UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL

(UCI)

PROYECTO FINAL DE GRADUACION PRESENTADO COMO REQUISITO

PARCIAL PARA OPTAR POR EL TITULO DE MÁSTER EN ADMINISTRACIÓN DE TECNOLOGIAS DE LA INFORMACION

DESARROLLO DE UN MODELO PARA LA EVALUACIÓN Y ADMINISTRACIÓN DE RIESGOS DE INFORMACIÓN A NIVEL DE TI EN PYMES DE LA CIUDAD DE MONTERÍA A PARTIR DEL MARCO DE TRABAJO COBIT 5

JOSE ANDRES DURANGO GARCIA

San José, Costa Rica

Mayo 2017

UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL

(UCI)

Este Proyecto Final de Graduación fue aprobado por la Universidad como

Requisito parcial para optar al grado de Máster en Administración de Tecnologías de la Información

_____

MSc. Fausto Fernández Martínez

PROFESOR TUTOR

_____

MSc. Marco Ugarte Ulate

LECTOR No.1

_____

MSc. Melissa Vincenzi García

LECTOR No.2

Ing. José Andrés Durango García

SUSTENTANTE

DEDICATORIA

Dedicar este proyecto a una sola persona, sería injusto, por eso quiero dedicarle este logro a todas las personas que han estado siempre para mi e incluso a las que no lo han hecho, a las personas que me han apoyado y a las que no, porque de todos aprendemos algo en la vida. Mi dedicatoria es para todas las personas que me han rodeado en la vida, porque todas han hecho que este sacrificio valga la pena, que haya valido la pena superarme como profesional y como persona; he aprendido de todos un poco y de eso se trata nuestra vida, de seguir aprendiendo hasta perfeccionar nuestro espíritu. Gracias a todos por todo lo que me han brindado, porque me han enseñado a llegar a la meta sin importar si soy ultimo o primero, a tomar mi propio camino y recorrerlo, algunos me han enseñado a no ser como ellos y otros solo me enseñan a vivir plenamente; pero más importante a mi madre Carmen García que lo ha sido y lo será todo en mi vida y mi esposa Liliana Sotelo que es la persona que escogí para que me acompañara el resto de mi vida.

AGRADECIMIENTOS

A Dios por ser el guía de mis actos y darme bendiciones constantemente.

A mi madre por haberme dado la vida y ser la mujer más luchadora del mundo, porque sola, ella pudo levantarme y ser mi ejemplo cada día.

A mi novia, quien hoy es mi esposa por ser mi impulso cada día a mejorar y quien me lanzo a hacer esta maestría, por tolerarme, aguantarme y sobre todo impulsarme a ser mejor esposo y mejor persona.

A mi familia por estar siempre aquí, cerca, donde más los quiero y donde más se necesitan y apoyarme en este proceso.

A mis amigos, porque fueron la familia que escogimos y siempre me dan lecciones.

A mis colegas y excompañeros, por ayudarme a realizar es proyecto.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

ÍNDICE DE ABREVIATURAS

CCTV: Circuito Cerrado de televisión. El cual se utiliza para monitoreo a través de cámaras de seguridad.

IAP: Investigación - Acción – Participación, es una metodología de investigación que funciona con la retroalimentación de la población objetivo.

MINCIT: El Ministerio de Comercio, Industria y Turismo de Colombia, es el ente encargado de propiciar y complementar la actividad comercial, la producción de bienes y gestionar el turismo en Colombia.

MINTIC: El Ministerio de Tecnologías de la Información y las Comunicaciones es la entidad que se encarga de diseñar planes y políticas para que la tecnología llegue a todos los departamentos y ciudades de Colombia.

PYMES: Comprende el marco empresarial de las pequeñas y medianas empresas, aunque a partir de 2008 se incluyeron las microempresas dentro de esta nomenclatura.

TI: Tecnologías de la Información o también por sus siglas en inglés IT (Information Technology), las cuales se refieren al uso de dispositivos tecnológicos como hardware y software en general para sacar provecho de la información.

TICs: Tecnologías de Información y Comunicación, se refiere al uso de recursos para el compartimiento de información a través de diversos canales de comunicación.

RESUMEN EJECUTIVO

El proyecto nació como una oportunidad de crecimiento para PYMES en la ciudad de Montería, ya que cifras del ministerio de industria y comercio y el ministerio de las TIC en Colombia, reflejan que muchas de las PYMES no cuentan con una gestión de riesgos que aborde los temas de TI, sobre todo aquellos que son estrictamente tecnológicos, es por tanto que surge este proyecto como iniciativa de solución viable y que se pueda adaptar a los parámetros de las micro, pequeñas y medianas empresas de la ciudad.

Las PYMES se verían beneficiadas en la medida en que adopten dicho modelo y lo apliquen, para así sacar el mejor provecho de las TIC en la empresa, de manera que se vea reflejado en temas tecnológicos como seguridad en la información, iniciativas de proyectos de TI, infraestructura de TI, software e información.

El proyecto tuvo como objetivo principal desarrollar un modelo el cual sea capaz de suplir necesidades para la gestión de riesgos de información a nivel de TI en las PYMES y/o que también pueda reforzarlos en aquellas organizaciones que ya estén establecidos como estrategia de negocio. Fue posible lograr cada uno de los objetivos planteados como metas específicas, para llegar a nuestro objetivo final, los cuales establecieron considerar un previo conocimiento general acerca de la problemática, ya sea de manera local o regional, para luego profundizar en las PYMES de la ciudad de Montería, esto con la intención de hallar puntos comunes dentro de las organizaciones investigadas entre sus estados actuales y los estados deseados con respecto a la administración y evaluación de riesgos de información a nivel de TI, de esta manera se pudo desarrollar el modelo y ahondar más en su perfeccionamiento a través de los profesionales de TI.

El proyecto se llevó a cabo en 4 etapas básicas del modelo de investigación acción-participativa, que son la pre-investigación donde su objetivo es tener un panorama general acerca de la situación a través de la recolección de información en diarios, artículos, prensa u otros medios que puedan brindar información acerca de la

problemática. Luego se encuentra la investigación la cual consiste en profundizar la problemática y segmentarla en las PYMES por medio de las entrevistas y encuestas para conocer el estado actual y el estado deseado de las organizaciones en la gestión de riesgos de información a nivel de IT; continuo a ello sigue la etapa de programación, la cual consiste en planificar y desarrollar el modelo de evaluación y administración de riesgos de información a nivel de TI basados en el marco de trabajo COBIT, teniendo como base el resultado de las encuestas previas y puntos comunes encontrados para cerrar las brechas entre el estado actual y el deseado del común de las organizaciones, de igual manera se incluye el ajuste de acuerdo los profesionales de TI y finalmente en la última etapa se concluye nuestro proyecto realizando las recomendaciones y conclusiones adecuadas.

Se obtuvo el modelo de evaluación y administración de riesgos de información a nivel de TI, el cual cierra las brechas entre el estado actual y el estado deseado de acuerdo al marco de trabajo COBIT sobre las PYMES de la ciudad de Montería, siguiendo las actividades descritas como parte del modelo, las cuales no necesariamente son de estricto cumplimiento para la implementación del mismo.

Las organizaciones que deseen implementar el modelo desarrollado deben tener en cuenta que los pasos no son de estricto cumplimiento, teniendo en cuenta que hay organizaciones unas más grandes que otras, haciendo que su personal para la ejecución y puesta en marcha del modelo sea escaso, lo que dificultará el proceso. Las organizaciones también se necesitarán conocimientos básicos en COBIT, lo que les permitirá facilitar el proceso, ya sea en la designaciones de roles y responsabilidades como en la ejecución de actividades.

1 INTRODUCCION

1.1 Antecedentes

De acuerdo a cifras de la Cámara de Comercio de Montería para el 2016 existían aproximadamente más de 1500 empresas censadas en Montería, de las cuales en contraste con información de MinCIT las PYMES ocupan más del 85% en la ciudad, es decir, que en Montería existen más de 1000 (mil) Pymes, ocupando la mayor parte del comercio local. (Revista Dinero, 2016)

En estos momentos, se puede inferir que de acuerdo con estudios realizados al interior del Departamento de Córdoba en materia organizacional, todas las pequeñas y medianas empresas que existen en el departamento de Córdoba vinculadas al proceso productivo, requieren de grandes inversiones para poder enfrentar el reto de la competitividad para exportar en gran escala y ponerse de cara al tratado de libre comercio y por consiguiente al proceso de globalización de la economía con todas sus derivaciones; de otra parte puede decirse que el principal problema reportado es la falta de fondos, seguido por un incremento fuerte de la poca rentabilidad y, en menor medida, la carencia de mercado (Osorio, 2008).

Las PYMES en Montería han ocupado por varios años el 85% del mercado en Montería, pues a medida de que unas cierran sus instalaciones por diversos motivos, cada dia hay nuevos emprendedores, dispuestos a empezar una nueva etapa como comerciantes y/o negociantes. Esto se debe a que cada vez en colegios y universidades se enseña más la manera de cómo hacerlo, cómo ser emprendedor, cómo construir una empresa; para poder ser líder y trabajar por nuestras propias metas.

1.2 Problemática

El riesgo ha existido inherente a cada acción que realiza el ser humano. Sin embargo, en la sociedad actual, inmersa en un ambiente altamente tecnológico y donde la información es el centro de las actividades, se ha desarrollado una

creciente dependencia de las TI, lo que las ha convertido en un gran factor de riesgo y quizás, uno de los más importantes de este siglo. Por supuesto, las empresas no han sido ajenas a este proceso porque, al apoyarse en TI para mejorar su eficiencia y productividad, entregan a éstas una buena porción de responsabilidades críticas para el negocio. Pero no existe tecnología perfecta, todas presentan deficiencias, vulnerabilidades, errores, entre otros. Además, si los procesos de negocio dependen de TI, el riesgo incrementa y más aún si esta tecnología es utilizada por personas en el desarrollo de dichos procesos. Lo anterior genera lo que se conoce como riesgo de TI; es necesario gestionar estos riesgos porque no hacerlo puede generar altos costos para la organización. (Gomez, 2010)

Cuando se trata de adoptar TI, una continua preocupación en las empresas es adaptar sus procesos empresariales y asegurar sus sistemas de información, minimizando los riesgos asociados a la incorporación de las nuevas tecnologías, de forma que éstas mejoren los procesos y no repercutan de forma negativa en la empresa. En este contexto, la seguridad de las TI trata los incidentes más relevantes, medidas, controles y procedimientos aplicados por las empresas, con el fin de garantizar la integridad, confidencialidad y disponibilidad, de sus datos y de los sistemas de TI. (De la Camara M., 2015)

El problema radica como una oportunidad de crecimiento para las PYMES en la ciudad de Montería, siendo TI un factor fundamental en la continuidad y crecimiento de los negocios. Estas organizaciones no cuentan con el presupuesto suficiente y la experticia en su equipo de TI para implementar un estándar o marco de mejores prácticas, el cual pueda evaluar y administrar los riesgos de Información a nivel de TI de una mejor manera.

La gestión de riesgos se realiza para decidir qué acción se puede tomar con respecto a aquellos eventos que pueden afectar la integridad de la empresa, ya sea negativa o positivamente, de este modo y tratándose de los temas de IT se enuncia la siguiente pregunta:

¿De qué manera se pueden gestionar los riesgos de información a nivel de TI de las Pymes en Montería, teniendo en cuenta los parámetros y restricciones de conocimiento y recursos?

1.3 Justificación del problema

Entendiendo la información como la mayor ventaja competitiva de una organización dentro de un mercado cambiante y creciente, es indispensable que todas las empresas de la ciudad de Montería, una ciudad que también está en continuo crecimiento y expansión, cuenten con un modelo para el análisis de riesgos de información a nivel de TI, para que de esta forma la gerencia de las PYMES pueda entender con mayor aforo, cómo estos pueden afectar de manera directa o indirecta la continuidad del negocio.

De acuerdo a lo anterior, este proyecto busca principalmente una alternativa de solución para aquellas empresas y organizaciones que dentro de sus actividades estratégicas y de competencia se benefician de las tecnologías y la información, pero desconocen los riesgos de información a los que están expuestas las áreas de TI, por tal motivo este proyecto busca de manera asertiva crear un modelo de implementación para aquellas micro, pequeñas y medianas empresas que no cuentan con un sistema de evaluación y administración de riesgos de información a nivel de TI.

Es importante resaltar que las PYMES en la ciudad de Montería en su gran mayoría no cuentan con un presupuesto y la experiencia suficiente para implementar un estándar de alto nivel como ITIL, COBIT, ISO 27001 u otro, es por tanto que este proyecto dentro de sus objetivos también pretende ajustarse a dichos parámetros, ya que el producto resultante de este proyecto, es un modelo de gestión de evaluación y administración de riesgos de información a nivel de TI, donde su base tal y como está enunciada en su título es COBIT, que es un marco de mejores prácticas de TI aceptado internacionalmente, el cual abarca toda la gestión de TI como un activo estratégico y fundamental para la organización. Según BITCompany

(2014) “COBIT es el marco de mejores prácticas más completo y amplio dentro de esta gama de estándares para organizaciones”.

1.4 Objetivo general

Diseñar un modelo para la evaluación y administración de riesgos de información a nivel de TI, para PYMES en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT.

1.5 Objetivos específicos

- Diagnosticar el estado actual de la gestión de riesgos de información dentro del área de IT de las PYMES en la ciudad de Montería, con el fin de conocer el estado actual de acuerdo al estándar COBIT para iniciar la búsqueda del estado deseado.
- Establecer un estado deseado común de las organizaciones encuestadas en cuanto al proceso de gestión de riesgos de IT, para identificar puntos comunes de las distintas organizaciones en el desarrollo de los procesos de gestión de riesgos de IT, estableciendo un consenso de acuerdo a los parámetros encuestados.
- Planear y desarrollar el modelo a partir del estado deseado común de las organizaciones y recomendaciones basadas en profesionales de TI, incluyendo otros marcos de gestión de riesgos de TI, con el fin de cerrar la brecha entre el estado actual y el estado deseado de las organizaciones con respecto al proceso de gestión de IT.

2 MARCO TEORICO

2.1 Marco institucional

Comprendiendo como base del proyecto un modelo a desarrollar a partir de ciertos parámetros establecidos por las PYMES en la ciudad de Montería-Colombia, se hace referencia al marco constitucional de las PYMES y su clasificación.

2.1.1 Marco constitucional de las PYMES

En Montería se ha convertido en un fenómeno el uso de las TIC en las empresas, ya sea por moda, por ventaja competitiva, por decisión administrativa o simple gusto del área gerencial. Con la llegada de las TIC a las empresas, muchas han optado por modelos y sistemas informáticos que les permitan agilizar sus procesos, desde lectores de tarjeta hasta sistemas de inteligencia de negocio y otros más, lo que les permite a muchas empresas ganar una ventaja competitiva en relación a aquellas que no han entrado en esta nueva metodología de negocio, la cual ya ha sido implementada en varios países a través del uso de las TIC.

Las Pymes por su parte corresponden al 80% del mercado nacional en Colombia *(Revista Dinero, 2016)* y cifras de la Cámara de Comercio de Montería revelan que, de la totalidad de las empresas en Montería las pymes representan mucho más que el 85%, lo que indica que en la ciudad estas están por encima de la media nacional.

Cuadro 1: Clasificación de las PYMES en Colombia

Clasificación de las PYMES		
Tipo	Número de empleados	Activos
Micro	Menos de 10	344´727.000 COP
Pequeñas	De 11 a 50	3.447´720.000 COP
Medianas	De 51 a 200	20.683´620.000 COP

Fuente: (MINCIT, 2016)

Para todos los efectos, se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana, que responda a los parámetros enunciados adelante (Colombia, C. D., 2000).

El Ministerio de Comercio, Industria y Turismo (MINCIT) también afirma que el 65% de las empresas que utilizan los servicios de TI como ventaja competitiva desconoce los riesgos de TI a los que se enfrenta y el 33% de esas empresas clausuran en su segundo año de mercado debido a estos factores. Por lo tanto este componente necesita ser analizado para intentar buscar soluciones que se amolden a los parámetros de las PYMES en Montería.

Es por ello que este proyecto pretende como objetivo principal desarrollar un modelo de evaluación y gestión de riesgos de información a nivel de TI basados en COBIT, en la ciudad de Montería, el cual pueda ser adaptado a los parámetros de las PYMES que componen el mercado local de la ciudad.

- **Mediana Empresa**:

Planta de personal entre cincuenta y uno (51) y doscientos (200) trabajadores; Activos totales por valor entre cinco mil uno (5.001) y quince mil (15.000) salarios mínimos mensuales legales vigentes.

- **Pequeña Empresa:**

Planta de personal entre once (11) y cincuenta (50) trabajadores;

Activos totales por valor entre quinientos uno (501) y menos de cinco mil (5.001) salarios mínimos mensuales legales vigentes.

- **Microempresa:**

Planta de personal no superior a los diez (10) trabajadores;

Activos totales por valor inferior a quinientos uno (501) salarios mínimos mensuales legales vigentes. (Colombia, C. D., 2000)

2.2 IT dentro de las PYMES

Según estudios realizados por docentes de distintas universidades en el tema de tecnologías de la información, en Montería son muy pocas las empresas que cuentan con un departamento de TI correctamente gestionado, donde sus procesos centrales estén en un nivel aceptable u óptimo; esto se da, debido a que no cuentan con personal calificado el cual pueda garantizar procesos óptimos y estables durante un periodo de tiempo considerable, para garantizar la continuidad de los procesos de negocio. (Departamento de TI, 2009)

Por otra parte y de acuerdo a lo anterior se puede deducir que los riesgos empresariales a los que se enfrenta las organizaciones en términos de información a nivel de TI son muchos y su probabilidad aunque sea baja, tendrán un alto impacto sobre las organizaciones, ya que si no cuentan con el personal calificado será difícil conseguir que dichas organizaciones puedan alcanzar niveles óptimos o aceptables en términos de procesos de gestión de riesgos.

Este problema se presenta complementando con la información anterior, debido a que las organizaciones que tienen un departamento de TI prefieren contratar personal con formación técnica, a personal con formación profesional especializada, lo cual se hace de manera ocasional para “apagar incendios” del entorno de procesos estratégicos y administrativos del área de TI; de esta manera las empresas “ahorran recursos” sin entender cómo un profesional de TI puede contribuir a los objetivos de negocio continuamente.

> Un estudio realizado en 2012 en Europa, encontró que las Pymes están destinando más recursos para sus departamentos de TI. En el transcurso del año, los presupuestos han incrementado, en promedio, de US$ 152.000 a US$ 162.000 al año. Sin embargo, la contratación de personal no ha aumentado. Solo el 26% de las Pymes tienen planes de contratar personales de TI en el segundo semestre de 2012, una disminución frente al 31% de 2011. (Santos, 2012).

En relación a las microempresas, es decir, empresas con menos de 10 empleados y activos por menos de 500 salarios mínimos vigentes, El 60% de los encuestados aseguran que no usan internet simplemente porque no creen que lo necesiten, o solo lo utilizan de manera informal. Esta cifra obliga a pensar que hay una falta de educación sobre las ventajas de las tecnologías de información para hacer crecer una empresa y conseguir nuevos mercados. También se puede especular que muchos microempresarios piensan que usar internet es costoso, desconociendo las herramientas gratuitas pero exitosas que hay en la red para emprendedores (Santos, 2014).

> Además de las relaciones positivas entre la adopción de TI y el crecimiento empresarial, la investigación encontró los riesgos que tropiezan algunas compañías. Muchas Pymes no cuentan con acceso a redes de banda ancha y no tienen el recurso humano para la implementación de nuevas herramientas digitales. Otras empresas pequeñas todavía tienen hardware y software viejo que impiden el aprovechamiento de la tecnología. Las

> compañías también atribuyeron el bajo nivel de adopción a los costos de los equipos generados por los impuestos de importación y a la preocupación que genera la privacidad y seguridad en línea (Santos, 2013).

TI deberia jugar siempre un papel fundamental dentro de cualquier organización, teniendo el control de todos los sistemas de gestión de la organización, es decir, que TI es transversal a todos los procesos de una organización, y en la ciudad de Montería, solo hasta hace pocos años, las empresas se han dado cuenta de esa realidad, que TI es más que un departamento de equipos y dispositivos tecnológicos, el cual podría convertirse en el centro de la organización partiendo del punto de que manejan el activo más importante, la información.

2.2.1 La información como activo de las organizaciones

La información se define como los datos que han pasado por algún tipo de manejo o procesamiento y se pueden presentar de forma clara a los usuarios que dependen de ellos para tomar sus decisiones. Es por ello que las organizaciones han dejado atrás el capital financiero como su recurso más importante, sin que este pierda su importancia.

> Al considerar a la información como activo, se encuentra una denotación económica, mejor dicho en la economía de la información, la cual concibe una preocupación de la cantidad de información procesada en una organización, mediante la interacción de sus integrantes, para la toma de decisiones (Musiño, 2010).

Según un artículo de Business Value Exchange dice:

> La Información debe ser percibida como uno de los más importantes activos estratégicos de la empresa. Los sistemas de información y en concreto el ciclo de vida de ésta, tienen que dotar de palancas que habiliten nuevos canales de venta, incrementen el volumen de clientes sumergiéndolos en la globalización de los mercados, e incluso creen nuevas formas de consumir

> nuestros productos que propicien una imagen de marca verdaderamente especial. (Gallo, 2014, p4).

COBIT por su parte en su versión 4.1 define los criterios de la información, para poder establecer realmente un gobierno de TI.

- La **efectividad** atributo o criterio de información relativo a precisión de los datos.
- La **eficiencia** es el atributo que hace referencia al uso de los recursos para la generación de información.
- La **confidencialidad** se define como el nivel de seguridad y acceso a los datos.
- La **integridad** podria definirse como un sinónimo de la validez de la información, haciendo referencia a su precisión y cambios que se generen en ésta.
- La **disponibilidad** se refiere al momento de tiempo en que se requiera la información.
- El **cumplimiento** atributo que hace referencia a las leyes que debe cumplir la información, e incluso las que están por encima del nivel empresarial.
- La **confiabilidad** se refiere a la veracidad de los datos para tomar decisiones por parte de la gerencia de la organización.

De acuerdo a lo anterior se entiende que la información es crucial para los procesos de las organizaciones, y mas aún, tratándose de las PYMES, en donde la correcta gestión de la información puede ser decisiva a la hora de sacar ventajas competitivas.

Estos conceptos desde el punto de vista de las PYMES en la ciudad de Montería también hacen referencia a un mercado que hace más énfasis en la información, que en la compra-venta de productos, es decir, y de acuerdo al artículo de Santos (2013), las PYMES están invirtiendo más en sistemas de información y personal de

TI que maneje y gestione esos sistemas de información para sacar el mayor provecho de ésta, viendo reflejados esa inversión en sus objetivos de negocio y en sus finanzas a corto y mediano plazo.

2.2.2 Riesgos de información en PYMES

> La tendencia del mundo actual a emplear nuevos mecanismos para hacer negocios, a contar con información actualizada permanentemente que permita la toma de decisiones, ha facilitado el desarrollo de nuevas tecnologías y sistemas de información, que a su vez son vulnerables a las amenazas informáticas crecientes y por ende a nuevos riesgos (Ministerio de Agricultura y Desarrollo Rural, 2012).

"La gestión de riesgos de información se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos" (Universidad Nacional de Luján, 2013). Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riesgos que presentan los activos de información a niveles aceptables para la misma.

De acuerdo a cifras de la cámara de comercio, se entiende que las PYMES cada día están incrementando sus inversiones en TI, dándose cuenta de la realidad que las embarga, y es que pueden sacar mayor ventaja competitiva a partir de éstas. Las PYMES en su afán de crecimiento deberán invertir en personal de TI calificado, sistemas de información, computación en la nube entre otras herramientas, las cuales son vulnerables debido a la información que procesan.

Es aquí donde el proyecto comienza a tomar importancia, ya que las PYMES adquieren sus ventajas competitivas a través de TI, pero sin un marco de apoyo que sustente la importancia de la seguridad de la información a nivel de IT, ya sea por

desconocimiento de normatividad, falta de recursos, falta de experiencia, u otro motivo.

Según MINTIC entre los riesgos más comunes a los que está expuesta la información de los recursos de TI se encuentran los siguientes:

- ***SPAM***: El Spam o Correo electrónico no solicitado puede definirse como e-mails no deseados, habitualmente de tipo publicitario, que se envían aleatoriamente en grandes cantidades de usuarios. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.
- ***HOAX:*** es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos informan sobre virus desastrosos, otros apelan a la solidaridad con un niño enfermo o cualquier otra noble causa, otros contienen fórmulas para hacerse millonario o crean cadenas de la suerte como las que existen por correo postal. Los objetivos que persigue quien inicia un *hoax* son: alimentar su ego, captar direcciones de correo y saturar la red o los servidores de correo.
- ***Malware***: Con este nombre software malicioso (malware) se agrupan los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto.
- ***Phishing***: Cualquier mensaje que se recibe, bien por email, bien por SMS, o por cualquier otro medio, que suplanta a entidades que son de tu confianza solicitándote datos personales o contraseñas.
- ***Vishing****:* Es una vuelta de tuerca a la estafa, que combina teléfono e Internet. Recibimos un SMS de que se ha efectuado una compra con tarjeta de crédito en un establecimiento de nuestra zona a nuestro nombre, por ejemplo.

Alarmados, en lugar de buscar el teléfono de la sucursal o de atención al cliente de la entidad, utilizamos el número de teléfono que viene en el mensaje.

- ***Smishing:*** Es una técnica fraudulenta en la cual los delincuentes usan mensajes de texto a celulares para engañarte a través de técnicas de ingeniería social y obtener tu información.
- **Ingeniería Social**: La ingeniería social es la práctica de manipular psicológicamente a las personas para que compartan información confidencial o hagan acciones inseguras. La mayoría de veces, los ataques se realizar por medio de correo electrónico o por teléfono. Los atacantes se hacen pasar por otra persona y convencen a la víctima para entregar información sensible de la organización o sus contraseñas. Como es un tema más humano, las herramientas tecnológicas que implementan las compañías no pueden prevenir los ataques (ENTER.CO, 2016)

Esto por mencionar algunos, entre los más comunes.

También se puede mencionar que la información se encuentra en manos de usuarios, ya sea internos o externos de la organización lo cual indica que también es susceptible a riesgos, de ahí que la organización debe tener políticas internas de seguridad de la información fuera de las que ya existen reglamentadas por Colombia, como la ley de protección de datos, ley 1581 de 2012. (EL CONGRESO DE COLOMBIA, 2012).

2.2.3 Riesgos y TI

Para hablar propiamente de los riesgos es necesario definir y entender conceptos previamente:

Según Serfinansa (2014) “el riesgo es una amenaza, peligro o incertidumbre a que se ve enfrentada la organización por un evento o acción relacionada con sus objetivos, líneas de negocios, operaciones y demás actividades, que pudiera afectar el logro de sus objetivos”.

ISACA (2009, p. 21) define:

> Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos.

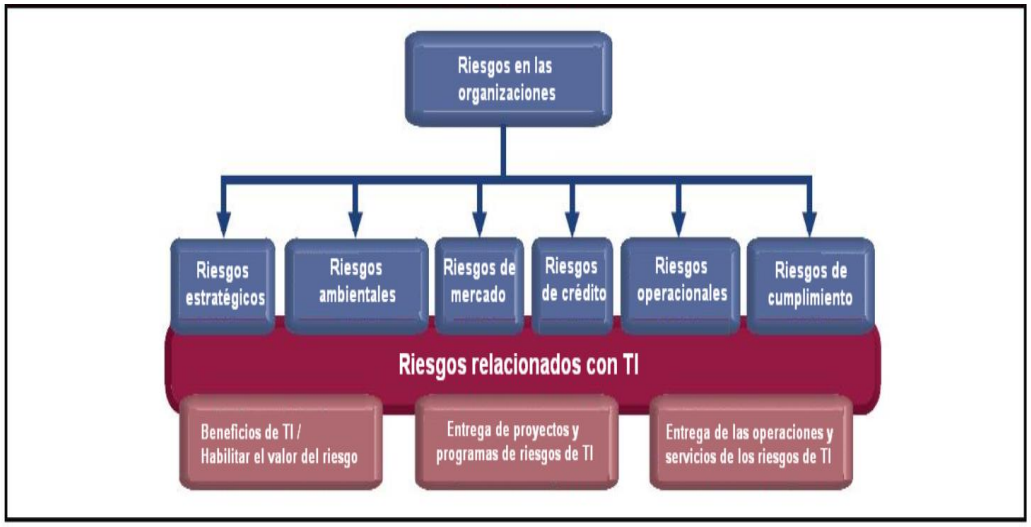


Ilustración 1: Riesgos de TI en la jerarquía de riesgos

Fuente: (ISACA, 2009, p.28)

Toda organización siempre estará expuesta a los riesgos, ya sea internos como de negocio, de proyectos, fallas en los equipos, errores humanos, etc., asi como también a los riesgos externos que habitan en el mercado como legislaciones, leyes, normas, clientes, proveedores, etc. De igual manera también existen los riesgos de TI anteriormente definidos, que comprenden todos aquellos riesgos a los que está expuesta una organización que utiliza servicios de TI, comprendido desde dispositivos electrónicos hasta herramientas de crecimiento organizacional. La información también tiene sus riesgos, los cuales pueden ser significativamente perturbadores para la organización dependiendo de qué información fue indebidamente manipulada, alterada o simplemente observada por entes no

organizacionales. En este aspecto los riesgos de información a nivel de TI son riesgos de información asociados al uso de las tecnologías de información y comunicación, que al ser la información el activo más importante y las tecnologías de información herramientas significativas pero con grandes riesgos detrás, estos riesgos podrian presentarse en cualquier escenario.

Una vez dicho esto, también se debe entender que existen distintos marcos de trabajo para la gestión de riesgos que ayudan a las organizaciones en el proceso de administración de riesgos, que para este proyecto se segmentará y se profundizará en los riesgos de información a nivel de TI.

En el manual de preparación para el examen CISM, ISACA (2012, p.47) establece:

> La gestión de riesgos es el objetivo principal de todas las actividades relacionadas con la seguridad de la información y, en realidad, de todos los esfuerzos realizados con respecto al aseguramiento organizacional. Aún cuando la efectividad en la gestión de riesgos no está sujeta a una medición directa, existen indicadores que guardan una estrecha relación con un enfoque exitoso. Un programa exitoso de gestión de riesgos puede definirse como aquel que cumple con las expectativas y alcanza objetivos definidos de manera efectiva y consistente.

Para continuar con la administración de riesgos también se deben definir los siguientes conceptos; los cuales serán de gran utilidad más adelante.

2.3 La administración de Riesgos

El estándar australiano define “la administración de riesgo como la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos” (Standards Australia, 1999, p.23).

De acuerdo al marco de desarrollo para este proyecto es correcto basar nuestras ideas en el marco de trabajo COBIT, como aquel marco de mejores prácticas de TI mundialmente aceptado, y de acuerdo a él se podría definir la administración de riesgos como un proceso central gestionado por la organización, en aras de

minimizar el impacto y la probabilidad de los eventos adversos, fortaleciendo la organización y aumentando las posibilidades de crecimiento, generando valor siempre y cuando esté alineado con los objetivos de negocio y procesos claves de la organización.

Se pueden definir dos conceptos fundamentales relacionados con la gestión de riesgos organizacionales.

El apetito de riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar cuando se trata de alcanzar sus objetivos.

La tolerancia al riesgo "es la desviación tolerable desde el nivel establecido por la definición del apetito de riesgo" (ISACA, 2009, p. 34).

2.4 Marcos de Gestión de riesgos

COBIT 5: ISACA (2013, p.20) define COBIT:

> Es un marco de referencia internacional aceptado por la mayoría de empresas como buenas prácticas para el control interno de la información. COBIT ha sido diseñado para facilitar el uso de las TI desde un enfoque de inversión que debe estar bien administrado y está basado en los estándares y las mejores prácticas de la industria, y ayuda a salvar la brecha entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos. COBIT provee de buenas prácticas, gracias a un marco de dominios: planificar y organizar; adquirir e implementar; entrega y soporte; y monitorear y evaluar (ISACA, 2013, p.20)

ISO 27005: La Organización Internacional de Normalización (2011) (originalmente en inglés: International Organization for Standardization, conocida por las siglas ISO) establece:

> Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación

> satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información.

ITIL v3: La empresa AXELOS (2011) establece lo siguiente acerca de ITIL v3:

> Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos, lo que ha dado como resultado la creciente necesidad de servicios informáticos de calidad que correspondan a los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar en el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

Normas internacionales como la ISO 38500:2008 y marcos de referencia como COBIT establecen lineamientos en materia de riesgos como parte del gobierno y gestión de riesgos de tecnologías de información, que son complementados con las diversas metodologías de riesgos de tecnologías de información que han promulgado diferentes organizaciones a nivel internacional y que a partir de diversos trabajos académicos y profesionales han realizado propuestas de similitudes entre sus estructuras, incluso con las metodologías de riesgo organizacional, lo que nos lleva a determinar dos aspectos críticos que las diferencian: los activos objeto de análisis y los factores de impacto a evaluar, los cuales requieren especial atención al momento de desarrollar un proceso de gestión de riesgos. (Revista UIS, 2016).

2.5 COBIT 5

ISACA (2013) construye el siguiente concepto:

> COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (*Stakeholders*). permite el desarrollo de políticas claras y de buenas prácticas para el control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.
>
> Dicho de otra forma, se puede decir que COBIT ayuda a cerrar las brechas existentes entre los riesgos de negocio, necesidades de control y aspectos técnicos. Además proporciona prácticas sanas a través de un marco referencial (*framework*) de dominios y procesos, y presenta actividades en una estructura manejable y lógica. Las prácticas sanas de COBIT representan el consenso de los expertos.

Descrito de otra manera se entiende que COBIT es el marco de mejores prácticas en TI, aceptado en el comercio internacional, con el fin garantizar los objetivos de negocio y entregando como producto final un gobierno de TI. Así mismo, las organizaciones se han dado cuenta del impacto y la necesidad de información a través de sus distintos procesos almacenamiento y distribución, lo cual genera riesgos sin importar el tipo de empresa o su clasificación.

COBIT 5, consta de 5 principios y 37 procesos, de los cuales para el actual proyecto se toman aquellos que estén directamente relacionados con la gestión de riesgos de información a nivel de TI, para poder adaptarlo como un modelo de evaluación y administración de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería. En la siguiente ilustración se puede observar todo el marco de gestión de COBIT 5.

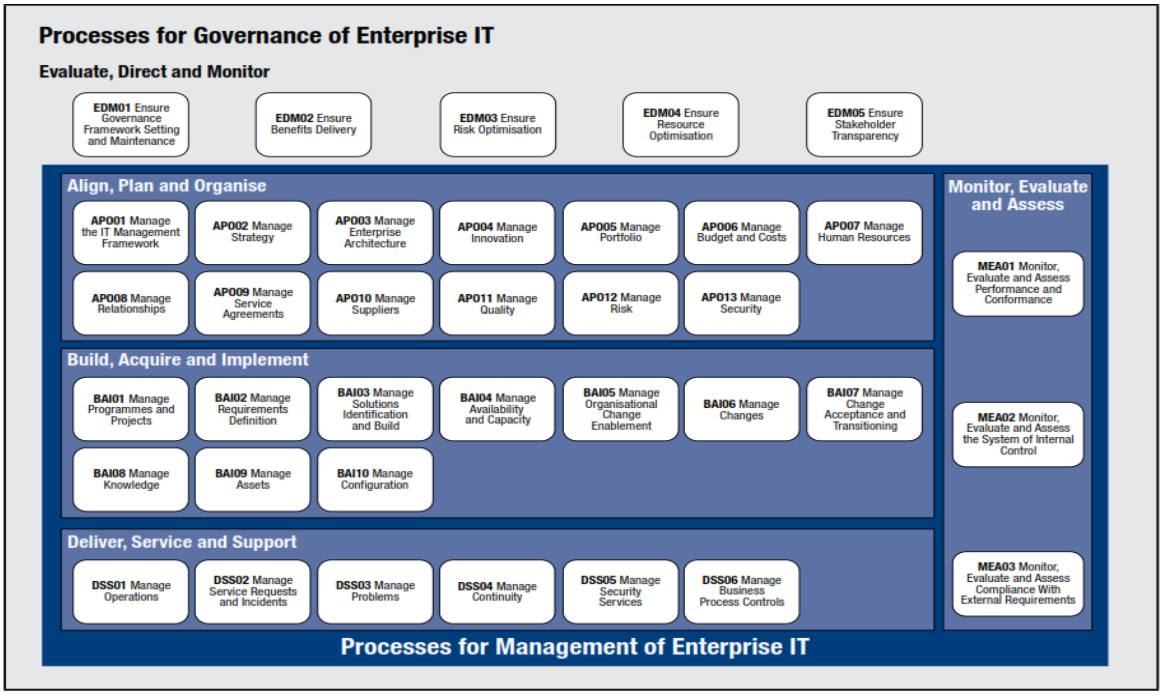


Ilustración 2: Procesos Habilitadores

Fuente: (ISACA INC., 2013, p. 33)

2.6 Gobierno de TI

Para el siguiente proyecto es necesario comentar acerca de los aspectos que contemplan el marco de trabajo COBIT, ya que este marco está orientado al gobierno de TI en todas sus versiones, de los cuales se basan sus principios y procesos, que son base para el proceso de evaluación y administración de riesgos de información a nivel de TI, por lo tanto es importante mencionar la importancia del gobierno de TI para este proyecto.

La estrategia de TI debe estar estrechamente ligada a las estrategias y políticas organizacionales, del estado o las entidades del sector. Para apoyar la construcción de un Gobierno TI es fundamental desarrollar un plan normativo y legal, las políticas organizacionales, los procesos, el modelo de gobierno y los mecanismos de compras y contratación de la entidad. Para que las TIC cumplan su papel es necesario contar con un modelo de gobierno de TI que contemple los siguientes aspectos:

- Marco legal y normativo
- Estructura de TI y procesos
- Toma de decisiones
- Gestión de relaciones con otras áreas y entidades
- Gestión de proveedores
- Acuerdos de servicios y de desarrollos
- Alineación con los procesos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017)

El Álvarez (2009) define:

> El Gobierno Corporativo de las TI es el sistema por el cual el uso actual y futuro de las TI es dirigido y controlado. El gobierno corporativo de las TI (GCTI) consiste en evaluar y dirigir el uso de las TI para apoyar la organización y hacer seguimiento de su uso para lograr los planes. Esto incluye las estrategias y políticas para el uso de las TI en una organización. El principal objetivo del GCTI es conseguir la alineación entre la estrategia del negocio y la estrategia de las TI. Este proceso es básico para que el GCTI cumpla su función primordial de generación de valor para los grupos de interés, minimizando los riesgos. (Álvarez, 2009).

De acuerdo a los conceptos anteriores, se puede deducir que para que el gobierno de TI surta efecto sobre la organización, TI debe estar alineado con los objetivos de negocio de la organización para contribuir de manera integral con los procesos de la organización.

Para Van Grembergen (2004):

> la gestión de las TI se centra en el eficaz abastecimiento interno de los servicios de las TI y de los productos y la gestión de las actuales operaciones de TI. El gobierno de las TI a su vez es mucho más

amplio, y se concentra en la realización y la transformación de las TI para satisfacer las demandas presentes y futuras de la organización (enfoque interno) y de los clientes del negocio (enfoque externo)”

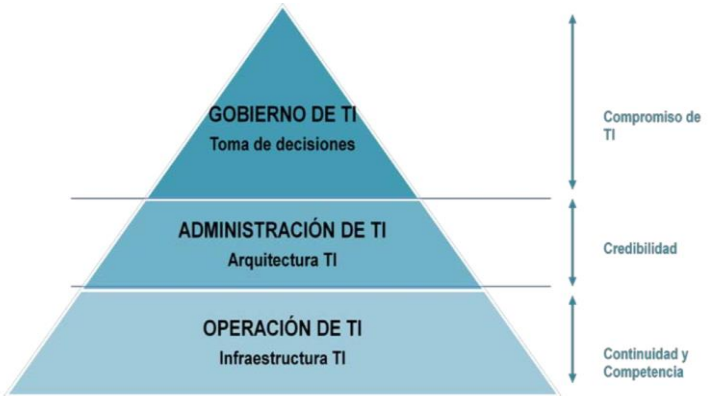


Ilustración 3: Gestión y Gobierno de TI

Fuente: (Chajón, 2015)

2.6.1 Evaluar y Administrar los riesgos de TI

ISACA en su libro COBIT 4.1 plantea la siguiente estrategia a seguir para la evaluación y administración de riesgos de TI, estableciendo el área de TI como los principales encargados de la evaluación y administración de riesgos de información a nivel de TI, los cuales serán tratados en este proyecto, por lo tanto se plantea la siguiente estrategia:

- Marco de Trabajo de Administración de Riesgos

Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

- Establecimiento del Contexto del Riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

- Identificación de Eventos

Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

- Evaluación de riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

- Respuesta a los Riesgos

Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar qué controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

- Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección. (IT Governance Institute, 2007).

Con base en lo anterior se establecen las siguientes actividades:

2.6.2 Actividades principales del proceso de evaluación y administración de riesgos de información a nivel de TI

Las siguientes son las actividades consideradas para el proceso tratado en el proyecto, las cuales están basadas bajo el estándar COBIT de manera que se establecen las siguientes actividades:

- **Determinar la alineación de la administración de riesgos**

Actividad que indica el rumbo que tomará la administración de riesgos en la organización y si esta formará parte de los planes estratégicos organizacionales.

- **Entender los objetivos de negocio estratégicos relevantes**

Direccionar la organización hacia fines máximos apuntando hacia la sostenibilidad y crecimiento empresarial.

- **Entender los objetivos de los procesos de negocio relevantes**

Definir y documentar los procesos que contribuyen al funcionamiento de la organización.

- **Identificar objetivos internos de TI y establecer el contexto de los riesgos de información**

Determinar la importancia de un área de TI y sus funciones sin importar el tamaño y personal, con el fin de establecer y armonizar los objetivos de negocio con los del área de TI, la cual contemple dentro de sus funciones la administración de riesgos de información.

- **Identificar los riesgos de información asociados a los objetivos**

Relacionar los riesgos de información con mayor impacto dentro de los objetivos organizacionales.

- **Evaluar y seleccionar respuestas a riesgos de información**

Establecer planes de contingencia eficaces para responder de manera adecuada a los riesgos que se presenten.

- **Priorizar y planear actividades de control**

Realizar monitoreo y evaluación a los riesgos residuales. De igual manera establecer de manera periódica la evaluación y administración de riesgos.

- **Aprobar y asegurar fondos para planes de acción**

Controlar los recursos asociados a las actividades de respuesta y control de riesgos.

- **Mantener y monitorear un plan de acción de riesgos**

Establecer regularmente un monitoreo de todos los recursos y actividades asociados a la evaluación y administración de riesgos de información a nivel de TI.

2.6.3 Conceptos asociados al tratamiento o respuesta a los riesgos

- **Evitar riesgos** significa salir de las actividades o de las condiciones que dan lugar a riesgo.
- **La reducción del riesgo** significa, qué medidas están tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo.
- **Transferir el riesgo** significa reducir el impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes son los seguros y la subcontratación.
- **Aceptación de riesgo** significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es aceptada. (ISACA, 2009).

2.6.4 Modelo de madurez del proceso de Evaluar y Administrar los riesgos de TI de acuerdo al estándar COBIT 4.1 de ISACA.

- **No existente** - cuando la evaluación de riesgos para los procesos y las decisiones de negocio no ocurre
- **Inicial / Ad Hoc** - cuando los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine

cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos, pero se asignan rara vez a gerentes específicos.

- **Repetible pero Intuitivo** - cuando existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.
- **Definido** - cuando una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo.
- **Administrado y Medible** - cuando la evaluación y administración de riesgos son procedimientos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con TI
- **Optimizado** - cuando la administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo

el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI (IT Governance Institute, 2007, p.131).

2.7 Marco conceptual

Cuadro 2: Marco Conceptual

Problema de investigación:				
Enfoque teórico	**Concepto central (Variable)**	**Subvariables**	**Indicadores (deben ser medibles)**	**Fuente de información**
Seguridad de la Información.	**Administración de Riesgos**: el conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su	**Riesgos:** Es el efecto de la incertidumbre en la consecución de los objetivos (ISACA, 2009)	**Probabilidad:** La probabilidad es la posibilidad que existe entre varias posibilidades, que un hecho o condición se produzcan. La probabilidad, entonces, mide la frecuencia con la cual se obtiene un resultado en oportunidad de la realización de un experimento sobre el cual se conocen todos los resultados posibles gracias a las condiciones de estabilidad que el contexto supone de antemano. (Florencia Ucha, 2008) **Impacto:** Consecuencias de los problemas asociados con el riesgo. (Pressman, 2001)	(Caviedes, 2014) (ISACA, 2009) (Universidad Nacional de Luján, 2013) (Rouse, 2014). (IT Governance Institute, 2007) (Florencia Ucha, 2008) (Pressman, 2001)

	función (Andres Caviedes, 2014) **Gestión de riesgos:** Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables	**Información**: es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. (IT Governance Institute, 2007)	**Riesgo Inherente:** Se considera el resultado de la probabilidad del riesgo por el impacto de éste. Puede ser medido cualitativa o cuantitativamente (Pressman, 2001)	

	para la misma. (Universidad Nacional de Luján, 2013) **Gestión de TI:** Es el proceso de supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización. La gestión de TI asegura que todos los recursos tecnológicos y los empleados asociados son utilizados correctamente y de una manera que proporciona valor para la organización (Rouse, 2014).			

Fuente: Elaboración propia

3 MARCO METODOLOGICO

3.1 Métodos de Investigación

Para el siguiente proyecto se toma como referencia el marco metodológico de Investigación Acción Participativa (IAP), Durston y Miranda (2002) afirman que la metodologia IAP:

> Consiste en un proceso metodológico que rompiendo los moldes de la investigación tradicional, conjuga las actividades del conocimiento de la realidad mediante mecanismos de participación de la comunidad, para el mejoramiento de sus condiciones de vida. En su conjunto se configura como una herramienta de motivación y promoción humana, que permitiría garantizar la participación activa y democrática de la población, en el planeamiento y la ejecución de sus programas y proyectos de desarrollo" (Durston & Miranda, 2002).

Para este proyecto, la metodología propone 4 etapas de investigación, las cuales se harán a cabalidad, pero teniendo en cuenta magnitud del proyecto éstas no serán llevadas a profundización exhaustiva, es decir, que solo se centrará en los procesos relacionados a la administración y evaluación de riesgos de información a nivel de IT.

- **Pre-investigación**

0. Detección de unos síntomas y realización de una demanda de intervención.

1. Planteamiento de la investigación

- **Diagnóstico**

2. Recogida de información.

3. Constitución de la Comisión de Seguimiento.

4. Constitución del Grupo de IAP.

5. Introducción de elementos analizadores.

6. Inicio del trabajo de campo (entrevistas individuales a representantes institucionales y asociativos).

7. Entrega y discusión del primer informe.

- **Programación**

8. Trabajo de campo (entrevistas grupales a la base social).

9. Análisis de textos y discursos.

10. Entrega y discusión del segundo informe.

11. Realización de talleres.

- **Conclusiones y propuestas**

12. Construcción del Programa de Acción Integral (PAI).

13. Elaboración y entrega del informe final (MARTI, 2012).

La hoja de ruta de esta metodología consiste en identificar los objetivos, los cuales están previamente definidos; seguido de ello la metodología propone realizar un diagnóstico, que para este proyecto se realizarán entrevistas a personal de TI de distintas empresas, recogiendo una muestra del estado actual de la gestión de riesgos de información a nivel de TI en la organización, continuo a ello, se realizará un consenso del estado deseado de estas empresas para riesgos de información a nivel de TI, esto se hará también con el fin de tratar de obtener a través del personal de TI, bases para la creación del modelo; del mismo modo una vez finalizada la etapa de entrevistas, consenso y retroalimentación se puede dar inicio a la creación del modelo de administración y evaluación de riesgos de información a nivel de TI.

3.1.1 Pre-investigación

Para este proyecto consiste en consultar fuentes de información que indiquen ya sea un problema o una oportunidad de crecimiento en relación a la gestión de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería. Se consultarán páginas web, artículos, prensa, radio, entrevistas, u otro tipo de fuente de información que esté relacionado con el proyecto, de esta manera se indicará

cómo será abordado el proyecto, es decir, como problema a solucionar o como oportunidad de negocio.

3.1.2 Diagnóstico

En esta fase de la metodología de diagnóstico, se harán entrevistas ya sea de manera de personal o a través de formularios, en donde se recogerá la información acerca del estado actual de las PYMES en Montería acerca de la gestión de riesgos de información a nivel de TI, para posteriormente analizarla y encontrar la falla o punto de explotación para crecimiento de las organizaciones.

3.1.3 Programación

Luego de realizar el diagnóstico de las PYMES en su estado actual y haber encontrado el problema en cuestión o el punto de explotación como oportunidad de crecimiento de negocio; se presentará una nueva entrevista para conocer el estado deseado de las PYMES con respecto al tema del proyecto, para luego analizar dicha información generando un punto promedio en realización al estado deseado, dando bases para ir generando un modelo de evaluación y administración de riesgos de información a nivel de TI y retroalimentar el modelo con la información de las PYMES.

3.1.4 Conclusiones y propuestas

Después de realizar la etapas previas se iniciará la etapa final, en donde se da inicio al modelo de evaluación y administración de riesgos de información a nivel de TI en las Pymes de Montería, teniendo en cuenta la información almacenada y las sugerencias de los gerentes y operativos de las empresas entrevistadas.

3.2 Fuentes de información

3.2.1 Fuentes Primarias

De acuerdo a la metodología de investigación para este proyecto, se entiende como fuente de información primaria aquel ente que brinde información y esté involucrado

con el proyecto de manera directa, por lo que se puede definir como fuentes de información primaria las siguientes:

- Entrevistas al departamento de TI de las PYMES de Montería para conocer su estado actual en la gestión de riesgos de información.
- Encuestas y/o entrevistas para conocer el estado deseado de las PYMES con respecto al proceso de gestión de riesgos de información a nivel de TI.

3.2.2 Fuentes Secundarias

Para las fuentes de información secundarias se toman aquellas fuentes que brinden información acerca del proyecto de manera indirecta o a nivel general, es decir, aquellas fuentes de información que aunque están relacionadas con la temática no están afectadas directamente, pero si nos brindan información válida y sostenible acerca del proyecto.

- Diarios, Noticias, artículos e informes relacionados con el estado de las PYMES en referencia al estado de la gestión de riesgos de información o de TI.
- Organismos gubernamentales como la cámara de comercio de Montería, el Ministerio de Tecnologías Información y Comunicaciones (MinTIC), el Ministerio de Comercio, Industria y Turismo de Colombia, entre otras entidades que puedan brindar información acerca de las PYMES y su constitución o, acerca de la normatividad vigente que contribuya a la gestión de riesgos de información.
- Gerentes de organizaciones, líderes de TI, docentes y personas con conocimiento de TI que puedan brindar información acerca de cómo hacer frente a la gestión de riesgos de información a nivel de TI en las PYMES de Montería.

Cuadro 3: Fuentes de información

Objetivos	Fuentes de información		Instrumentos
	Primarias	**Secundarias**	
Diseñar un modelo para la evaluación y administración de riesgos de información a nivel de IT, en Pymes en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT 5.	PYMES de la ciudad de Montería, Marco de buenas prácticas COBIT.	Profesionales de IT, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Normas y acuerdos presentes y actuales,	
Diagnosticar el estado actual de la gestión de riesgos de información dentro del área de IT de las PYMES en la ciudad de Montería, con el fin de conocer el estado actual de acuerdo al estándar COBIT para inciar la búsqueda del estado deseado.	PYMES de la ciudad de Montería	Cámara de Comercio de Montería, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Ministerio de Comercio, Industria y Turismo, Revistas, Noticias, artículos de prensa, radio y televisión, blogs, páginas web, libros entre otros.	Entrevistas, encuestas, informes e información legítima de las organizaciones

Establecer un estado deseado común de las organizaciones encuestadas en cuanto al proceso de gestión de riesgos de IT, para intentar identificar puntos comunes de las distintas organiazaciones en el desarrollo de los procesos de gestión de riesgos de IT, estableciendo un consenso de acuerdo a los parámetros encuestados.	PYMES de la Ciudad de Montería, Profesionales de IT con conocimiento en gestión de riesgos de IT	Cámara de Comercio de Montería, Ministerio de Tecnología, Información y Tecnologías, Ministerio de Comercio, Industria y Turismo, Revistas, Noticias, artículos de artículos de prensa, radio y televisión, blogs, páginas web, libros entre otros.	Entrevistas y encuestas.
Planear y desarrollar el modelo a partir del estado deseado común de las organizaciones, con el fin de cerrar la brecha entre el estado actual y el estado deseado de las organizaciones con respecto al proceso de gestión de IT.	PYMES de la ciudad de Montería, RISK IT COBIT 5 de ISACA, Profesionales de IT	Marcos de buenas prácticas de TI y gestión de riesgos, profesionales de TI	Investigación, Entrevistas

Fuente: Elaboración propia

3.3 Alcances y limitaciones.

Los alcances y limitaciones y su relación con los objetivos del proyecto final se ilustran en el cuadro 4, a continuación.

Cuadro 4: Alcances y limitaciones

Objetivos	Alcances	limitaciones
Diseñar un modelo para la evaluación y administración de riesgos de información empresarial a nivel de IT, en Pymes en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT 5.	Modelo de evaluación y administración de riesgos de información a nivel de IT en las PYMES de la ciudad de Montería.	Cronograma demasiado extenso. Presupuesto insuficiente. Actividades incompletas.
Diagnosticar el estado actual de la gestión de riesgos de información dentro del área de IT de las PYMES en la ciudad de Montería.	Un estado actual acerca del estado de la gestión de riesgos de información a nivel de TI dentro de las PYMES de la ciudad de Montería.	Poca información que puedan brindar las organizaciones. Sin acceso a la información de la organización. Información imprecisa acerca del tema.
Establecer un estado deseado común de las organizaciones encuestadas en cuanto al proceso de gestión de riesgos de IT.	Un consenso de las organizaciones entrevistadas y/o encuestadas, acerca de hacia dónde quieren llegar	Falta de información. Incoherencia de la información, es decir, información tergiversada.

	en su desarrollo del proceso de gestión de riesgos de información a nivel de TI	No existen puntos comunes. Demasiados puntos comunes.
Planear y desarrollar el modelo a partir del estado deseado común de las organizaciones en cuanto al proceso de evaluación y administración de riesgos de información a nivel de TI.	Planear y desarrollar el modelo de gestión de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería, teniendo en cuenta sus parámetros de PYMES.	Imperfecciones en el modelo. Modelo insuficiente. Modelo demasiado ambicioso. Modelo inadaptable a los parámetros de las PYMES.

Fuente: Elaboración propia

3.4 Entregables.

Los entregables y su relación con los objetivos del proyecto se ilustran en el cuadro 5, a continuación.

Cuadro 5: Entregables

Objetivos	Entregables
Diseñar un modelo para la evaluación y administración de riesgos de información empresarial a nivel de IT, en Pymes en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT 5.	Documento del modelo para la evaluación y administración de riesgos de información empresarial a nivel de IT, en Pymes en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT 5.

Diagnosticar el estado actual de la gestión de riesgos de información dentro del área de IT de las PYMES en la ciudad de Montería.	Informe como resultado de las entrevistas y encuestas del estado actual de la gestión de riesgos de información a nivel de TI de las PYMES de la ciudad de Montería, de acuerdo al estándar COBIT 5, donde se podrá observar a través de las entrevistas y/o encuestas su nivel de madurez del proceso.
Establecer un estado deseado común de las organizaciones encuestadas en cuanto al proceso de gestión de riesgos de IT.	Informe como resultado de las entrevistas y encuestas en consenso con las organizaciones y basado en el estándar COBIT 5 y en diferentes estándares de marcos de gestión de riesgos y gestión de TI, acerca del estado deseado con respecto al proceso de gestión de riesgos de información a nivel de TI en las PYMES.
Planear y desarrollar el modelo de evaluación y administración de riesgos de información a nivel de TI en las Pymes de la ciudad de Montería, a partir del análisis de información.	Documento con el modelo a seguir para la evaluación y administración de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería, basados en el estándar COBIT 5.

Fuente: Elaboración propia

4 DESARROLLO

4.1 Pre-investigación

En materia de consulta y recolección de información acerca de la seguridad de información a nivel de TI en PYMES, se encontró con un panorama alentador en el contexto de que este tipo de empresas son conscientes de los eventos adversos sobre la información que pueden sufrir y de a poco comienzan a implementar fracciones de los marcos de trabajo relacionados para intentar tener un plan de contingencia o estar preparados en caso de estos eventos.

4.1.1 Recolección de Información

Se tomó información acerca del tema de seguridad de información a nivel de TI en PYMES en fuentes de información secundarias como diarios, prensa, artículos y web, la información encontrada fue minúscula, estrictamente hablando de la ciudad de Montería, es decir que muy poca estaba relacionada con la temática de profundización. Por otra parte la información buscada en históricos como libros, artículos de prensa y otro tipo de fuente de información se consideró demasiado obsoleta. No obstante, la poca información que se encontró hacía referencia al poco conocimiento que tenían los profesionales de TI acerca de las amenazas de la época, pues la mayor parte de robos de información y pérdidas de información ocurrían por descuidos o lo que se puede llamar hoy en día como ingeniería social.

De acuerdo a ello se puede decir que las empresas que tenían un control más avanzado quizás entre un nivel definido y administrado para ese entonces (años 1990 a principios de 2000), eran las grandes empresas, empresas con un capital y recursos fuertes en materia de infraestructura y personal de TI, que podían hacer frente a tales crisis. Tal es el caso de Postobon, Aguila, Supermercados Vivero, y otras más; las cuales contaban con sistemas de CCTV, *firewalls*, sistemas de almacenamiento distribuido, profesionales de TI especializados, entre otras grandes herramientas del momento. En definitiva eran las grandes empresas las que tenían un mejor control sobre los riesgos de información que podían presentarse. Las

PYMES por su parte difícilmente pueden implementar estas rigurosidades en temas de seguridad de la información, tan solo alcanzan a apegarse a los estatutos de la ley de protección de información y cláusulas de confidencialidad acerca de la información que manejaban sus profesionales en todas las áreas. Una situación que realmente al transcurrir los años y al estar introducidos en una era digital se determina que ya no son suficientes, por lo que muchas PYMES se arriesgan o arriesgaban a realizar grandes inversiones en TI para proteger la información o se exponían a riesgos de alto nivel que los podían dejar en bancarrota.

4.1.2 Consulta con profesionales de TI

La consulta se realizó a 10 docentes de 7 universidades locales de la ciudad y a profesionales que tienen un gran recorrido en distintas empresas, siendo éstas de gran participación en el mercado local, regional y algunas con presencia internacional, ocupando altos cargos en las áreas de TI.

En términos generales los profesionales afirman que la cultura organizacional en materia de riesgos y exposición a eventos adversos en relación a la seguridad de la información, ha cambiado radicalmente, pero este cambio ha venido acompañado de grandes eventos y de grandes cambios en el campo informático, es decir, fue necesario ver algunas tragedias comerciales para tomar conciencia al respecto de la seguridad de la información. Personal que sale de una empresa y entra a laborar en la competencia, y de manera deliberada revela información, planes y estrategias de lo que se piensa llevar a cabo en un corto plazo la anterior empresa para la que trabajaba, de esta manera la información se convierte en factor clave para la competitividad empresarial. Por otra parte, también se tiene el caso de los virus, los cuales han sido una causa perturbadora en relación a la seguridad de la información y aunque Colombia no es un centro de hechos para estos actos, cabe resaltar que la ingeniería social y otros aspectos como archivos de información corruptos intencionalmente o *software* mal intencionado, correos spam, competen una fuerza de riesgos que debe ser controlada o al menos mínimamente gestionada para cualquier empresa.

En respuesta a la pregunta ¿Cómo considera usted que puede mejorar esta situación dentro de las PYMES de la ciudad de Montería?, más del 85% afirmaron que con la implementación de normas y marcos de trabajo podría ser una buena opción, pero que es indispensable que los profesionales de TI estén preparados para afrontar nuevos retos, lo cual requiere de una preparación absoluta en esta área. “Es algo que aunque tiene un costo para las empresas, debe llevarse a cabo, recientemente un *ransonware* llamado *wannacry* causó grandes estragos en una universidad reconocida, imagine si esto llegase a pasar no en una empresa, sino en un negocio que apenas inicia, en donde todos los inversionistas tienen diseñados procesos, gestión, contactos, información, etc., en las máquinas de la organización y este virus por error de un usuario inexperto, inexperiencia o por simple intencionalidad, convierte estos datos en víctimas del virus informático. Tomaría meses de tiempo volver a iniciar, algunos contactos se perderán, otros inversionistas desistirán de la idea, básicamente el proyecto de negocio que puede convertirse en una PYME caería en un abismo tan profundo difícil de sacar” (Baena, 2017).

Es primordial que toda empresa por pequeña que sea, debe garantizar primeramente su información y todo lo que a ella concierne, para ello es importante revisar normas y marcos de trabajo amplios que puedan cubrir todos los aspectos relacionados a la seguridad de la información; del mismo modo, deben tener la capacidad de implementarlos o al menos considerar sus puntos más fuertes para ponerlos en práctica.

4.2 Diagnóstico

Para la investigación fue necesario realizar encuestas y entrevistas, pero debido al tiempo que se disponía para contestar la encuesta fue necesario completar la información con la ayuda de profesionales de TI locales. Aunque no se obtuvo la participación esperada por los gerentes de TI de las PYMES, se logró recaudar información valiosa, haciendo ver la realidad de la problemática.

4.2.1 Entrevistas y encuestas

La encuesta y la entrevista se realizó a aproximadamente 45 personas, pero solo 20 fueron consideradas como respuestas apropiadas; las restantes no fueron tenidas en cuenta debido a la falta de profundización y argumentación; entre esas 20 personas, se obtuvo respuesta de profesionales de TI y gerentes de empresas comerciales en categoría PYMES. De acuerdo a lo anterior las respuestas fueron las siguientes teniendo en cuenta argumento utilizado:

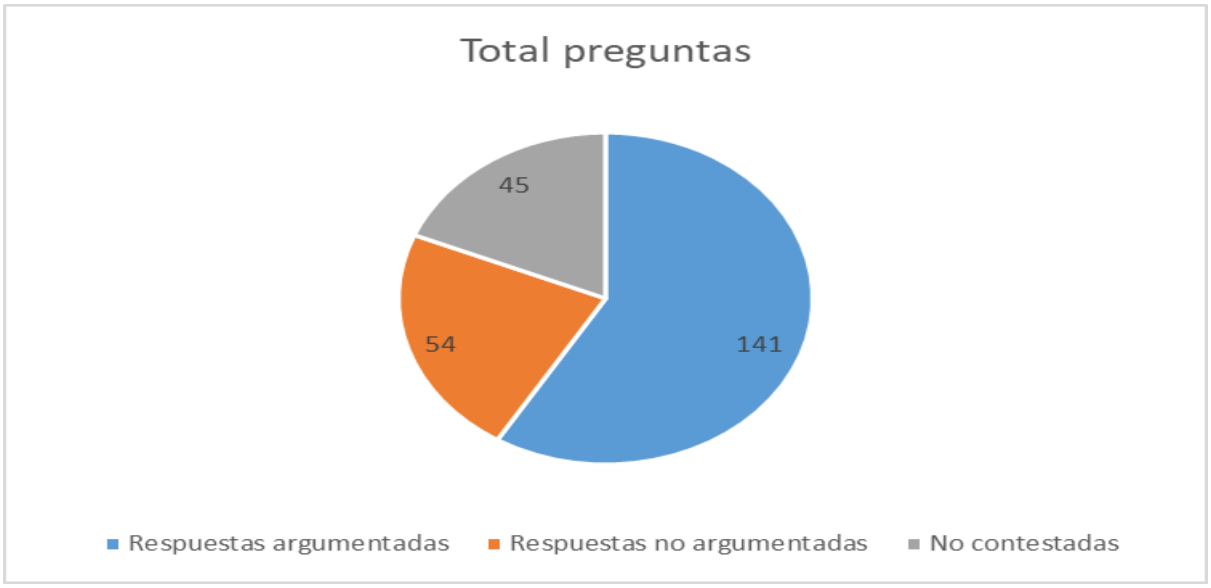


Ilustración 4: Total de preguntas realizadas

Fuente: Elaboración Propia

- ¿Cómo ha sido su experiencia en la gestión de riesgos de información a nivel de TI de la empresa?

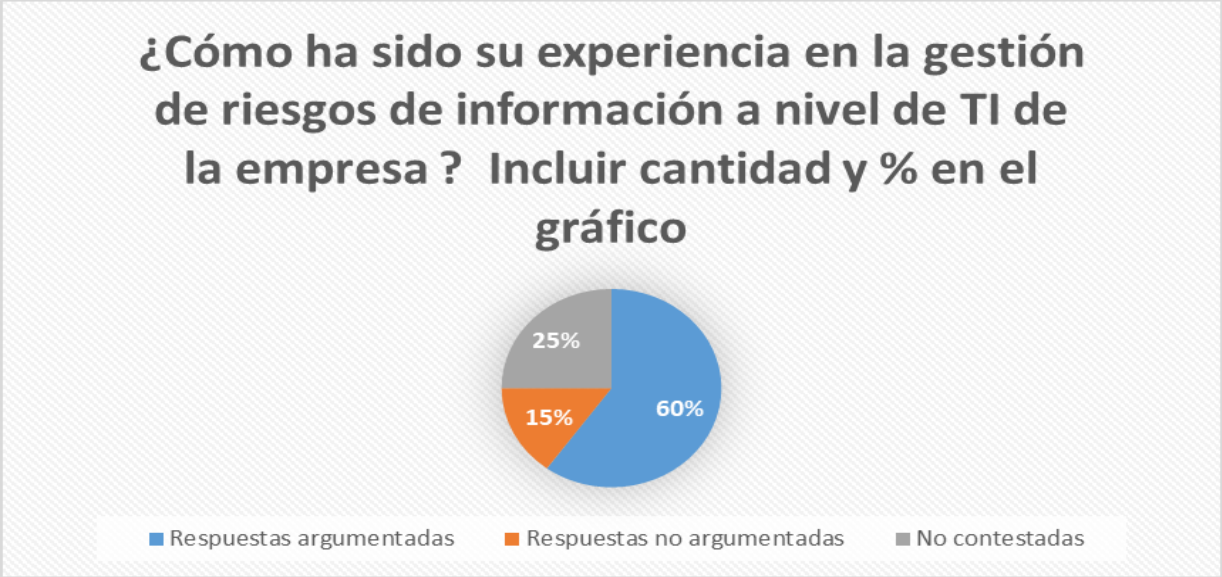


Ilustración 5: Pregunta 1

Fuente: Elaboración Propia

Muchos profesionales encuestados afirman haber desarrollado varios cargos relacionados con la alta gerencia de TI en distintas organizaciones, que se puede decir están directamente relacionados con la gestión de riesgos de información y aunque la empresa tenía sus cimientos de seguridad de información ya sea basado en las leyes Colombianas, por lo general siempre se complementaba con marcos de trabajo o normas técnicas. De igual manera siempre fue necesario establecer políticas de seguridad más robustas con el pasar de los años, al igual que capacitar al personal del área en riesgos de seguridad de la información.

Se manifestó el compromiso por parte del área de TI en asuntos de seguridad de la información como manejo de correos sospechosos, cambio de claves con relativa frecuencia, antivirus, copias de seguridad, independencia de red LAN y WAN, herramientas en la nube con respaldo incluido, intercambio de información en línea. Otros por su parte manifiestan que la seguridad de la información se enmarca en la identificación de amenazas (vulnerabilidades), establecer el impacto que éstas

podrían ocasionar en la empresa y posteriormente establecer el plan de acción a seguir en caso de presentarse alguna contingencia relacionada con los riesgos identificados, y lo más importante definir y establecer los controles necesarios para que dichas vulnerabilidades se minimicen.

- ¿Tiene la organización algún marco de trabajo implementado a nivel de IT para la gestión de riesgos, o los profesionales del área de tecnología están certificados con algún estándar que puedan utilizarlo dentro de la organización?

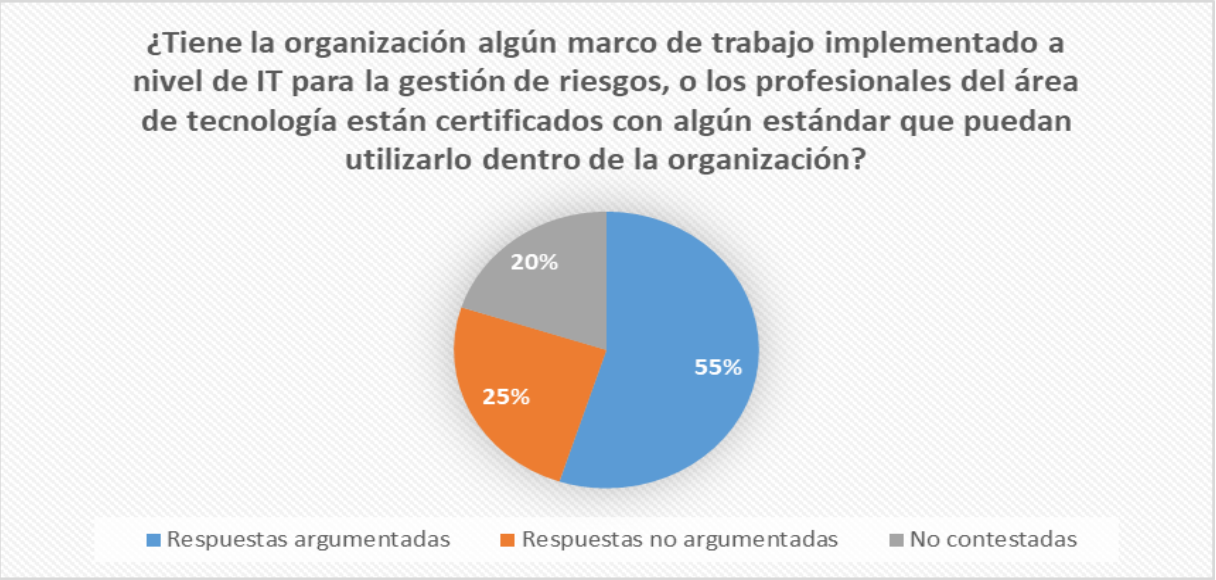


Ilustración 6: Pregunta 2

Fuente: Elaboración Propia

Aproximadamente el 80% de los encuestados respondió que la empresa no utiliza un marco de trabajo para la seguridad de la información a nivel de TI, pero que a pesar de esto, capacitan al personal sobre la responsabilidad y el uso de la información empresarial, pero a pesar de eso, el 35% manifestó que dentro de su equipo de trabajo tiene personal especializado en temas de seguridad de la información con algún posgrado o certificación vigente, que le brinda cierto tipo ideas para la gestión de riesgo.

Otro porcentaje, 10% manifestó que intenta hacer frente a los riesgos de seguridad de la información basada en marcos de trabajo como ITIL o ISO 27001, poniendo en práctica algunas de las recomendaciones que aquí se plantean para la seguridad de la información empresarial.

Por otra parte también existe un mínimo porcentaje del 5%, el cual desconoce marcos de trabajo y solo se apega a los conocimientos empíricos y de otros profesionales para la gestión de riesgos de información.

Sin embargo existe una realidad expuesta por la gran mayoría con casi el 90% de los encuestados, y es que aunque se tengan los conocimientos y la experiencia, no se cuenta con la capacidad, la infraestructura, los recursos y el personal para llevar a cabo ciertas implementaciones en materia de gestión de riesgos de información, por lo que muchos puntos críticos en este tema pueden quedar abiertos y expuestos.

- ¿La organización es consciente de los riesgos de información a nivel de TI, y qué tan perjudiciales pueden ser para ella?

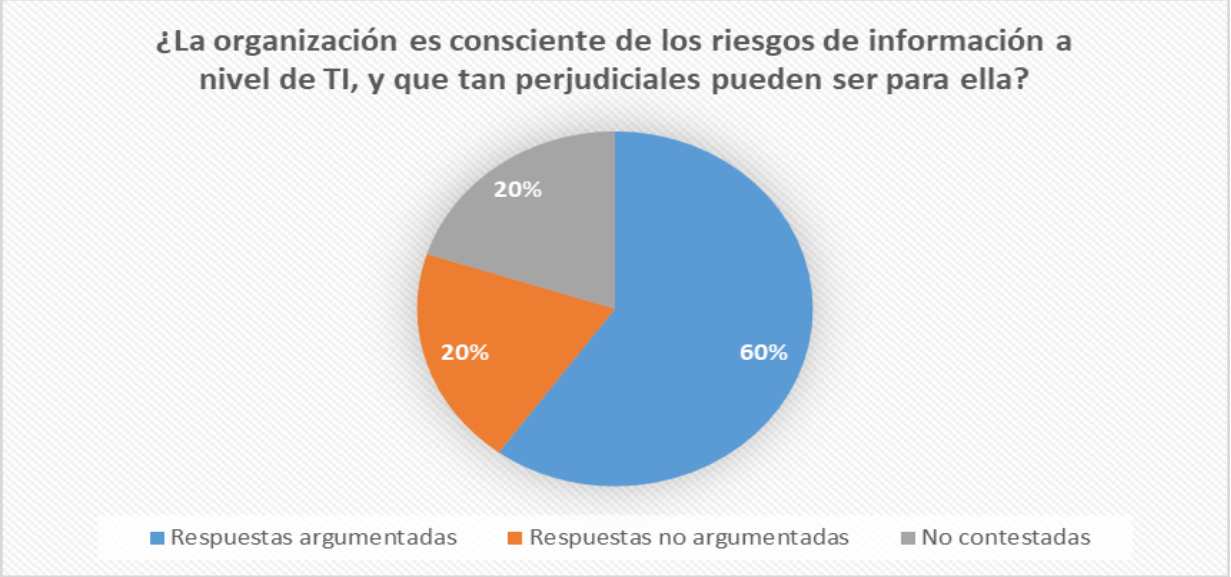


Ilustración 7: Pregunta 3

Fuente: Elaboración Propia

En términos generales la cultura organizacional ha tenido un cambio bastante asertivo en temas de seguridad informática, que aunque las prácticas no lo reflejen debido a falta de capacidad en muchos términos, los gerentes y personal de TI son conscientes de los riesgos a los que está expuesta la organización. Por tal motivo utilizan prácticas comunes adheridas a las normas y leyes constitucionales de Colombia para minimizar los riesgos, así como algunas empresas regularmente realizan capacitaciones a su personal en esta materia.

Se puede decir que hay una concientización acerca de los aspectos relacionados con la seguridad de la información en las organizaciones, pero en efectos de confidencialidad, integridad y disponibilidad de la información, realmente son pocas las que conocen y aplican técnicas más avanzadas para garantizar estos principios.

- ¿Están plenamente identificados los riesgos de información a nivel de TI en la organización?

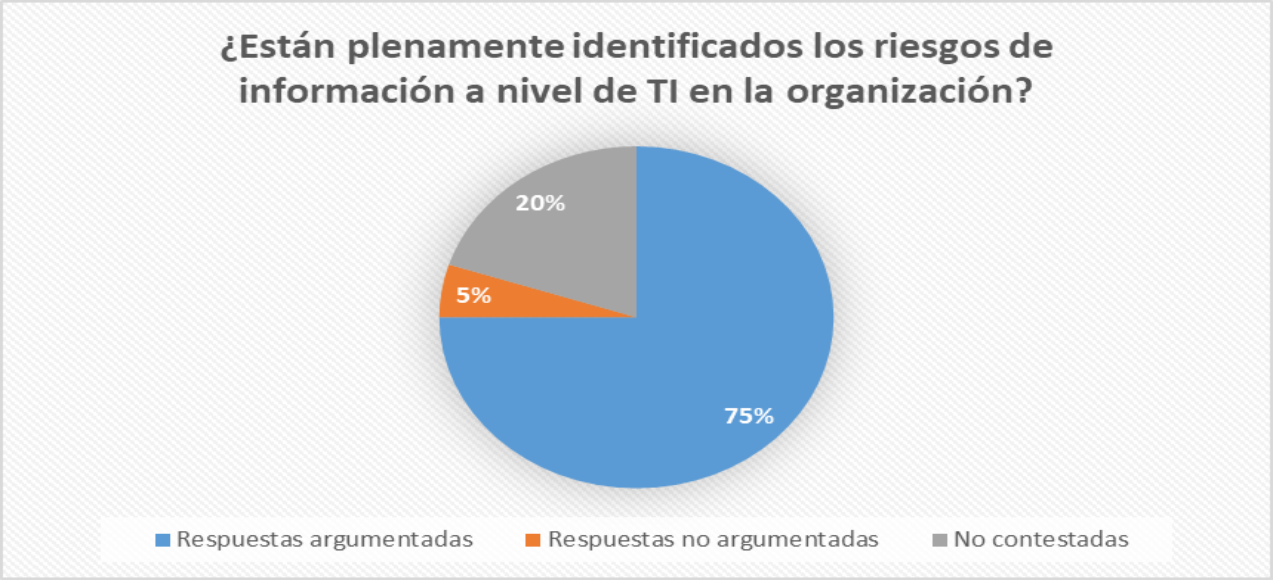


Ilustración 8: Pregunta 4

Fuente: Elaboración Propia

Las empresas aseguraron que tienen pleno conocimiento sobre los riesgos a los que está expuesta la organización en términos de negocio y estrategias, por lo que regularmente desarrollan planes para minimizar su impacto. Esta situación

generaliza los riesgos, mas no aplica una estrategia específica a los riesgos de información, lo que indica, que los riesgos de información no se tiene como una categoría independiente en los planes de gestión de riesgos.

- ¿De qué manera son clasificados los riesgos de información a nivel de TI de la organización?

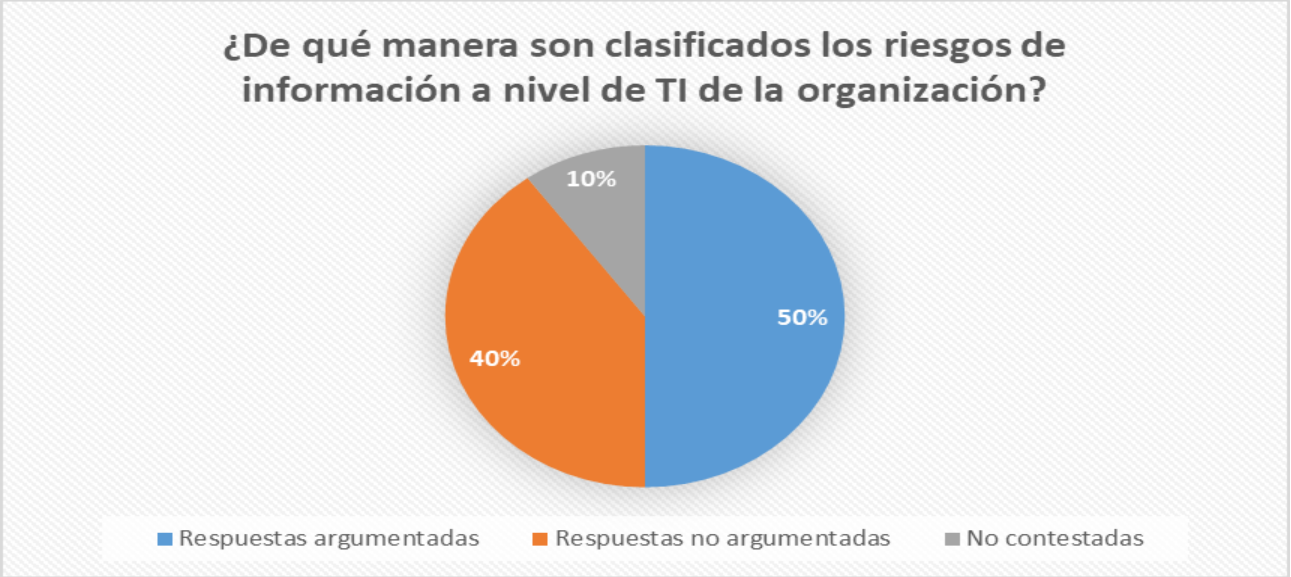


Ilustración 9: Pregunta 5

Fuente: Elaboración Propia

El 85% de las empresas encuestadas aseguraron tener su clasificación en tres niveles alto, medio y bajo, lo cual es muy común mas no de argumentos convincentes dada la situación de conocimiento, es decir, no hubo claridad sobre los criterios que se evaluaban para incluirlas dentro de estas categorías. Otras aseguraron tener un mayor conocimiento acerca de la clasificación de los riesgos, las cuales eran empresas con una presencia internacional, en la que su categoría no entraba dentro de lo que constitucionalmente y reglamentariamente se conoce como PYMES para el estado Colombiano; eran sucursales de grandes empresas las cuales tienen un esquema de trabajo estandarizado en la que se refleja una matriz de riesgos con su respectiva clasificación.

Es notable entender que los conocimientos acerca de la clasificación de riesgos son básicos y algunas veces un poco más avanzados, pero en términos estrictos acerca de los riesgos de información, el conocimiento es muy empírico, pero enfatizando sobre una gestión de riesgos de información, para las PYMES es como un “apaga incendios” de esta área, lo que indica que se debe realizar cierta profundización en estos temas de gestión de riesgos de información.

De las empresas encuestadas realmente son muy pocas las PYMES que tienen una clasificación robusta en torno a los criterios de información, y bien se ha mencionado antes, son PYMES que ya están entrando a competir dentro de grandes empresas, las cuales dejarían de ser foco para esta investigación.

- ¿Se realiza una evaluación en cuanto a probabilidad e impacto de los riesgos de información a nivel de TI de la organización?

Ilustración 10: Pregunta 6

Fuente: Elaboración Propia

A esta pregunta, aproximadamente el 70% de los encuestados afirmó que sí se realiza esta evaluación, la cual se refleja en una matriz de riesgos, o simplemente se mencionan en orden de importancia en una lista de riesgos como instructivo o manual dentro de la organización.

Solo uno de los encuestados respondió lo siguiente: *"Para recolectar la información se aplican las técnicas de la observación directa mediante visitas programadas y entrevistas* aplicadas *a los profesionales de sistemas encargados de la administración del área informática, la seguridad informática y usuarios de los sistemas. Con el conocimiento claro del área o sistema auditado, se definen y describen las vulnerabilidades o debilidades encontradas, las amenazas por parte de personal interno o externo al tratar de cometer un ilícito o un ataque, y los riesgos naturales y no naturales a que está expuesta la organización" (Barrios, 2017).*

Lo anterior se puede resumir que aunque esta evaluación se realice, carece de argumentos al hacer simplemente una lista en orden de importancia para los riesgos de información a los que la organización está expuesta. La gestión de riesgos de información debe ser incluida dentro de la estrategia de crecimiento de la organización, lo cual es fundamental para implementar marcos de trabajo.

- ¿Existen estrategias para mitigar, disminuir, compartir o aceptar los riesgos de información a nivel de TI en la organización, o al menos los que son de alto o medio impacto?

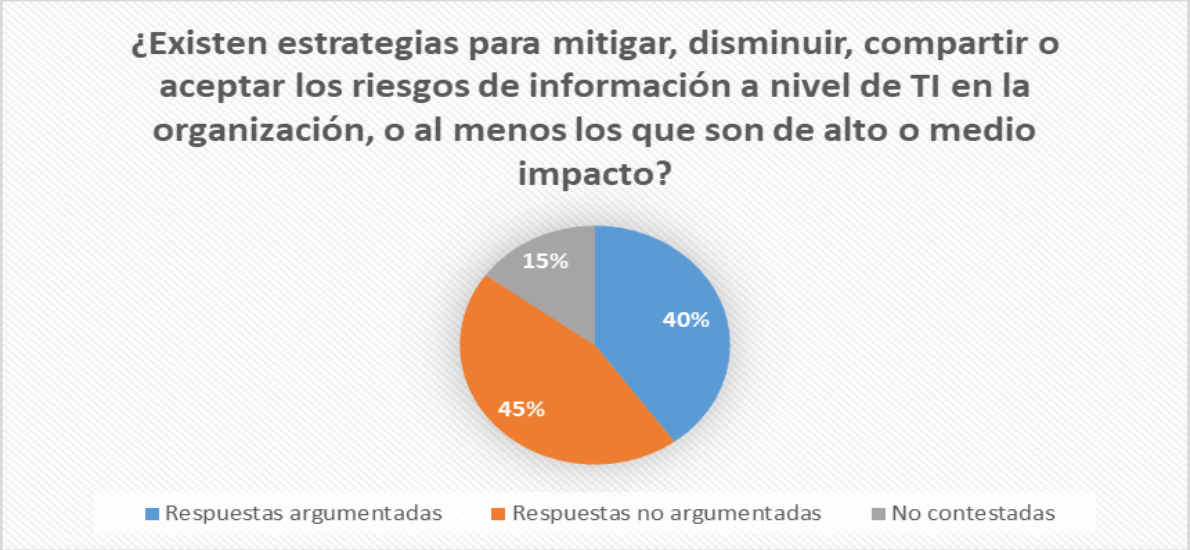


Ilustración 11: Pregunta 7

Fuente: Elaboración Propia

Se obtuvieron diversas respuestas con respecto a esta pregunta, en general todas afirmaron tener planes de contingencia para controlar los riesgos de alguna manera. Algunas de las organizaciones encuestadas siguen los procedimientos y prácticas de la norma ISO/IEC 270001 en la que se establece las directrices necesarias para el tratamiento de riesgos, como: evitar, reducir o mitigar, transferirlo o asignarlo a terceros y aceptarlo cuando esté por debajo del umbral aceptable.

Algunas empresas conocen y son conscientes de que es necesario tener planes y estrategias para controlar los riesgos relacionados con la información de la organización, pero también son conscientes que sus políticas y estrategias deben ser más robustas, es decir, deben complementarse con un marco de trabajo el cual abarque puntos que aún no han sido considerados ya sea por inexperiencia o falta de conocimiento en el área.

- ¿Se realiza un monitoreo periódico a la evaluación de los riesgos de información a nivel de TI de la organización, con el fin de mejorar dicha gestión?

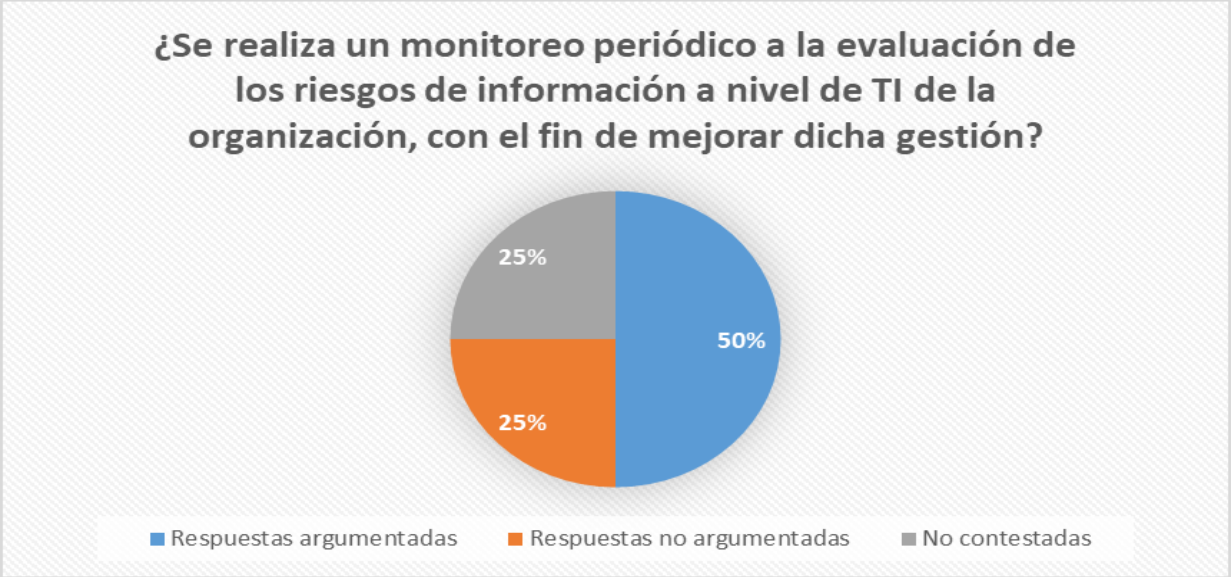


Ilustración 12: Pregunta 8

Fuente: Elaboración Propia

El 90% de los encuestados respondió sí, de manera anual, pero no se especificaron los parámetros con los que se realiza dicho monitoreo, o si la función de este monitoreo es el mejoramiento continuo o la actualización de normas y técnicas relacionado con la gestión de riesgos de información. Aunque algunos manifestaron que se realizan pruebas con la gestión de riesgos de información, ejecutando procedimientos como restauración de copias de seguridad, revisión de archivos de carácter fundamentales del negocio, restablecimiento de bases de datos, entre otras actividades.

Una mínima cantidad de las empresas encuestadas, respondió que no se realizaba monitoreo, porque no se consideraba pertinente para los procedimientos que tenían establecidos, quizás porque consideraban que los procedimientos que tenían implementados abarcaban todos los puntos relacionados con la seguridad de la información. Estos procedimientos pertinentes a la evaluación de riesgos, más bien se actualizaba de manera automática con los tópicos considerados por el director de TI de la organización. Para esto no se especificó que parámetros o si se utilizaba un marco de trabajo que se tuviera en cuenta para esta actualización.

- ¿Considera que es necesario mejorar la gestión de riesgos de información a nivel de TI en la organización?

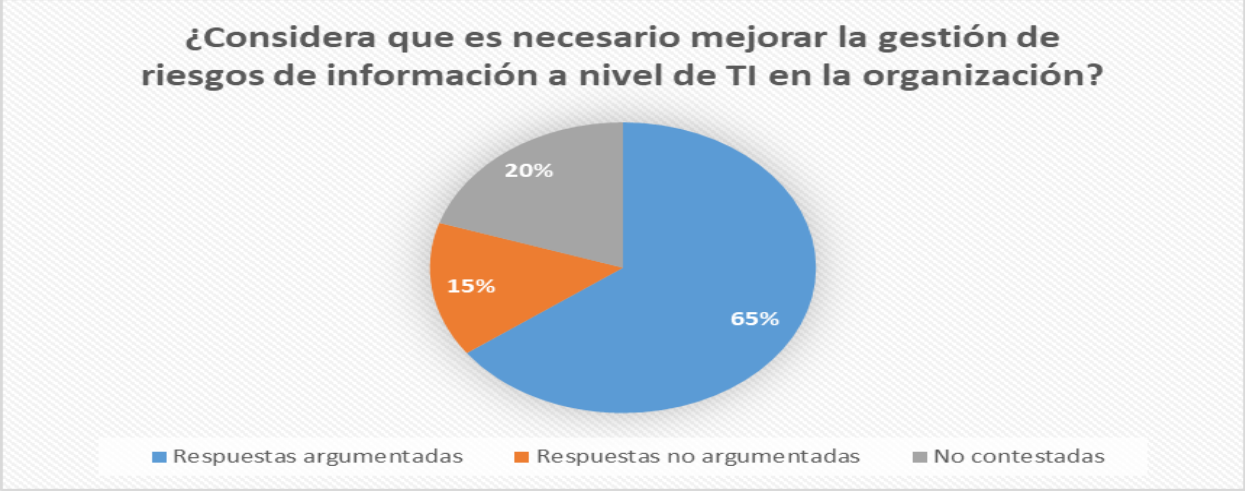


Ilustración 13: Pregunta 9

Fuente: Elaboración Propia

Todos los encuestados respondieron que sí, que de manera general la seguridad en todas sus áreas cada vez juega un papel más importante en las organizaciones, y más aún en el área de la información, que es donde más falencias existen, puesto que las leyes y normas existentes en el estado colombiano no son suficientes y donde las grandes empresas diariamente son mayormente atacadas para acceder a información clasificada con el fin de vender información a la competencia, como claves de acceso, uso de información empresarial, archivos históricos de la organización, entre otras; son todos estos blancos y objeto de estudio para la seguridad de la información.

Algunos encuestados aseguraron que es de vital importancia valorar el riesgo al que se está expuesto, teniendo en cuenta que esto prepara y minimiza el impacto para la organización ante la ocurrencia de eventos adversos, como la pérdida de información y revelar información ventajosa para la competencia.

- ¿Cómo considera usted que puede mejorar esta situación dentro de las PYMES de la ciudad de Montería?

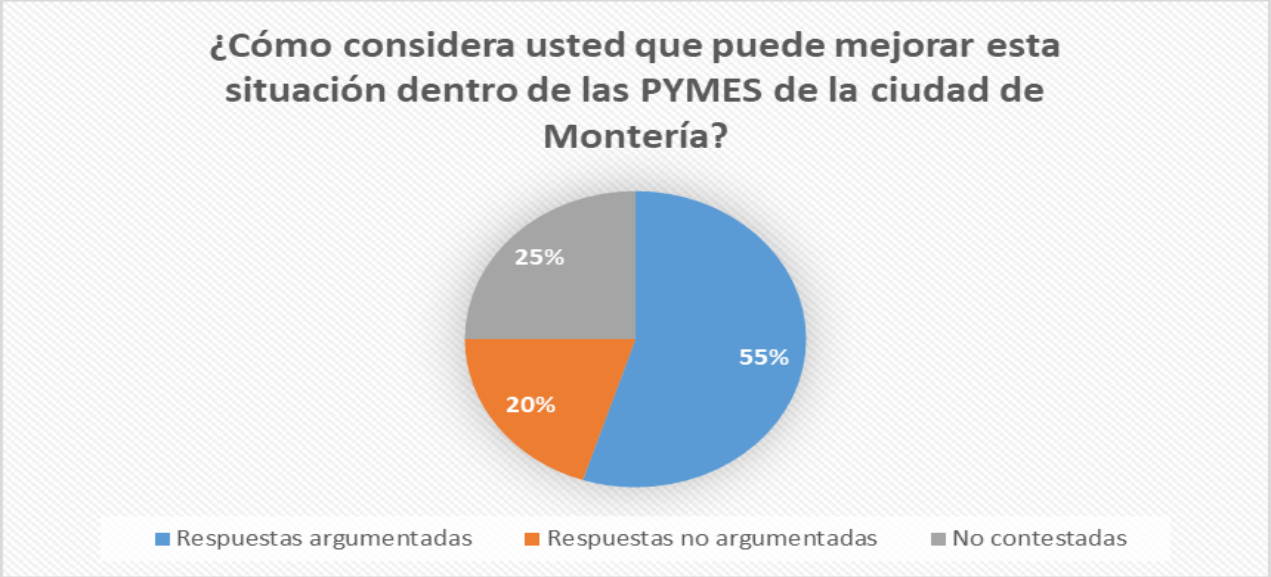


Ilustración 14: Pregunta 10

Fuente: Elaboración Propia

“La información es el activo principal que se debe proteger dentro cualquier organización, se deben adaptar metodologías que la protejan y que también considere: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas” (Barrios, 2017). Esta fue la respuesta de uno de los jefes de TI de una de las organizaciones encuestadas, que aunque previamente manifestó la falta de recursos para la implementación de marcos de trabajo, es consciente de la problemática y de las pérdidas que puede ocasionar la seguridad de información en una organización.

Aunque la mayoría de los encuestados consideran que el problema radica en cultura organizacional, presentan propuestas como la de fomentar entre directivos la importancia de la gestión de riesgos en estas empresas, que son más del 80% del mercado empresarial en la ciudad de Montería.

La utilización de técnicas, metodologías, estándares y marcos de trabajo es una forma muy precisa y exacta para tratar dicha problemática; esto considerablemente influiría positivamente en la manera en cómo las PYMES abarcan el tema de gestión de riesgos de información; y aunque son pocas las PYMES que tienen los recursos apropiados para aplicar dichas técnicas, quizás el empoderamiento de estos conocimientos y aplicar aunque sea un pequeño porcentaje de esto en las buenas prácticas de la organización reflejaría impactos muy positivos en el mercado, resultando con organizaciones PYMES mayormente sostenibles.

- ¿Conoce usted los marcos de trabajo como COBIT y RISK IT?

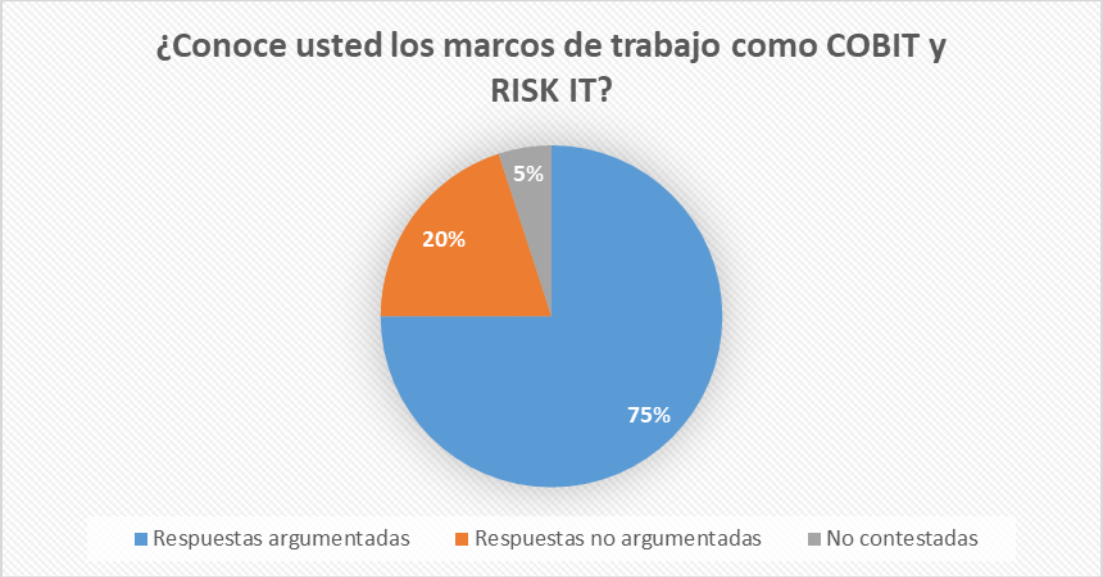


Ilustración 15: Pregunta 11

Fuente: Elaboración Propia

Entendiendo que Risk IT es complementario a COBIT, para la mayoría de estas organizaciones lo que se conoce acerca de estos marcos de trabajo es muy poco, solo pequeños conceptos que básicamente se podrían aplicar en sus empresas, pero al carecer de dichos conocimientos y experiencia, no se preocupan por intentar nuevas maneras de gestionar los riesgos de información.

Para la mayoría de empresas y encuestados incluyendo los profesionales de TI, son conscientes que en esta área como marco de trabajo el marco de trabajo más conocido es ITIL, debido a las múltiples certificaciones que tiene y por ser el más exigido en vacantes para empleo.

- ¿Considera usted que se podría mejorar el proceso de evaluación y administración de los riesgos de información a nivel de TI de las organizaciones PYMES de la ciudad de Montería a través de la implementación de alguno de estos marcos de trabajo para TI?

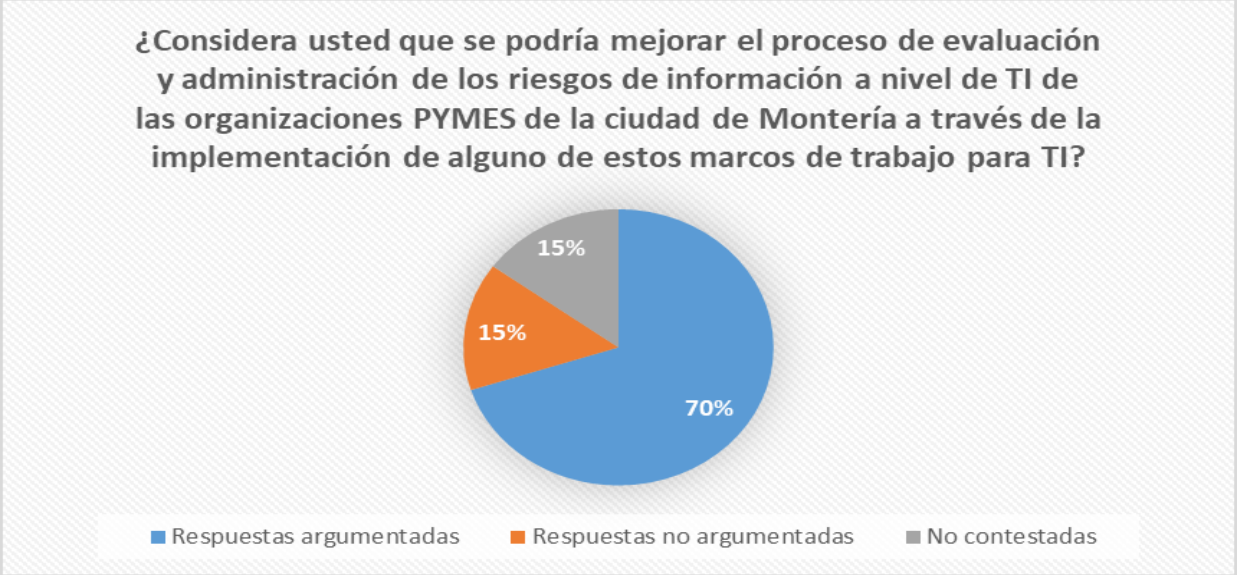


Ilustración 16: Pregunta 12

Fuente: Elaboración Propia

La gran mayoría de los encuestados, con aproximadamente el 95% considera que los marcos de trabajo y estándares siempre que son correctamente implementados contribuyen de manera significativa en la gestión de TI y más aún en el tema específico que es la gestión de riesgos de información a nivel de TI. ITIL es el estándar o marco de trabajo mayormente trabajado en las empresas Colombianas, pero COBIT al ser un marco de trabajo de mayor envergadura en el que especialistas del área de TI a nivel mundial afirman que este contiene los principios de ITIL y mucho más; las organizaciones considerarían que podría generar un mayor impacto en los temas relacionados a la seguridad de la información.

"Si, en tecnología se aprende que si una técnica se convierte en estándar, norma o marco de trabajo se debe a que se ha pasado por unas experiencia que validan la existencia de las mismas, por tal razón el aplicar estos marcos seguramente

aportarán en la gestión del riesgo en las organizaciones" (Barrios C. , 2017). Esta fue la respuesta de uno de los profesionales de TI, en la que actualmente se piensa implementar un proceso de certificación de ITIL a la alta gerencia de TI y capacitar al personal operativo de TI en conceptos y mejores prácticas de ITIL. Así la empresa estaría gestionando mejor sus procesos y ciertamente la gestión de riesgos ascendería en materia de gestión de 6 puntos a 8 al cabo de finalizar la implementación.

Lo anteriormente enunciado no es otra cosa que resaltar la importancia de los marcos de trabajo dentro de TI en las PYMES de la ciudad de Montería, esto realmente es un gran paso para las empresas, al demostrar que están calificadas y entrenadas y no solamente para la gestión de riesgos de información.

4.2.2 Análisis de información recolectada

De acuerdo a las respuestas se puede resaltar lo importante que es para las PYMES el aprovechamiento de las tecnologías de información como herramienta para una mayor ventaja competitiva en el mercado, por lo tanto se hacen los siguientes aportes como focos de atención en las encuestas realizadas:

- **Crecimiento de las PYMES en TI**

Se concibe como información principal la naturaleza de las PYMES en su afán de crecer y aprovechar las ventajas ofrecidas a través de las tecnologías de información, es por ello que aunque la mayoría de estas pretendan alcanzar niveles de satisfacción más altos en sus procesos de evaluación y administración de riesgos de información a nivel de TI, deben iniciar procesos de implementación de estándares a baja escala, en la medida que éstos sean posibles.

- **Estándares comunes en las PYMES para TI**

Aunque el estándar más conocido para la mayoría de profesionales de TI es ITIL, COBIT es un estándar con mayor alcance y que no necesita estar certificado para su implementación, ambos pueden implementarse a menor escala, pero al implementar COBIT, se consideraría que las organizaciones pueden estar

adquiriendo mayor valor en sus productos o servicios ofrecidos al igual que sus oportunidades de crecimiento estarían más garantizadas. No se infiere que COBIT sea mejor que ITIL, pero sí que COBIT abarca muchos más aspectos que ITIL, siendo el estándar de mejores prácticas mayormente utilizado en las grandes empresas del mundo.

Aunque en este aspecto las PYMES colombianas se guían mayormente por ITIL, también existe otro porcentaje que utiliza las prácticas de ISO 27001 en sus distintas versiones, algunas actuales y otras no tanto. Se puede decir que COBIT también recoge algunas de sus guías en los marcos de trabajo para la administración de riesgos de TI como lo es RISK IT, que es material complementario a COBIT; por ende se puede decir que COBIT sigue creciendo y al aplicarlo correctamente las organizaciones se podrían complementar de igual forma con RISK IT.

- **La seguridad de la información en TI**

Es uno de los temas principales en el proyecto, algo que se ha hecho tema de conversación más frecuente en muchas capacitaciones y conversaciones con empleados de las organizaciones. Un tema que ha tomado mayor interés con el uso de las tecnologías de la información. La idea de utilizar estándares y prácticas de TI para proteger la información como el recurso más valioso de las organizaciones, es un tema que toma fuerza cada día, esto convierte las tecnologías de información en herramientas para proteger y velar dichos recursos, y como herramientas que son, también deben existir políticas de uso más robustas para su uso e incluso para su desuso.

- **La clasificación de los riesgos de información**

Es un aspecto en el que varias organizaciones discreparon y por razones entendibles como su razón social, su proyección, mercado objetivo, entre otras, pero se puede decir que el 100% de ellas tiene algún tipo de clasificación por muy básico que sea, lo cual es positivo y facilita el desarrollo e implementación de políticas y estándares para el mejoramiento de estos procesos de evaluación y administración de riesgos de información a nivel de TI.

- **El futuro de la gestión de riesgos de información a nivel TI**

El 100% concuerda que siempre habrán mejoras que realizar en este aspecto, a medida que la tecnología avance los riesgos cambian y toman forma más amenazante, proteger la información se convertirá en un objetivo de negocio, en el cual no solamente esté involucrado el área de TI, sino también todas las áreas de las organizaciones, entendiendo el área de TI como un área transversal a todas y la información como el activo más valioso para la organización.

De lo anterior se puede inferir que el fin máximo a largo plazo al establecer la gestión de riesgos de información a nivel de TI como objetivo de negocio y colocando TI como área transversal en la organización, se busca integrar TI con los objetivos de negocio, lo cual es uno de los objetivos principales de COBIT.

4.2.3 Estado actual de las organizaciones

De acuerdo a las respuestas dadas por las distintas organizaciones y profesionales encuestados, al análisis de información realizado y otros ciertos parámetros del mercado y de normatividad vigente en Colombia con respecto a las PYMES y la seguridad de la información en TI, se puede establecer el estado actual de las PYMES de la ciudad de Montería con base en el estándar COBIT, el cual define parámetros a través de una serie de tópicos con respecto al proceso de evaluación y administración de riesgos de TI.

Las PYMES en general se encuentran en un estado INICIAL/AD HOC (1), el cual COBIT lo define como “Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentes específicos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un

entendimiento emergente que los riesgos de TI son importantes y necesitan ser considerados” (IT Governance Institute, 2007).

De acuerdo a lo anterior y enfocándonos en los riesgos de información a nivel de TI en las PYMES de la ciudad de Montería, se puede inferir que éstos son tomados en cuenta cuando los gerentes ven que alguno de los riesgos puede representar grandes pérdidas para la organización, lo cual indica que la administración de riesgos de información no se tiene en cuenta en los planes estratégicos de la organización; también se puede decir que no existe un rol o una entidad con responsabilidades exclusivas para dicho proceso, los riesgos de TI no son valorados correctamente, por tanto la mitigación tampoco lo es.

4.2.3.1 Diagrama de flujo

El diagrama de flujo, es la representación gráfica de un proceso.

De acuerdo a la ilustración, se deduce que lo anteriormente dicho y plasmado en las encuestas con respecto a la evaluación y administración de riesgos de información a nivel de TI, en el cual, este proceso es considerado solo si existe un riesgo de información alto o que el gerente de la compañía o del proyecto considere que el riesgo puede afectar de manera significativa los planes, procesos, infraestructura, proyectos u otras entidades en desarrollo de la organización; es decir, no es una decisión estratégica basada en conocimientos, hechos o datos históricos, sino que es una decisión basada en supuestos de acuerdo a la consideración de un grupo de personas con facultades para el proceso de toma de decisiones dentro de las organizaciones; de manera que solo así es considerada la gestión de riesgos de información como parte de los planes estratégicos de la organización. De esta manera se incluye el área de TI, como parte de los procesos operativos de mitigación de riesgo, es decir, lo que comúnmente llaman “apaga incendios”, más no un área estratégica de la organización.

Para el proceso de evaluación y administración de riesgos de información a nivel de TI, se tiene el siguiente diagrama:

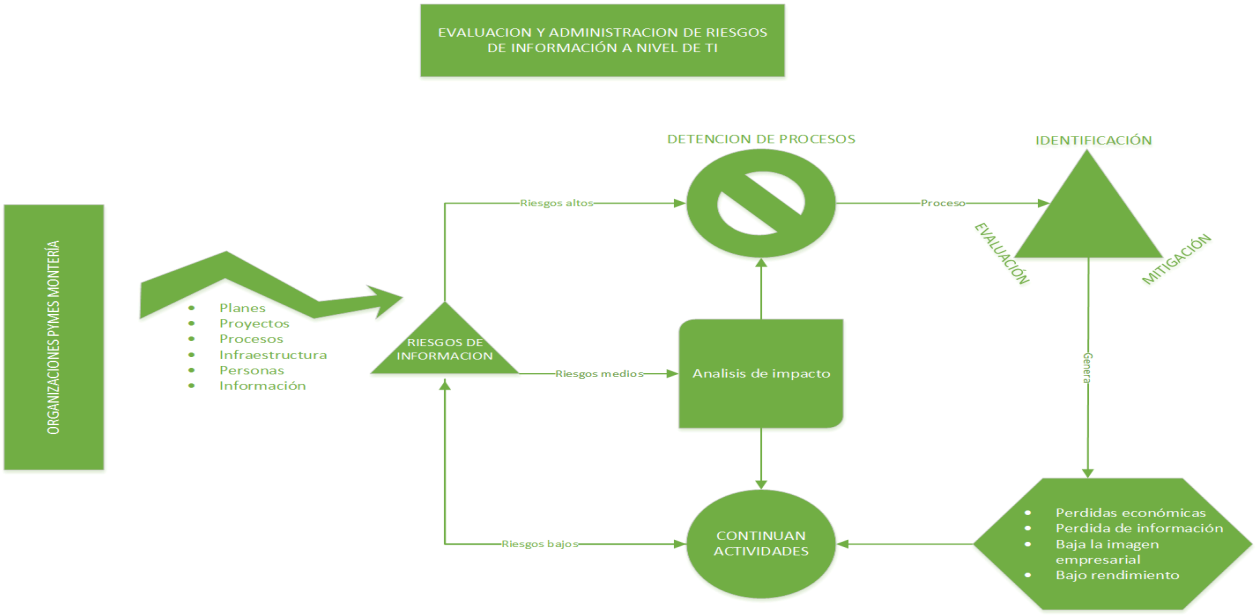


Ilustración 17: Diagrama de flujo del estado actual

Fuente: Elaboración propia

Las PYMES de Montería continuamente desarrollan planes, proyectos, llevan a cabo procesos, basados en su infraestructura, personas e información, para llegar a sus objetivos de negocio, pero solo tienen en cuenta la administración de riesgos como una alternativa para mitigar los eventos adversos que sean potenciales, o de acuerdo a decisiones gerenciales inmediatas, es decir, en donde no existe una gestión organizada.

Una vez aparece un evento y es clasificado de acuerdo a los parámetros gerenciales que se tengan en el momento, es decir, sin el conocimiento adecuado acerca de ello, sino por creencias y supuestos, se inicia un proceso minúsculo de administración de riesgo de acuerdo al nivel que considere la gerencia de la organización, el cual consiste en la identificación del riesgo, evaluar su potencial de acuerdo a su probabilidad e impacto y finalizar con un método de mitigación el cual no es gestionado previamente sino de acuerdo a una decisión de inmediatez, lo cual genera una serie de circunstancias adversas para la organización.

4.2.3.2 Roles del proceso dentro de las PYMES

Debido a que en muchas PYMES la matriz de roles y responsabilidades no está completamente definida, se desarrolla el siguiente cuadro de acuerdo a las respuestas de la encuesta y asesoramiento de profesionales de TI, estableciendo roles y responsabilidades para el proceso de evaluación y administración de riesgos de información a nivel de TI.

Cuadro 6: Roles y responsabilidades del estado actual

AREAS	ROL
GERENCIAL	Encargada de tomar las decisiones acerca de la administración de riesgos
ADMINISTRATIVA	Solventar las adversidades generadas por los riesgos a través de planes improvisados y recomendaciones externas con respecto al proceso.
OPERATIVA	Encargada de atender a las actividades de mitigación y respuesta a los riesgos
TI	Colaborar en las actividades que sean requeridas por el área operativa a través de las tecnologías de información y comunicación como herramientas administrativas y operativas para solventar adversidades.
MERCADO	Mermar actividades hasta que el riesgo sea totalmente depurado o mitigado.
INTERESADOS (Socios, proveedores, enlaces, contactos, clientes, etc.)	El proceso es transparente a ellos, por tanto rara vez intervienen.

Fuente: Elaboración propia

4.2.3.3 Actividades de la evaluación y administración de riesgos de información a nivel de TI.

Estas actividades están previamente definidas en el proyecto y comprenden la estrategia de manera eficiente y eficaz para la evaluación y administración de riesgos de información a nivel de TI.

Entendiendo el estado actual en el que se encuentran las organizaciones, estas actividades básicamente son casi irrelevantes para las organizaciones, al no conocer el marco de trabajo COBIT y no estar al tanto de otros marcos de trabajo para los aspectos relacionados al proceso tratado en el proyecto, las actividades se realizan de forma indocumentada y poco ortodoxa, basadas en las suposiciones de cómo creen los gerentes y administrativos que deberían funcionar las cosas para un mejor desarrollo del proceso.

- **Determinar la alineación de la administración de riesgos**

Al no tener una entidad o personal responsable acerca de la administración de riesgos, es difícil determinar una adecuada dirección para la administración de riesgos en las PYMES de la ciudad de Montería, lo cual se convierte en un factor determinante para lograr sus objetivos de negocio.

- **Entender los objetivos de negocio estratégicos relevantes**

Se ha mencionado anteriormente que las PYMES ocupan más del 80% del comercio en la ciudad, por lo tanto, las PYMES tienen identificados algunos objetivos estratégicos básicos y que no van más allá de la obtención de utilidades y la permanencia en el mercado.

- **Entender los objetivos de los procesos de negocio relevantes**

De acuerdo a las cifras de la Cámara de Comercio de Montería, más del 75% de las PYMES basan sus objetivos estratégicos en los procesos transaccionales de compra-venta, por lo tanto los objetivos de estos procesos están dados por fines de utilidad y rentabilidad en la organización y muchas veces son demasiado ambiciosos. Por otra parte son raras las empresas en las que se encuentran

objetivos de procesos relacionados con la seguridad de la información y/o al área de TI.

- **Identificar objetivos internos de TI y establecer el contexto de los riesgos de información**

Las empresas no cuentan con un área de TI establecida o correctamente estructurada. Es normal encontrar el área de TI de una organización como el área de soporte a equipos y dispositivos, mas no un área de TI con un verdadero objetivo de negocio, o incluida dentro de un organigrama empresarial. Por lo tanto y de acuerdo a lo anterior, es válido aclarar que el contexto de los riesgos de información no está definido y puede variar de acuerdo a las operaciones empresariales del día.

- **Identificar los riesgos de información asociados a los objetivos**

De manera que la información es el principal activo de una organización, los riesgos relacionados a ésta en las PYMES de la ciudad de Montería son claramente un factor clave para la supervivencia de la empresa. Dado que estas empresas no cuentan con un personal para la administración de riesgos o un personal de TI establecido, por ende será más difícil identificar los riesgos de información relacionados al área de TI.

El conocimiento que tienen las empresas es poco acerca del tema de riesgos de información y aunque algunas tengan conciencia al respecto, rara vez se preocupan por implementar marcos de trabajo o normas que minimicen el impacto sobre los eventos adversos que puedan ocurrir en este aspecto.

- **Evaluar y seleccionar respuestas a riesgos de información**

No existe una actividad relacionada acerca de la evaluación y selección de medidas contra los riesgos de información. Este proceso es llevado a cabo de manera inmediata al evento, lo cual deja expuesta la organización en términos de presupuesto y personal capacitado; y muchas veces sin margen de tiempo para elegir la mejor alternativa.

- **Priorizar y planear actividades de control**

Por lo general los riesgos residuales son aceptados por las organizaciones PYMES, de manera que no se implementan actividades para controlar futuros eventos, pero se debe tener en cuenta que las grandes catástrofes ocurren por la sumatoria de los riesgos residuales y rara vez por el impacto de un solo evento.

- **Aprobar y asegurar fondos para planes de acción**

Las PYMES al tener un presupuesto limitado, realmente no cuentan con fondos para establecer un plan de acción para contrarrestar eventos adversos, rara vez son implementados métodos como la capacitación de personal de la empresa para minimizar el impacto del evento o la contratación directa de manera temporal para solventar estas adversidades.

- **Mantener y monitorear un plan de acción de riesgos de información**

El plan de acción de las organizaciones generalmente se realiza de manera inmediata al evento, es por esto que mantener y monitorear estos planes se hace un proceso casi inexistente. Aunque muy pocas organizaciones rara vez implementan métodos como una auditoria interna para identificar falencias e incluso probabilidades de riesgos asociados con la información.

4.2.3.4 Gráfico RACI

El siguiente gráfico describe las actividades principales del proceso de evaluación y administración de riesgos de información a nivel de TI, enlazados a quienes son sus responsables (R), rendir cuentas(A), consultados (C) y/o informado (I).

El gráfico dentro de las PYMES prácticamente es inexistente con respecto al proceso de evaluación y administración de riesgos de información a nivel de TI, por tal motivo, se decide desarrollar un gráfico RACI entendiendo de manera general el común de las organizaciones:

Cuadro 7: Gráfico RACI – Estado Actual

GRÁFICO RACI						
	GERENCIAL	ADMINISTRATIVA	OPERATIVA	TI	MERCADO	INTERESADOS
Determinar la alineación de la administración de riesgos	**R**	**A**	**I**			**R/I**
Entender los objetivos de negocio estratégicos relevantes	**A**	**R**				**I**
Entender los objetivos de los procesos de negocio relevantes	**A**	**R**	**I**			
Identificar objetivos internos de TI y establecer el contexto del riesgo de información	**C**	**R**		**C**		**I**
Identificar los riesgos de información asociados a los objetivos	**A**	**R**	**I**	**A**	**C**	

Evaluar y seleccionar respuestas a riesgos de información	**R**	**R**	**I**	**I**	**I**	
Priorizar y planear actividades de control	**R**	**R**	**A**	**I**		
Aprobar y asegurar fondos para planes de acción	**A**	**R**	**I**			
Mantener y monitorear un plan de acción de riesgos	**R**	**C**	**I**		**I**	

Fuente: Elaboración propia

4.2.4 Estado deseado de las organizaciones

En cuanto al estado deseado de las organizaciones se puede establecer con las mismas bases de COBIT para el siguiente estado REPETIBLE PERO INTUITIVO (2), sin dejar atrás las mejoras que sugieren las organizaciones a partir de las encuestas realizadas y sus necesidades, entendiendo los parámetros a los que están sometidas; las mejores prácticas de TI a partir de estándares aceptados internacionalmente e incluso recomendaciones por expertos en temas de gestión de seguridad de la información a nivel de TI. Por tanto se define el estado deseado como para el proceso de evaluación y administración de riesgos de TI como REPETIBLE PERO INTUITIVO (2), aunque se podría extender logrando mejores avances en este aspecto, es decir, pasando al siguiente estado, de manera que las PYMES de la ciudad de Montería puedan afrontar con mayor capacidad los riesgos relacionados con la información a nivel de TI, del mismo modo que estas organizaciones establecen políticas y planes para este proceso.

Por lo tanto y de acuerdo a lo anterior y al marco de mejores prácticas COBIT, las PYMES pretenden alcanzar un nivel cerca del DEFINIDO (3); de manera que combinando ambos niveles (2) y (3) para el proceso de evaluación y administración de riesgos de TI, se puede definir como:

Identificar los riesgos de información claves para la organización y definir planes para la mitigación, desarrollando políticas sólidas sobre evaluación de riesgos de información de manera regular y no a disposición de los gerentes de proyecto; documentar las actividades a seguir para la administración de riesgos de información abarcando toda la organización y que estén a disposición de todos los usuarios, las cuales sean eficaces y aceptadas en todos los roles organizacionales considerando que es una responsabilidad de toda la organización, los cuales deben estar alineados con los objetivos estratégicos de negocio y los procesos claves de la organización.

4.2.4.1 Diagrama de flujo

La ilustración 18 muestra el diagrama de flujo ideal para el estado deseado de las organizaciones y las actividades que se deben realizar para alcanzarlo.

Normalmente en las organizaciones PYMES existe un flujo constante de información, personas, planes, proyectos y estructuras, para llevar a cabo los objetivos estratégicos de negocio y los procesos claves para el cumplimiento de estos; a partir de aquí, se debe desarrollar la gestión de riesgos en toda la organización, designando responsabilidades en el proceso de evaluación y administración de riesgos de información a nivel de TI.

El área de TI o el responsable de TI, es quien debe tener la mayor responsabilidad en el proceso, la cual se expresa con una serie de actividades que conforman la estrategia para alcanzar el estado deseado. Actividades que no solamente minimizarán el impacto de los riesgos de información, sino que también menos tiempo de interrupción de procesos, continuidad de los procesos, valor agregado en los productos/servicios, solidez competitiva, mejora de la imagen/reputación de la organización, menor impacto de adversidades relacionadas a los riesgos de

información, metas alcanzables, mayor sostenibilidad e incluso se podría decir que una mejora en el retorno de la inversión de los interesados.

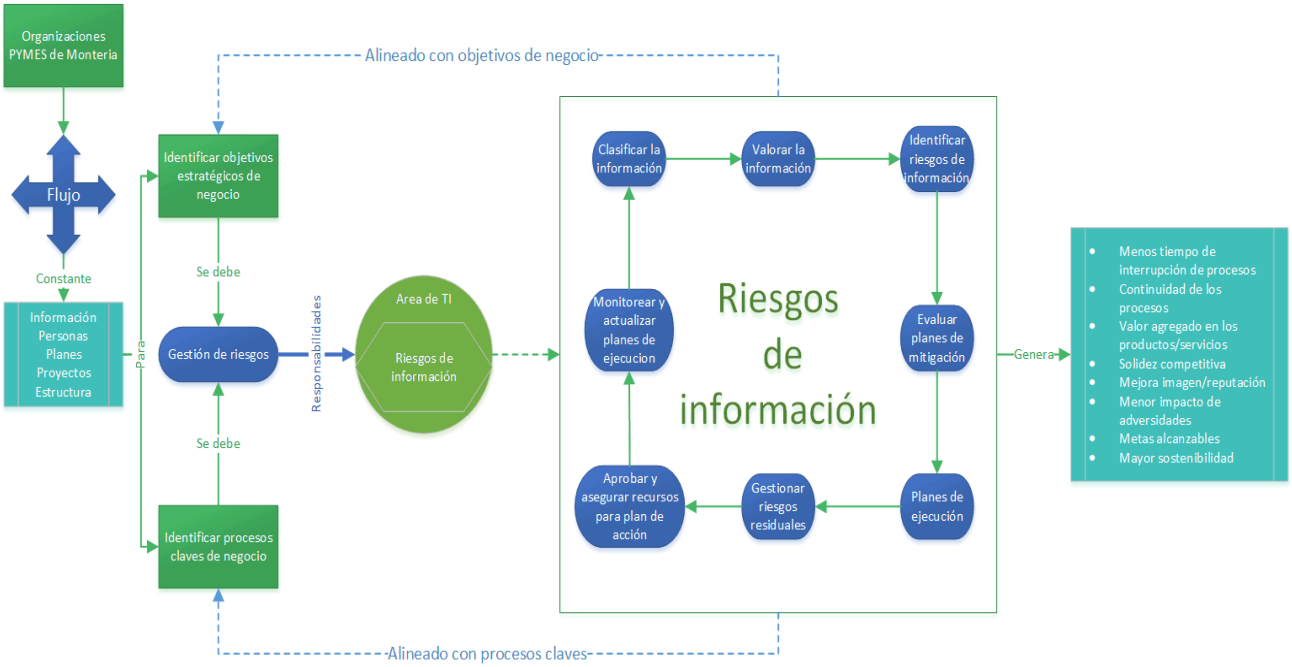


Ilustración 18: Diagrama de flujo del estado deseado

Fuente: Elaboración propia

4.2.4.2 Roles del proceso dentro de una PYMES

De acuerdo al estado deseado para el proceso, se redefine el cuadro de roles y responsabilidades de las PYMES para el proceso de evaluación y administración de riesgos de información a nivel de TI.

Cuadro 8: Roles y responsabilidades del estado deseado

AREAS	ROL
GERENCIAL	Encargada de tomar las decisiones acerca de la administración de riesgos
ADMINISTRATIVA	Realizar control y monitoreo, y designar responsabilidades para una correcta gestión de riesgos
OPERATIVA	Encargada de atender a las actividades de mitigación y planes de acción
TI	Minimizar el impacto de los riesgos de información sobre la organización, a través de un control sobre las actividades del proceso.
MERCADO	Continuidad de los procesos
INTERESADOS (Socios, proveedores, enlaces, contactos, clientes, etc.)	Interesarse por los procesos que repercuten en su inversión.

Fuente: Elaboración propia

4.2.4.3 Actividades de la evaluación y administración de riesgos de información a nivel de TI

Comprenden la estrategia correspondiente al estado deseado para la evaluación y administración de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería:

- **Determinar la alineación de la administración de riesgos**

Se debe incluir la administración de riesgos de la organización como parte de los planes estratégicos de la organización.

- **Entender los objetivos de negocio estratégicos relevantes**

Identificar los objetivos de negocio estratégicos claves para la generación de utilidades y sostenibilidad de la organización durante un largo periodo de tiempo. A su vez, revisar que dichos objetivos que se ajusten a la realidad y contexto empresarial.

- **Entender los objetivos de los procesos de negocio relevantes**

Identificar cuáles son los procesos claves y el fin determinado de éstos, para desarrollar y documentar actividades concretas para llevarlo a cabo.

- **Identificar objetivos internos de TI y establecer el contexto de los riesgos de información**

Establecer roles y responsabilidades para el área de TI, definiendo objetivos claves que estén alineados con los objetivos estratégicos de negocio y objetivos claves de negocio; para establecer una gestión de riesgos de información a nivel de TI.

- **Identificar los riesgos de información asociados a los objetivos**

Tomar conciencia que la información es el activo más importante de las organizaciones y por ende hay que protegerlo, identificando los riesgos de información que afecten de manera más significativa los objetivos de negocio estratégicos y los objetivos de los procesos de la organización.

- **Evaluar y seleccionar respuestas a riesgos de información**

Establecer planes de manera anticipada que hagan frente a los riesgos de información que se puedan presentar y que afecten los objetivos estratégicos de la organización.

- **Priorizar y planear actividades de control**

Tomar conciencia acerca de los riesgos residuales y el perjuicio que pueden generar, si no realizar actividades de control, en la misma medida que se deben establecer políticas para la seguridad de la información de acuerdo a su clasificación con respecto a los objetivos de negocio.

- **Aprobar y asegurar fondos para planes de acción**

Intentar establecer un fondo de recursos para los planes de acción y respuesta a los riesgos de información, de manera que se puedan anticipar posibles eventos adversos con menor impacto sobre la organización y sus objetivos.

- **Mantener y monitorear un plan de acción de riesgos de información**

Revisar y actualizar periódicamente los planes de acción de riesgos de información al contexto organizacional.

4.2.4.4 Gráfico RACI estado deseado

De acuerdo al estado deseado y las actividades que conforman la estrategia para alcanzarlo, se redefine el gráfico RACI indicando las responsabilidades, consultas, informe y rendición de cuenta expresado de la siguiente manera.

Cuadro 9: Grafico RACI - Estado deseado

GRAFICO RACI						
	GERENCIAL	ADMINISTRATIVA	OPERATIVA	TI	MERCADO	INTERESADOS
Determinar la alineación de la administración de riesgos	**A**	**R**	**I**	**C**	**I**	**I**
Entender los objetivos de negocio estratégicos relevantes	**R**	**A**	**I**	**I**	**I**	**C**
Entender los objetivos de los procesos de negocio relevantes	**A**	**R**	**I**	**C**	**C**	**I**
Identificar objetivos internos de TI y establecer el contexto del riesgo de información	**A**	**R**	**I**	**R**		**I**

Identificar los riesgos de información asociados a los objetivos	**A**	**C**	**I**	**R**	**I**	**I**
Evaluar y seleccionar respuestas a riesgos de información	**R/A**	**R**	**I**	**C**	**I**	**C**
Priorizar y planear actividades de control	**R**	**R**	**A**	**C**	**I**	**I**
Aprobar y asegurar fondos para planes de acción	**R**	**A**	**I**	**I**		**I**
Mantener y monitorear un plan de acción de riesgos	**A**	**R**	**I**	**C**	**I**	

Fuente: Elaboración propia

4.3 PROGRAMACION

4.3.1 Desarrollo de un modelo para la evaluación y administración de riesgos de información a nivel de ti en pymes de la ciudad de montería a partir del marco de trabajo cobit 5

Para el desarrollo del modelo se debe tener claro que las organizaciones previamente deben definir sus procesos claves de negocio y objetivos estratégicos, pues el principio que plantea COBIT como marco de trabajo, de otra manera la gestión de riesgos no convergerá hacia los objetivos de negocio y descuidará los procesos claves de la organización.

De acuerdo a lo anterior se debe establecer roles y responsabilidades en la gestión de riesgos, para luego ir profundizando en los riesgos de información a nivel de TI.

4.3.2 Estableciendo roles y responsabilidades

De acuerdo al planteamiento de las actividades, se deben seguir previamente las siguientes recomendaciones para lograr un correcto establecimiento de roles y responsabilidades dentro de la organización:

- Establecer un personal encargado o responsable de la gestión de riesgos en las distintas áreas de la organización, o si es posible, un área de gestión de riesgos de manera independiente para toda la organización.
- Establecer un área o personal encargado de los temas relacionados con Tecnología e Información de la organización.
- Asegurar que los nuevos roles y responsabilidades estén alineados con los objetivos de negocio y procesos claves de la organización.

De acuerdo a lo anterior se puede definir una nueva relación de organigrama o cuadro de mando con la gestión de riesgos, estableciendo las nuevas áreas de Tecnología e Información y gestión de riesgos, como parte fundamental de la organización, incluidas en la estrategia organizacional.

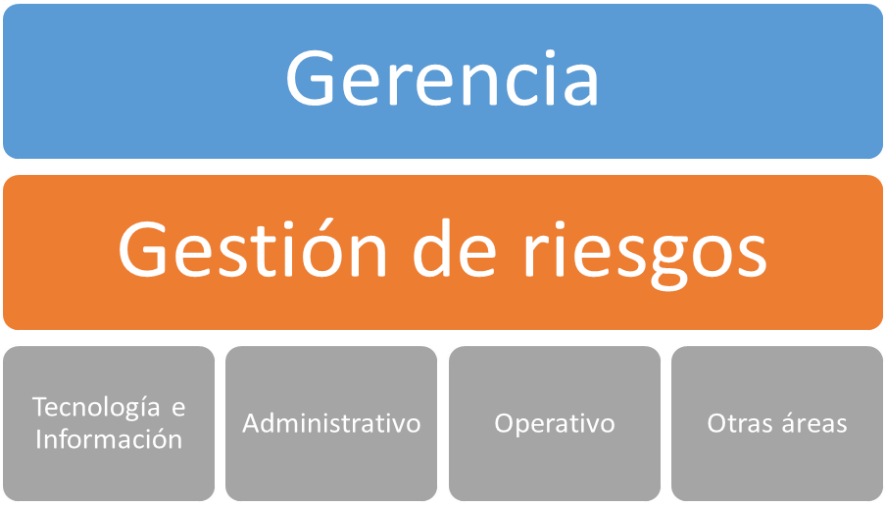


Ilustración 19: Esquema de relación de la gestión de riesgos

Fuente: Elaboración propia

De esta manera se incluye la gestión de riesgos en el plan estratégico de las organizaciones, designando funciones a cada una de las áreas como parte de un conjunto de elementos que contribuyen a la gestión de riesgos, para que la gerencia se encargue de tomar decisiones basadas en el conocimiento, hechos y datos históricos relevantes para la gestión de riesgos.

Las organizaciones serán autónomas en sus decisiones de la creación de nuevas áreas, pero deben ser conscientes que éstas son creadas para beneficio de los objetivos de negocio.

4.3.3 Establecer área de Tecnología de la Información

La organización debe ser consciente que las tecnologías de información son parte de la estrategia de la organización para alcanzar sus objetivos. A nivel gerencial se deben designar funciones acerca de las tecnologías de información, tanto para su infraestructura, procesos, desarrollo, monitoreo y todas las actividades que la componen. Esta designación se debe realizar de manera responsable, otorgando privilegios y responsabilidades a la (las) persona (personas) encargada de área.

- El área deberá tener como primer objetivo, garantizar que las tecnologías de la información estén alineadas y contribuyan con los objetivos estratégicos de la organización.
- Las personas encargadas del área de Tecnologías de la Información deberán contar con los conocimientos suficientes para hacer frente a las responsabilidades asignadas.
- Se deben designar roles y responsabilidades internamente en el área, para garantizar la completa armonía y la no redundancia de tareas.
- Se deberá tener en cuenta que la gerencia de la organización puede hacer uso de sus facultades para designar otras funciones relacionadas con el cargo, que se consideren de importancia para el área de tecnologías de la información.

4.3.4 Estableciendo la gestión de riesgos

Se debe establecer un área de gestión de riesgos determinada por la gerencia y la administración de la organización, entendiendo sus fines y propósitos. Al igual que en todas las organizaciones grandes o pequeñas, privadas o públicas, u otro tipo de clasificación, la gestión de riesgos:

- Su objetivo principal será garantizar la continuidad de los procesos claves de la organización mientras se siguen ejecutando actividades propias del área.
- Designar roles y responsabilidades por área o grupo en particular, encargados de la gestión de riesgos de la organización, garantizando que no exista redundancia de tareas.
- La gestión de riesgos debe responder a todo tipo de adversidades que se puedan presentar en la organización, por ello deberá ser un área de gestión participativa e incluyente al personal de la organización.
- Será la gerencia que con base al área de gestión de riesgos, tome la decisión final para garantizar la continuidad los procesos claves de la organización.

La gestión de riesgo aparte de ser un área de la organización, también se debe considerar como un proceso clave y estratégico para la organización, el cual debe considerar los riesgos de todas las áreas de la organización, incluyendo las nuevas áreas que se vayan creando.

Por su parte el área de Tecnologías de la Información también deberá responder a los asuntos relacionados a su campo de acción en las demás dependencias, incluyendo la gestión de riesgos de TI como principal conocedor del tema, apoyados en el proceso o área de gestión de riesgos.

4.3.5 Riesgos de información a nivel de TI

Es la unión y convergencia entre la gestión de riesgos y el área de TI, para coordinar, ejecutar y monitorear las actividades relacionadas con los riesgos de información dentro del área. Se definirá como un proceso parte de la gestión de riesgos, en el cual su principal actor son los organismos y personal encargado del área de TI.

- Tiene como objetivo principal, garantizar la continuidad de los procesos de TI, como estrategia fundamental para el alcance de los objetivos de negocio y los procesos claves de la organización.
- Se considera el área de TI como principal actor, ya que es la dependencia que posee los conocimientos suficientes para abordar el proceso. Esto sin dejar de tener en cuenta las demás dependencias.

De acuerdo a lo anterior, se pueden definir las actividades o procesos para llegar a cabo la correcta evaluación y administración de riesgos a nivel de TI en las PYMES de la ciudad de Montería.

4.3.6 Procesos para la evaluación y administración de riesgos de información a nivel de TI en las PYMES de la ciudad de Montería.

Una vez definidas las áreas de gestión de riesgos y el área de Tecnologías de la Información dentro de la organización, se dirige al objetivo final del proyecto, a través de una serie de actividades que integran y conforman el estado deseado de

las PYMES con respecto al proceso. Estas actividades están destinadas a los activos de información del área de TI.

Ilustración 20: Representación gráfica del modelo

Fuente: Elaboración propia

4.3.6.1 Clasificar la información

La clasificación de la información está afectada por tres criterios disponibilidad, integridad y confidencialidad.

- Disponibilidad: Se basa en el tiempo de inaccesibilidad de la información y que podría causar pérdidas a la organización.

- Integridad: Se basa en la modificación no autorizada a la información.
- Confidencialidad: Se basa en los niveles de acceso a la información.

Cuadro 10: Niveles de disponibilidad

DISPONIBILIDAD		
Tipo	**Descripción**	**Valor**
No afecta	Sin importar el tiempo que esta información no sea accedida, no afectan los procesos de TI o de la organización.	1
Mensual	Genera pérdidas después de un mes sin poder acceder a la información.	2
Semanal	Genera pérdidas después de una semana sin poder acceder a esta información.	3
Diaria	Genera pérdidas después de 2 o 3 días sin poder acceder a esta información.	4
Horas	Genera pérdidas después de unas 2 o 3 horas sin poder acceder a esta información.	5

Fuente: Elaboración propia

Cuadro 11: Niveles de Integridad

INTEGRIDAD		
Tipo	**Descripción**	**Valor**
Fácil	Se puede reparar fácilmente	1
Medio	Se puede reparar pero aun así dejará pérdidas.	2
Difícil	Se puede reparar pero dejará pérdidas significativas	3
Muy difícil	Se recuperará parcialmente, y dejará pérdidas significativas	4
Imposible	No se puede reparar, las pérdidas son grandes.	5

Fuente: Elaboración propia

Cuadro 12: Niveles de confidencialidad

CONFIDENCIALIDAD		
Tipo	**Descripción**	**Valor**
Pública	Información que puede ser consultada por cualquier persona, interna o externa de la organización.	1
Semiprivada	Información de uso interno de la organización y compartida solo con los interesados. Puede ser accedida por los niveles gerenciales y administrativo.	3
Privada	Información de uso interno para la organización, que no debe ser compartida por fuera de la organización. Solo puede ser accedida por el nivel gerencial y administrativo.	3
Restringida	Información de uso estratégico interno, que solo es de acceso con permisos especiales de la gerencia.	4
Secreta	Información gerencial de la organización. Solo puede ser accedida por el gerente o directivo de la empresa	5

Fuente: Elaboración propia

4.3.6.2 Valorar la información

La valoración se realizará de acuerdo a la clasificación y el resultado promedio de los 3 criterios de información. Se valorará la criticidad de la información de acuerdo al resultado, es decir, entre más se aproxime a 5 el valor resultado, más crítica será la información y por tal motivo su seguridad deberá ser mayor.

- **Criticidad Alta:** Se concibe el resultado promedio superior a 3.
- **Criticidad media:** Se concibe el resultado promedio entre 1.6 y 2.9

- **Criticidad baja:** se concibe el resultado promedio entre 1 y 1.5

4.3.6.3 Identificar los riesgos de información:

Los riesgos se pueden presentar de manera imprevista antes, durante o después de la ejecución de una actividad. En este punto el área de TI debe analizar previamente qué eventos pueden presentarse en la ejecución de las actividades del área de TI, y dependiendo de su origen se identifican los riesgos que se pueden presentar:

Cuadro 13: Tipos de riesgos

Tipos de riesgos		
Tipo	**Descripción**	**Ejemplos**
Infraestructura	Aquellos eventos que están relacionados con catástrofes en los equipos y dispositivos tecnológicos	Daño de equipos, equipos obsoletos, tecnologías no compatibles, energía eléctrica, entre otros.
Seguridad	Eventos que atenten contra los criterios de la información u otro activo tecnológico	Virus, acceso no autorizado a la información, fallas de seguridad, bases de datos sin restricciones, entre otros.
Gestión	Eventos desencadenados por la ausencia de políticas y procedimientos para el uso de las tecnologías de la información	Políticas de seguridad inexistente o ineficiente, fallas en los manuales de procedimientos, mala reglamentación contractual, entre otros.

Operación	Mal uso de las tecnologías de información, ya sea por falta a los procedimientos y políticas de la organización	Uso inadecuado de los equipos, manuales de usuario y de sistema inexistentes, roles y responsabilidades mal definidos, entre otros.
Recursos Humanos	Eventos relacionados con las fallas humanas, ya sea por descuido o intencionalidad	Ingeniería social, error humano, error intencional, entre otros.

Fuente: Elaboración propia

Es necesario que las organizaciones puedan identificar las causas y las consecuencias relacionadas al riesgo, de esta manera se podrán implementar planes y estrategias de respuesta más acertadas y que puedan dar solución al problema presentado.

4.3.6.4 Evaluar los riesgos de Información:

De acuerdo a la identificación de los riesgos, el área de TI de realizar una clasificación ajustada a la probabilidad e impacto de cada de uno de los eventos, es decir, qué eventos y por qué traerían consecuencias más o menos perjudiciales para los objetivos de la organización.

- **Probabilidad**: Evaluar el riesgo y su probabilidad de ocurrencia.

Cuadro 14: Probabilidad del riesgo

Probabilidad		
Valor	Significado	Porcentaje
1	Raro	1 a 15%
2	Poco probable	16 a 40%
3	Probable	41 a 60%
4	Muy probable	61 a 79%
5	Casi seguro	80 a 99%

Fuente: Elaboración propia

- **Impacto**: Evaluar la consecuencia causada por efecto de un evento.

Cuadro 15: Impacto del riesgo

Impacto	
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Fuente: Elaboración propia

4.3.6.5 Clasificar los riesgos de Información:

Consiste en emparejar el resultado de la clasificación de riesgos. Por tal motivo los riesgos se clasifican de acuerdo a su resultado de riesgo inherente.

Cuadro 16: Rangos de los riesgos

Rango del riesgo o severidad	
1	Bajo
2	Medio
3	Alto
4	Extremo

Fuente: Elaboración propia

De esta manera el mapa de clasificación de riesgos estaría dado por el siguiente cuadro:

Cuadro 17: Matriz probabilidad-impacto

Riesgo Inherente		Impacto				
		1 Muy bajo	2 Bajo	3 Medio	4 Alto	5 Muy alto
Probabilidad	1 Muy bajo	Bajo	Bajo	Bajo	Medio	Medio
	2 Bajo	Bajo	Medio	Medio	Alto	Alto
	3 Medio	Bajo	Medio	Alto	Alto	Extremo
	4 Alto	Medio	Alto	Alto	Extremo	Extremo
	5 Muy alto	Medio	Alto	Extremo	Extremo	Extremo

Fuente: Elaboración propia

La matriz de clasificación combina los valores de probabilidad e impacto, asignándoles una valoración cualitativa, pero de manera general la matriz de clasificación también se le puede asignar valores cuantitativos, y teniendo en cuenta el nivel de severidad de los riesgos la clasificación estaría dada de la siguiente manera:

- **Severidad baja:** Valores menores que 3
- **Severidad media:** valores entre 4 y 6
- **Severidad alta:** Valores entre 7 y 10
- **Severidad extrema:** Valores superiores a 11

4.3.6.6 Priorizar los riesgos

Una vez realizada la clasificación de los riesgos en la matriz de clasificación, se procede a priorizar los riesgos de acuerdo a su severidad o rango.

- **Severidad extrema:** Son riesgos totalmente inaceptables para la organización. Aquellos riesgos que amenazan significativamente los objetivos de negocio y su probabilidad e impacto tienen valores altos. Si llegan a suceder se deben tener planes de respuesta para minimizar su impacto.
- **Severidad alta:** Riesgos que significan una amenaza potencial para la organización y sus objetivos de negocio, son riesgos inaceptables que necesitan atención de la gerencia y sustancialmente desencadenan opciones de respuesta si suceden.
- **Severidad media:** Riesgos que son aceptados de acuerdo a los niveles de tolerancia y apetito del riesgo de las organizaciones. Pueden ser tratados a nivel gerencial o administrativo. Considerablemente son riesgos que se le pueden aplicar planes de respuesta con el fin de reducir su probabilidad o impacto.
- **Severidad baja:** Son riesgos que no tienen un mayor impacto y generalmente son aceptados por la organización y representan una oportunidad de crecimiento generalmente. Algunas veces son tratados con planes de respuesta.

Se puede expresar también que la priorización de los riesgos se realiza de acuerdo a los recursos de la organización, es decir, a su capacidad para afrontar cada uno

de los riesgos identificados y priorizados. Los recursos varían desde presupuesto, infraestructura, personas y conocimientos.

El riesgo general en la organización indica el promedio general de los riesgos específicos, priorizados dentro de cada organización.

4.3.6.7 Plan de respuesta a los riesgos de Información:

Basado en el resultado de la priorización de los riesgos, se establecen las estrategias para cada uno de los riesgos, aquellos con mayor severidad regularmente se le deben aplicar estrategias preventivas tales como eliminar, mitigar o transferir, al igual que aquellos riesgos con severidad baja las organizaciones pueden tomar la decisión de aceptarlos o escalarlos.

La siguiente es la designación del plan de respuesta de acuerdo al resultado de priorización. Para resaltar que la siguiente información no es camisa de fuerza para ser ejecutado a cabalidad, también debe considerarse la valoración de expertos dentro del área de TI para afrontar los riesgos.

- **Riesgos de severidad extrema:** Generalmente son riesgos que deben ser evitados o eliminados, reducidos o mitigados y algunas veces si es posible transferirlo, con el fin de minimizar su probabilidad de ocurrencia o impacto.
- **Riesgos de severidad alta:** Son riesgos que preferiblemente deben ser evitados; y aunque algunos no pueden serlo, se recurre a la mitigación o transferencia, con el fin de reducir su probabilidad y/o impacto.
- **Riesgos de severidad media:** Son riesgos que pueden ser aceptados por la organización, siempre y cuando su probabilidad de impacto sea considerada teniendo en cuenta la tolerancia y el apetito del riesgo de cada organización. Su estrategia de respuesta varía entre la mitigación, aceptación, transferencia o escalabilidad, ya que quien toma la decisión final es la alta gerencia.

- **Riesgos de severidad baja:** Generalmente son aceptados, de manera que pocas veces se utiliza una estrategia de respuesta contra éstos, aunque en algunos casos pueden ser escalados.

Se debe aclarar que esta información varía de acuerdo a los niveles de tolerancia y apetito del riesgo de cada organización, teniendo en cuenta también la asignación de los recursos y que se cuenten con ellos para cada estrategia.

Elegir la estrategia más adecuada para la atenuación del riesgo, es crucial para las organizaciones, por ello es fundamental que se definan cada una de las estrategias independientemente de cuáles sean las acciones que se requieran para llevarlas a cabo.

- **Evitar el riesgo:** Necesariamente es la estrategia ideal en aquellos riesgos con severidad alta o extrema; esta estrategia consiste en reducir a cero la probabilidad o el impacto del riesgo, de este modo podemos bloquear la manera en cómo el riesgo pueda afectar los objetivos estratégicos de la empresa. Las actividades tienden generalmente hacer cero el impacto pues la probabilidad de ocurrencia normalmente es externa a la organización.
- **Reducir el riesgo:** Es la estrategia para reducir la probabilidad o el impacto de los riesgos, con el fin de que si existe un riesgo de nivel alto, este puede ser disminuido a niveles de tolerancia aceptados por la organización. Las actividades que conforman esta estrategia pueden variar desde implementar controles y políticas para afrontar el riesgo con la experticia necesaria de la gestión de riesgos, hasta definir procedimientos lo suficientemente claros para la ejecución de actividades, que puedan disminuir la probabilidad de ocurrencia.
- **Transferir el riesgo:** Transferir el riesgo consiste en transportar el impacto negativo del riesgo a un tercero, dándole permisos para la administración y gestión del riesgo transferido. La estrategia puede ser

utilizada mediante la adquisición de seguros relacionados con los incidentes de información en el área de TI, o fijar acuerdos de riesgo compartido entre tanto la información sea compartida.

Esta estrategia no elimina el riesgo de la organización, pero si puede equilibrar las cargas en cuanto a esfuerzo y consecuencias económicas si llegasen a presentarse.

- **Escalar el riesgo:** Es una estrategia reciente que consiste en escalar el riesgo a un área de mayor operación sobre el riesgo gestionado, es decir, que el riesgo puede ser escalado del área de TI a recursos humanos e incluso directamente a la gerencia, de acuerdo al área mayormente afectada. En este caso la estrategia puede ser escalable y similar a transferible, pues de acuerdo a la escalabilidad las dos áreas podrán unir esfuerzos para reducir o mitigar el riesgo.
- **Aceptar el riesgo:** Aceptar el riesgo es una estrategia que generalmente debe ser utilizada para riesgos de nivel bajo y algunos otros de nivel medio que considere la organización. La estrategia consiste en no lanzar contramedidas hacia un riesgo y aceptar las pérdidas, asumiendo que el riesgo al que se enfrenta la organización es conocido y previamente clasificado.

  La decisión de aceptación debe ser a nivel gerencial con el soporte del área de TI; de este modo, el área de TI debe encargarse de contar con un plan de contingencia en caso de que el riesgo llegase a ocurrir en el transcurso de las actividades.

Los riesgos de información a nivel TI suelen ser perjudiciales para las empresas, pues comúnmente se ven enfrentadas a implementar nuevas tecnologías en la que sus requerimientos son altos en términos de software, hardware y otro tipo de recursos. El área de TI debe ser consciente que la información es el activo más valioso y puede significar una ventaja competitiva; pues la información en su ciclo como activo es transformada en conocimiento.

Información analizar:	Base de datos										
Clasificar la información											
Disponibilidad	Integridad	Confidencialidad									
4	4	4									
Identificar los riesgos		Causa	Efecto	Evaluar los riesgos		Clasificar los riesgos	Nuevo orden a partir de la priorización	Priorizar los riesgos	Plan de respuesta		Asegurar fondos	Monitorear y actualizar
Evento	Tipo de riesgo			Probabilidad	Impacto	Severidad			Estrategia	Actividad		
Servidor averiado o con fallas físicas	Infraestructura	Mal instalado, partes defectuosas	Perdida de información, ritmo de trabajo desacelerado	1	4	Media		Datos corruptos	Reducir el impacto	Disponer de un script para validación de datos	Disponer de recursos	Clasificación de la información
Virus en el servidor	Seguridad	Ataques externos en la red	Robo de información, perdida de información	2	3	Alta		Acceso no autorizado	Reducir la propabilidad	Control de usuarios en plataforma	personal calificado	Identificación de nuevos riesgos asociados
Acceso no autorizado	Gestión	No hay control de acceso	Robo de información, información adulterada	3	3	Alta		Virus en el servidor	Reducir la propabilidad	Antivirus licenciado y actualizado	Compra de licencia de antivirus	Priorización de riesgos
Datos corruptos	Operación	Virus, acceso indebido, error humano, error intencional	Información corrupta, malas decisiones en la compañía	4	4	Extrema		Servidor averiado o con fallas	Transferir	Asegurar la infraestructura con el proveedor de equipos y dispositivos	Seguro por la compra de equipos y dispositivos	Planes de respuesta
Ampliacion del servidor de base de datos	Infraestructura	Se requiere realizar una ampliacion de la base de datos o migrar la BD a un servidor mas actual	Cambios en el modelo relacional y sintaxis de la BD	2	2	Media		Ampliacion del servidor de base de datos	Transferir	Alquiler de los servicios de otro servidor	Recursos economicos para el alquiler de los servicios	Priorización de riesgos
Incompatibilidad con software empresarial	Infraestructura	Instalacion de un nuevo software no compatible con la base de datos de la empresa	Instalar un servidor de base de datos adicional	2	1	Media		Incompatibilidad con software empresarial	Transferir	Compartir los servicios con la empresa manufacturera	Recursos economicos para compartir las responsabilidades de gestión	Priorización de riesgos
Backups incompletos	Operación	Los Backups automaticos de la base de datos no se realizaron completamente.	Pasar a los procesos manuales de backups	1	2	Bajo		Backups incompletos	Aceptar	Realizar los backups manualmente	Recursos de tiempo disponibles	Identificación de nuevos riesgos asociados

Ilustración 21: Ejemplo de aplicación del modelo

Fuente: Elaboración propia

4.3.6.7.1 Asegurar los recursos del plan de respuestas

Fuera de ser una actividad dentro del proceso, siempre será necesario que la organización revise adecuadamente su presupuesto para la gestión de riesgos, incluyendo aquellos relacionados con el área de TI. Del mismo modo la organización que sea capaz de tomar una decisión de ejecutar un plan de respuesta, debe contar con los recursos suficientes para su ejecución.

4.3.6.8 Monitorear y actualizar el plan de respuesta

Monitorear y actualizar es la última actividad del modelo, la cual consiste en después de una exhaustiva revisión responder preguntas como, ¿El modelo aún es efectivo? ¿Qué es necesario mejorar? ¿Qué otras alternativas existe? ¿Cómo se pueden implementar?

De este modo, la organización se encargará de revisar cada una de las actividades comprendidas en este modelo y validar si el modelo aún está vigente de acuerdo al contexto organizacional, entendiendo que el contexto organizacional es cambiante constantemente, que es dinámico, que a medida que las tecnologías de información crecen en aplicación y utilidad, la información también varía su flujo e incluso en su

transcurso sufre cambios, cambios que están asociados a nuevos riesgos que son a los que estará expuesta la organización.

Una vez dicho lo anterior, es necesario reevaluar los riesgos de información de acuerdo al contexto organizacional, es decir, una vez la organización se encuentre frente a un cambio, el cual puede ser estructural, organizacional, de contexto, de funciones u otro tipo de cambio, será necesario aplicar nuevamente la clasificación y valoración de la información, identificación y clasificación de los riesgos, para finalmente revisar sus planes de respuesta, de acuerdo también a su nivel general del riesgo, niveles de tolerancia y apetito, sin dejar de lado la valoración de expertos.

La revisión y actualización periódica será necesaria cada cuanto lo considere la gerencia de la organización, con un periodo no mayor a 6 meses, mejorando y actualizando todos los aspectos que sean considerados.

4.3.6.9 Recomendaciones de aplicación del modelo

- Para tener en cuenta en la aplicación del modelo la creación del área de TI y los procesos relacionados a la gestión de riesgos, deben estar previamente definidos.
- Revisión previa del modelo y su aplicabilidad dentro de la organización.
- El contexto organizacional al que está expuesta la organización y los cambios periódicos comunes.
- Revisar los parámetros de seguridad aplicados a la información clasificada como sensible dentro del área de TI, el acceso a esta información debe estar definido correctamente.
- Los riesgos que se presentan en otras áreas y son asociados a la información también pueden ser abordados con el apoyo del área de TI, siempre y cuando dichos riesgos aprehendan tecnologías de información.
- Revisar continuamente el presupuesto asignado para la gestión de riesgos.

4.4 Resultados de mejora esperados

1) Mejora en los tiempos de interrupciones en los procesos claves de negocio, al estar la información disponible de manera regular, los procesos claves de la organización se verán muy levemente afectados; mucho menos que los tiempos en donde no se tiene un proceso de evaluación y administración de riesgos de información.
2) La continuidad de los procesos abarcando no solo el área de TI, sino también la información entre dependencias de la organización, habiendo un flujo constante de información los procesos claves de negocio no se verán mayormente afectados.
3) El valor agregado y la solidez competitiva es un factor que brinda la información siempre y cuando ésta sea correctamente gestionada y tomando decisiones acertadas acerca de las nuevas estrategias a implementar.
4) Menor impacto de riesgos en la información, notablemente es el punto fuerte del proyecto, tanto a nivel de TI como en la gestión de riesgos de la organización. Si la gestión de riesgos en la organización está correctamente definida, no solamente se ocuparán de los riesgos de TI sino de los riesgos de la organización y todas sus dependencias.

❖ **Ejemplo de aplicación del modelo**.

Para el siguiente ejemplo se tomará la empresa **La casa del médico**, una mediana empresa que se dedica a la comercialización de equipos médicos. Cuenta con una base de datos, sistema de facturación e incluso cuenta con un sistema de gestión documental. La organización no cuenta con área de TI, pero si cuenta con personal capacitado para hacerse cargo de las actividades relacionadas; tampoco cuenta con un área de gestión de riesgos, pero cuenta con personal profesional que aplica conocimientos básicos para la gestión de riesgo.

- La empresa inicialmente debe establecer el área de TI, o responsabilidades asociadas al área de TI.
- Establecer la gestión de riesgos como parte fundamental de la empresa, integrando las dependencias de la empresa.

Para el ejemplo se tomará parte de la información contenida en la base de datos y se aplicarán las actividades.

1. Clasificar la información de la base de datos:
   - Disponibilidad: 4
   - Integridad: 4
   - Confidencialidad: 4
2. Valorar la información

   Criticidad = 4: Criticidad alta
3. Identificar riesgos de información

   Se pueden identificar muchísimos riesgos de información relacionada con los ítems, pero para el caso práctico, se tomarán el o los riesgos más comunes.

1) Servidor averiado o con fallas físicas (Infraestructura)

2) Virus en el servidor (Seguridad)

3) Acceso no autorizado (Gestión)

4) Datos corruptos (Recursos humanos)

4. Evaluar los riesgos

Para este caso se deben asignar los valores que se consideren para probabilidad e impacto de cada uno de los riesgos.

1) Probabilidad = 1 : Impacto = 4

2) Probabilidad = 2 : Impacto = 3

3) Probabilidad = 3 : Impacto = 3

4) Probabilidad = 4 : Impacto = 4

5. Clasificar los riesgos

Se multiplican los valores relacionados de probabilidad e impacto

1) 1 x 4 = 4: Severidad media

2) 2 x 3 = 6: Severidad media

3) 3 x 3 = 12: Severidad Alta

4) 4 x 4 = 16: Severidad extrema

6. Priorizar los riesgos

Para este ejemplo, se priorizan los riesgos según el resultado de severidad:

1) Datos corruptos

2) Acceso no autorizado

3) Virus en el servidor

4) Servidor averiado o con fallas

Y de acuerdo a ello, la empresa se encargará de establecer un plan de respuesta para cada riesgo identificado.

7. Plan de respuesta

Para los riesgos extremos y altos se recomiendan estrategias preventivas como evitar, reducir o transferir, mientras que para los medios o bajos, pueden ser aceptados, transferidos, mitigados o escalados.

1) Datos corruptos:

Para este caso y en vista de que el error humano puede ocurrir al momento de ingresar información, y es una actividad en la que no se puede salir evitando el riesgo, ni tampoco transferir, se dispone de un plan de respuesta que busque reducir la probabilidad o el impacto de este riesgo:

- Disponer de un script para validación de datos (Reducir)
- Capacitar al personal que ingresará los datos (Reducir)
- Realizar backups diarios de la base de datos (Reducir)

2) Acceso no autorizado:

El acceso no autorizado, puede estar dado por personas internas o externas de la empresa, en este caso se definen controles preventivos como estrategias de reducción de probabilidad o impacto del riesgo:

- Control de usuarios en plataforma (Reducir)

- Definir roles de administrador para el acceso a la base de datos (Reducir)

3) Virus en el servidor:

Los virus se pueden dar de muchas formas y en cualquier momento, para tal caso, es necesario de contar con estrategias preventivas de reducción de impacto:

- Antivirus licenciado y actualizado (Reducir)
- Parches de seguridad actualizados (Reducir)
- Firewall robusto (Reducir)

4) Servidor averiado o con fallas físicas:

Esto sucede a menudo que las condiciones de ubicación del servidor no son óptimas, pero es muy importante identificar la causa de la falla del servidor. En este punto se pueden aplicar diferentes estrategias:

- Asegurar la infraestructura con el proveedor de equipos y dispositivos (Transferir)
- Migrar a servicios en la nube (Transferir)
- Revisión periódica de las condiciones de ubicación (Reducir)
- Planta eléctrica regulada para las condiciones eléctricas (Reducir)

8. Asegurar los fondos

1) Datos corruptos:

- Disponer de recursos para las actividades: contratación de desarrolladores u otro tipo.
- Asegurar los fondos para el plan de capacitación

- Almacenamiento extra para los backups

2) Acceso no autorizado:

- Disponer del personal calificado para desarrollar las actividades

3) Virus en el servidor:

- Compra de licencia de antivirus
- Compra de licencias de servidores
- Recursos económicos para infraestructura y software especializado.

4) Servidor averiado o con fallas físicas:

- Seguro por la compra de equipos y dispositivos
- Recursos económicos y de personal capacitado para el cloudcomputing
- Asignación de actividades en el personal
- Recursos económicos y de infraestructura para planta eléctrica regulada

9. Monitorear y actualizar

Esta actividad requiere de revisar periódicamente el modelo como tal si es efectivo y sus actividades más importantes:

- Clasificación de la información
- Identificación de nuevos riesgos asociados
- Priorización de riesgos
- Planes de respuesta

5 CONCLUSIONES PRELIMINARES

- La utilización de la tecnología en una organización no supone una ventaja competitiva inmediata, es la correcta gestión de esta tecnología asociada a los riesgos derivados del uso, lo que realmente puede ser diferencial.
- Se puede concluir que el modelo desarrollado fue logrado con éxito gracias a los avances en COBIT 5, incluyendo en su manual COBIT Quickstart nuevos parámetros los cuales permitieron la inclusión de las PYMES; esto, debido a que anteriormente solo hubiera sido exitoso si las PYMES cumplían con los requisitos exigidos anteriormente por COBIT para la implementación de este estándar.
- Las organizaciones inicialmente consideraban que la utilización e implementación de estos marcos de buenas prácticas en TI eran complejos y no les ofrecían mayor ventaja frente al mercado, algo que cambió radicalmente a raíz de ciertos sucesos adversos a los que se vieron enfrentadas las grandes organizaciones, hecho que por supuesto tuvo trascendencia en las PYMES al tomar mayor conciencia sobre los efectos de los riesgos de información en TI.
- A nivel internacional y nacional se ha demostrado que la implementación de mejores prácticas de TI mejora considerablemente la calidad del servicio y prolonga la actividad comercial de las organizaciones.
- A través de la evaluación y administración de riesgos de información a nivel de TI, es posible crear un modelo que sea capaz de ofrecer ventajas competitivas en el mercado, al igual que tener una mayor estabilidad en los procesos internos del área de TI, respaldando el resto de procesos de la organización.
- La gestión de riesgos en conjunto con la gestión de TI dentro de una organización representan procesos claves para el respaldo de los activos de información de las PYMES, sin importar si se implementa un marco de mejores prácticas.

- El área de TI requiere de mayor participación en la estrategia de negocio de las organizaciones PYMES de Montería, pues no está siendo tenida en cuenta para decisiones claves en los procesos de negocio, generando falta de compromiso en las demás áreas y mayor preocupación en la gerencia y administración acerca de los temas relacionados con TI.
- Una vez realizado el diagnóstico de las empresas PYMES de la ciudad de Montería en cuanto al estado actual y el estado deseado acerca de la evaluación y administración de riesgos de información a nivel de TI, a través de encuestas y entrevistas, se pudo establecer los cimientos del proyecto, evidenciando que las PYMES de la ciudad de Montería se encuentran en un estado inicial (1) en cuanto al proceso y que es necesario aplicar mejoras para sacar un mejor provecho de la información a nivel de TI y ayudar a proteger la información.
- Las brechas analizadas entre el estado actual y el estado deseado del proceso de evaluación y administración de riesgos de información a nivel de TI fueron abarcadas en su gran mayoría en la planeación y desarrollo del modelo, teniendo en cuenta todos los aspectos que se relacionan con el manejo de información en el área de TI, desarrollando un modelo capaz de afrontar el marco de mejores prácticas desarrollado por COBIT.
- El sector comercial de la ciudad de Montería está siendo abordado por PYMES en un 85%, representando la mayoría del comercio en la ciudad, lo que significa que contribuye al crecimiento de la economía de la región, razón por la cual se debe realizar un mayor apoyo y acompañamiento a los futuros emprendedores, con modelos y estándares del mercado nacional e internacional para que su negocio tenga mejoras continuas constantes a partir de las buenas practicas implementadas.
- Se puede inferir que el 90% del personal encuestado improvisa los procesos de administración y gestión de riesgos de información, con base a otras experiencias y modelos implementados en otras organizaciones, ejecutándolos

a pequeña escala, teniendo en cuenta la reducción de recursos que se tienen como PYMES, dificultando las actividades para ejecución que se desconocen.

- En su gran mayoría las organizaciones PYMES tienen sus sistemas de información unidos a la red, lo que representa que la mayoría de los daños que puedan ser producidos en los activos de información son externos y estas organizaciones dependan estrictamente del personal de TI, el cual necesariamente debe estar calificado para implementar las metodologías y procedimientos necesarios.

6 RECOMENDACIONES

- Es necesario un conocimiento previo en el área de TI y parte del área directiva de la organización acerca del estándar COBIT 5 y COBIT Quickstart para la implementación del modelo, ya que de lo contrario el personal encargado de la ejecución de actividades en los procesos y en la designación de funciones no será suficientemente clara para ellos.
- Basados en COBIT, es necesario instaurar la gestión de riesgos o designar responsabilidades en la organización, previamente a la aplicación del modelo, pues desconocer temas de trasfondo como la clasificación de la información, identificación de riesgos y planes de respuesta, puede resultar adverso en la implementación del modelo.
- La gerencia debe identificar plenamente los objetivos y procesos claves de negocio, pues con base en éstos se realizará la evaluación y administración de riesgos de información a nivel de TI, pues sin éstos será difícil iniciar las actividades de clasificación de la información.
- Dentro de las organizaciones entrevistadas y profesionales encuestadas se presentan varios casos de monarquía de negocios, es decir, donde los superiores o área directiva de la organización toman decisiones sin ninguna restricción acerca del manejo de las demás áreas de la organización. Por lo tanto se recomienda la posibilidad de utilizar modelos como el gobierno de TI para un mejoramiento continuo y mayor distribución de los roles y responsabilidades dentro de la organización.
- Es importante la participación activa de todo el personal de la organización para la implementación del modelo, ya que es un trabajo en equipo que no depende única y exclusivamente del área de TI; de lo contrario los resultados obtenidos no serán los mejores o esperados.
- La mayoría de las inversiones realizadas por las PYMES en materia de TI, se realiza en infraestructura, lo que si bien es cierto, no es errado, se

recomendaría utilizar parte de dicho presupuesto en estrategias de negocio que contribuyan a sacar un mejor provecho de la tecnología implementada y poder generar ventajas competitivas frente al mercado.

- En cuanto a las estrategias de respuesta es importante asegurar previamente los recursos a utilizar, puesto que de otra manera las actividades de la estrategia de respuesta no serán llevadas a cabo en su totalidad y no abarcará el riesgo en cuestión.
- Se recomienda a partir de la aplicación y complementación de métodos y estándares que contribuyan al mejoramiento de la gestión de riesgos, tanto a nivel de TI como en las demás áreas, desarrollar un modelo más adaptable al tipo de organización, teniendo en cuenta que este es un modelo general y no específico para una determinada organización.
- Se recomienda a las organizaciones PYMES la actualización periódica de la identificación de nuevos riesgos y los planes de respuesta, puesto que el mercado es cambiante y las amenazas pueden variar, así como los planes de respuesta y estrategias pueden ser mejorados.
- Los planes de respuesta no son de estricto cumplimiento en cuanto a los niveles de severidad del riesgo, pues en algunos casos las organizaciones deben tener en cuenta la valoración de expertos y la relación costo-beneficio de afrontar el riesgo.
- Las actividades pueden estar sujetas a cambios dependiendo de la razón social de la PYME; en el contexto existen PYMES que no necesariamente deben cerrar las actividades de acuerdo al modelo, es decir, que las actividades no son de estricto cumplimiento y algunas pueden ser omitidas o aplicadas o mayor o menor escala dependiendo del contexto organizacional.

7 BIBLIOGRAFÍA

Álvarez, L. S. (2009). *¿Cómo implantar el Gobierno de las Tecnologías de Información en Instituciones de Educación Superior?* Almeria: Universidad de Almería España.

Andres Caviedes, J. M. (2014). *GOBIERNO DE TI EN PYMES: ESTADO ACTUAL DEL GOBIERNO DE TI EN EMPRESAS PRIVADAS DE SEGURIDAD EN BOGOTÁ* . Bogota: UNIVERSIDAD CATÓLICA DE COLOMBIA.

Chajón, M. Y. (2015). *IMPACTO DEL ESTÁNDAR DE CALIDAD COBIT EN LOS PROCESO DE DEPARTAMENTOS DE TI EN LAS PYMES.* Universidad de San Carlos de Guatemala.

CIIFEN, Centro Internacional para la Investigación del Fenómeno de El niño. (2016). *Aproximación para el calculo del riesgo*. Obtenido de CIIFEN: http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es

Colombia, C. D. (2000). Ley 590 de 2000. En *Ley 590 del 2000.* Bogota.

Departamento de TI, U. d. (2009). TI en las organizaciones. (C. Montería, Entrevistador)

Durston, J., & Miranda, F. (2002). *Experiencias y metodología de la investigación participativa.* Santiago de Chile: CEPAL.

EL CONGRESO DE COLOMBIA. (2012). LEY ESTATUTARIA 1581 DE 2012. *Diario Oficial*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

ENTER.CO. (16 de 07 de 2016). *LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO.* Obtenido de ENTER.CO S.A.S.: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

Florencia Ucha. (2008). *Definición ABC.* Obtenido de Definición de Probabilidad: https://www.definicionabc.com/general/probabilidad.php

Gallo, J. M. (5 de Mayo de 2014). *La información como activo estratégico de la empresa*. Obtenido de Business Value Exchange:

https://businessvalueexchange.com/es/2014/05/05/la-informacion-como-activo-estrategico-de-la-empresa/

Gomez, R. P. (2010). *Metodologia y gobierno de la gestion de riesgos de tecnologías de la información.* Obtenido de Revista de Ingenieria.

ISACA. (2009). *Marco de Riesgos de TI.* Estados Unidos: ISACA: Serving IT Governance Professionals.

ISACA. (2012). *CERTIFIED INFORMATION SECURITY MANAGER.* Estados Unidos: CRISC.

ISACA INC. (2013). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* ISACA.

IT Governance Institute. (2007). *COBIT 4.1.* Estados Unidos: IT Governance Institute.

MARTI, J. (2012). *LA INVESTIGACIÓN - ACCIÓN PARTICIPATIVA ESTRUCTURA Y FASES.* MADRID: UNIVERSIDAD COMPLUTENSE DE MADRID.

Ministerio de Agricultura y Desarrollo Rural. (2012). *Amenazas y Riesgos en el manejo de la Información.* Bogota: FIDUAGRARIA.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). *Gobierno TI.* Obtenido de Fortalecimiento de la gestion de TI en el estado: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6797.html

Musiño, C. M. (2010). *El valor de la información, su administración y alcance en las organizaciones.* Mexico D.F.: Universidad Nacional Autónoma de Mexico.

Osorio, B. C. (2008). *DINAMICA DE LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) EN LA CIUDAD DE MONTERÍA Y SU IMPACTO EN LA GENERACIÓN DE EMPLEO.* Montería: Universidad del Sinú. Sede Montería.

Pressman, R. (2001). *Ingeniería del Software, un enfoque practico.* Mexico D.F.: Mc Graw Hill.

Revista Dinero. (2016). *Pymes contribuyen con más del 80% del empleo en Colombia.* Bogota.

Rouse, M. (Agosto de 2014). *Gestión de TI.* Obtenido de TechTarget, S.A. de C.V.: http://searchdatacenter.techtarget.com/es/definicion/Gestion-de-TI

Santos, M. (2012). *EL ESTADO DE TI EN LAS PYMES.* Bogota: ENTER.CO Enterprise.

Santos, M. (2013). *LAS PYMES QUE ADOPTAN TI CRECEN MÁS RÁPIDO: BCG.* Bogota: ENTER.CO Enterprise.

Santos, M. (2014). *RECTIFICACIÓN: "EL 60,6% DE LAS PYMES USA INTERNET", DICE MINTIC.* Bogota: ENTER.CO Enterprise.

Serfinansa, Compañia de Financiamiento. (2014). *Buen Gobierno, Sistema de Riesgo*. Obtenido de Serfinansa: http://www.serfinansa.com.co/relacioninversionistas/gobiernocorporativo/buengobierno/sistemariesgo

Standards Australia. (1999). *AS/NZS ISO 31000:2009: Risk management - Principles and guidelines.* New Zealand: Standards Australia.

Universidad Nacional de Luján. (2013). Riesgo vs. Seguridad de la Información. Luján, Argentina.

8 ANEXOS

Se contemplará la información complementaria al documento central según se explica en la Guía del Protocolo Base

Anexo 1: Acta de constitución

ACTA DE CONSTITUCIÓN DEL PROYECTO FINAL DE GRADUACIÓN			
Nombre completo del estudiante:	***Jose Andres Durango Garcia***		
Nombre de la carrera:	***Maestria en Administracion de Tecnologias de la Información***	***Generación***	***MATI-06***
Título del proyecto	***DESARROLLO DE UN MODELO PARA LA EVALUACIÓN Y ADMINISTRACIÓN DE RIESGOS DE INFORMACIÓN A NIVEL DE TI EN PYMES DE LA CIUDAD DE MONTERÍA A PARTIR DEL MARCO DE TRABAJO COBIT 5***		
Fecha de inicio del proyecto:	***05/07/2017***	***Fecha tentativa de finalización del proyecto:***	***18/10/2017***

Justificación del proyecto	*Según el Ministerio de Comercio, Industria y Turismo (MinCIT) las Pymes en Colombia abarcan más del 80% del comercio (Revista Dinero, 2016), es por ello que en su afán de crecer y avanzar, deben plantearse una mejora que les permita evaluar y administrar el riesgo de IT de una mejor manera, entendiendo IT como la mayor ventaja competitiva de una organización dentro de un mercado cambiante y creciente. Por tanto es indispensable que todas las empresas de la ciudad de Montería, una ciudad que también está en continuo crecimiento y expansión, cuenten con un modelo para el análisis de riesgos de IT, y así la gerencia pueda lograr entender como éstos pueden afectar de manera directa o indirecta la continuidad del negocio.* *De acuerdo a lo anterior, este proyecto busca principalmente una alternativa de solución para aquellas empresas y organizaciones que dentro de sus actividades estratégicas y de competencia se benefician de las tecnologías y la información, pero desconocen los riesgos a los que están expuestas en este campo, por tal motivo este proyecto busca de manera asertiva crear un modelo de implementación para aquellas micro, pequeñas y medianas empresas, que no cuentan con un sistema de evaluación y administración de riesgos de IT.* *Es importante resaltar que las PYMES en la ciudad de Montería en su gran mayoría no cuentan con un presupuesto y la experiencia suficiente para implementar un estándar de alto nivel como ITIL, COBIT, ISO 27001 u otro, es por tanto que este proyecto dentro de sus objetivos también pretende ajustarse a dichos requisitos, ya que el producto resultante*

	de este proyecto, es un modelo de gestión de evaluación y administración de riesgos, donde su base tal y como está enunciada en su título es COBIT, que es un marco de buenas prácticas de IT que abarca toda la gestión de IT como un activo estratégico y fundamental para la organización. Cabe decir, que COBIT es el marco de mejores prácticas más completo y amplio dentro de esta gama de estándares (BitCompany, 2014) para organizaciones.
Diagnóstico Identificación del Problema	*El problema radica como una oportunidad de crecimiento para las PYMES en la ciudad de Montería, siendo IT un factor fundamental en la continuidad y crecimiento de los negocios.* *Estas organizaciones al no contar con el presupuesto suficiente y la experticia en su equipo de IT para implementar un estándar o marco de mejores prácticas en IT el cual pueda evaluar y administrar los riesgos de una mejor manera. Por lo tanto y de acuerdo a estudios realizados por el Ministerio De Comunicaciones, Tecnología Y Comunicación (MINTIC) y el Ministerio de Comercio, Industria y Turismo (MinCIT), resultados confirman que más del 65% de las PYMES en Montería que utilizan los servicios de IT como ventaja competitiva, desconocen la severidad con que los riesgos puedan afectar negativamente la organización, llevándola al punto de liquidación empresarial (Cámara de Comercio, 2014). Profesionales del campo de las TICS* (Baena, Ramirez, Nassiff, & Barrios, 2010) *a través de estudios e investigaciones han demostrado que este problema ha hecho que más del 33% empresas clausuren en el segundo año de mercado, ya que la competencia ha aprovechado de una mejor manera este análisis de riesgo, llevándolas a un punto*

	más alto y ganando un poco más de terreno con respecto a las que no gestionan correctamente los riesgos de información. Para aclarar que la gestión de riesgos se realiza para decidir qué acción se puede tomar con respecto a aquellos eventos que pueden afectar la integridad de la empresa, ya sea negativa o positivamente.
Metodología	*Se pretende tomar una metodología cualitativa, en donde se aspira conocer el estado actual de cómo se realiza la evaluación y administración de riesgos dentro de una organización y a qué estado pretende ser llevada, generando así un modelo de implementación, el cual indique las acciones que se deben tomar para llegar al estado deseado, esta metodología se realizará a través de entrevistas y encuestas tomando una muestra de PYMES en la ciudad de Montería.*
Alternativas, Ideas o Soluciones	• *Implementar estándares aceptados internacionalmente, como Risk IT y COBIT para el mejoramiento de los procesos de la gestión de riesgos de TI.* • *Contratación de profesionales especializados en el área, que contribuyan a de una mejor manera en la gestión de los riesgos de TI.* • *Implementar otros estandáres de menor rango y con menor amplitud que COBIT para mejorar los procesos de gestión de riesgos de TI.* • *Buscar otro tipo de estrategias en la que los riesgos de TI se puedan compartir o evitar, generando el menor impacto de los eventos adversos dentro de la organización.*

Selección de la mejor alternativa	*Basados en el marco de trabajo COBIT la mejor alternativa de solución es estudiar el estado actual de la gestión de riesgos de IT dentro de las PYMES en Montería, intentar unificar las ideas más acertadas acerca del estado deseado en la gestión de dicho proceso y a partir de ello construir el modelo de evaluación y administración de riesgos de IT.* *Se considera que la mejor opción debido a los parámetros del proyecto, teniendo en cuenta el tiempo de desarrollo del proyecto y que evaluar o entrevistar el 100% de las PYMES en Montería sería una labor que tomaría mucho tiempo. Es por ello que tomar una muestra significativa sería lo más viable, teniendo en cuenta que ésta se realizará a organizaciones que posean un área de TI con procesos ya definidos o en desarrollo de definición de procesos para complementar dichos procesos.*
Resultados, productos e impactos obtenidos	*Diagnóstico del estado actual de los procesos de gestión de riesgos de TI en PYMES en la ciudad de Montería.* *Modelo de evaluación y administración de riesgos en TI para las PYMES en la ciudad de Montería.*
Beneficiados con el proyecto(involucrados)	*El proyecto estará dirigido principalmente a las micro, pequeñas y medianas empresas que cuenten con un área de IT con procesos establecidos o en desarrollo y que deseen implementar un modelo adaptable a los parámetros de sus organizaciones que les permita gestionar los riesgos de IT a partir de un marco de trabajo internacional como COBIT.* *De igual manera a pequeñas y medianas empresas que aunque ya cuenten con un estándar o marco de trabajo*

<table>
<tr><td></td><td colspan="2">establecido puedan beneficiarse de este modelo para la gestión de riesgos de IT.</td></tr>
<tr><td>Recursos necesarios</td><td colspan="2">Mano de obra

Insumos de oficina (papelería, impresora, computador, etc.)</td></tr>
<tr><td rowspan="2">Alcances y Limitaciones</td><td>Limitaciones

Indicar los riesgos que podrían presentarse para la culminación del PFG.</td><td>Alcances

Enumerar el alcance del PFG: toma de decisión empresarial, nuevo nicho de mercados, giros de negocio entre otros.</td></tr>
<tr><td>Acceso parcial a la información de las PYMES en Montería
Recursos económicos insuficientes para el desarrollo del modelo</td><td>Cubre los aspectos estrictamente necesarios de las PYMES, para el desarrollo del modelo de evaluación y administración de riesgos en IT

No cubre los riesgos externos al área de IT</td></tr>
<tr><td>Objetivos del proyecto</td><td colspan="2">General:
Diseñar un modelo para la evaluación y administración de riesgos de información empresarial a nivel de IT, en Pymes en la ciudad de Montería-Colombia, a partir del marco de trabajo COBIT 5.
Específicos:
Diagnosticar el estado actual de la gestión de riesgos de información dentro del área de IT de las PYMES en la ciudad de Montería.</td></tr>
</table>

	• *Establecer un estado deseado común de las organizaciones encuestadas en cuanto al proceso de gestión de riesgos de IT.* • *Planear y desarrollar el modelo a partir del estado deseado común de las organizaciones.* • *Realizar ajustes basados en profesionales de TI al modelo desarrollado incluyendo otros marcos de gestión de riesgos de IT.*
Resumen Ejecutivo del Proyecto	*El proyecto nace como una oportunidad de crecimiento para PYMES en la ciudad de Monteria, ya que cifras del ministerio de industria y comercio y el ministerio de las TIC en Colombia, reflejan que muchas de las PYMES no cuentan con una gestión de riesgos que aborde los temas de IT, es por tanto que surge este proyecto como iniciativa de solución viable y que se pueda acomodar a los parámetros de las micro, pequeñas y medianas empresas de la ciudad.* *Las PYMES se verían beneficiadas en la medida en que adopten dicho modelo y lo apliquen, para así sacar el mejor provecho de las TIC en la empresa, de manera que se vea reflejado en temas de seguridad en la información, planes de negocio, iniciativas de proyectos, infraestructura, software e información.* *La idea fundamental es crear un modelo capaz de suplir necesidades para la gestión de riesgos en IT y que también pueda reforzarlos en aquellas organizaciones que ya estén establecidos como estrategia de negocio.* *El proyecto se llevará a cabo en 4 etapas básicas que son la recolección de información a través de las entrevistas y encuestas para conocer el estado actual y el estado*

	deseado de las organizaciones en la gestión de riesgos de IT, realizar un análisis de información y establecer puntos comunes e importantes para el desarrollo del modelo, desarrollar el modelo de evaluación y administración de riesgos basados en el marco de trabajo COBIT y realizar los afinamientos y ajustes necesarios para el caso.		
Nombre completo y Firma del estudiante	 José Andrés Durango García	**Fecha:**	11/06/2017
Nombre completo y firma del profesor (a) que aprueba el PFG		**Fecha:**	_____ ___

Anexo 2: Formulario de entrevistas

La siguiente es una entrevista o encuesta que se hará al personal de TI de las organizaciones elegidas como muestra de las PYMES en la ciudad de Montería y a personal profesional en TI que haya laborado en empresas de la ciudad de Montería.

Esta entrevista se hará con fines netamente académicos para estudiar el estado actual y el estado deseado de las organizaciones en cuanto al proceso de evaluación y administración de riesgos de información a nivel de IT.

Las preguntas a continuación fueron redactadas por el Ingeniero Informático José Durango García, identificado con Cédula de Ciudadanía 1067886414 de Montería, quien es el encargado de almacenar y analizar la información como investigador.

Datos del encuestador

Investigador:	**JOSE ANDRES DURANGO GARCIA**
Fecha:	
Identificación:	**1067886414**
Organización:	**Universidad para Cooperación Internacional, Costa Rica**

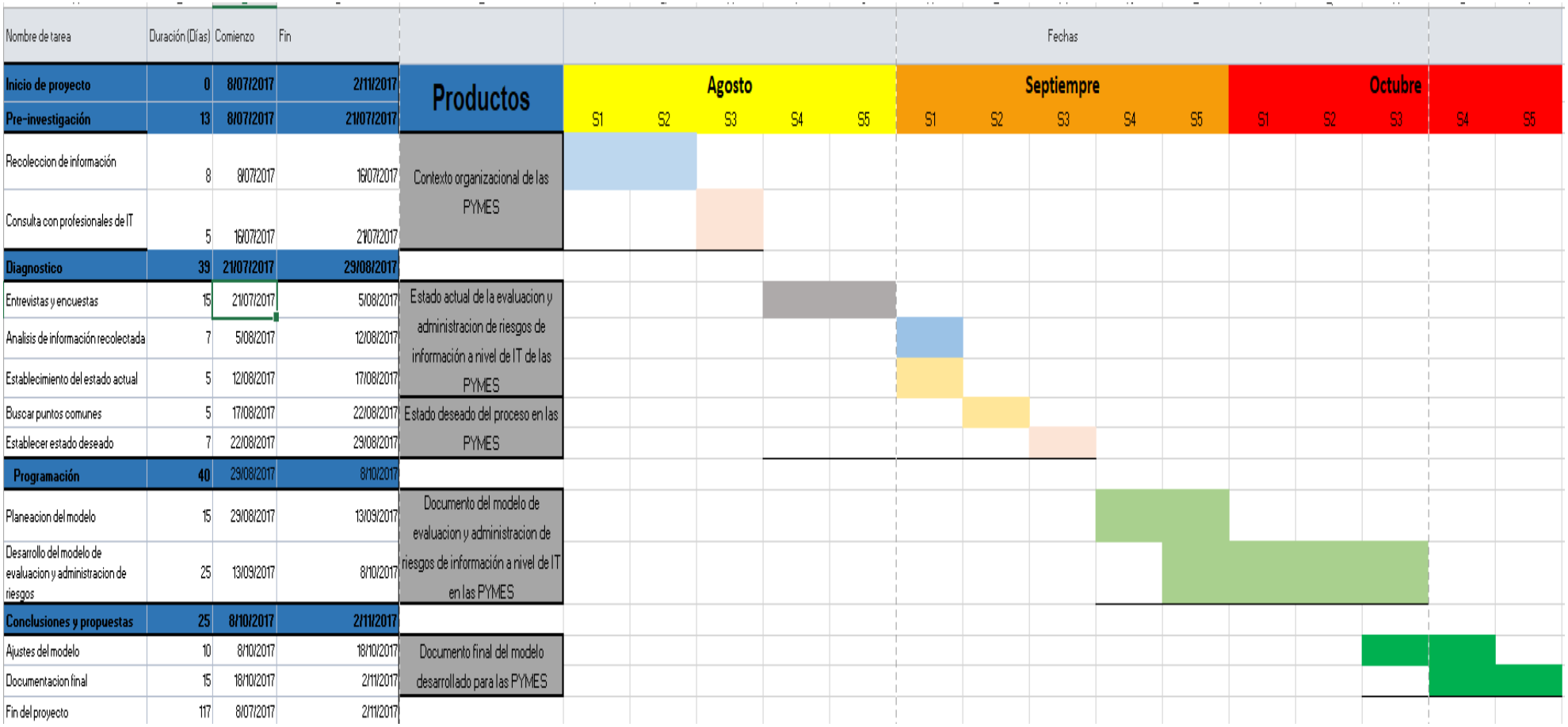
Datos del encuestado

Encuestado	
Empresa	
Dirección de la empresa	
Profesión	
Cargo	

- ¿Cómo ha sido su experiencia en la gestión de riesgos de información a nivel de TI de la empresa?
- ¿Tiene la organización algún marco de trabajo implementado a nivel de IT para la gestión de riesgos, o los profesionales del área de tecnología están certificados con algún estándar que puedan utilizarlo dentro de la organización?
- ¿La organización es consciente de los riesgos de información a nivel de TI, y qué tan perjudiciales pueden ser para ella?
- ¿Están plenamente identificados los riesgos de información a nivel de TI en la organización?
- ¿De qué manera son clasificados los riesgos de información a nivel de TI de la organización?

- ¿Se realiza una evaluación en cuanto a probabilidad e impacto de los riesgos de información a nivel de TI de la organización?
- ¿Existen estrategias para mitigar, disminuir, compartir o aceptar los riesgos de información a nivel de TI de la organización, o al menos los que son de alto o medio impacto?
- ¿Se realiza un monitoreo periódico a la evaluación de los riesgos de información a nivel de TI de la organización, con el fin de mejorar dicha gestión?
- ¿Considera que es necesario mejorar la gestión de riesgos de información a nivel de TI en la organización?
- ¿Cómo considera usted que puede mejorar esta situación dentro de las PYMES de la ciudad de Montería?
- ¿Conoce usted los marcos de trabajo como COBIT y RISK IT?
- ¿Considera usted que se podría mejorar el proceso de evaluación y administración de los riesgos de información a nivel de TI de las organizaciones PYMES de la ciudad de Montería a través de la implementación de alguno de estos marcos de trabajo para TI?

Anexo 3: Cronograma del proyecto



Nombre de tarea	Duración (Días)	Comienzo	Fin
Inicio de proyecto	**0**	**8/07/2017**	**2/11/2017**
Pre-investigación	**13**	**8/07/2017**	**21/07/2017**
Recoleccion de información	8	8/07/2017	16/07/2017
Consulta con profesionales de IT	5	16/07/2017	21/07/2017
Diagnostico	**39**	**21/07/2017**	**29/08/2017**
Entrevistas y encuestas	15	21/07/2017	5/08/2017
Analisis de información recolectada	7	5/08/2017	12/08/2017
Establecimiento del estado actual	5	12/08/2017	17/08/2017
Buscar puntos comunes	5	17/08/2017	22/08/2017
Establecer estado deseado	7	22/08/2017	29/08/2017
Programación	**40**	**29/08/2017**	**8/10/2017**
Planeacion del modelo	15	29/08/2017	13/09/2017
Desarrollo del modelo de evaluacion y administracion de riesgos	25	13/09/2017	8/10/2017
Conclusiones y propuestas	**25**	**8/10/2017**	**2/11/2017**
Ajustes del modelo	10	8/10/2017	18/10/2017
Documentacion final	15	18/10/2017	2/11/2017
Fin del proyecto	117	8/07/2017	2/11/2017

Ilustración 22: Anexo 3: Cronograma del proyecto

Fuente: Elaboración propia

Anexo 4: Ejemplo de aplicación del modelo

Información analizar:	Base de datos												
Clasificar la información													
Disponibilidad	Integridad	Confidencialidad											
4	4	4											
Identificar los riesgos				Evaluar los riesgos		Clasificar los riesgos		Priorizar los riesgos	Plan de respuesta		Asegurar fondos	Monitorear y actualizar	
Evento	Tipo de riesgo	Causa	Efecto	Probablidad	Impacto	Severidad	Nuevo orden a partir de la priorización		Estrategia	Actividad			
Servidor averiado o con fallas físicas	Infraestructura	Mal instalado, partes defectuosas	Perdida de información, ritmo de trabajo desacelerado	1	4	Media		Datos corruptos	Reducir el impacto	Disponer de un script para validación de datos	Disponer de recursos	Clasificación de la información	
Virus en el servidor	Seguridad	Ataques externos en la red	Robo de información, perdida de información	2	3	Alta		Acceso no autorizado	Reducir la propabilidad	Control de usuarios en plataforma	personal calificado	Identificación de nuevos riesgos asociados	
Acceso no autorizado	Gestión	No hay control de acceso	Robo de información, información adulterada	3	3	Alta		Virus en el servidor	Reducir la propabilidad	Antivirus licenciado y actualizado	Compra de licencia de antivirus	Priorización de riesgos	
Datos corruptos	Operación	Virus, acceso indebido, error humano, error intencional	Información corrupta, malas decisiones en la compañía	4	4	Extrema		Servidor averiado o con fallas	Transferir	Asegurar la infraestructura con el proveedor de equipos y dispositivos	Seguro por la compra de equipos y dispositivos	Planes de respuesta	
Ampliacion del servidor de base de datos	Infraestructura	Se requiere realizar una ampliacion de la base de datos o migrar la BD a un servidor mas actual	Cambios en el modelo relacional y sintaxis de la BD	2	2	Media		Ampliacion del servidor de base de datos	Transferir	Alquiler de los servicios de otro servidor	Recursos economicos para el alquiler de los servicios	Priorización de riesgos	
Incompatibilidad con software empresarial	Infraestructura	Instalacion de un nuevo software no compatible con la base de datos de la empresa	Instalar un servidor de base de datos adicional	2	1	Media		Incompatibilidad con software empresarial	Transferir	Compartir los servicios con la empresa manufacturera	Recursos economicos para compartir las responsabilidades de gestión	Priorización de riesgos	
Backups incompletos	Operación	Los Backups automaticos de la base de datos no se realizaron completamente.	Pasar a los procesos manuales de backups	1	2	Bajo		Backups incompletos	Aceptar	Realizar los backups manualmente	Recursos de tiempo disponibles	Identificación de nuevos riesgos asociados	