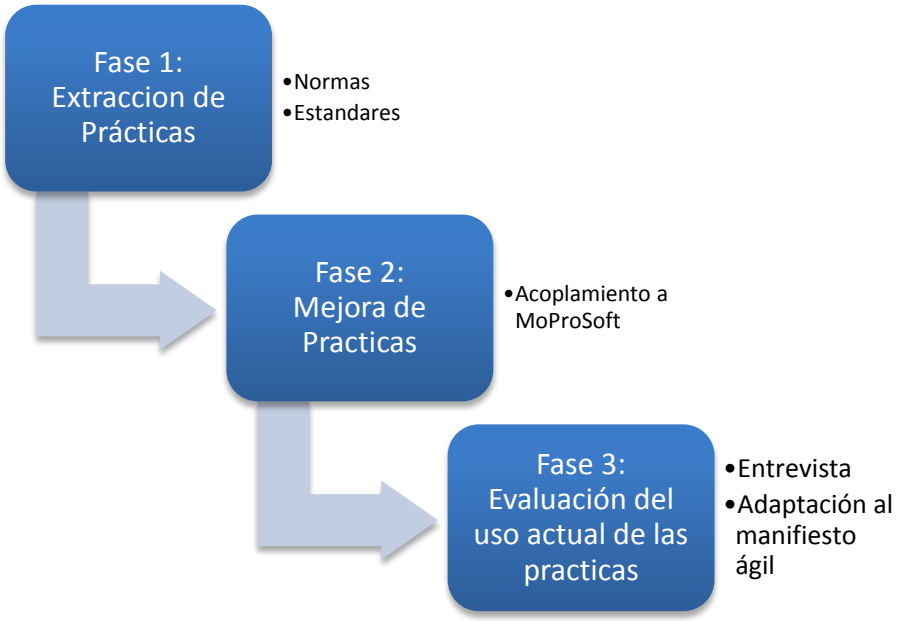


Figura 4.1 – Proceso para el establecimiento de la propuesta

Para la ejecución de la Fase 1, la cual tiene una duración de 6 meses, se establecen 3 filtros para la selección de prácticas, tal y como se muestra en la Figura 4.2, en donde además se puede observar con un poco más a detalle los resultados de las Fases 2 y 3 para el establecimiento de dicha propuesta. En la Fase 1, durante el primer filtro solo son seleccionadas aquellas prácticas que tienen relación con la *gestión de riesgos y el mantenimiento de software*, para el segundo filtro son descartadas todas aquellas prácticas que no tienen relación con la *preservación y aseguramiento de la integridad y privacidad* de datos, y finalmente en el tercer filtro las prácticas son mejoradas y adaptas para el desarrollo de software dentro del cómputo en la nube.

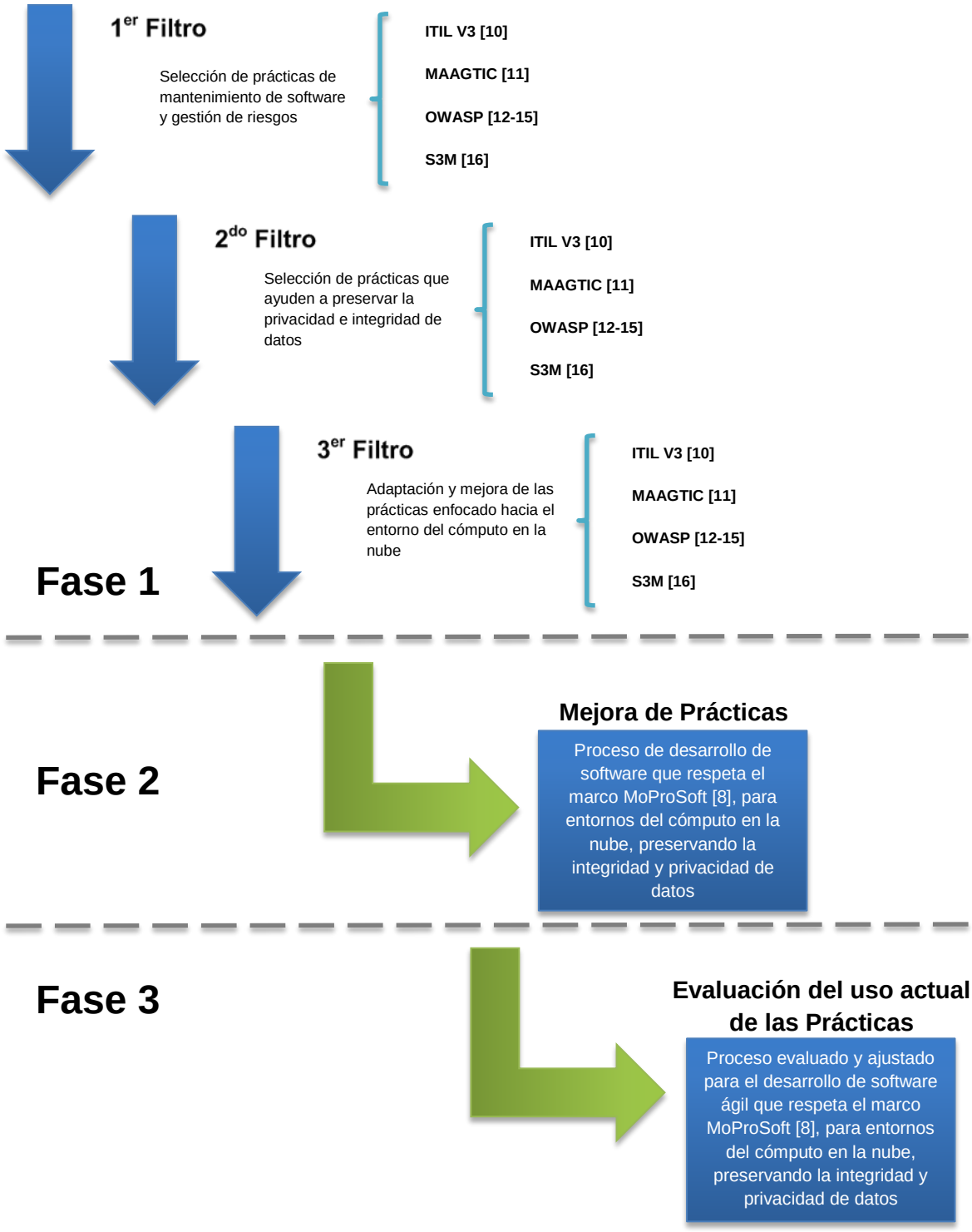


Figura 4.2 – Metodología para el establecimiento de la propuesta

Continuando con las fases mostradas en la Figura 4.1, una vez ejecutada la Fase 1, se procede con la Fase 2, la cual tiene una duración de 2 meses, en donde se debe realizar una integración y adaptación de las prácticas obtenidas en la fase anterior a la norma MoProSoft. Finalmente se lleva a cabo la Fase 3, la cual tiene una duración de un

mes, en donde se realiza una entrevista al personal de una empresa real, que para este caso de estudio es la empresa Softlogik S.A. de C.V., la cual es descrita en la sección 1.1 de este documento, específicamente al personal que esté involucrado en el desarrollo de servicios de software, y así poder conocer la factibilidad de la implementación de dicha propuesta en una empresa de desarrollo de software. Durante la entrevista se pregunta ¿Si la práctica es implementada?, ¿Desde cuándo?, ¿Qué beneficios se han obtenido a partir de su implementación? y ¿Cómo es implementada dicha práctica?. Con los resultados obtenidos durante las entrevistas, se procede a realizar los ajustes necesarios al proceso para que respete cada uno de los principios del manifiesto ágil.

Se seleccionó la empresa Softlogik S.A. de C.V. por ser una empresa mexicana, que desarrolla aplicaciones SaaS, que tiene además pensado certificarse en un futuro próximo en MoProSoft y además implementa metodologías de desarrollo de software ágil, encajando perfectamente con la propuesta desarrollada a lo largo de este documento.

4.2 Conclusiones

Los tres filtros descritos anteriormente permitirán seleccionar las mejores prácticas de las diferentes normas y estándares que mejor confronten los problemas de privacidad e integridad de datos, al igual que adaptarlas al entorno del cómputo en la nube, para que sucesivamente sean integradas dentro del marco de MoProSoft.

El adaptar cada una de estas prácticas respetando cada uno de los 12 principios del manifiesto ágil, dará una flexibilidad en dónde el proceso resultante pueda ser aplicado, ya que podrá ser implementado con empresas que implementen MoProSoft, en empresas que utilicen metodologías agiles o empresas que tengan una combinación de ambas.

Al estar la propuesta dentro del marco MoProSoft, permite a las pymes obtener recursos del programa federal de PROSOFT, y por consecuente permitiendo a las pymes crecer y madurar empresarialmente.

Finalmente la realización de entrevistas a la empresa Softlogik S.A. de C.V., que es una empresa que implementa metodologías agiles para el desarrollo de software y a que además tiene pensado en un futuro próximo certificarse en MoProSoft, nos indicará que tan factible es la realización de cada una de las prácticas que integran el proceso resultante.

Con la realización de todas estas actividades, se espera tener un proceso que este dentro del marco de MoProSoft, respete cada uno de los 12 principios del manifiesto ágil y que a partir del desarrollo de software para el cómputo en la nube, permita atacar los problemas de privacidad e integridad de datos presentados en este entorno.

En suma, el propósito de la metodología es *crear un proceso a nivel de prácticas de desarrollo de software ágil para pymes que deseen preservar la privacidad e integridad*

de datos en sus servicios o productos de software, además de facilitar el acceso a recursos financieros en México (PROSOFT).

Capítulo 5. Resultados de la investigación

De acuerdo con todo lo descrito en el capítulo anterior, se desarrolló un proceso enfocado a combatir los problemas de privacidad e integridad de datos, aunque cubrir estos problemas con prácticas de desarrollo de aplicaciones para la nube brinda una solución parcial del problema. Esta propuesta es un principio para ofrecer una mejor privacidad e integridad de datos dentro de las aplicaciones ofrecidas dentro del cómputo de la nube.

Dicha propuesta fue desarrollada seleccionando y adaptando las mejores prácticas ofrecidas en las diferentes normas y estándares analizados, para así dar origen a un proceso de desarrollo de software concreto y capaz de enfrentar los problemas de privacidad e integridad de datos dentro del cómputo en la nube.

Los resultados de todo este proceso de investigación, selección y adaptación pueden ser observados en la siguiente sección de este capítulo.

5.1 Análisis de los datos

Como ya se ha mencionado se seleccionaron prácticas de las normas ITIL V3, MAAGITIC, OWASP y S3M, para la elaboración de la propuesta expuesta aquí, y de acuerdo a lo descrito en el capítulo anterior se implementaron 3 filtros para dicha selección de prácticas.

El objetivo del primer filtro es tener el listado de todas aquellas prácticas relacionadas con la gestión de riesgos y el mantenimiento de software, lo cual es el primer paso para afrontar los problemas de privacidad e integridad de datos.

Para realizar el primer filtro, primero se hizo una revisión bibliográfica sobre cada uno de los estándares y normas (ITIL V3, MAAGTIC, OWASP y S3M), luego fueron seleccionadas todas aquellas prácticas que dentro de su definición o contexto tuvieran las palabras, un sinónimo de estas y/o además tuvieran relación con la gestión de riesgos o el mantenimiento de software.

Tal y como se observa en la Tabla 5.1, se encuentran todas aquellas prácticas seleccionadas durante el primer filtro, prácticas que corresponden específicamente a la *gestión de riesgos y al mantenimiento de software*.

Tabla 5.1 – Prácticas seleccionadas durante el primer filtro

Prácticas del 1er filtro - *gestión de riesgos y al mantenimiento de software*
• **ITIL V3** o Gestión de Incidentes ▪ Registro – Notificación del incidente: en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo

habitual de trabajo.
        - Clasificación
            - Monitorización del estado y tiempo de respuesta esperado: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.
        - Diagnostico
            - Análisis de incidente
- Gestión de Problemas
        - Control de Problemas
            - Identificación y Registro
            - Análisis y Diagnóstico: Error Conocido
        - Control de Errores
            - Análisis y solución
            - Revisión Post Implementación y Cierre
    - Gestión de niveles de Servicio
        - Planificación
            - Establecimiento del catálogo de servicios
        - Implementación
            - Establecimiento de SLA
            - Establecimiento de OLA (Acuerdos de Nivel de Operación)
            - Establecimiento de UC (Contrato de Soporte)
        - Monitorización
            - Monitorización de la calidad del servicio
            - Elaboración de reportes
        - Revisión
            - Revisión de la calidad de los servicios ofrecidos.
    - Gestión de la Continuidad del Servicio
        - Evaluación de Riesgos
            - Analizar las posibles amenazas y estimar su probabilidad.
            - Detectar los puntos más vulnerables de la infraestructura TI.
        - Estrategias
            - Actividades Preventivas
            - Actividades de Seguridad
        - Organización y Planificación
            - Plan de prevención de Riesgos
            - Plan de gestión de emergencias
            - Plan de recuperación
        - Supervisión
            - Actualización y auditorias
    - Gestión de la Seguridad
        - Políticas y Plan de seguridad

- Establecimiento del plan y políticas de seguridad
- Aplicación de las medidas de seguridad
  - Coordinar la implementación de los protocolos y medidas de seguridad
  - Establecer las políticas y protocolos de acceso a la información.
  - Monitorizar las redes y servicios en red para detectar intrusiones y ataques.
  - Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
  - Generar la documentación de referencia necesaria.
- Evaluación y Mantenimiento
  - Evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs
  - Mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs

- MAAGTIC
  - Cumplimiento regulatorio
    - 7.2.2.2.2 CR-1 Identificar los requerimientos de las leyes, reglamentos y regulaciones aplicables: Identificar, de manera continua, los requerimientos en materia de TIC que se desprenden de las leyes aplicables a nivel federal e internacional, así como de reglamentos, regulaciones y otras disposiciones que deban ser observadas por la dependencia o entidad, a fin de incorporar estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC que sean necesarios en la dependencia o entidad para darles cumplimiento.
  - Administración de riesgos de TIC
    - 7.2.3.2.2 ARTI-2 Evaluar los riesgos de TIC: Asegurar que los riesgos en materia de TIC sean evaluados y presentados en términos del impacto a los procesos y servicios de la dependencia o entidad: financieros, de transparencia y seguridad de la información, regulatorios, entre otros.
      - Recopilar datos relevantes para los riesgos de TIC.
      - Identificar y analizar escenarios de riesgo que permitan definir los impactos potenciales a la entidad o dependencia sobre elementos como:
        - Servicios
        - Proceso
        - Datos (operativos, nómina, contables, entre otros).
        - Software (sistemas, aplicaciones, entre otros).
        - Hardware
        - Equipos informáticos que hospedan datos, aplicaciones y servicios.

- Equipos de comunicación
- Dispositivos de almacenamiento (cintas, CDs, DVDs, entre otros).
- Personas (empleados internos y terceros).

– Identificar amenazas para aquellos activos identificados, dichas amenazas pueden ser clasificadas al menos en las siguientes categorías:
  - No causadas por el hombre:
    - Malfuncionamiento de TIC (fallas de software y de hardware)
    - Naturales (terremotos, huracanes, entre otros.)
    - De origen industrial (fallas eléctricas, aire acondicionado)
  - Causados por el hombre:
    - Maliciosas
      - Externas (espionaje industrial, hackers, entre otros.)
      - Internas (personal mal intencionado)
    - No maliciosas
      - Errores humanos

– Identificar riesgos; algunos tipos de riesgos son:
  - Fraudes
  - Robos
  - Degradación o perdida de continuidad en las operaciones
  - Fuga o modificación de información no autorizada
  - Accesos no autorizados
  - Falta o no cumplimiento de regulaciones, entre otros

– Identificar impactos a la entidad o dependencia; dichos impactos pueden ser, por lo menos, los siguientes:
  - Financieros
  - Niveles de servicios
  - Imagen o reputación
  - Regulatorios

- 7.2.3.2.2 ARTI-3 Responder a los riesgos de TIC: Asegurar que se responde a los riesgos de TIC con base a su nivel de severidad, con base en las decisiones para su tratamiento y tomado los criterios de priorización de implantación de controles.

– Identificar el nivel de severidad del riesgo.
– Identificar opciones para el tratamiento del riesgo el cual involucra tomar las decisiones para:
  - Aceptar el riesgo: no se efectúa ninguna acción debido a que el nivel de riesgo está dentro de los niveles

aceptables por la entidad o dependencia.
- Evitar el riesgo. se elimina la causa que produce el riesgo
- Transferir el riesgo: se transfiere y comparte el riesgo con una organización aseguradora o un tercero.
- Mitigar el riesgo: se implementan controles para reducir el riesgo a un nivel aceptable por la entidad o dependencia

– Identificar controles predictivos, preventivos y correctivos y mapearlos para cada uno de los escenarios de riesgos identificados. Estos controles deben ser documentados en la SoA
– Definir planes de mitigación del riesgo que consideren las actividades para implantar los controles identificados en las Sentencias de aplicabilidad. Para cada escenario de riesgo la prioridad de implantación debe ser definida y acordada. Algunos de los parámetros que pueden ser considerados en la priorización de la implantación de los controles o contramedidas son los siguientes:
  - Severidad del riesgo (nivel de riesgo)
  - Nivel de impacto de la implantación del control en la disminución de las consecuencias del riesgo sobre los procesos y servicios de la entidad o dependencia
  - Costo de implantación
– Definir un Plan de contingencia para reaccionar a eventos o incidentes en caso de presentarse un riesgo

- Administración de proyectos de TIC
  - 7.3.2.2.2 APTI-5: Administrar los riesgos: Eliminar o minimizar los riesgos por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados.
    – Identificar riesgos. La identificación de riesgos es un proceso iterativo debido a que se pueden descubrir nuevos riesgos a medida que el proyecto avanza a lo largo de su ciclo de vida. El equipo de trabajo del proyecto debe participar en la identificación de los riesgos para poder desarrollar y mantener un sentido de pertenencia y responsabilidad por los riesgos y las acciones asociadas a la respuesta a los riesgos. Los riesgos identificados se documentan en un registro de riesgos.
    – Clasificar riesgos. Los riesgos se categorizan por tipo de riesgo, se identifican y agrupan por la causa raíz y se elaboran propuestas que los minimicen o eliminen. Para clasificarlos se pueden utilizar metodologías como la matriz FODA que analiza

fortalezas, oportunidades, debilidades y amenazas.

- Responder a los riesgos. Se determina la prioridad de atención de los riesgos identificados y las acciones que serán realizadas para atender el riesgo, incluyendo las acciones de mitigación y la definición de un Plan de contingencia
- Dar seguimiento y controlar riesgos. Realizar el seguimiento de los riesgos identificados, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto.
- Adecuar el Plan de proyecto, incluyendo la documentación del alcance, el cronograma y el presupuesto, para incorporar las decisiones derivadas de la administración de riesgos que impacten al plan.

- Operación del sistema de gestión y mejora de procesos de la UTIC
  - 7.4.1.2.2 OSGP-3: Monitorear y evaluar la operación del Sistema de gestión y mejora de procesos de la UTIC
- Administración de proveedores
  - 7.5.2.2.2 APV-1 Generar lista de verificación de acuerdos: Con base al contrato establecido, se elabora una lista de verificación para dar seguimiento al desarrollo del contrato.
  - 7.5.2.2.2 APV-2 Monitorear el avance y desempeño del proveedor: Verificar que las actividades del proveedor sean desempeñadas como está especificado en el contrato.
  - 7.5.2.2.2 APV-3 Revisión de cumplimiento al contrato TIC: Verificar y evaluar que la totalidad de las actividades desarrolladas se realicen con apego a lo estipulado en los contratos establecidos, con la finalidad de identificar riesgos y oportunidades, que permitan evitar incumplimientos de los compromisos contractuales, inclusive por parte de la UTIC y/o del área solicitante del objeto del contrato.
  - 7.5.2.2.2 APV-4 Cierre administrativo del contrato: Comprobar que el proveedor cumplió con la totalidad de sus compromisos, para cerrar el contrato.
- Administración de servicios de terceros
  - 7.9.2.2.2 AST- 4 Realizar pruebas técnicas de la prestación del servicio: Asegurar que los servicios seleccionados cumplen con los requerimientos.
- Administración de niveles de servicio
  - 7.9.3.2.2 ANS-1 Crear y mantener acuerdos de niveles de servicio: Definir los SLA basados en el catálogo de servicios de las UTIC, de acuerdo con los requerimientos de la operación y las necesidades de los usuarios de cada uno de los servicios definidos
  - 7.9.3.2.2 ANS-2 Monitorear y reportar el grado de cumplimiento de los niveles de servicio: Elaborar reportes de resultados sobre el grado de

cumplimiento de los SLA. Esta actividad sigue las directrices del proceso de Administración del desempeño de TIC.

- 7.9.3.2.2 ANS-4 Formular el Plan de mejora de servicios: Recomendar mejoras a los SLA, como consecuencia de las insatisfacciones del cliente o el no cumplimiento de acuerdos establecidos.

- Administración de la operación
  - 7.11.1.2.2 AO-3 Monitorear la infraestructura de TIC: Asegurar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que sustentan las operaciones.
- Administración de ambiente físico
  - 7.11.2.2.2 AAF-2: Establecer las medidas de seguridad física.: Definir e implementar medidas de seguridad físicas, alineadas a los procesos de administración de la seguridad de la información y administración de riesgos de TIC, de la dependencia o entidad. Definir e implementar las reglas de operación de acceso a los centros de datos.
  - 7.11.2.2.2 AAF-3: Establecer medidas de control de acceso físico a las áreas reservadas de la UTIC: Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las ubicaciones de la UTIC, de acuerdo con los requerimientos de seguridad indicados por el SGSI, incluyendo las salidas de emergencia.
  - 7.11.2.2.2 AAF-4: Establecer la protección contra riesgos ambientales: Diseñar e implementar medidas de protección contra riesgos ambientales

- **OWASP**
  - Guía de desarrollo
    - Establecimiento de políticas de seguridad de acuerdo a la legislación nacional y estándares industriales (se recomienda COBIT o ISO 17799)
    - Establecimiento de metodología de desarrollo
    - Diseñar controles (para prevenir un mal uso de la aplicación)
    - Modelado de amenaza de riesgo
      - Documentar amenazas conocidas
    - Educar al usuario en cuestiones de seguridad tales como phishing, malware, instalación de antivirus, etc.
    - Establecer mecanismos de seguridad en los mecanismos de comunicación de la aplicación
    - Establecer cifrado de mensajes
    - Realización de auditorías a la aplicación
    - Establecimiento de mecanismos de estampado de tiempos en mensajes para asegurar la frescura de estos
    - Establecimiento de mecanismos de control de acceso a la aplicación
    - Gestión de usuarios

Prácticas del 1er filtro - *gestión de riesgos y al mantenimiento de software*

- Realizar validaciones de reglas de negocio
- Manejo de errores
- Generación de logs

o Top 10

- Revisar el documento top 10 de OWASP a la hora de realizar una gestión de riegos, para conocer las principales amenazas actuales dentro de las aplicaciones web.

o Legal Project

- Definir actividades del ciclo de vida relacionadas con seguridad
- Definir áreas de requerimientos de seguridad
- Requerir análisis y pruebas de seguridad utilizando estándares acordados
- Revisiones de seguridad

o Guía de Testeo

- Revisión de políticas y estándares
- Revisión de requerimientos de seguridad
- Creación y revisión del modelo de amenazas
- Pruebas de penetración de la aplicación
- Pruebas de gestión de la configuración
- Conducir revisiones de gestión operacional

- **S3M**

o Enfoque a Procesos de Mantenimiento

- Mapa a la recolección de información
  - Los datos en fallas de software son recogidas y utilizadas para identificar candidatos a mejora para dar mantenimiento a procesos/productos y además para muchas interfaces con otros grupos de interface
  - La organización de mantenimiento está sujeta a auditorías internas y los resultados son utilizados para identificar candidatos a mejora.

o Desempeño del Proceso de Mantenimiento

- Mapa para la Identificación de la línea base
  - Medidas de la línea base en la calidad y desempeño son recolectadas, almacenadas, revisadas y usadas con varios stakeholders. Son usados para mejorar el proceso, servicio y producto actual.
- Mapa para la Administración Cuantitativa
  - La organización de mantenimiento ha establecido objetivos de desempeño y calidad

o Innovación y Ejecución de Mantenimiento

- Nivel de madurez 1
  - La organización de mantenimiento informalmente evalúa los beneficios de su mejora e innovación de proyectos

Prácticas del 1er filtro - *gestión de riesgos y al mantenimiento de software*
– Asesoramiento de nuevos procesos, tecnologías, metodologías y herramientas para mantenimiento son desempeñadas informalmente ▪ Mapa para Investigación de Innovación/Mejoras – Nuevos procesos, servicios, tecnologías, metodologías y herramientas son identificadas e investigadas para su uso potencial en el mantenimiento de software. ▪ Mapa de Ejecución de Innovación/Mejora – Mejoras para algunos procesos, servicios, tecnologías, metodologías y herramientas de mantenimiento han sido iniciadas, de una forma controlada, localmente

Cabe resaltar y como puede ser observado en la Tabla 5.1 fueron ITIL V3 y MAAGTIC quienes aportaron un mayor número de prácticas, ya que presentan prácticas muy bien fundamentadas y están enfocadas a la gestión de tecnologías de la información, mientras que OWASP solo sugiere un conjunto de prácticas a seguir basado en las tendencias actuales durante el desarrollo de un software, sin indicar explícitamente las prácticas a seguir para estar dentro de dicha norma. Y finalmente la aportación de S3M no fue de gran apoyo ya que las prácticas analizadas no eran lo suficientemente maduras debido a que el acceso a la información es limitada, por lo tanto solo se pudo analizar solamente hasta el nivel 2 de madurez.

El segundo filtro tiene como objetivo descartar todas aquellas prácticas que no tengan relación con la privacidad e integridad de datos.

Durante la ejecución del segundo filtro, se analizó la definición y los contextos de cada una de las prácticas obtenidas en el primer filtro, y fueron descartadas todas aquellas prácticas que no tuvieran relación alguna con la conservación de la privacidad e integridad de datos.

En la Tabla 5.2 muestra que prácticas fueron conservadas y cuales fueron eliminadas durante el segundo filtro, ya que este filtro tuvo como criterio conservar todas aquellas prácticas que ayudaran a *preservar la privacidad e integridad de datos*.

Tabla 5.2 – Prácticas seleccionadas y descartadas durante el segundo filtro

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*
• **ITIL V3** o Gestión de Incidentes ▪ Registro – Notificación del incidente: en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*

- Clasificación
  - Monitorización del estado y tiempo de respuesta esperado: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.
- Diagnostico
  - Análisis de incidente

o Gestión de Problemas
- ~~Control de Problemas~~
  - ~~Identificación y Registro~~
  - ~~Análisis y Diagnóstico: Error Conocido~~
- ~~Control de Errores~~
  - ~~Análisis y solución~~
  - ~~Revisión Post Implementación y Cierre~~

o Gestión de niveles de Servicio
- ~~Planificación~~
  - ~~Establecimiento del catálogo de servicios~~
- Implementación
  - Establecimiento de SLA
  - Establecimiento de OLA (Acuerdos de Nivel de Operación)
  - Establecimiento de UC (Contrato de Soporte)
- Monitorización
  - Monitorización de la calidad del servicio
  - Elaboración de reportes
- Revisión
  - Revisión de la calidad de los servicios ofrecidos.

o Gestión de la Continuidad del Servicio
- Evaluación de Riesgos
  - Analizar las posibles amenazas y estimar su probabilidad.
  - Detectar los puntos más vulnerables de la infraestructura TI.
- Estrategias
  - Actividades Preventivas
  - Actividades de Seguridad
- Organización y Planificación
  - Plan de prevención de Riesgos
  - Plan de gestión de emergencias
  - Plan de recuperación
- Supervisión
  - Actualización y auditorias

o Gestión de la Seguridad
- Políticas y Plan de seguridad
  - Establecimiento del plan y políticas te seguridad

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*

- Aplicación de las medidas de seguridad
  - Coordinar la implementación de los protocolos y medidas de seguridad
  - Establecer las políticas y protocolos de acceso a la información.
  - Monitorizar las redes y servicios en red para detectar intrusiones y ataques.
  - Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
  - Generar la documentación de referencia necesaria.
- Evaluación y Mantenimiento
  - Evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs
  - Mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs

- **MAAGTIC**
  - Cumplimiento regulatorio
    - 7.2.2.2.2 CR-1 Identificar los requerimientos de las leyes, reglamentos y regulaciones aplicables: Identificar, de manera continua, los requerimientos en materia de TIC que se desprenden de las leyes aplicables a nivel federal e internacional, así como de reglamentos, regulaciones y otras disposiciones que deban ser observadas por la dependencia o entidad, a fin de incorporar estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC que sean necesarios en la dependencia o entidad para darles cumplimiento.
  - Administración de riesgos de TIC
    - 7.2.3.2.2 ARTI-2 Evaluar los riesgos de TIC: Asegurar que los riesgos en materia de TIC sean evaluados y presentados en términos del impacto a los procesos y servicios de la dependencia o entidad: financieros, de transparencia y seguridad de la información, regulatorios, entre otros.
      - Recopilar datos relevantes para los riesgos de TIC.
      - Identificar y analizar escenarios de riesgo que permitan definir los impactos potenciales a la entidad o dependencia sobre elementos como:
        - Servicios
        - Proceso
        - Datos (operativos, nómina, contables, entre otros).
        - Software (sistemas, aplicaciones, entre otros).
        - Hardware
        - Equipos informáticos que hospedan datos, aplicaciones y servicios.
        - Equipos de comunicación

- Dispositivos de almacenamiento (cintas, CDs, DVDs, entre otros).
- Personas (empleados internos y terceros).

– Identificar amenazas para aquellos activos identificados, dichas amenazas pueden ser clasificadas al menos en las siguientes categorías:
  - No causadas por el hombre:
    - Malfuncionamiento de TIC (fallas de software y de hardware)
    - Naturales (terremotos, huracanes, entre otros.)
    - De origen industrial (fallas eléctricas, aire acondicionado)
  - Causados por el hombre:
    - Maliciosas
      - Externas (espionaje industrial, hackers, entre otros.)
      - Internas (personal mal intencionado)
    - No maliciosas
      - Errores humanos

– Identificar riesgos; algunos tipos de riesgos son:
  - Fraudes
  - Robos
  - Degradación o perdida de continuidad en las operaciones
  - Fuga o modificación de información no autorizada
  - Accesos no autorizados
  - Falta o no cumplimiento de regulaciones, entre otros

– Identificar impactos a la entidad o dependencia; dichos impactos pueden ser, por lo menos, los siguientes:
  - Financieros
  - Niveles de servicios
  - Imagen o reputación
  - Regulatorios

- 7.2.3.2.2 ARTI-3 Responder a los riesgos de TIC: Asegurar que se responde a los riesgos de TIC con base a su nivel de severidad, con base en las decisiones para su tratamiento y tomado los criterios de priorización de implantación de controles.
  – Identificar el nivel de severidad del riesgo.
  – Identificar opciones para el tratamiento del riesgo el cual involucra tomar las decisiones para:
    - Aceptar el riesgo: no se efectúa ninguna acción debido a que el nivel de riesgo está dentro de los niveles aceptables por la entidad o dependencia.

- Evitar el riesgo. se elimina la causa que produce el riesgo
- Transferir el riesgo: se transfiere y comparte el riesgo con una organización aseguradora o un tercero.
- Mitigar el riesgo: se implementan controles para reducir el riesgo a un nivel aceptable por la entidad o dependencia

– Identificar controles predictivos, preventivos y correctivos y mapearlos para cada uno de los escenarios de riesgos identificados. Estos controles deben ser documentados en la SoA

– Definir planes de mitigación del riesgo que consideren las actividades para implantar los controles identificados en las Sentencias de aplicabilidad. Para cada escenario de riesgo la prioridad de implantación debe ser definida y acordada. Algunos de los parámetros que pueden ser considerados en la priorización de la implantación de los controles o contramedidas son los siguientes:

- Severidad del riesgo (nivel de riesgo)
- Nivel de impacto de la implantación del control en la disminución de las consecuencias del riesgo sobre los procesos y servicios de la entidad o dependencia
- Costo de implantación

– Definir un Plan de contingencia para reaccionar a eventos o incidentes en caso de presentarse un riesgo

- Administración de proyectos de TIC
  - 7.3.2.2.2 APTI-5: Administrar los riesgos: Eliminar o minimizar los riesgos por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados.

– Identificar riesgos. La identificación de riesgos es un proceso iterativo debido a que se pueden descubrir nuevos riesgos a medida que el proyecto avanza a lo largo de su ciclo de vida. El equipo de trabajo del proyecto debe participar en la identificación de los riesgos para poder desarrollar y mantener un sentido de pertenencia y responsabilidad por los riesgos y las acciones asociadas a la respuesta a los riesgos. Los riesgos identificados se documentan en un registro de riesgos.

– Clasificar riesgos. Los riesgos se categorizan por tipo de riesgo, se identifican y agrupan por la causa raíz y se elaboran propuestas que los minimicen o eliminen. Para clasificarlos se pueden utilizar metodologías como la matriz FODA que analiza fortalezas, oportunidades, debilidades y amenazas.

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*

- Responder a los riesgos. Se determina la prioridad de atención de los riesgos identificados y las acciones que serán realizadas para atender el riesgo, incluyendo las acciones de mitigación y la definición de un Plan de contingencia
- Dar seguimiento y controlar riesgos. Realizar el seguimiento de los riesgos identificados, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto.
- Adecuar el Plan de proyecto, incluyendo la documentación del alcance, el cronograma y el presupuesto, para incorporar las decisiones derivadas de la administración de riesgos que impacten al plan.

o Operación del sistema de gestión y mejora de procesos de la UTIC
  - ~~7.4.1.2.2 OSGP-3: Monitorear y evaluar la operación del Sistema de gestión y mejora de procesos de la UTIC~~

o Administración de proveedores
  - 7.5.2.2.2 APV-1 Generar lista de verificación de acuerdos: Con base al contrato establecido, se elabora una lista de verificación para dar seguimiento al desarrollo del contrato.
  - 7.5.2.2.2 APV-2 Monitorear el avance y desempeño del proveedor: Verificar que las actividades del proveedor sean desempeñadas como está especificado en el contrato.
  - 7.5.2.2.2 APV-3 Revisión de cumplimiento al contrato TIC: Verificar y evaluar que la totalidad de las actividades desarrolladas se realicen con apego a lo estipulado en los contratos establecidos, con la finalidad de identificar riesgos y oportunidades, que permitan evitar incumplimientos de los compromisos contractuales, inclusive por parte de la UTIC y/o del área solicitante del objeto del contrato.
  - ~~7.5.2.2.2 APV-4 Cierre administrativo del contrato: Comprobar que el proveedor cumplió con la totalidad de sus compromisos, para cerrar el contrato~~.

o Administración de servicios de terceros
  - 7.9.2.2.2 AST- 4 Realizar pruebas técnicas de la prestación del servicio: Asegurar que los servicios seleccionados cumplen con los requerimientos.

o Administración de niveles de servicio
  - 7.9.3.2.2 ANS-1 Crear y mantener acuerdos de niveles de servicio: Definir los SLA basados en el catálogo de servicios de las UTIC, de acuerdo con los requerimientos de la operación y las necesidades de los usuarios de cada uno de los servicios definidos
  - 7.9.3.2.2 ANS-2 Monitorear y reportar el grado de cumplimiento de los niveles de servicio: Elaborar reportes de resultados sobre el grado de cumplimiento de los SLA. Esta actividad sigue las directrices del

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*

proceso de Administración del desempeño de TIC.

- ~~7.9.3.2.2 ANS-4 Formular el Plan de mejora de servicios: Recomendar mejoras a los SLA, como consecuencia de las insatisfacciones del cliente o el no cumplimiento de acuerdos establecidos~~.

- Administración de la operación
  - 7.11.1.2.2 AO-3 Monitorear la infraestructura de TIC: Asegurar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que sustentan las operaciones.
- Administración de ambiente físico
  - 7.11.2.2.2 AAF-2: Establecer las medidas de seguridad física.: Definir e implementar medidas de seguridad físicas, alineadas a los procesos de administración de la seguridad de la información y administración de riesgos de TIC, de la dependencia o entidad. Definir e implementar las reglas de operación de acceso a los centros de datos.
  - 7.11.2.2.2 AAF-3: Establecer medidas de control de acceso físico a las áreas reservadas de la UTIC: Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las ubicaciones de la UTIC, de acuerdo con los requerimientos de seguridad indicados por el SGSI, incluyendo las salidas de emergencia.
  - 7.11.2.2.2 AAF-4: Establecer la protección contra riesgos ambientales: Diseñar e implementar medidas de protección contra riesgos ambientales

- **OWASP**
  - Guía de desarrollo
    - Establecimiento de políticas de seguridad de acuerdo a la legislación nacional y estándares industriales (se recomienda COBIT o ISO 17799)
    - ~~Establecimiento de metodología de desarrollo~~
    - ~~Diseñar controles (para prevenir un mal uso de la aplicación)~~
    - Modelado de amenaza de riesgo
      - Documentar amenazas conocidas
    - Educar al usuario en cuestiones de seguridad tales como phishing, malware, instalación de antivirus, etc.
    - Establecer mecanismos de seguridad en los mecanismos de comunicación de la aplicación
    - Establecer cifrado de mensajes
    - Realización de auditorías a la aplicación
    - Establecimiento de mecanismos de estampado de tiempos en mensajes para asegurar la frescura de estos
    - ~~Establecimiento de mecanismos de control de acceso a la aplicación~~
    - Gestión de usuarios
    - ~~Realizar validaciones de reglas de negocio~~

        - Manejo de errores
        - Generación de logs
    - Top 10
        - Revisar el documento top 10 de OWASP a la hora de realizar una gestión de riegos, para conocer las principales amenazas actuales dentro de las aplicaciones web.
    - Legal Project
        - Definir actividades del ciclo de vida relacionadas con seguridad
        - Definir áreas de requerimientos de seguridad
        - Requerir análisis y pruebas de seguridad utilizando estándares acordados
        - Revisiones de seguridad
    - Guía de Testeo
        - Revisión de políticas y estándares
        - Revisión de requerimientos de seguridad
        - Creación y revisión del modelo de amenazas
        - Pruebas de penetración de la aplicación
        - ~~Pruebas de gestión de la configuración~~
        - ~~Conducir revisiones de gestión operacional~~
- **S3M**
    - Enfoque a Procesos de Mantenimiento
        - Mapa a la recolección de información
            - Los datos en fallas de software son recogidas y utilizadas para identificar candidatos a mejora para dar mantenimiento a procesos/productos y además para muchas interfaces con otros grupos de interface
            - ~~La organización de mantenimiento está sujeta a auditorías internas y los resultados son utilizados para identificar candidatos a mejora.~~
    - Desempeño del Proceso de Mantenimiento
        - Mapa para la Identificación de la línea base
            - ~~Medidas de la línea base en la calidad y desempeño son recolectadas, almacenadas, revisadas y usadas con varios stakeholders. Son usados para mejorar el proceso, servicio y producto actual.~~
        - Mapa para la Administración Cuantitativa
            - La organización de mantenimiento ha establecido objetivos de desempeño y calidad
    - Innovación y Ejecución de Mantenimiento
        - Nivel de madurez 1
            - ~~La organización de mantenimiento informalmente evalúa los beneficios de su mejora e innovación de proyectos~~
            - ~~Asesoramiento de nuevos procesos, tecnologías, metodologías~~

Prácticas del 2do filtro - *preservar la privacidad e integridad de datos*

~~y herramientas para mantenimiento son desempeñadas informalmente~~

- Mapa para Investigación de Innovación/Mejoras
  - Nuevos procesos, servicios, tecnologías, metodologías y herramientas son identificadas e investigadas para su uso potencial en el mantenimiento de software.
- Mapa de Ejecución de Innovación/Mejora
  - ~~Mejoras para algunos procesos, servicios, tecnologías, metodologías y herramientas de mantenimiento han sido iniciadas, de una forma controlada, localmente~~

Durante el segundo filtrado de prácticas, varias de ellas fueron descartadas ya que algunas se enfocaban a la mejora de procesos, la validación de reglas de negocio, la gestión de la configuración, el establecimiento del catálogo de servicios y a cierres administrativos, y mientras que otras tenían un enfoque más a nivel de un desarrollador. Las prácticas descartadas de ITIL fueron por su redundancia con otras dentro de la misma norma y por su nula relación con la privacidad e integridad de datos. MAAGTIC presentaba prácticas relacionadas con mejoras de procesos las cuales fueron eliminadas durante este filtro. Dentro de OWASP había varias prácticas enfocadas muy directamente con el desarrollador, otras que ya forman parte de MoProSoft, y además prácticas de validación de negocios y gestión de la configuración, todas estas fueron desechadas. Finalmente dentro de S3M había actividades muy informales y otras relacionadas con la búsqueda de mejoras y recolección de información, las cuales quedaron fuera con la ejecución de este filtro.

El tercer filtro tiene como objetivo adaptar a cada una de las prácticas obtenidas en el segundo filtro, al entorno del cómputo en la nube, ya que este paradigma es al que está enfocado el presente estudio.

En la ejecución de este filtro fueron analizadas cada una de las prácticas del segundo filtro, y fueron descartadas aquellas prácticas que tuvieran el mismo propósito que otras ya seleccionadas, conservando las que presentarán una definición más concreta, luego se procedió a conjuntar todas aquellas prácticas que tuvieran un propósito similar, para así generar prácticas más concretas y poder abordar de una mejor forma los problemas de privacidad e integridad de datos. Por último se volvieron a analizar las prácticas y se ajustaron aquellas prácticas que presentaban un enfoque muy general para que fueran específicas a los servicios del cómputo en la nube.

Finalmente se muestra en la Tabla 5.3 las prácticas eliminadas por su duplicidad con otras, su combinación con otras prácticas y como fueron adaptadas y mejoradas al ambiente del cómputo en la nube, todo esto durante la realización del tercer filtro.

Tabla 5.3 – Prácticas mejoradas y adaptadas al ambiente del cómputo en la nube

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

- **ITIL v3**
  - Gestión de Incidentes
    - Registro
      - Notificación del incidente: en los casos en que el incidente pueda afectar a otros usuarios dentro de la plataforma de la nube, estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.
    - Clasificación
      - Monitorización del estado y tiempo de respuesta esperado: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.
    - Diagnostico
      - Análisis de incidente
  - Gestión de niveles de Servicio
    - Implementación
      - Establecimiento de SLA
      - Establecimiento de OLA (Acuerdos de Nivel de Operación)
      - Establecimiento de UC (Contrato de Soporte)
    - Monitorización
      - Monitorización de la calidad de la infraestructura del cómputo en la nube ~~servicio~~
      - Elaboración de reportes
    - Revisión
      - Revisión de la calidad de la plataforma de la nube ~~los servicios ofrecidos.~~
  - Gestión de la Continuidad del Servicio
    - Evaluación de Riesgos
      - Documentar Amenazas conocidas
      - Revisar el documento top 10 de OWASP ~~a la hora de realizar una gestión de riegos~~, para conocer las principales amenazas actuales dentro de las aplicaciones web, específicamente las que estén relacionadas con el cómputo en la nube.
      - Analizar las posibles amenazas y estimar su probabilidad.
        - Identificar y analizar escenarios de riesgo que permitan definir los impactos potenciales a la entidad o dependencia sobre elementos como:
          - Servicios
          - Proceso
          - Datos (operativos, nómina, contables, entre otros).

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

- Software (sistemas, aplicaciones, entre otros).
- Hardware
- Equipos informáticos que hospedan datos, aplicaciones y servicios.
- Equipos de comunicación
- Dispositivos de almacenamiento (cintas, CDs, DVDs, entre otros).
- Personas (empleados internos y terceros).

o Identificar amenazas para aquellos activos identificados, dichas amenazas pueden ser clasificadas al menos en las siguientes categorías:

- No causadas por el hombre:
  - Malfuncionamiento de TIC (fallas de software y de hardware)
  - Naturales (terremotos, huracanes, entre otros.)
  - De origen industrial (fallas eléctricas, aire acondicionado)
- Causados por el hombre:
  - Maliciosas
    - Externas (espionaje industrial, hackers, entre otros.)
    - Internas (personal mal intencionado)
  - No maliciosas
    - Errores humanos

o Identificar riesgos; algunos tipos de riesgos son:

- Robos
- Degradación o perdida de continuidad en las operaciones
- Fuga o modificación de información no autorizada
- Accesos no autorizados
  - Falta o no cumplimiento de regulaciones, entre otros

o Identificar impactos a la entidad o dependencia; dichos impactos pueden ser, por lo menos, los siguientes:

- Niveles de servicios
- Regulatorios

– Detectar los puntos más vulnerables de la infraestructura Cloud.

- Establecimiento de Estrategias
  - Actividades Preventivas
  - Actividades de Seguridad
    - Establecer las medidas de seguridad física para la

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

infraestructura IaaS.: Definir e implementar medidas de seguridad físicas, alineadas a los procesos de administración de la seguridad de la información y administración de riesgos de TIC, de la dependencia o entidad. Definir e implementar las reglas de operación de acceso a los centros de datos.

- Establecer medidas de control de acceso físico a las áreas reservadas la infraestructura IaaS: Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las ubicaciones de la UTIC, de acuerdo con los requerimientos de seguridad indicados por el SGSI, incluyendo las salidas de emergencia.

- Organización y Planificación
  - Plan de prevención de Riesgos
  - Plan de gestión de emergencias
  - Plan de recuperación
    - Establecer la protección contra riesgos ambientales: Diseñar e implementar medidas de protección contra riesgos ambientales
- Supervisión
  - Actualización y auditorias
    - Generación de logs

- Gestión de la Seguridad
  - Políticas y Plan de seguridad
    - Establecimiento del plan y políticas de seguridad para la plataforma de la nube.
  - Aplicación de las medidas de seguridad
    - Coordinar la implementación de los protocolos y medidas de seguridad para la plataforma de la nube
    - Establecer las políticas y protocolos de acceso a la información dentro de la plataforma de la nube.
    - Monitorizar las redes y servicios en la nube ~~red~~ para detectar intrusiones y ataques.
    - Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad de la plataforma de la nube.
      - Nuevos procesos, servicios, tecnologías, metodologías y herramientas son identificadas e investigadas para su uso potencial en el mantenimiento ~~de software~~ de la plataforma de la nube.
    - Generar la documentación de referencia necesaria para la plataforma de la nube.
  - Evaluación y Mantenimiento

- Evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs
- Mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs

- **MAAGTIC**
  - Cumplimiento regulatorio
    - 7.2.2.2.2 CR-1 Identificar los requerimientos de las leyes, reglamentos y regulaciones aplicables: Identificar, de manera continua, los requerimientos en materia de TIC que se desprenden de las leyes aplicables a nivel federal e internacional, así como de reglamentos, regulaciones y otras disposiciones que deban ser observadas por la dependencia o entidad, a fin de incorporar estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC que sean necesarios en la dependencia o entidad para darles cumplimiento.
  - Administración de riesgos de TIC
    - ~~7.2.3.2.2 ARTI-2 Evaluar los riesgos de TIC: Asegurar que los riesgos en materia de TIC sean evaluados y presentados en términos del impacto a los procesos y servicios de la dependencia o entidad: financieros, de transparencia y seguridad de la información, regulatorios, entre otros.~~
      - ~~Recopilar datos relevantes para los riesgos de TIC.~~
      - ~~Identificar y analizar escenarios de riesgo que permitan definir los impactos potenciales a la entidad o dependencia sobre elementos como:~~
        - ~~Servicios~~
        - ~~Proceso~~
        - ~~Datos (operativos, nómina, contables, entre otros).~~
        - ~~Software (sistemas, aplicaciones, entre otros).~~
        - ~~Hardware~~
        - ~~Equipos informáticos que hospedan datos, aplicaciones y servicios.~~
        - ~~Equipos de comunicación~~
        - ~~Dispositivos de almacenamiento (cintas, CDs, DVDs, entre otros).~~
        - ~~Personas (empleados internos y terceros).~~
      - ~~Identificar amenazas para aquellos activos identificados, dichas amenazas pueden ser clasificadas al menos en las siguientes categorías:~~
        - ~~No causadas por el hombre:~~
          - ~~Malfuncionamiento de TIC (fallas de software y de hardware)~~
          - ~~Naturales (terremotos, huracanes, entre otros.)~~

- De origen industrial (fallas eléctricas, aire acondicionado)
- Causados por el hombre:
  - Maliciosas
    - Externas (espionaje industrial, hackers, entre otros.)
    - Internas (personal mal intencionado)
  - No maliciosas
    - Errores humanos

– Identificar riesgos; algunos tipos de riesgos son:
- Fraudes
- Robos
- Degradación o perdida de continuidad en las operaciones
- Fuga o modificación de información no autorizada
- Accesos no autorizados
- Falta o no cumplimiento de regulaciones, entre otros

– Identificar impactos a la entidad o dependencia; dichos impactos pueden ser, por lo menos, los siguientes:
- Financieros
- Niveles de servicios
- Imagen o reputación
- Regulatorios

- 7.2.3.2.2 ARTI-3 Responder a los riesgos de TIC: Asegurar que se responde a los riesgos de TIC con base a su nivel de severidad, con base en las decisiones para su tratamiento y tomado los criterios de priorización de implantación de controles.

– Identificar el nivel de severidad del riesgo.

– Identificar opciones para el tratamiento del riesgo el cual involucra tomar las decisiones para:
- Aceptar el riesgo: no se efectúa ninguna acción debido a que el nivel de riesgo está dentro de los niveles aceptables por la entidad o dependencia.
- Evitar el riesgo. se elimina la causa que produce el riesgo
- Transferir el riesgo: se transfiere y comparte el riesgo con una organización aseguradora o un tercero.
- Mitigar el riesgo: se implementan controles para reducir el riesgo a un nivel aceptable por la entidad o dependencia

– Identificar controles predictivos, preventivos y correctivos y mapearlos para cada uno de los escenarios de riesgos identificados. Estos controles deben ser documentados en la

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

SoA

- Definir planes de mitigación del riesgo que consideren las actividades para implantar los controles identificados en las Sentencias de aplicabilidad. Para cada escenario de riesgo la prioridad de implantación debe ser definida y acordada. Algunos de los parámetros que pueden ser considerados en la priorización de la implantación de los controles o contramedidas son los siguientes:
  - Severidad del riesgo (nivel de riesgo)
  - Nivel de impacto de la implantación del control en la disminución de las consecuencias del riesgo sobre los procesos y servicios de la entidad o dependencia
  - Costo de implantación
- Definir un Plan de contingencia para reaccionar a eventos o incidentes en caso de presentarse un riesgo

- Administración de proyectos de TIC
  - 7.3.2.2.2 APTI-5: Administrar los riesgos: Eliminar o minimizar los riesgos por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados.
    - Identificar riesgos. La identificación de riesgos es un proceso iterativo debido a que se pueden descubrir nuevos riesgos a medida que el proyecto avanza a lo largo de su ciclo de vida. El equipo de trabajo del proyecto debe participar en la identificación de los riesgos para poder desarrollar y mantener un sentido de pertenencia y responsabilidad por los riesgos y las acciones asociadas a la respuesta a los riesgos. Los riesgos identificados se documentan en un registro de riesgos.
    - Clasificar riesgos. Los riesgos se categorizan por tipo de riesgo, se identifican y agrupan por la causa raíz y se elaboran propuestas que los minimicen o eliminen. Para clasificarlos se pueden utilizar metodologías como la matriz FODA que analiza fortalezas, oportunidades, debilidades y amenazas.
    - Responder a los riesgos. Se determina la prioridad de atención de los riesgos identificados y las acciones que serán realizadas para atender el riesgo, incluyendo las acciones de mitigación y la definición de un Plan de contingencia
    - Dar seguimiento y controlar riesgos. Realizar el seguimiento de los riesgos identificados, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto.
    - Adecuar el Plan de proyecto, incluyendo la documentación del alcance, el cronograma y el presupuesto, para incorporar las

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

~~decisiones derivadas de la administración de riesgos que impacten al plan.~~

- Administración de proveedores
  - 7.5.2.2.2 APV-1 Generar lista de verificación de acuerdos: Con base al contrato establecido, se elabora una lista de verificación para dar seguimiento al desarrollo del contrato.
  - 7.5.2.2.2 APV-2 Monitorear el avance y desempeño del proveedor: Verificar que las actividades del proveedor sean desempeñadas como está especificado en el contrato.
  - 7.5.2.2.2 APV-3 Revisión de cumplimiento al contrato TIC: Verificar y evaluar que la totalidad de las actividades desarrolladas se realicen con apego a lo estipulado en los contratos establecidos, con la finalidad de identificar riesgos y oportunidades, que permitan evitar incumplimientos de los compromisos contractuales, inclusive por parte de la UTIC y/o del área solicitante del objeto del contrato.

~~o Administración de servicios de terceros~~

- ~~7.9.2.2.2 AST- 4 Realizar pruebas técnicas de la prestación del servicio: Asegurar que los servicios seleccionados cumplen con los requerimientos.~~

- Administración de niveles de servicio
  - ~~7.9.3.2.2 ANS-1 Crear y mantener acuerdos de niveles de servicio: Definir los SLA basados en el catálogo de servicios de las UTIC, de acuerdo con los requerimientos de la operación y las necesidades de los usuarios de cada uno de los servicios definidos~~
  - ~~7.9.3.2.2 ANS-2 Monitorear y reportar el grado de cumplimiento de los niveles de servicio: Elaborar reportes de resultados sobre el grado de cumplimiento de los SLA. Esta actividad sigue las directrices del proceso de Administración del desempeño de TIC.~~
- Administración de la operación
  - ~~7.11.1.2.2 AO-3 Monitorear la infraestructura de TIC: Asegurar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que sustentan las operaciones.~~
- Administración de ambiente físico
  - ~~7.11.2.2.2 AAF-2: Establecer las medidas de seguridad física.: Definir e implementar medidas de seguridad físicas, alineadas a los procesos de administración de la seguridad de la información y administración de riesgos de TIC, de la dependencia o entidad. Definir e implementar las reglas de operación de acceso a los centros de datos.~~
  - ~~7.11.2.2.2 AAF-3: Establecer medidas de control de acceso físico a las áreas reservadas de la UTIC: Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las ubicaciones de la UTIC,~~

Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

de acuerdo con los requerimientos de seguridad indicados por el SGSI, incluyendo las salidas de emergencia.

- 7.11.2.2.2 AAF-4: Establecer la protección contra riesgos ambientales: Diseñar e implementar medidas de protección contra riesgos ambientales

- **OWASP**
  - Guía de desarrollo
    - Establecimiento de políticas de seguridad de acuerdo a la legislación nacional y estándares industriales (se recomienda COBIT o ISO 17799)
    - Modelado de amenaza de riesgo
      - Documentar amenazas conocidas
    - Educar al usuario en cuestiones de seguridad tales como phishing, malware, instalación de antivirus, etc.
    - Establecer mecanismos de seguridad en las vías de comunicación de la aplicación
    - Establecer cifrado de mensajes
    - Realización de auditorías a la aplicación
    - Establecimiento de mecanismos de estampado de tiempos en mensajes para asegurar la frescura de estos
    - Gestión de usuarios
    - Manejo de errores
    - Generación de logs
  - Top 10
    - Revisar el documento top 10 de OWASP a la hora de realizar una gestión de riegos, para conocer las principales amenazas actuales dentro de las aplicaciones web.
  - Legal Project
    - Definir actividades del ciclo de vida relacionadas con seguridad
    - Definir áreas de requerimientos de seguridad
    - Requerir análisis y pruebas de seguridad utilizando estándares acordados
    - Revisiones de seguridad
  - Guía de Testeo
    - Revisión de políticas y estándares
    - Revisión de requerimientos de seguridad de la plataforma de la nube.
    - Creación y revisión del modelo de amenazas
    - Pruebas de penetración de la aplicación a la plataforma de la nube.
- **S3M**
  - Enfoque a Procesos de Mantenimiento
    - Mapa a la recolección de información
      - Los datos en fallas de software son recogidas y utilizadas para identificar candidatos a mejora para dar mantenimiento a procesos/productos y además para muchas interfaces con otros

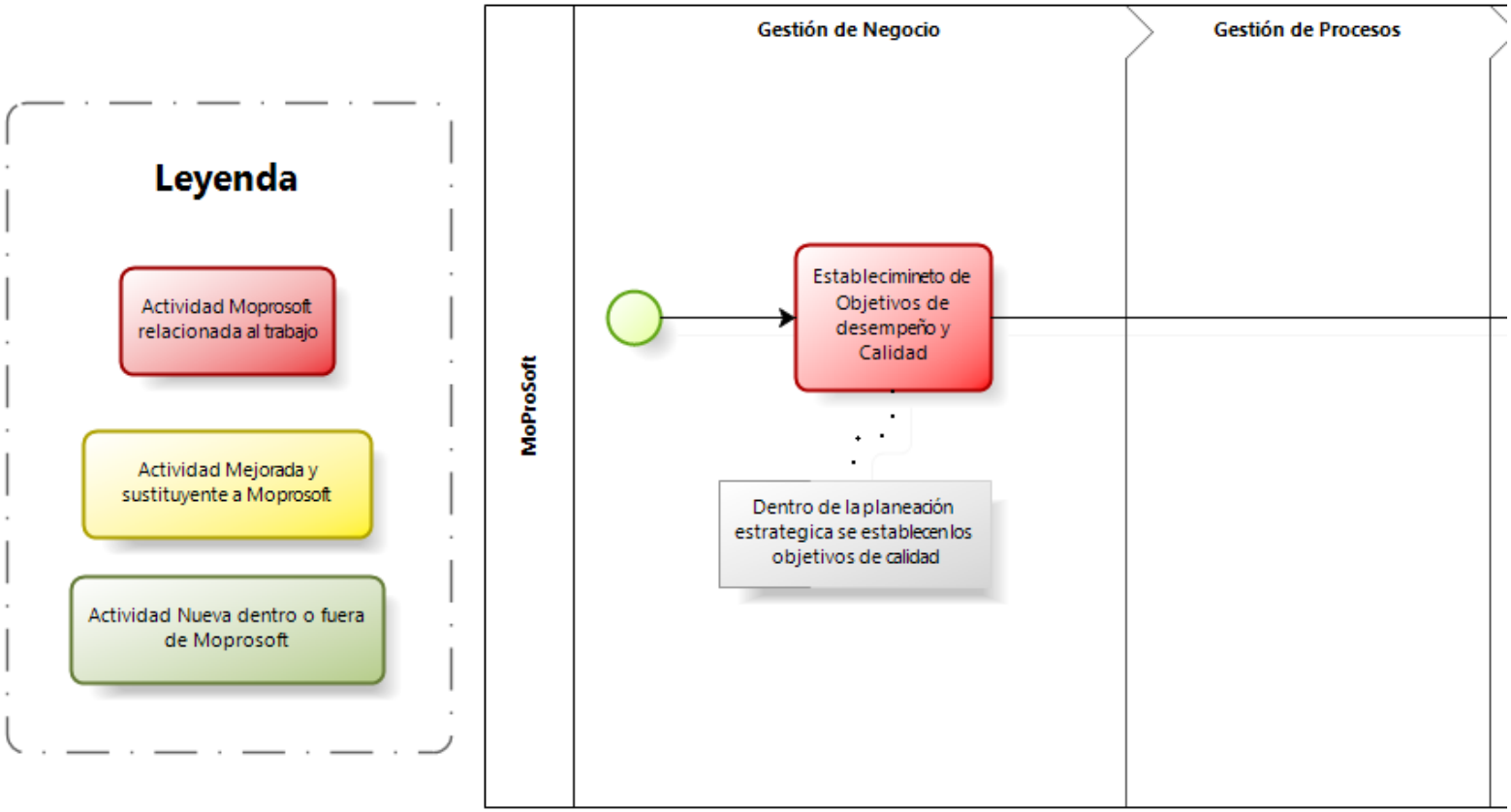
Prácticas del 3er filtro - Mejora y adaptación de prácticas para el cómputo en la nube

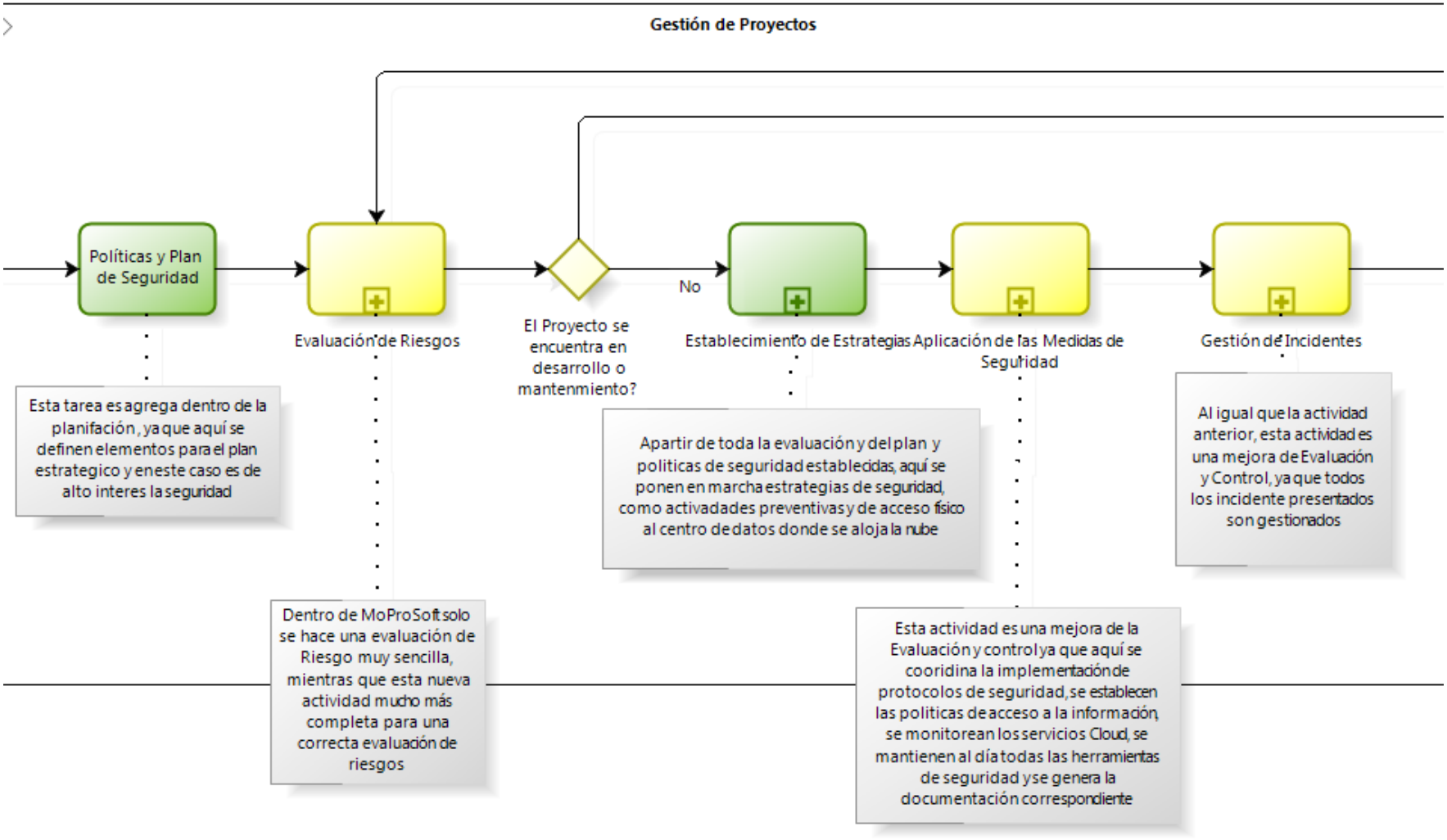
~~grupos de interface~~

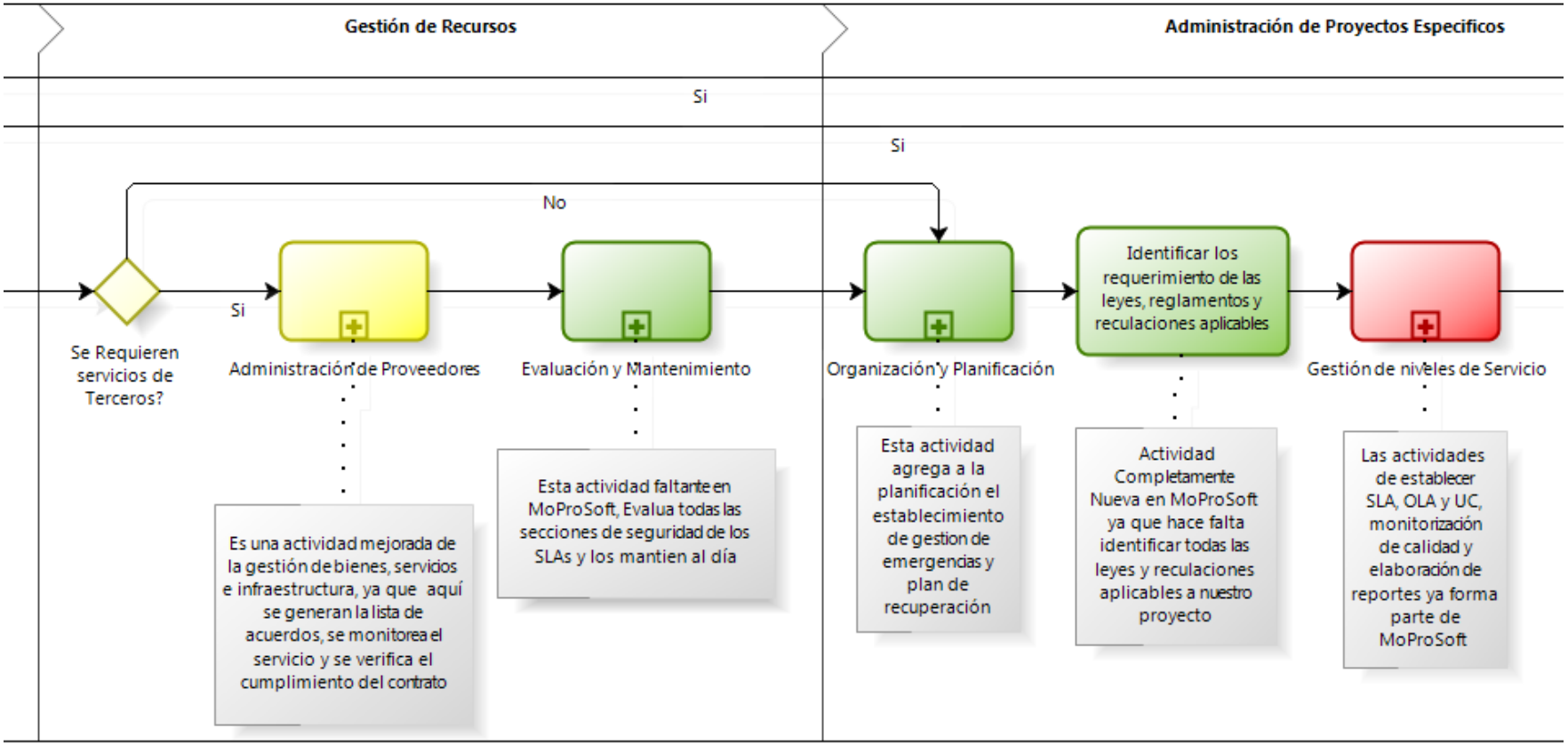
- o Desempeño del Proceso de Mantenimiento
  - ▪ Mapa para la Administración Cuantitativa
    - – La organización de mantenimiento ha establecido objetivos de desempeño y calidad para asegurar una mejor integridad y privacidad de datos dentro de la plataforma de la nube.
- o Innovación y Ejecución de Mantenimiento
  - ▪ Mapa para Investigación de Innovación/Mejoras
    - – ~~Nuevos procesos, servicios, tecnologías, metodologías y herramientas son identificadas e investigadas para su uso potencial en el mantenimiento de software.~~

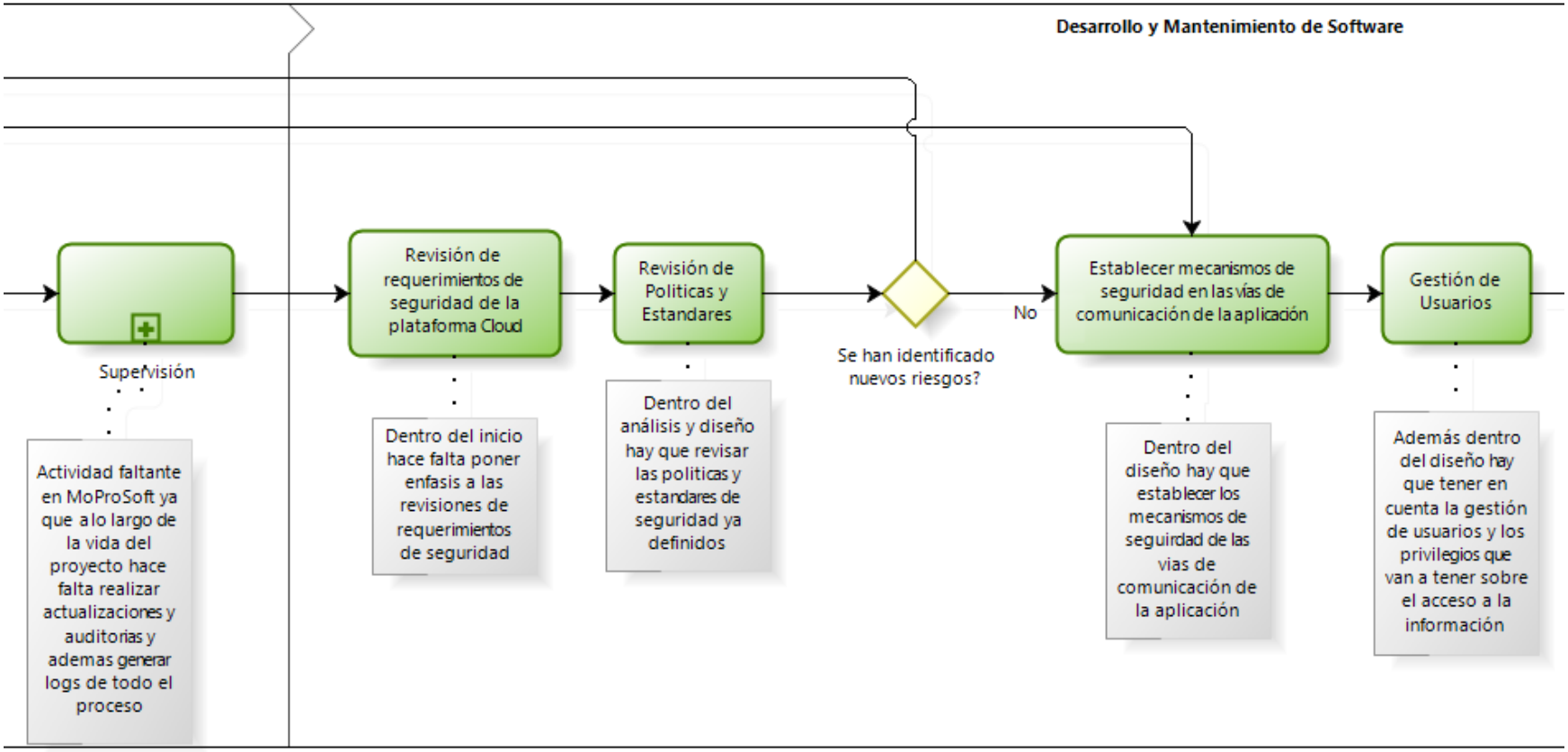
La tabla anterior contiene la selección final de todas las prácticas de las diferentes normas y estándares analizados, y adaptadas para el desarrollo de aplicaciones de la nube. Dichas prácticas forman parte del proceso final de la propuesta de este documento. Como podemos observar las prácticas de MAAGTIC, OWASP y S3M fueron insertadas dentro de ITIL, ya que esta norma presenta las bases para atacar los problemas de privacidad e integridad de datos y las prácticas de las otras normas ayudan a completar estas de ITIL. Algunas prácticas de MAAGTIC, OWASP y S3M fueron eliminadas por su similitud con otras dentro de ITIL. OWASP también contenía actividades similares de MAAGTIC, las cuales además fueron descartadas. Todas estas prácticas fueron adaptas para que pudieran ser implementadas dentro del cómputo en la nube.

Ya con todas las prácticas para el desarrollo de aplicaciones del cómputo en la nube que permitan mantener una mejor integridad y privacidad de datos, se procedió a integrarlas dentro del marco de MoProSoft. La Figura 5.1 muestra el proceso principal de esta propuesta (La figura puede ser además visualizada en el siguiente enlace: http://bit.ly/12kRTgw).


Leyenda
Actividad Moprosoft relacionada al trabajo
Actividad Mejorada y sustituyente a Moprosoft
Actividad Nueva dentro o fuera de Moprosoft
MoProSoft
Gestión de Negocio
Gestión de Procesos
Establecimineto de Objetivos de desempeño y Calidad
Dentro de la planeación estrategica se establecen los objetivos de calidad


Gestión de Proyectos
Políticas y Plan de Seguridad
Evaluación de Riesgos
El Proyecto se encuentra en desarrollo o mantenmiento?
No
Establecimiento de Estrategias
Aplicación de las Medidas de Seguridad
Gestión de Incidentes
Esta tarea es agrega dentro de la planifación, ya que aquí se definen elementos para el plan estrategico y en este caso es de alto interes la seguridad
Dentro de MoProSoft solo se hace una evaluación de Riesgo muy sencilla, mientras que esta nueva actividad mucho más completa para una correcta evaluación de riesgos
Apartir de toda la evaluación y del plan y politicas de seguridad establecidas, aquí se ponen en marcha estrategias de seguridad, como activadades preventivas y de acceso físico al centro de datos donde se aloja la nube
Esta actividad es una mejora de la Evaluación y control ya que aquí se cooridina la implementación de protocolos de seguridad, se establecen las politicas de acceso a la información, se monitorean los servicios Cloud, se mantienen al día todas las herramientas de seguridad y se genera la documentación correspondiente
Al igual que la actividad anterior, esta actividad es una mejora de Evaluación y Control, ya que todos los incidente presentados son gestionados


Gestión de Recursos
Administración de Proyectos Especificos
Si
Si
No
Si
Se Requieren servicios de Terceros?
Administración de Proveedores
Evaluación y Mantenimiento
Organización y Planificación
Identificar los requerimiento de las leyes, reglamentos y reculaciones aplicables
Gestión de niveles de Servicio
Es una actividad mejorada de la gestión de bienes, servicios e infraestructura, ya que aquí se generan la lista de acuerdos, se monitorea el servicio y se verifica el cumplimiento del contrato
Esta actividad faltante en MoProSoft, Evalua todas las secciones de seguridad de los SLAs y los mantien al día
Esta actividad agrega a la planificación el establecimiento de gestion de emergencias y plan de recuperación
Actividad Completamente Nueva en MoProSoft ya que hace falta identificar todas las leyes y reculaciones aplicables a nuestro proyecto
Las actividades de establecer SLA, OLA y UC, monitorización de calidad y elaboración de reportes ya forma parte de MoProSoft


Desarrollo y Mantenimiento de Software
Supervisión
Actividad faltante en MoProSoft ya que a lo largo de la vida del proyecto hace falta realizar actualizaciones y auditorias y ademas generar logs de todo el proceso
Revisión de requerimientos de seguridad de la plataforma Cloud
Dentro del inicio hace falta poner enfasis a las revisiones de requerimientos de seguridad
Revisión de Politicas y Estandares
Dentro del análisis y diseño hay que revisar las politicas y estandares de seguridad ya definidos
Se han identificado nuevos riesgos?
No
Establecer mecanismos de seguridad en las vias de comunicación de la aplicación
Dentro del diseño hay que establecer los mecanismos de seguirdad de las vias de comunicación de la aplicación
Gestión de Usuarios
Además dentro del diseño hay que tener en cuenta la gestión de usuarios y los privilegios que van a tener sobre el acceso a la información

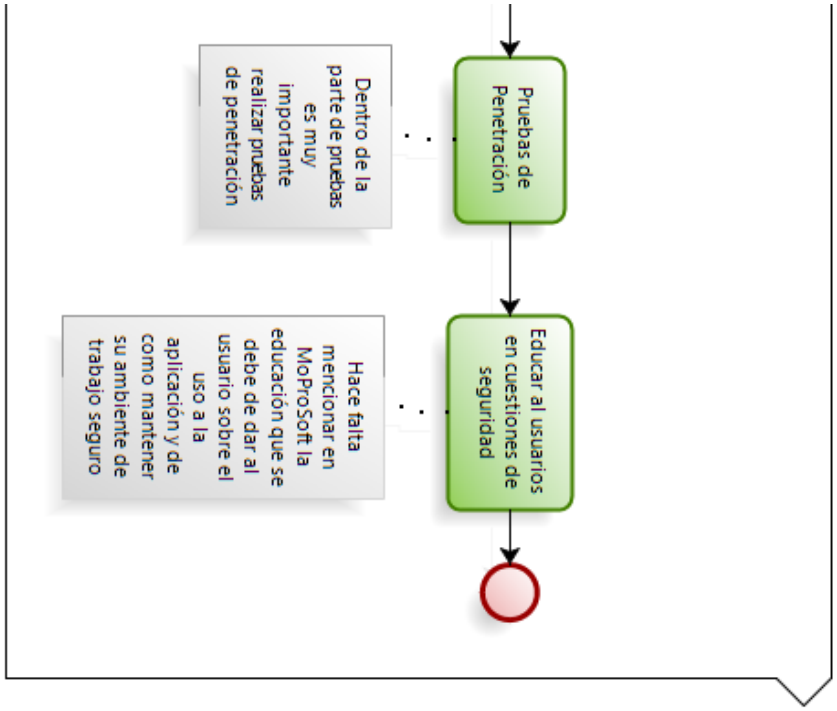


Figura 5.1 – Proceso de desarrollo de software propuesto para mejorar la privacidad e integridad de datos

En la Figura 5.1 se muestran todas las actividades resultantes de los filtros sobre las normas y modelos. Cada actividad fue insertada a MoProSoft acorde al propósito y descripción de cada uno de las áreas de proceso de la norma.

Acorde a la leyenda ilustrada en la Figura 5.1, todas aquellas actividades que tienen un color ***rojo***, encajan perfectamente dentro del marco de MoProSoft, por lo que no se modificó la actividad MoProSoft, las actividades de color ***amarillo*** son actividades mejoradas que reemplazan a las existentes dentro del marco de MoProSoft y finalmente las actividades de color ***verde*** son totalmente nuevas a MoProSoft. También se puede observar que se encuentran varios subprocesos y estos se ilustran en las siguientes figuras y respetan la leyenda de la Figura 5.1.

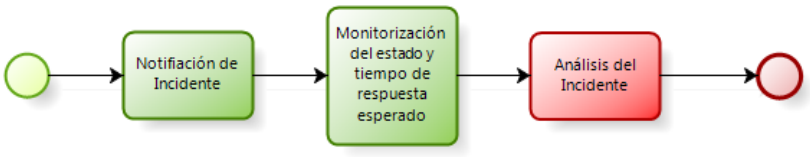


Figura 5.2 – Subproceso de gestión de incidentes

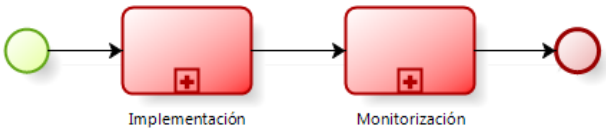


Figura 5.3 – Subproceso de gestión de niveles de servicio

Figura 5.4 – Subproceso de implementación

Figura 5.5 – Subproceso de monitorización

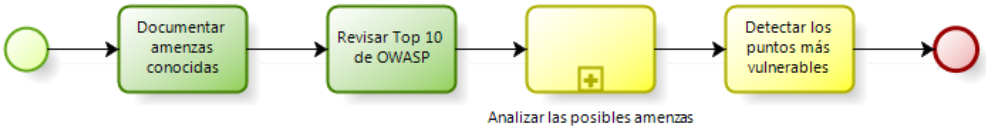


Figura 5.6 – Subproceso de evaluación de riesgos

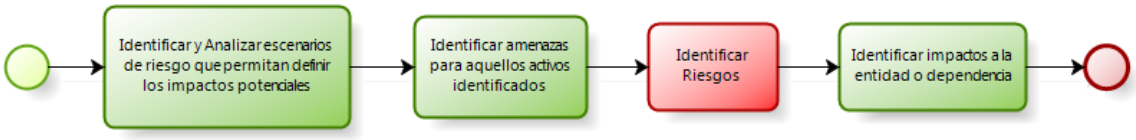


Figura 5.7 – Subproceso de analizar las posibles amenazas

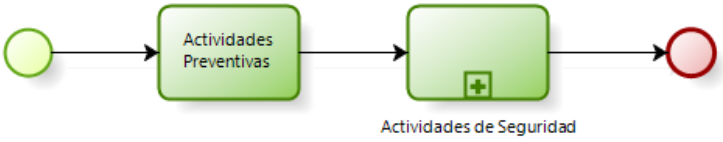


Figura 5.8 – Subproceso de establecimiento de estrategias

Figura 5.9 – Subproceso de actividades de seguridad

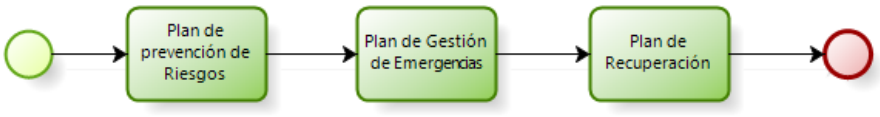


Figura 5.10 – Subproceso de organización y planificación

Figura 5.11 – Subproceso de supervisión

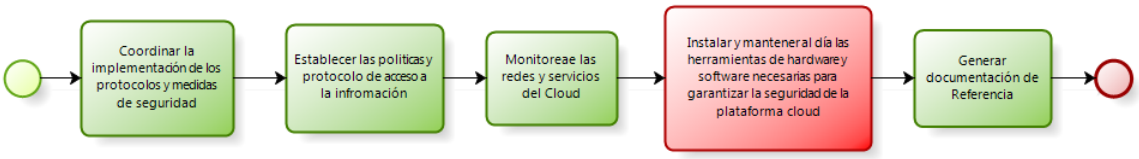


Figura 5.12 – Subproceso de aplicación de las medidas de seguridad

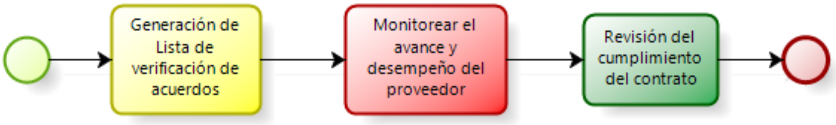


Figura 5.13 – Subproceso de administración de proveeedores

Figura 5.14 – Subproceso de evaluación y mantenimiento

Como ya se mencionó en el capítulo anterior, una vez establecido este proceso, se realizó una entrevista en la empresa en una empresa real, que para este caso de estudio fue la empresa Softlogik S.A. de C.V. con el objetivo de conocer cuántas actividades son implementadas y así poder determinar la factibilidad de implementación del proceso

propuesto. La entrevista fue realizada al director de operaciones y uno de los ingenieros senior, en donde se les si realizaba cada una de las actividades de la propuesta, desde cuándo, qué beneficios han tenido con ella y cómo es implementada. Los resultados de la entrevista pueden ser observados en la Tabla 5.4.

Tabla 5.4 – Resultados de la entrevista realizada a la empresa Softlogik S.A. de C.V.

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
PRO1	1	Establecer los Objetivos de Desempeño y Calidad	Solo los objetivos de calidad son establecidos	Desde siempre	Si, para establecer las pruebas y los requerimientos	Para establecer la estructura de los elementos que serán necesitados y para establecer las pruebas a realizar
PRO2	2	Establecer las Políticas y Plan de Seguridad	Solo cuando el cliente lo solicita	Desde siempre	Si, ya que queda establecido y plasmado los aspectos de seguridad que solicita el cliente	Para establecer los requerimientos del cliente
PRO3	3	Documentar todas las amenazas conocidas para el proyecto en cuestión	No	--	--	--
PRO3	4	Revisar el documento Top 10 de OWASP, para completar la documentación de amenazas conocidas	Si	Desde siempre	Si, conocer amenazas actuales	Es realizada durante la revisión de seguridad
PRO3	5	Identificar y Analizar escenarios de riesgos que permitan definir los impactos potenciales al proyecto en cuestión	Si	Desde siempre	Si, conocer los escenarios de riesgo	Es realizada durante la gestión de riesgos

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
PRO3	6	Identificar amenazas para aquellos activos identificados que pueden ser afectados	Si	Desde siempre	Si, conocer que activos pueden ser perjudicados	Es realizada durante la gestión de riesgos
PRO3	7	Identificar el resto de los riesgos	Si	Desde siempre	Si, conocer todos los riegos importantes de un proyecto en cuestión	Es realizada durante la gestión de riesgos
PRO3	8	Identificar impactos a la entidad o dependencia de la empresa desarrolladora de software	Si	Desde siempre	Si, conocer que entidad puede ser afectada por un riego materializado	Es realizada durante la gestión de riesgos
PRO3	9	Detectar los puntos más vulnerables del proyecto en cuestión	Si	Desde siempre	Si, se conoce y se pone una atención especial a los puntos vulnerables	Es realizada durante la gestión de riesgos
PRO4	10	Establecer las Actividades Preventivas	Si	Desde siempre	Tener tiempos cortos de desarrollo e identificar riesgos	Es implementada durante el desarrollo iterativo y con los clientes
PRO4	11	Establecer medidas de seguridad física	Si	Desde siempre	Si, evitar que personas no autorizadas tengan acceso al equipo de la empresa	Es implementada con cámaras de seguridad y restringiendo el acceso en los edificiones y en sitios de computadoras
PRO4	12	Establecer medidas de control de acceso físico	Si	Desde siempre	Si, para evitar que personas no tengan acceso a la empresa	Es implementada con cámaras de seguridad y restringiendo el acceso en los edificios y en

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
						sitios de computadoras
PRO5	13	Coordinar la implementación de los protocolos y medidas de seguridad	Si	Desde siempre	Si, para evitar fuga de información	Es implementada con autentificación de personal y con monitoreo de cámaras
PRO5	14	Establecer las políticas y protocolo de acceso a la información	Si	Desde siempre	Si, para evitar fuga de información	Es implementada con medidas de seguridad tomadas por la empresa
PRO5	15	Monitorear las redes y servicios del Cloud	Si	Desde siempre	Si, para tener un mejor control del correcto funcionamiento de las redes y servicios Cloud	Es implementada con medidas de seguridad tomadas por la empresa
PRO5	16	Instalar y mantener al día las herramientas de hardware y software necesarias para garantizar la seguridad de la plataforma Cloud	Si	Desde siempre	Si, para estar protegidos contra amenazas actuales	Es implementada con medidas de seguridad tomadas por la empresa
PRO5	17	Generar documentación de Referencia	Si	Desde siempre	Si, asi cuando una nueva persona se incorpora al equipo ya tiene documentos y manuales de que es lo que se realiza	Todos los diagramas de infraestructura están documentados
PRO6	18	Realizar notificaciones cuando un incidente haya sucedido	Si	Desde siempre	Si, así el equipo de trabajo puede atender inmediatamente el incidente	Existe una mesa de ayuda donde los incidentes son reportados
PRO6	19	Monitorizar el	Si	Desde	Si, conocer que	La mesa de

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
		estado y tiempo de respuesta esperado para la recuperación de un incidente		siempre	el incidente se esté atendiendo en tiempo y forma	ayuda está encargada de esta actividad
PRO6	20	Análisis del Incidente	Si	Desde siempre	Si, para conocer que lo provocó y como repararlo	La mesa de ayuda está encargada de esta actividad
PRO7	21	Generar una lista de verificación de acuerdos con el proveedor	Si	Desde siempre	Si, la credibilidad del proveedor	Es implementada en el proceso de gestión de proveedores
PRO7	22	Monitorear avance y desempeño del proveedor	Si	Desde siempre	Si, conocer cómo va el cumplimiento del proveedor	Es implementada en el proceso de gestión de proveedores
PRO7	23	Revisar el cumplimiento del contrato del proveedor	Si	Desde siempre	Si, para conocer qué tan responsable es el proveedor	Es implementada en el proceso de gestión de proveedores
PRO8	24	Evaluar el complimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs	Si	Desde siempre	Si, para conocer si no ha habido fallos de seguridad	Todos los SLA son acordados, pero no hay un documento físico en donde son evaluados
PRO8	25	Mantener al día el plan de Seguridad y las secciones de seguridad de los SLAs	Si	Desde siempre	Si, solo se hace de una manera interna y se está preparado para tendencias actuales de seguridad	Es realizado internamente y es realizado mientras el proyecto no sea terminado
PRO9	26	Establecer el plan de prevención de riegos	Si	Desde siempre	Si, Genera prestigio a la empresa	Es realizado automáticamente por los diferentes especialistas de la empresa
PRO9	27	Establecer el plan de gestión	Si	Desde siempre	No, se depende mucho de una	Es realizado en parte con el

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
		de emergencias			sola persona	cliente, y toda la responsabilidad recae en el director de operaciones de la empresa
PRO9	28	Establecer el plan de recuperación	Si	Desde siempre	Si, ya que ahorra tiempo y tiempo es dinero	Un plan de recuperación de desastres es implementado
PRO10	29	Identificar los requerimientos de las leyes, reglamento y regulaciones aplicables	Si	Desde siempre	Si, da prestigio a la empresa porque realiza proyectos de acuerdo a la ley	Es realizado antes de realizar un propuesta del software a desarrollar
PRO11	30	Establecer los SLAs, OLAs y UCs	Si	Desde siempre	Si, da prestigio porque todo queda plasmado en los documentos	Los OLAs son realizados internamente, los SLAs son establecidos antes de realizar la propuesta del cliente y los UCs son implementados en Compulogic
PRO11	31	Monitorear la calidad de la plataforma Cloud	Si	Desde siempre	Si, ayuda a detectar fallas lo más pronto posible	Es implementada con empresas asociadas como Microsoft y Cisco
PRO11	32	Elaborar reportes sobre la calidad de la plataforma Cloud	Si	Desde siempre	Si, conocer y tener plasmado el comportamiento que está teniendo la plataforma de la nube	Es realizada durante el monitoreo de la nube y se generan reportes
PRO12	33	Actualización y auditorias sobre la plataforma Cloud	Si	2 meses	Si, tener al día la plataforma y ayuda a detectar la falla lo más pronto posible	Es implementada bajo los estándares ISO 9000 e ISO 20000
PRO12	34	Generación de	Si	Desde	Si, conocer	Existe un

Proceso	#	Práctica	¿Es Implementada?	¿Desde cuándo?	¿Tuvo algún Beneficio? ¿En qué?	¿Cómo es implementada?
		Logs de la plataforma		siempre	quién ha entrado al sistema y que realizó	servidor de logs que realiza esta actividad
PRO13	35	Revisar los requerimientos de seguridad de la plataforma Cloud	Si	Desde siempre	Si, permite solo tener pocos problemas	Es realizada durante la licitación de requerimientos
PRO14	36	Revisar las políticas y estándares de seguridad	Si	Desde siempre	Si, ayuda a tener un mejor control y seguridad	Ha sido reforzada y se realiza bajo los estándares de ISO 9000 es ISO 20000
PRO15	37	Establecer mecanismos de seguridad en las vías de comunicación de la aplicación en desarrollo	Si	Desde siempre	Si, evitar que la información sea interceptada por terceros	Es realizada durante la implementación del software
PRO16	38	Gestión de los usuarios que tendrán acceso a la aplicación Cloud	Si	Desde siempre	Si, para que usuarios no autorizados tengan acceso a información confidencial	Es realizada durante el diseño del software
PRO17	39	Realizar pruebas de penetración a la aplicación Cloud	Si	Desde siempre	Si, ayuda a desarrolla una aplicación menos vulnerable a ataques	Es realizada durante las pruebas del software, por medio de un software especializado
PRO18	40	Educar a los usuarios en cuestiones de seguridad	Si	Desde siempre	Si, ya que son menos llamadas, menos soporte y mayor fidelidad a la empresa	Es realizado cuando el software es entregado al cliente

Como visto anteriormente, la fábrica de software Softlogik S.A. de C.V. que trabaja en conjunto con la empresa Compulogic, en su conjunto cumple con gran parte de la

propuesta realizada para solucionar la privacidad e integridad de datos para el desarrollo de aplicaciones del cómputo en la nube, estando dentro del marco de la norma MoProSoft. Además se puede inferir que todas aquellas actividades que son realizadas por la empresa respetan el manifiesto ágil, ya que Softlogik S.A. de C.V. es una empresa que trabaja puramente con metodologías ágiles.

Solo son 3 actividades no realizadas por Softlogik S.A. de C.V.:

(1) Establecer y documentar los objetivos de Calidad y Rendimiento.
(2) Definir Planes y políticas de seguridad.
(3) Documentar todas las amenazas conocidas del proyecto en cuestión.

Softlogik S.A. de C.V. desarrolla software bajo la combinación de las metodologías agiles de Kanban, Scrum y XP, pero durante el desarrollo de un proyecto, se maneja la fase de preventa y es aquí donde se pueden introducir las actividades (1) y (2), sin tener impacto alguno a la metodología ágil.

Dentro de Softlogik S.A. de C.V. la práctica (1) se desarrolla parcialmente, ya que solo los objetivos de calidad son establecidos más no plasmadas, y estos son utilizados para establecer las pruebas a realizar una vez que el sistema de software haya sido desarrollado, pero es necesario que estos sean documentados al igual que los objetivos de rendimiento para así formalizar los requerimientos solicitados por el cliente y tenerlos como referencia para otras actividades dentro del proyecto cómo el establecimiento de pruebas. Estos objetivos no deben de ser fijos, ya que de acuerdo al segundo principio del manifiesto ágil, los requerimientos pueden cambiar en cualquier momento.

La práctica (2) es solo realizada cuando el cliente lo haya solicitado, ya que muchos clientes desconocen la gravedad de los problemas de seguridad informática presentados hoy en día, pero como medida de prevención esta práctica debe de ser realizada ya que dará un mayor prestigio a Softlogik S.A. de C.V. por desarrollar aplicaciones seguras. Al igual que la práctica (1) los planes y políticas de seguridad pueden ser modificables y así cumplir con el segundo principio del manifiesto ágil.

Finalmente la práctica (3), es una práctica muy sencilla, ya que en cada proyecto son identificados todos los riesgos y solo es cuestión de documentarlos, formalizando esta información y haciendo más fácil su transmisión a todos los miembros del equipo de desarrollo. Además como es una tarea sencilla, basada en otra ya realizada anteriormente, no interfiere con la metodología ágil.

Tabla 5.5 – Prácticas, la necesidad a la que atacan y principio del manifiesto ágil al que se dirigen

Práctica	Solución a la necesidad	Problemas relacionados	Principio del Manifiesto Ágil
Establecer y documentar los objetivos de Calidad y Rendimiento.	▪ Privacidad de datos ▪ Integridad de datos	▪ Establecer el uso acordado de los datos del cliente ▪ Aseguramiento	▪ Segundo principio: "*Aceptamos que los requisitos cambien, incluso en etapas tardías*

		de la integridad de los datos del cliente	*del desarrollo. Los procesos Ágiles aprovechan el cambio para proporcionar ventaja competitiva al cliente*". ▪ Sexto principio: "*El método más eficiente y efectivo de comunicar información al equipo de desarrollo y entre sus miembros es la conversación cara a cara*".
Definir Planes y políticas de seguridad.	▪ Privacidad de datos ▪ Integridad de datos	▪ Establecer evidencias de que la información del cliente ha sido realmente eliminada ▪ Establecer el uso acordado de los datos del cliente ▪ Aseguramiento de la integridad de los datos del cliente	▪ Segundo principio: "*Aceptamos que los requisitos cambien, incluso en etapas tardías del desarrollo. Los procesos Ágiles aprovechan el cambio para proporcionar ventaja competitiva al cliente*". ▪ Sexto principio: "*El método más eficiente y efectivo de comunicar información al equipo de desarrollo y entre sus miembros es la conversación cara a cara*".
Documentar todas las amenazas conocidas del proyecto en cuestión.	▪ Privacidad de datos ▪ Integridad de datos	▪ Establecer el uso acordado de los datos del cliente ▪ Aseguramiento de la integridad de los datos del cliente	▪ Sexto principio: "*El método más eficiente y efectivo de comunicar información al equipo de desarrollo y entre sus miembros es la conversación cara a cara*".

Cómo visto en la Tabla 5.5 estas tres prácticas son sencillas y después de haber sido comparadas con el manifiesto ágil, únicamente se tiene relación con 2 de los 12 principios de este manifiesto. Estas prácticas abordan los problemas de privacidad e integridad de datos, y básicamente de formalización de información y su ejecución dentro de Softlogik S.A. de C.V. reforzará el sexto principio del manifiesto ágil, ya que con documentación en mano y una comunicación cara a cara, aumenta la eficiencia y eficacia de la comunicación de información dentro del equipo de desarrollo.

Cada de una de estas tres prácticas no cumplidas en la empresa Softlogik S.A. de C.V. son de gran importancia para asegurar una mejor integridad y privacidad de datos, ya que la práctica (1) se puede establecer y documentar en cuestiones de calidad y desempeño como deberán ser utilizados los datos del cliente al igual que establecer el nivel de seguridad para asegurar la integridad de los datos del cliente. En la práctica (2) permite definir las políticas y planes de seguridad, los cuales abarcan en como deberán ser tratados los datos del cliente, de esta manera se le podrá comprobar al cliente que sus datos han sido eliminados y los mecanismos de seguridad que serán implementados para asegurar la integridad de los datos del cliente, finalmente en la práctica (3) nos permite conocer y tener documentado cada una de las amenazas que pueden afectar el uso de los datos del cliente y que puedan comprometer la integridad de estos datos.

Ya que Softlogik S.A. de C.V. realiza gran parte de las actividades del proceso propuesto, y con lo justificado anteriormente, podemos concluir que el proceso presentado respeta cada uno de los 12 principios del manifiesto ágil.

5.2 Conclusiones

Con la implementación de los tres filtros para la selección de prácticas de las diferentes normas y estándares analizados, se logró la creación de un proceso formal para el desarrollo de software dentro del cómputo en la nube, abordando específicamente los problemas de privacidad e integridad de datos que se presentan dentro de este ambiente.

A partir de las prácticas extraídas, se cubren directamente problemas relacionados con la *intercepción de mensajes*, como el aseguramiento de canales de comunicación, gestión de incidentes, establecimiento de políticas de seguridad, gestión de riesgos, entre otras más. Para los problemas relacionados con el *establecimiento del uso acordado de los datos del cliente*, hay actividades como establecimiento de SLAs, monitorización de los servicios, administración de proveedores entre otros más para abordar este problema. Y finalmente para el problema de *la falta de evidencias que la información del cliente ha sido realmente eliminada*, hay prácticas para llevar un mejor seguimiento a los SLAs que atacan parcialmente este problema, ya que explícitamente no está establecido que durante la elaboración del SLA se debe incluir que se entregaran evidencias de que la información del cliente realmente ha sido eliminada de la nube.

Además considerar que el proceso deberá de respetar los 12 principios del manifiesto ágil, aumenta el rango de empresas que puedan implementar esta propuesta.

Haber evaluado la factibilidad del desarrollo de este proceso dentro de la empresa de Softlogik S.A. de C.V., permitió conocer si realmente este proceso puede ser aplicable o no, además de conocer qué y cómo son implementadas dichas prácticas y lo beneficios que han brindado ya dentro de la práctica dentro de la empresa.

Al aplicar la entrevista en Softlogik S.A. de C.V. se encontró que se realizaban el 92.5% de las actividad contendidas en el proceso, esto se debe a que la mayoría del personal cuenta con gran experiencia y ha laborado en sectores de gobierno e iniciativa privada en donde han afrontado con grandes retos.

Con los resultados obtenidos en base a la entrevista realizada a Softlogik S.A. de C.V. se puede concluir que la propuesta realizada aquí es factible para su implementación dentro del desarrollo de servicios de software. Como trabajo futuro se debe de realizar un análisis si existe o no diferencia alguna en las aplicaciones del cómputo en la nube desarrolladas antes y después en la implementación del proceso aquí propuesto en cuestiones de integridad y privacidad de datos.

Capítulo 6. Conclusiones

Se hizo un estudio en la presente tesis de maestría para ofrecer una mejor privacidad e integridad de datos enfocado a las pymes que desarrollan software ágil para el entorno del cómputo en la nube. Para esto se analizaron los diferentes problemas como lo son:

1. La generación de evidencias de que la información del cliente realmente ha sido eliminada.
2. El uso acordado de los datos del cliente.
3. El aseguramiento de la integridad de los datos de cliente.

En relación a estos problemas se buscó una primer solución dentro de las normas y modelos de gestión de riesgos y mantenimiento de software. En la solución se encontraron diversas prácticas resultantes de aplicar los tres filtros de extracción mostrados en la Figura 4.2, (1) selección de prácticas de gestión de riesgos y mantenimiento de software, (2) selección de prácticas de privacidad e integridad de datos, y (3) mejora y adaptación al entorno del cómputo en la nube.

Durante la mejora e integración de prácticas al marco de trabajo de MoProSoft, se pudo observar que algunas de ellas encajaban perfectamente en la norma, otras eran actividades mucho mejor definidas a lo que está dentro de la norma, y finalmente muchas otras prácticas eran completamente nuevas a la norma pero por la descripción de las categorías de cada uno de los niveles básicos de la estructura de la organización manejados en dicha norma. Y finalmente obteniendo un proceso para el desarrollo de servicios de software que permite estar dentro de MoProSoft.

El proceso resultante fue analizado dentro de la empresa Softlogik S.A. de C.V. en donde se pudo verificar que un 92.5% de las prácticas ya son realizadas dentro de la empresa, haciendo altamente factible su completa adopción dentro de la empresa. Las 3 prácticas no realizadas por la empresa fueron analizadas y ajustadas para que respetaran el manifiesto ágil, generando así un proceso de desarrollo ágil para aplicaciones del cómputo en la nube. Estas actividades afrontan los problemas de privacidad e integridad de datos que son:

- La documentación de objetivos de calidad y rendimiento,
- La documentación de amenazas conocidas
- El establecimiento de políticas y planes de seguridad.

Esta propuesta presenta una gran flexibilidad la cual puede ser utilizada en tres diferentes formas:

1. En empresas que estén certificadas o en vías de certificación dentro de MoProSoft y quieran ofrecer servicios de software con privacidad e integridad de datos.
2. En empresas que implementen metodologías ágiles con el mismo ofrecimiento de servicios.

3. En empresas que planifiquen implementar MoProSoft y metodologías ágiles.

El objetivo de esta tesis de maestría es: *"Crear una propuesta de proceso a nivel de prácticas de desarrollo de software ágil que cumpla con MoProSoft integrando prácticas de mantenimiento, servicio y seguridad, para generar evidencias de que la información del cliente realmente ha sido eliminada, establecer el uso acordado de los datos del cliente y establecer el aseguramiento de la integridad de los datos con el cliente dentro de un ambiente de cómputo en la nube"*. Con el proceso obtenido en el capítulo anterior, podemos llegar a la conclusión, que dicho proceso, desde el punto de vista de desarrollo de servicios de software, aborda los problemas de privacidad e integridad de datos, estando dentro del marco de trabajo de MoProSoft y respetando cada uno de los 12 principios del manifiesto ágil.

Con las prácticas extraídas, podemos ver que muchas de ellas cubren directamente problemas relacionados con la *intercepción de mensajes*, y el *establecimiento del uso acordado de los datos del cliente*, pero para el problema de *la falta de evidencias que la información del cliente ha sido realmente eliminada* no hay prácticas que aborden directamente este problema, ya que no hay prácticas que explícitamente establezcan que durante la elaboración del SLA se debe incluir que la entrega de evidencias de que la información del cliente realmente ha sido eliminada de la nube.

En conclusión y con lo dicho anteriormente, el proceso aquí establecido, fue elaborado con prácticas de mantenimiento, servicio y seguridad de las diferentes normas y estándares analizadas. Dicho proceso se encuentra dentro del marco de trabajo de MoProSoft, respeta cada uno de los 12 principios del manifiesto ágil y aborda los problemas del aseguramiento de la integridad de los datos del cliente y el uso acordado de los datos de este, pero el problema de la comprobación de la eliminación de los datos del cliente, es parcialmente cubierto, ya que ninguna práctica establece explícitamente mecanismos para realizar dicha comprobación, solo se establecen prácticas para un mejor seguimiento de los SLAs para abordar dicho problema. Por lo tanto el objetivo queda parcialmente cubierto, pero la propuesta aborda en gran parte estos problemas de privacidad e integridad de datos que preocupan a los usuarios de la nube. El proceso expuesto brinda una solución a nivel propuesta, sin embargo no se ha ejecutado una validación de esta propuesta en uno o más proyectos de desarrollo de SaaS.

La propuesta aquí presentada se enfocó principalmente en estar dentro del marco de MoProSoft, en donde hace falta realizar, en base a este proceso propuesto aquí, la creación de un proceso en el cual una pyme pueda certificarse en la norma MoProSoft.

Además hace falta conocer que tan efectivo es el proceso propuesto aquí ante los problemas de privacidad e integridad de datos presentados ante el cómputo en la nube. La evaluación debe de ser realizada mínimamente ante dos o más servicios de software de diferentes empresas, para que así se puedan realizar los ajustes necesarios a esta propuesta para cumplir con los objetivos establecidos en este documento. A partir de esto se podrán generar estadísticas de la efectividad que presenta este proceso, y así la

empresa desarrolladora de software pueda utilizarlas a su favor para convencer a todos aquellos clientes que no estén convencidos de implementar una solución SaaS por los problemas de privacidad e integridad de datos dentro del cómputo en la nube.

Una vez que el proceso sea evaluado y ajustado de acuerdo a las necesidades actuales de las empresas de software, se deberá de crear indicadores de medición para cada una de las prácticas, y así cuando una empresa desee adoptar dicho proceso, pueda medir cada una de las nuevas prácticas que está incorporando a su proceso de desarrollo de software para el ambiente del cómputo en la nube.

Referencias

[1] B. Furht and A. Escalante, *Handbook of Cloud Computing*. New York: Springer, 2010, p. 634.

[2] S. Zhang, S. Zhang, X. Chen, and X. Huo, “Cloud Computing Research and Development Trend,” *2010 Second International Conference on Future Networks*, pp. 93–97, Jan. 2010.

[3] A. Khalid, “Cloud Computing: Applying Issues in Small Business,” *2010 International Conference on Signal Acquisition and Processing*, pp. 278–281, Feb. 2010.

[4] T. Dillon, C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 27–33, 2010.

[5] Y. Wei, M. B. Blake, and N. Dame, “Service-Oriented Computing and Cloud Computing Challenges and Opportunities,” 2010.

[6] M. Laanti, O. Salo, and P. Abrahamsson, “Agile methods rapidly replacing traditional methods at Nokia: A survey of opinions on agile transformation,” *Information and Software Technology*, vol. 53, no. 3, pp. 276–290, Mar. 2011.

[7] “Secretaría de Economía - Tecnologías de la información TI.” [Online]. Available: http://www.economia.gob.mx/comunidad-negocios/industria-y-comercio/informacion-sectorial/tecnologias-de-la-informacion-ti. [Accessed: 17-Apr-2013].

[8] NYCE, “NMX-I-059-NYCE-2011 (MOPROSOFT).” [Online]. Available: http://www.nyce.org.mx/verificacion/ti.aspx. [Accessed: 27-Oct-2012].

[9] H. Oktaba, “Modelo de Procesos para la Industria de Software MoProSoft Agosto 2005 Grupo Editor :,” 2005.

[10] I. Macfarlane, A. Cartlidge, A. Hanna, C. Rudd, J. Windebank, S. Rance, X.- Steria, HP, itEMS Ltd, IBM, and Sun, *An Introductory Overview of ITIL ® V3 An Introductory Overview of ITIL ® V3*. The UK Chapter of the itSMF, 2007.

[11] Unidad De Gobierno Digital, “Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones,” p. 372, 2010.

[12] “OWASP Application Security Verification Standard - Web Application Standard.” p. 38, 2009.

[13] A. Agarwwal, D. Bellucci, and A. Coronel, *OWASP Testing Guide v3. 0*. 2008.

[14] A. Kang, A. Wiesmann, A. Russell, A. Klein, A. van der Stock, B. Greidanus, C. Todd, D. Grundy, D. Endler, D. Piliptchouk, D. Groves, D. Browne, E. Kary, E. Arroyo, F. Lemmon, G. McKenna, H. Lockhart, I. By-Gad, J. Poteet, J. P. Arroyo, K.

K. Mookhey, K. McLaughlin, M. Curphey, M. Eizner, M. Howard, M. Simonsson, N. Krawetz, N. Tranter, R. Endres, R. Stirbei, R. Parke, R. Hansen, R. McNamara, S. Taylor, S. Huseby, T. Smith, and W. Hau, *Una Guía para Construir Aplicaciones y Servicios Web Seguros*, 2.0 Black . 2005, p. 311.

[15] "Category:OWASP Legal Project - OWASP." [Online]. Available: https://www.owasp.org/index.php?title=Category:OWASP_Legal_Project&setlang=es. [Accessed: 01-May-2013].

[16] "S3M - Basic Process Management (0,1 and 2)." Redwood City, p. 34, 2008.

[17] "Principios del Manifiesto Ágil." [Online]. Available: http://agilemanifesto.org/iso/es/principles.html. [Accessed: 17-Feb-2013].

[18] "Softlogik Software Commpany." [Online]. Available: http://www.softlogik.mx. [Accessed: 09-Apr-2013].

[19] T. A. L. C. B. W. Mario Barbacci, Marck H. Klein, "Technical Report CMU/SEI-95-TR-021 ESC-TR-95-021," *Software Engineering Institute - Carnegie Mellon University*, no. December, 1995.

[20] L. Bass, P. Clements, and R. Kazman, *Software architecture in practice*, 2nd ed. Software Architecture in Practice, 2003, p. 560.

[21] Google, "Google Trends - Web search interest: Cloud Computing," 2012. [Online]. Available: https://www.google.com/trends/explore?q=Cloud+Computing#q=Cloud Computing&cmpt=q. [Accessed: 13-Mar-2012].

[22] I. Standard, "INTERNATIONAL STANDARD ISO 31000 - Risk management - Princples and guidelines," p. 36, 2009.

[23] I. Standard, *INTERNATIONAL STANDARD ISO / IEC 14764:2006 Software Engineering — Software Life Cycle Processes — Maintenance*, vol. 2006. 2006.

[24] "Nyce - Niveles de Capacidad MoProSoft." [Online]. Available: null.

[25] "Fundamentos de la Gestión TI - ITIL - ¿Qué es ITIL?" [Online]. Available: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php. [Accessed: 01-May-2013].

[26] "Curso ITIL v3 > ITIL v3." [Online]. Available: http://itilv3.osiatis.es/itil.php. [Accessed: 01-May-2013].

[27] "Qué es MAAGTIC - Instituto Politécnico Nacional." [Online]. Available: http://www.cgsi.ipn.mx/MAAGTIC-SI/Paginas/Que-es.aspx. [Accessed: 01-May-2013].

[28] “About The Open Web Application Security Project - OWASP.” [Online]. Available: https://www.owasp.org/index.php?title=About_OWASP&setlang=es. [Accessed: 01-May-2013].

[29] OWASP, “OWASP Top 10,” 2010.

[30] “S3M - Software Maintenance Maturity Model - Frequently Asked Questions.” [Online]. Available: http://www.s3m.ca/en/aboutUs/faq.html. [Accessed: 06-May-2013].

[31] J. Mejia, M. Muñoz, E. Muñoz, D. Estrada, A. Almaraz, and J. Mauricio, “Dirigiendo el Esfuerzo de la Mejora de Procesos Software en Pymes,” pp. 868–874, 2013.

Anexo 1. Sesión de derechos de autor

CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.

BIBLIOTECA

AUTORIZACION
PUBLICACION EN FORMATO ELECTRONICO DE TESIS

El que suscribe

Autor(s) de la tesis: I.S.C. Diego Estrada Jiménez

Título de la tesis: Proceso de Desarrollo de Software Ágil para preservar la Privacidad e Integridad de Datos en la Nube

Institución y Lugar: Centro de Investigación en Matemáticas, A.C. - Unidad Zacatecas

Grado Académico: Licenciatura ( ) Maestría (X) Doctorado ( ) Otro ( )

Año de presentación: 2013

Área de Especialidad: Ingeniería de Software

Director(es) de Tesis: Dr. Hugo Mitre Hernández, M.A. Juan Gabriel Hernández Carrillo

Correo electrónico: destrada@cimat.mx

Domicilio: Francisco I. Madero 208, Col. Centro, Moyahua de Estrada, Zacatecas

Palabra(s) Clave(s): Cómputo en la Nube, MoProSoft, Privacidad de datos, Integridad de datos, Desarrollo de software ágil, Seguridad en la nube

Por medio del presente documento autorizo en forma gratuita a que la Tesis arriba citada sea divulgada y reproducida para publicarla mediante almacenamiento electrónico que permita acceso al público a leerla y conocerla visualmente, así como a comunicarla públicamente en la Página WEB del CIMAT.

La vigencia de la presente autorización es por un periodo de 3 años a partir de la firma de presente instrumento, quedando en el entendido de que dicho plazo podrá prorrogar automáticamente por periodos iguales, si durante dicho tiempo no se revoca la autorización por escrito con acuse de recibo de parte de alguna autoridad del CIMAT

La única contraprestación que condiciona la presente autorización es la del reconocimiento del nombre del autor en la publicación que se haga de la misma.

Atentamente

_____

Nombre y firma del tesista

CALLE JALISCO S/N MINERAL DE VALENCIANA APDO. POSTAL 402
C.P. 36240 GUANAJUATO, GTO., MÉXICO
TELÉFONOS (473) 732 7155, (473) 735 0800 EXT. 49609 FAX. (473) 732 5749
E-mail: biblioteca@cimat.mx