UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"

ESCUELA DE POSGRADO

MAESTRIA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE

"MODELO PARA LA GESTION DE RIESGOS DE DESARROLLO DE SOFTWARE BAJO LA PERSPECTIVA DE LA GESTION DE PROYECTOS"

TESIS

PRESENTADA PARA OPTAR EL GRADO ACADÉMICO DE MAESTRA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

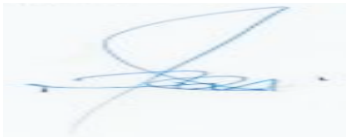
AUTORA:
NORA NOELIA SERNAQUE ZAPATA

ASESOR:
DR. ALBERTO ENRIQUE SAMILLÁN AYALA

Lambayeque, 2022

"MODELO PARA LA GESTION DE RIESGOS DE DESARROLLO DE SOFTWARE BAJO LA PERSPECTIVA DE LA GESTION DE PROYECTOS"

Nora Noelia Sernaque Zapata
AUTORA



Dr. Alberto Enrique Samillán Ayala
ASESOR

Presentada a la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado Académico de: MAESTRA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE.

Aprobado por:

DR. ERNESTO KARLO CELI ARÉVALO
Presidente

Firmado digitalmente por: AQUINO LALUPU Janet Del Rosario FAU 20105685875 soft
Motivo: Soy el autor del documento
Fecha: 15/12/2021 18:27:38-0500

MG. JANET DEL ROSARIO AQUINO LALUPÚ
Secretaria

DR. SANTOS HENRY GUEVARA QUILICHE
Vocal

UNPRG	ESCUELA DE POSGRADO M.Sr. Franck Villena Rodriguez	Versión:	01
		Fecha de Aprobación	29-8-2020
UNIDAD DE INVESTIGACION	FORMATO DE ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS	Pág. 1 de 3	

ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS

Siendo las 4:00 p.m. del lunes 10 de enero de 2022, se dio inicio a la Sustentación Virtual de Tesis soportado por el sistema Google Meet, preparado y controlado por la Unidad de Tele Educación de la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, con la participación en la Video Conferencia de los miembros del Jurado, nombrados con Resolución N°1047-2019-EPG, de fecha 19 de agosto de 2019, conformado por:

Dr. ERNESTO KARLO CELI AREVALO	Presidente
Mg. JANET DEL ROSARIO AQUINO LALUPU	Secretaria
Dr. SANTOS HENRY GUEVARA QUILICHE	Vocal
Dr. ALBERTO ENRIQUE SAMILLAN AYALA	Asesor

Para evaluar el informe de tesis de la tesista NORA NOELIA SERNAQUE ZAPATA, candidata a optar el grado de MAESTRA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE con la tesis titulada "MODELO PARA LA GESTION DE RIESGOS DE DESARROLLO DE SOFTWARE BAJO LA PERSPECTIVA DE LA GESTION DE PROYECTOS".

El Sr. Presidente, después de transmitir el saludo a todos los participantes en la Video Conferencia de la Sustentación Virtual ordenó la lectura de la Resolución N°1241-2021-EPG de fecha 29 de diciembre de 2021, que autoriza la Sustentación Virtual del informe de tesis correspondiente, luego de lo cual autorizó a la candidata a efectuar la Sustentación Virtual, otorgándole 20 minutos de tiempo y autorizando también compartir su pantalla.

Culminada la exposición de la candidata, se procedió a la intervención de los miembros del jurado, exponiendo sus opiniones y observaciones correspondientes, posteriormente se realizaron las preguntas a la candidata.

Culminadas las preguntas y respuestas, el Sr. Presidente, autorizó el pase de los miembros del Jurado a la sala de video conferencia reservada para el debate sobre la Sustentación Virtual del Informe de tesis realizada por la candidata, evaluando en base a la rúbrica de sustentación y determinando el resultado total de la tesis con **18** puntos, equivalente a **Muy Bueno**, quedando la candidata apta para optar el Grado

UNPRG	ESCUELA DE POSGRADO M.Sc. Francis Villena Rodríguez	Versión:	01
		Fecha de Aprobación	29-8-2020
UNIDAD DE INVESTIGACION	FORMATO DE ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS	Pág. 2 de 3	

de MAESTRA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE.

Se retomó a la Video Conferencia de Sustentación Virtual, se dio a conocer el resultado, dando lectura del acta y se culminó con los actos finales en la Video Conferencia de Sustentación Virtual.

Siendo las 5:13 p.m. se dio por concluido el acto de Sustentación Virtual.

PRESIDENTE

SECRETARIO

VOCAL

ASESOR

CERTIFICO: Que, es copia fiel del Original
Fecha: 22/…/2022
Lic. Gloria Luisa Carranza Velásquez
Unidad de Investigación - EPG
VALIDO PARA TRAMITES INTERNOS DE LA UNPRG

DEDICATORIA

A Dios por haberme permitido llegar hasta aquí, y por haber sido mi fortaleza y mi guía en todo momento para culminar mis objetivos trazados.

A mi madre que ha sido el soporte esencial para no decaer en el proceso y desarrollo de mi aprendizaje, además haber sido la persona quien me ha inculcado los principios y valores de toda mi formación académica.

A mi esposo e hijos quien con su amor, cariño y apoyo incondicional me ayudaron a salir adelante y de una u otra forma me acompañan en todos mis sueños y metas.

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con sus bendiciones ha alimentado siempre mi vida y la de toda mi familia para estar siempre presentes.

Mi profundo agradecimiento a mis padres, esposo e hijos por su apoyo y paciencia en este proyecto de estudio.

Finalmente quiero expresar mi más grande y sincero agradecimiento a mi Asesor, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo, además también a los directivos y docentes por la organización del programa de la Maestría de Gerencia de TI y Gestión de Software de la Universidad Nacional Pedro Ruiz Gallo.

INDICE

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN

La presente investigación aborda el problema que tienen las empresas del sector de la industria de desarrollo de software en la ciudad de Chiclayo-Perú, en relación a la gestión de riesgos en sus proyectos de desarrollo de software, como un requisito esencial y una exigencia de los clientes, para tener confianza en los productos y servicios que ofrece la empresa como parte del negocio. La necesidad de implementar un SGR en la empresa, motivó el desarrollo del estudio a través de un enfoque metodológico descriptivo propositivo no experimental, utilizando como guía base las normas ISO/IEC 27000 y la metodología Magerit, con la finalidad de desarrollar la propuesta de un modelo de gestión de riesgos relacionados con las tecnologías de la información en los principales procesos de las empresas del sector. Como resultado de la investigación, se construyó un modelo de SGR el cual fue validado a través del juicio de expertos, lográndose como resultado un nivel aceptable del modelo, lo que significa que se puede pasar a la fase de su implementación.

Palabras clave: gestión de riesgos de TI, ISO/IEC 27001, metodología Magerit

ABSTRACT

This research addresses the problem that companies in the software development industry have in the city of Chiclayo-Peru, in relation to risk management in their software development projects, as an essential requirement and a requirement of customers, to have confidence in the products and services offered by the company as part of the business. The need to implement an SGR in the company, motivated the development of the study through a descriptive, non-experimental, descriptive methodological approach, using the ISO / IEC 27000 standards and the Magerit methodology as a base guide, in order to develop the proposal of a risk management model related to information technologies in the main processes of companies in the sector. As a result of the research, an SGR model was built which was validated through the judgment of experts, achieving as a result an acceptable level of the model, which means that the implementation phase can be passed.

Keywords: IT risk management, ISO / IEC 27001, Magerit methodology

INTRODUCCIÓN

La investigación abordó el problema de los fracasos de proyectos de desarrollo de software cuando no se realizaba una adecuada gestión de riesgos. La revisión literaria nos indicó que el 29% de proyectos son exitosos a nivel mundial, el 52% de proyectos se enfrentó a riesgos que pueden paralizarlos y el 15% han sido fracasos. Los métodos y metodologías de gestión de riesgos que existen actualmente no son aplicados o no son correctamente aplicados por ser muy complicados para implementarlos. Frente a este escenario se formuló la siguiente pregunta: ¿De qué manera un modelo de gestión de riesgos basado en la metodología Magerit ayuda a gestionar proyectos de desarrollo de software? El propósito de la investigación fue elaborar un modelo de gestión de riesgos que permita identificar, evaluar y hacer seguimiento de los riesgos de manera fácil e intuitiva, como parte de la gestión de proyectos de desarrollo de software. Primero se realizó una revisión de los diferentes métodos y metodologías de gestión de riesgos en el desarrollo de software, con la finalidad de identificar los componentes principales que se deben considerar en un modelo de este tipo. Aplicando las recomendaciones y buenas prácticas de la metodología Magerit y la familia ISO/IEC 2700x, se desarrolló una propuesta de modelo de gestión de riesgos para las fases de análisis y tratamiento de riesgos, utilizando métodos descriptivos. El modelo se probó con datos reales obtenidos de empresas colaboradoras y finalmente fue evaluado por dos expertos desde las perspectivas de: suficiencia, claridad, coherencia y relevancia, concluyendo que la propuesta cumple con los criterios mencionados.

I. PROBLEMA DE LA INVESTIGACIÓN

1.1. Situación problema

En la actualidad las empresas desarrolladoras de software enfrentan un elemento crítico en el proceso de desarrollo de productos de software, que son los riesgos que se presentan a nivel de cada una de las fases del desarrollo, estos deben ser objeto de una gestión adecuada la cual debe ser iniciativa por la gerencia, supervisada y controlada por cada uno de los jefes de las áreas importantes involucradas en el desarrollo de software. La gestión de riesgos en proyectos de software es una actividad expresada en múltiples metodologías, pero en la práctica se aplican de forma particular dependiendo la lógica del negocio de cada organización.

En la actualidad son muchos los proyectos de desarrollo de software que fracasan ya sean porque incumplen con sus plazos de entrega o la tangibilización de los riesgos asociados a éstos. Los resultados del Standish Group 2015 Chaos Report (Info Q Con, 2019) indica que todavía hay trabajo por hacer para lograr resultados exitosos de los proyectos de desarrollo de software. El siguiente cuadro resume el estado de los proyectos de desarrollo de software hasta el 2015, y esta tendencia sigue siendo la misma.

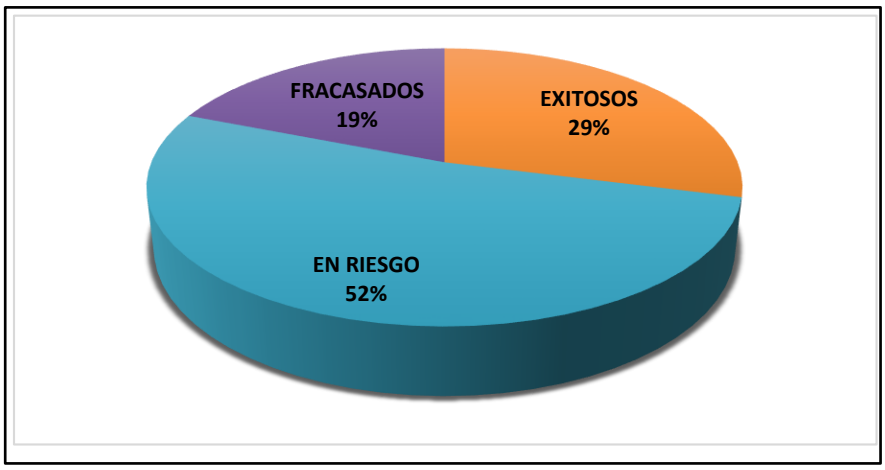


Gráfico N° 1. Resultado de informe Chaos para todos los proyectos de desarrollo de software
Fuente: (Info Q Con, 2019)

El informe muestra que los proyectos de software ahora tienen una tasa de éxito del 29% frente al 28% del estudio anterior en el 2014, y el 31% en el año 2013. Por otro lado, el 52% de los proyectos fueron impugnados (con algunos riesgos de presupuesto y recursos humanos), mientras que el 19% son fracasados (cancelados antes de la finalización o entrega y nunca utilizado).

Tabla N° 1. Estado de los proyectos de desarrollo de software

Estado del proyecto	2011	2012	2013	2014	2015
EXITOSO	29%	27%	31%	28%	29%
DESAFIADO	49%	56%	50%	55%	52%
FRACASADO	22%	17%	19%	17%	19%

Fuente: (Info Q Con, 2019)

Por lo tanto, se concluye que el éxito del proyecto, es un poco peor que en 2014 (29% vs 28%), pero sin duda mejor que en 2012 (27%). Por supuesto, hay una mejor experiencia en la gestión del proyecto (los directores de proyectos más certificados), mejor formación y mejores herramientas y técnicas.

Una tendencia de los informes anteriores que continuaron en la última encuesta es cómo los proyectos más pequeños tienen una probabilidad de éxito mucho mayor que los más grandes, como se muestra en esta tabla.

Tabla N° 2. Estado de los proyectos de desarrollo de software según su tamaño

TAMAÑO DEL PROYECTO	SATISFACTORIO	DESAFIADO	FRACASADOS
MUY GRANDE	2%	7%	17%
GRANDE	6%	17%	24%
MEDIO	9%	26%	31%
MODERADO	21%	32%	17%
PEQUEÑO	62%	16%	11%
TOTAL	**100%**	**100%**	**100%**

Fuente: (Info Q Con, 2019)

La disciplina de Gestión de Riesgos ha crecido mucho en el área de tecnologías de la información en los últimos años, particularmente ha tenido un gran impulso en proyectos de desarrollo de software. Éste impulso se puede atribuir a las malas experiencias que se suscitan al intentar culminar un proyecto con éxito.

Hoy en día es posible encontrar métodos formales para realizar una gestión de riesgos seria y que brinde resultados positivos al proyecto. Quizás el que más se destaque, ya sea por su probada eficiencia o por ser un estándar de hecho, sea el propuesto por el Instituto de Gestión de Proyecto (PMI por sus siglas en inglés). Sin embargo, no es el único, encontrándose en el mercado otras opciones valederas como lo es el denominado método RiskIt, el cual fue creado justamente en el entorno de proyectos de software.

Según el PMI, el riesgo de un proyecto es un evento o condición incierta que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos del proyecto, tales como el alcance, el cronograma, el costo y la calidad. Un riesgo puede tener una o más causas y, de materializarse, uno o más impactos. Una causa puede ser un requisito especificado o potencial, un supuesto, una restricción o una condición que crea la posibilidad de consecuencias tanto negativas como positivas. Por lo tanto, es de vital importancia realizar una adecuada gestión de riesgos donde se dé inicio en la primera fase del proyecto, para llevar seguimiento y controles adecuados de estos en cada una de las fases del desarrollo del software, hasta la aceptación del producto del proyecto.

Al no aplicar métodos de gestión de riesgos en los proyectos de desarrollo de software surgen preguntas como ¿Por qué su proyecto tiene problemas constantemente? A partir de ello, se pueden derivar otras interrogantes como: ¿Será necesario adaptar un modelo de gestión de riesgos para el desarrollo de los proyectos?, ¿Cuáles serán las fases correctas para la evaluación de riesgos en el desarrollo de software que debería aplicar en un determinado proyecto?, ¿Los métodos de evaluación de riesgos lograran gestionar y prevenir los riesgos para el de desarrollo de un software?, ¿Se podrá obtener mediante un modelo analizar y evaluar los riesgos de un proyecto de desarrollo de Software?.

Esta tesis analizará los conceptos básicos de la gestión de riesgos y evaluará los principales marcos de referencia para la gestión de riesgos en proyectos de desarrollo de software con el propósito de presentar una propuesta, a modo de un modelo para identificar, evaluar y hacer un seguimiento de diferentes escenarios de riesgos durante las diferentes fases del desarrollo de software, como parte de la gestión de este tipo de proyectos.

1.2. Formulación del problema

Se formula el siguiente problema científico:

¿De qué manera un modelo de gestión de riesgos para identificar, evaluar y hacer seguimiento de los ayuda a gestionar proyectos de desarrollo de software?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Elaborar un modelo de gestión de riesgos que permita identificar, evaluar y hacer seguimiento de los riesgos en el desarrollo de software, como parte de la gestión que se realiza de este tipo de proyectos.

1.3.2. Objetivos específicos

1. Obtener un diagnóstico de la industria de software en la ciudad de Chiclayo a partir de la experiencia de las empresas de desarrollo de software, de tal forma que permita generar un modelo de negocio genérico que recoja la mayoría de las características de este tipo de negocio y su relación con los riesgos a los que se enfrentan.
2. Identificar los componentes que deben ser considerados en el modelo de gestión de riesgos; así como las interrelaciones existentes entre ellos.
3. Definir las clasificaciones y mecanismos de valoración, control y seguimiento de cada componente considerado en el modelo propuesto.
4. Elaborar un procedimiento para la aplicación práctica del modelo propuesto, en cada una de las fases de la gestión de riesgos de un proyecto de desarrollo de software.
5. Evaluar el modelo propuesto desde las perspectivas de su relevancia, coherencia, claridad y suficiencia.

1.4. Justificación de la investigación

1.4.1. Relevancia social

Los resultados de esta investigación, servirán como fuente de consulta para los gestores de proyectos de desarrollo de software, en relación a sus responsabilidades y funciones de análisis y evaluación de riesgos; y a partir de ello, elaborar sus propios instrumentos de identificación, análisis, control y seguimiento de los riesgos durante el ciclo de vida del desarrollo de software que se haya acogido para un proyecto en particular.

1.4.2. Implicancia práctica

El modelo de gestión de riesgos que se propondrá contemplará, un conjunto de definiciones, clasificaciones de los diferentes elementos que se considerarán en el modelo, sistemas de valoración o ponderación y un procedimiento documentado, que permita ser utilizado y aplicado en la práctica, durante la ejecución de actividades de gestión de riesgos en proyectos de software.

1.5. Limitaciones

a. Debido a las políticas de confidencialidad de información que tienen las empresas de desarrollo de software, no es fácil acceder a la información completa de los proyectos que hayan desarrollado o estén desarrollando, por lo que se convierten una limitante para evaluar la funcionalidad y la eficacia del modelo propuesto. En base a ello, el modelo propuesto será evaluado en base a la percepción y opinión que tengan expertos en gestión de proyectos de desarrollo de software o en gestión de riesgos. Para ello, se elaborará instrumentos adecuados que permitan recolectar y valorar esta información.
b. Las empresas que se tomarán como muestra para la recopilación de la información pertenecen al ámbito local de la ciudad de Chiclayo, Perú.

II. MARCO TEÓRICO

2.1. Bases teóricas

2.1.1. Fundamentos sobre gestión de proyectos

2.1.1.1. Proyecto

Según la definición del Project Management Institute (PMI), “un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único” (Project Management Institute, Inc, 2016)

Bajo este concepto el término temporal, se refiere a que cada proyecto siempre tendrá un comienzo y un fin determinado, un tiempo delimitado, una duración cuantificable (Chamoun, 2017), esto no significa que necesariamente un proyecto deba tener una corta duración, pero si, que la duración es limitada y el proyecto no será un esfuerzo continuo.

Se definen como únicos dado que cada proyecto posee características y funciones específicas que le confieren la cualidad de único (Chamoun, 2017).

Otra característica fundamental es la elaboración gradual (Guerrero, 2016), pues para facilitar la gestión, los proyectos tienden a dividir sus diferentes etapas en fases que conforman el ciclo de vida del proyecto.

2.1.1.2. Ciclo de vida de un proyecto

El ciclo de vida de un proyecto como lo sugiere el PMBOK (2) es la “serie de fases por las que atraviesa un proyecto desde su inicio hasta su cierre”.

“Estas fases deben seguir una secuencia lógica, con un comienzo y un final, y deben utilizar recursos para proporcionar resultados. Generalmente, las fases del proyecto se dividen por puntos de decisión que pueden variar dependiendo del ambiente organizacional” (ISO, 2016)

Según lo establece PMBOK figura (Ballefín, 2017) “todos los proyectos pueden configurarse dentro de la siguiente estructura genérica de ciclo de vida:

- Inicio del proyecto,
- Organización y preparación,

- Ejecución del trabajo y
- Cierre del proyecto.”

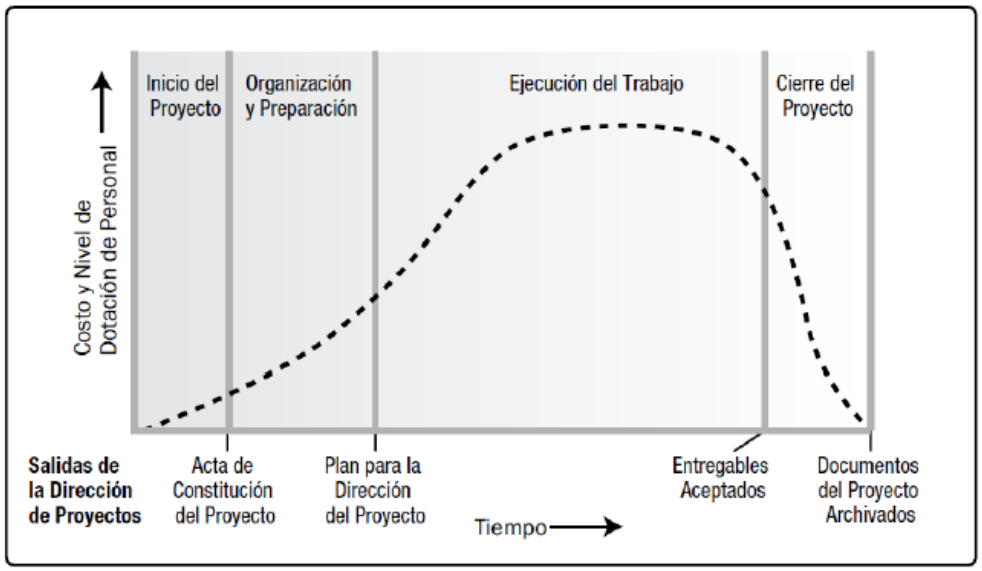


Gráfico N° 2. Ciclo de vida en proyectos (PMBOK-PMI)
Fuente: (Project Management Institute, Inc, 2016)

2.1.1.3. Factores de éxito de un proyecto

Dado que los proyectos son de naturaleza temporal, “el éxito de un proyecto debe medirse en términos de completar el proyecto dentro de las restricciones de alcance, tiempo, costo, calidad, recursos y riesgo” (Project Management Institute, Inc, 2016)

Standish Group, organización dedicada a la consultoría y principalmente a la investigación sobre el desempeño de los proyectos de software, genera cada dos años desde 1994 un Informe llamado CHAOS que presenta una instantánea del estado de la industria de desarrollo de software. El informe más reciente fue publicado en el 2015 y presenta el análisis de 50.000 proyectos de todo el mundo, la figura (Ballefín, 2017) resume los resultados de los proyectos en los últimos cinco años teniendo en cuenta tres factores de éxito (en tiempo, en presupuesto y satisfacción con los resultados (calidad).

“La gestión de proyectos incluye la integración de las diversas fases del ciclo de vida del proyecto” (ISO, 2016), el conocimiento requerido puede clasificarse en áreas diferenciadas que permiten segmentar el tipo de trabajo

requerido a lo largo del ciclo. Estas áreas pueden variar dependiendo del estándar, guía o norma a seguirse en cada organización.

En este caso de estudio, se han revisado tres estándares utilizados internacionalmente que sugieren un compilado de buenas prácticas para la Gestión de Proyectos, la Guía de los fundamentos para la Dirección de Proyectos PMBOK, el estándar creado en el Reino Unido PRINCE2 (Projects In Controlled Environments) y la Guía de Orientación sobre la gestión de proyectos ISO 21500, con el fin de identificar sus planteamientos sobre la estructura propuesta para la gestión de proyectos, en la tabla (Project Management Institute, Inc, 2016) se presenta un cuadro comparativo con cada uno de estas.

Tabla N° 3. Áreas del conocimiento Estándares Internacionales

ISO 21500	PMBOK	PRINCE2
Integración	Integración	Business Case
Partes Interesadas	Interesados	
Alcance	Alcance	
Recursos	Recursos humanos	Organización
Tiempo	Tiempo	
Costos	Costos	
Riesgos	**Riesgos**	**Riesgos**
Calidad	Calidad	Calidad
Adquisiciones	Adquisiciones	
Comunicación	Comunicación	
		Planes
		Cambios
		Progreso

Fuente: (Cardoza & Guerrero, 2016)

Dentro de las áreas donde hay convergencia en los tres estándares se encuentra el área del conocimiento de Riesgos, que cobra un valor importante y necesario a incluir en la gestión de un proyecto.

2.1.2. Fundamentos sobre gestión de riesgos en proyectos

2.1.2.1. Riesgo

Según PMBOK, "*el riesgo de un proyecto es un evento o condición incierta que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos del proyecto, tales como el alcance, el cronograma, el costo y la*

calidad. Un riesgo puede tener una o más causas y, si se produce, uno o más impactos".

La asociación (APM) (Group APM, 2015) usa una definición similar, definiendo riesgo como "*un evento incierto o un conjunto de circunstancias que, si se producen, tendrán un efecto en la consecución de los objetivos del proyecto*".

La norma AS9100C (SAE International Group, 2018) define riesgo como "*una situación o circunstancia indeseable que tiene tanto una probabilidad de ocurrir como una consecuencia potencialmente negativa*".

Por su parte la ISO 31000, define riesgo como "*efecto de la incertidumbre sobre los objetivos", entendiendo el efecto como una desviación de aquello que se espera, sea positivo, negativo o ambos, la incertidumbre como el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad y los objetivos pueden tener aspectos diferentes (por ejemplo financieros, salud y seguridad, y metas ambientales) y se pueden aplicar en niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos*" (ICONTEC, 2017).

Las organizaciones según PMBOK presentan diferentes actitudes frente al riesgo, las cuales clasifican en tres categorías apetito de riesgo: grado de incertidumbre que una organización está dispuesta a aceptar, tolerancia al riesgo: grado de riesgo que podría resistir la organización y umbral de riesgo: definición del parámetro a partir del cual la organización aceptará el riesgo.

Estas características generalmente se definen para poder llevar a cabo los procesos de análisis y evaluación de los riesgos ya que se establecen los criterios que clasificaran el tipo de riesgo y que conllevará a la selección de una respuesta diferente dependiendo del riesgo.

2.1.2.2. Gestión del riesgo

Se define gestión del riesgo como "*las actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo*". Definición 2.1. ISO Guía 73:2009 (ISO International organization for Standardization, 2016)

En proyectos, el riesgo tiene su origen en la incertidumbre, que está presente en todos los proyectos. Los riesgos que pueden ser identificados representan riesgos potenciales que de manera anticipada se prevén y que en caso de manifestarse pueden tener un efecto perjudicial en el desarrollo del proyecto, y para los cuales se puede estar preparado a través de un plan de respuesta. Los Riesgos no identificados representan aquellos que se surgen inesperadamente, y que no pueden preverse ni administrarse de forma proactiva.

Por tanto, para los riesgos identificados tempranamente o aquellos que surgen de modo inesperado se aplica la Administración de Riesgos la cual incluye todos los procesos relacionados con la planeación de la gestión, la identificación y registro, la evaluación cualitativa y cuantitativa, la planeación de la respuesta a los riesgos, y su seguimiento y control.

Se puede entonces considerar como administración de riesgos el método sistemático que permite planear, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso, para que la organización pueda reducir pérdidas y aumentar sus oportunidades.

Existen diversos esquemas y opiniones acerca de la estructura ideal del proceso de la Gestión de Riesgos. Sin embargo, casi todos concuerdan con el siguiente esquema básico: los riesgos son primero identificados, luego registrados, cuantificados, y finalmente controlados hasta el final de del Proyecto.

2.1.2.3. Modelos de gestión de riesgos

Actualmente se utilizan una serie de modelos para realizar un proceso lógico y sistemático que puede ser utilizado cuando se toman decisiones para mejorar la efectividad y eficiencia de las empresas. Los modelos permiten identificar y estar preparados para lo que puede suceder, se trata de tomar acciones destinadas a eludir y reducir la exposición a los costos u otros efectos de aquellos eventos que ocurran, en lugar de reaccionar después de que un evento ya ha ocurrido e incurrir en los costos que implican recuperar una situación.

En la tabla siguiente se presentan algunos modelos que presentan propuestas para la Gestión de Riesgos.

Tabla N° 4. Modelos de gestión de riesgos

ETAPAS	PMI PMBOK	Magerit	ISO 27005	PRINCE2
Planificación	X		X	
Identificación	X	X	X	X
Análisis / Valoración	X	X	X	X
Respuesta a los Riesgos	X	X	X	X
Monitoreo / Control	X	X	X	X
Registro de Riesgos		X	X	X
Reporte / Retroalimentación		X		

Fuente: (Muñoz & Cuadros, 2017)

Existen dos posibles enfoques frente a la gestión de los riesgos de un proyecto, dejar que sucedan o intentar prevenirlos.

El primero es el enfoque Reactivo. Este enfoque se basa en no preocuparse del problema hasta que éste ocurre y entonces reaccionar rápidamente de alguna manera. Es la estrategia comúnmente conocida como Modo Bombero ya que se limita a remediar el problema con urgencia una vez ocurrido. En el caso en que no se pueda solucionar el incidente, el proyecto peligra y es entonces cuando entra en escena la Gestión de Crisis para tomar el control. En el mejor de los casos, el enfoque reactivo supervisa el proyecto en previsión de posibles riesgos.

El segundo enfoque es el Proactivo y consiste en realizar una gestión efectiva de los riesgos antes que éstos se transformen en una amenaza para el éxito del proyecto. En la actualidad existen varios métodos que proponen una cierta organización de las actividades básicas que se deben llevar a cabo para realizar esta tarea satisfactoriamente.

2.1.2.4. Métodos de gestión de riesgos

Gestión de Riesgos son todas aquellas actividades que se implementan para identificar, analizar y controlar riesgos.

Estas actividades son genéricas por lo que es necesario mencionar que su implementación será diferente según la rama de actividad, es decir, ya sean proyectos de ingeniería civil, de ingeniería de software (de interés para esta tesis), en el área financiera, en el área de la salud entre otros. Esta diferenciación es una posible primera forma de categorizar métodos de gestión de riesgos.

Otro posible agrupamiento entre los distintos métodos se puede hacer dependiendo de la etapa de la gestión de riesgos en la que hacen hincapié. Es así que encontramos métodos que ponen todo su esfuerzo en la identificación de los riesgos, otros que lo hacen en el análisis y la priorización y finalmente otros que se concentran en estrategias de control de riesgos.

En esta tesis estaremos viendo métodos que cubren todas las actividades. Algunos de los métodos más reconocidos y aplicados en la industria son:

- Método de Gestión de Riesgos de Boehm,
- RiskIt (Kontio),
- Project Risk Management (PRM - Project Management Institute),
- Safe Activities For Enhancement (SAFE - Meli),
- RIMAM

2.1.2.5. Riesgos de Software

Según el autor Pressman (2015) sobre las estrategias reactivas de riesgo frente a estrategias proactivas de riesgo nos dice: *"Que una estrategia considerablemente más inteligente para la administración del riesgo es ser proactivo. Una estrategia proactiva comienza mucho antes de iniciar el trabajo técnico. Los riesgos potenciales se identifican, su probabilidad e impacto se valoran y se clasifican por importancia. Luego, el equipo de software establece un plan para gestionar el riesgo. El objetivo principal es evitarlo, pero, dado que no todos los riesgos son evitables, el equipo trabaja para desarrollar un plan de contingencia que le permitirá responder en forma controlada y efectiva".*

Cuando se analizan los riesgos es importante cuantificar el nivel de incertidumbre y el grado de pérdidas asociados con cada riesgo. Para lograr esto, se consideran diferentes categorías de riesgos.

A. **Riesgos del proyecto.** Amenazan el plan de proyecto, es decir, si los riesgos del proyecto se vuelven reales, es probable que el calendario del proyecto se deslice y que los costos aumenten.

   Los riesgos del proyecto identifican potenciales problemas de presupuesto, calendario, personal (tanto técnico como en la organización), recursos, participantes y requisitos, así como su impacto sobre un proyecto de software.

B. **Riesgos técnicos.** Amenazan la calidad y temporalidad del software que se va a producir. Si un riesgo técnico se vuelve una realidad, la implementación puede volverse difícil o imposible.
   Los riesgos técnicos amenazan la calidad y temporalidad del software que se va a producir. Si un riesgo técnico se vuelve una realidad, la implementación puede volverse difícil o imposible o también los problemas de diseño, implementación, interfaz, verificación y mantenimiento. Además, la ambigüedad en la especificación, la incertidumbre técnica, la obsolescencia técnica y la tecnología "de punta" también son factores de riesgo. Los riesgos técnicos ocurren porque el problema es más difícil de resolver de lo que se creía.

C. **Riesgos empresariales.** amenazan la viabilidad del software que se va a construir y con frecuencia ponen en peligro el proyecto o el producto. Los candidatos para los cinco principales riesgos empresariales son: (1) Construir un producto o sistema excelente que realmente no se quiere (riesgo de mercado), (2) construir un producto que ya no encaje en la estrategia empresarial global de la compañía (riesgo estratégico), (3) construir un producto que el equipo de ventas no sabe cómo vender (riesgo de ventas), (4) perder el apoyo de los administradores debido a un cambio en el enfoque o en el personal (riesgo administrativo) y (5) perder apoyo presupuestal o de personal (riesgos presupuestales).

2.1.2.6. Identificación de riesgos en proyectos de software

La identificación de riesgos es un intento sistemático por especificar amenazas al plan del proyecto (estimaciones, calendario, carga de recursos, etc.). Al identificar los riesgos conocidos y predecibles, el gerente de proyecto

da un primer paso para evitarlos cuando es posible y para controlarlos cuando es necesario.

Un método para identificar riesgos es crear una lista de verificación de ítem de riesgo. La lista de verificación puede usarse para identificación del riesgo y así enfocarse sobre algún subconjunto de riesgos conocidos y predecibles en las siguientes subcategorías genéricas:

a. **Tamaño del producto:** riesgos asociados con el tamaño global del software que se va a construir a modificar.
b. **Impacto empresarial:** riesgos asociados con restricciones impuestas por la administración o por el mercado.
c. **Características de los participantes:** riesgos asociados con la sofisticación de los participantes y con la habilidad de los desarrolladores para comunicarse con los participantes en forma oportuna.
d. **Definición del proceso:** riesgos asociados con el grado en el que se definió el proceso de software y la manera como se sigue por parte de la organización desarrolladora.
e. **Entorno de desarrollo:** riesgos asociados con la disponibilidad y calidad de las herramientas por usar para construir el producto.
f. **Tecnología por construir:** riesgos asociados con la complejidad del sistema que se va a construir y con lo “novedoso” de la tecnología que se incluye en el sistema.
g. **Tamaño y experiencia del personal:** riesgos asociados con la experiencia técnica y de proyecto global de los ingenieros de software que harán el trabajo.

2.1.2.7. Estimación del riesgo en proyectos de software

También llamada estimación del riesgo, intenta calificar cada riesgo en dos formas: 1) la posibilidad o probabilidad de que el riesgo sea real y 2) las consecuencias de los problemas asociados con el riesgo, en caso de que ocurra. Usted trabaja junto con otros gerentes y personal técnico para realizar cuatro pasos de proyección de riesgo:

1. Establecer una escala que refleje la probabilidad percibida de un riesgo.

2. Delinear las consecuencias del riesgo.
3. Estimar el impacto del riesgo sobre el proyecto y el producto.
4. Valorar la precisión global de la proyección del riesgo de modo que no habrá malos entendidos.

2.1.2.8. Elaboración de una tabla de riesgos

Una tabla de riesgos proporciona una técnica simple para proyección de riesgos. Para cada riesgo se valora la probabilidad de ocurrencia de cada riesgo, la cual puede estimarse individualmente por los miembros del equipo hasta que su valoración colectiva de la probabilidad del riesgo comience a convergir. A continuación, se valora el impacto de cada riesgo. Normalmente se consideran como categorías de los componentes de riesgo a: rendimiento, apoyo, costo y calendario, y finalmente se promedian para determinar un valor de impacto global.

2.2. Definiciones conceptuales

a. **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. **Grupos de interés:** Personas u organizaciones que se ven impactadas por las operaciones de una empresa. Ejemplos: clientes, socios del negocio, empleados, proveedores, accionistas, entidades gubernamentales, entre otros.

c. **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

d. **Periodo máximo tolerable de interrupción:** Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.

e. **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

f. **Riesgo:** La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.

g. **Riesgo operacional:** La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

h. **Tiempo objetivo de recuperación:** Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

III. METODOS Y TÉCNICAS DE INVESTIGACIÓN

3.1. Tipo de investigación

Este trabajo de tesis se ha tipificado como **aplicada, descriptiva – propositiva, no experimental y cualitativa**.

a. La investigación es **aplicada** porque se utilizan los fundamentos teóricos de los marcos de referencia PMBOK y Magerit, para la elaboración del modelo de la gestión de riegos en el proceso de desarrollo de software.
b. Es de tipo **descriptiva** porque se utilizan métodos descriptivos para explicar cada uno de los componentes del modelo de gestión de riesgos que se propone; así como las interrelaciones entre éstos.
c. La investigación es de tipo **propositiva** por que se pretende cubrir una necesidad o vacío dentro de las empresas del sector de desarrollo de software de la ciudad de Chiclayo, para luego generalizar; a través de una propuesta de modelo de gestión de los riesgos asociados al desarrollo de software que ayude en la gestión de proyectos de software.
d. **No experimental**, porque no se pretende medir el efecto de la propuesta en la realidad. Para la validación del modelo propuesto se aplicará una técnica cualitativa no experimental.
e. **Cualitativa**, porque los métodos de investigación aplicados para la recopilación de la información, análisis y síntesis de los resultados son del tipo cualitativos.

3.2. Técnicas e instrumentos de recolección de datos

La ejecución efectiva de la investigación cualitativa supone algunas técnicas de recolección de datos que incluyen un análisis progresivo mientras se las realiza la construcción de la propuesta. Las técnicas de investigación, que se aplicaron fueron:

a. **Análisis documental:** Esta técnica se aplicó como punto de entrada a la investigación, con la finalidad de comprender y caracterizar el origen del problema de investigación. Se revisaron documentos estadísticos que permitieron describir la problemática de la gestión de los proyectos de desarrollo de software, en relación al fracaso de los proyectos de software iniciados. Así mismo, el análisis de los proyectos de software que se revisaron, permitió evidenciar que los proyectos fracasados tenían una relación directa con la ausencia de métodos y técnicas de gestión de riesgos durante la gestión de los proyectos.

Ne el análisis documental se desarrollaron en cinco acciones: búsqueda e inventario de los documentos existentes, clasificarlos, seleccionar los documentos más pertinentes para los propósitos de la investigación, lectura en profundidad el contenido de los documentos seleccionados, análisis en forma cruzada y comparativa los documentos en cuestión.

b. **La entrevista estructurada, formal e individual**. Se lo realizó a partir de una guía prediseñada que contiene las preguntas que fueron formuladas al personal que tiene autoridad y responsabilidad en la gestión de proyectos de desarrollo de software en las empresas seleccionadas intencionalmente. En este caso se desarrolló una guía de entrevista como instrumento (ver anexo 1).

   El propósito de aplicar esta técnica, fue hacer una indagación exhaustiva para descubrir las razones más fundamentales de las actitudes y comportamientos de los responsables de la gestión de proyectos de software, en relación a problemas a los que se puede enfrentar un proyecto de esta naturaleza y la forma cómo es que actuaron para superar los mismos. La idea principal, era encontrar problemas comunes que tienen las empresas de desarrollo de software en el desarrollo de sus proyectos, evitando particularidades de cada empresa.

c. **La encuesta.** Esta técnica se utilizó en el proceso de validación del modelo de gestión de riesgos propuesto, a través de un cuestionario estructurado, cuyas preguntas estuvieron dirigidas a obtener la opinión de los encuestados en relación a su percepción y valoración de cada uno de los componentes del modelo (ver anexo 2).

3.3. Método para la construcción del modelo de riesgos

3.3.1. Alcance del modelo de gestión de riesgos

La Guía PMBOK, determina que el alcance de un Sistema de Gestión de Riesgos (SGR) se determina tomando como referencia el contexto y entorno de la organización, considerando su estructura organizativa, procesos, activos, tecnología y otros elementos relacionados (Project Management Institute, Inc., 2017)

El propósito de definir el alcance del SGR, es identificar los activos de TI que serán considerados en la evaluación de los riesgos, independientemente de

su ubicación, quienes son los responsables de su gestión o quienes tiene los privilegios para su uso.

Las tareas consideradas en esta fase se describen a continuación:

a. **Identificación de procesos de negocio:** Para la identificación de los procesos negocio se utilizó la técnica de mapeado de procesos y sub procesos. Los procesos que deberán ser considerados en el alcance del SGR serán los procesos misionales o principales.

b. **Definición del catálogo de activos de TI:** A partir de los procesos de negocio identificados dentro del alcance del SGR, se identifica el catálogo o inventarios que dan soporte a los procesos considerados en la selección.

Para la catalogación del inventario se utilizará el siguiente formato:

- Denominación del activo de TI
- Categoría del activo de TI. Para categorizar a los activos se utilizaron las siguientes nominaciones: (1) Información, (2) Software, (3) Hardware, (4) Servicios y (5) Personal
- Clasificación. Para la clasificación de los activos de TI, se utilizó un criterio de accesibilidad, de la siguiente manera: (1) Confidencial, (2) Uso Interno y (3) Público
- Frecuencia de uso. Para determinar la frecuencia de uso y explotación del activo de TI, se utilizó la siguiente nominación: (1) Diario, (2) Mensual, (3) Anual y (4) Otro
- Ubicación del activo. Dependiendo del tipo de activo, la ubicación puede ser física o lógica
- Usuario responsable del uso o explotación del activo de TI
- Responsable de la custodia del activo de TI
- Responsable del activo de TI
- Criticidad del activo. Para valorar de la criticidad o importancia de los activos de TI, se utilizó la escala: (1) Alto, (2) Medio o (3) Bajo
- Procesos relacionados. Se identificaron los procesos que están relacionados con cada activo de TI.

3.3.2. Procedimiento para la construcción del componente: Evaluación de riesgos

Para realizar las tareas de construcción de este componente, se tomó como referencia principalmente la metodología Magerit para la identificación de componentes, y la ISO 27005 para la parte procedimental.

En la gráfica siguiente se aprecia que los elementos de un modelo de gestión de riesgos de TI, según la metodología Magerit, son:

- Los activos de TI
- La estimación de la criticidad de los activos de TI
- Las amenazas que pueden afectar los activos de TI
- El impacto en el negocio debido a la ejecución de una amenaza
- La frecuencia de una amenaza

Gráfico N° 3. Elementos de la gestión de riesgos de TI

Fuente: (Magerit - Libro 1, 2012)

En base al modelo de gestión de riesgos de TI mostrado y el marco teórico referente a gestión de riesgos, se definieron las siguientes tareas:

a. **Inventario de activos**

Se analizarán los procesos de negocio que han sido definidos dentro del alcance del SGSI, para identificar los activos de información y de TI que serán considerados en la evaluación de riesgos.

El inventario de activos debe considerar las categorías de activo propuesto en la metodología Magerit. El formato para el registro del inventario de activos se muestra a continuación.

Tabla N° 5. Tabla de referencia para la tipificación de los activos de TI

Tipo	Código	Detalle
Activo de información (I)	I1	Información electrónica
	I2	Información escrita
	I3	Documentos administrativos en papel
	I4	Documentos en formato digital (.doc. pdf, etc.)
Activo de software (SW)	SW1	Sistemas operativos
	SW2	Aplicaciones comerciales y utilitarios
	SW3	Aplicaciones desarrolladas por terceros
	SW4	Aplicaciones desarrolladas a medida
	SW5	Sistemas DBMS
	SW5	Otro tipo de aplicaciones
Activo de hardware (HW)	HW1	Equipo de procesamiento
	HW2	Equipo de comunicaciones
	HW3	Medio de almacenamiento
	HW4	Mobiliario y equipamiento
	HW5	Otros equipos
Servicios terceros (S)	S1	Procesamiento y comunicaciones
	S2	Servicios generales
	S3	Otros servicios

Fuente: Elaboración propia, adaptado de (Magerit - Libro 1, 2012)

Así mismo, para cada activo se debe registrar la siguiente información:

- Clasificación: Confidencial, Restringido (o de uso interno), Público
- Frecuencia de uso: Anual, Mensual, Diario
- Ubicación física o lógica
- Usuario responsable de su uso
- Usuario responsable de su custodia
- Usuario responsable del activo
- Procesos donde se usa el activo
- Valor del activo. Para la valoración del activo se utilizará la siguiente tabla de referencia:

b. Determinación de la criticidad de los activos

Cada uno de los activos inventariados fueron evaluados para determinar su nivel de criticidad.

Para determinar el nivel de criticidad de los activos inventariados se evaluó y valoró las características de seguridad de la información considerados por la ISO 27001 como son: confidencialidad, integridad y disponibilidad. Para la valoración de los tres criterios mencionados se utilizó una escala de 1 a 3, en la que cada nivel de la escala representa el nivel de afectación del criterio de seguridad en caso de que el activo evaluado sea impactado negativamente por algún evento o incidente de seguridad de la información (amenaza).

La siguiente tabla muestra las escalas de valoración de cada uno de las tres características de seguridad de la información.

Tabla N° 6. Escala para la valoración de los criterios de seguridad de la información en los activos de TI

Criterio	Valor en escala	Descripción
Disponibilidad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, si el activo no está disponible o se destruye.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, si el activo no está disponible o se destruye.
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, si el activo no está disponible o se destruye.
Integridad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, si el activo no está completo o está modificado.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, si el activo no está completo o está modificado.
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, si el activo no está completo o está modificado.
Confidencialidad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, porque el activo es de conocimiento público.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, porque el activo podrá ser utilizado o divulgado hacia o entre el personal de la empresa
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, porque el activo contiene información muy sensible de la empresa

Fuente: Desarrollo propio, basado en las escalas de valoración de la metodología Magerit

Para estimar el nivel de criticidad de los activos de TI se utiliza la siguiente relación:

Criticidad del activo = valor de confidencialidad + valor de integridad + valor de disponibilidad

(fórmula N° 1)

c. Identificación de las amenazas y vulnerabilidades

Para la tarea de identificación de amenazas, consideradas como eventos que pueden que causar un incidente imprevisto o que puede degradar los activos, se tomará como referencia el catálogo de amenazas propuesto en la metodología Magerit, bajo la siguiente clasificación:

- Amenazas del tipo natural (algún tipo de sismo, incendio natural, tormentas, etc.)
- Amenazas del tipo industrial (fuego, explosiones, corto circuito, sobrecalentamiento, etc.)
- Amenazas de origen humano (descuidos, mal intensiones, irresponsabilidades, incumplimiento de funciones, etc.)
- Amenazas del tipo tecnológico (fallas en la red, fallas en la BD, virus, hackeo, etc.)
- Amenazas de origen operacional (mala logística, fallas en el proceso, obsolescencia, etc.)
- Amenazas del tipo social (huelgas, vandalismo, protestas, etc.)

Del mismo modo, para la tarea de identificación de vulnerabilidades, consideradas como las debilidades, incongruencias, ausencias, fallas, etc., en los mecanismos de seguridad, que pueden ser aprovechadas por las amenazas, se utilizó la siguiente clasificación:

- Debilidades en el control de accesos
- Debilidades en la seguridad ligada a los Recursos Humanos
- Debilidades en la seguridad física y del entorno
- Debilidades en la gestión de las comunicaciones y las operaciones
- Debilidades en el adquisición, desarrollo y mantenimiento de sistemas de información”

d. Estimación del impacto

Para estimar el impacto de una amenaza se utilizará una escala de cinco ítems. Los criterios para la valoración de estos escenarios de riesgo han sido tomados de la metodología Magerit en base a los objetivos de la investigación, seleccionándose los siguientes:

- Continuidad o interrupción de los servicios
- Economía de la empresa e intereses comerciales
- Seguridad.

Tabla N° 7. Escala de valoración del impacto de una amenaza

Nivel de impacto	Continuidad de los servicios	Economía de la empresa e intereses	Seguridad
5: Muy Alto	Ocasiona interrupciones serias en las actividades de la empresa, generando mala reputación en los clientes. Ocasiona destrucción de los equipos o en las instalaciones	Ocasiona pérdidas económicas muy elevadas. Ocasiona incumplimientos muy graves con las obligaciones y responsabilidades contractuales importantes	Causan incidentes muy graves relacionados con la seguridad No se puede realizar seguimiento o investigación de los incidentes.
4: Alto	Ocasiona interrupciones graves en las actividades de la empresa, con paralizaciones en la prestación de algunos servicios. Ocasionan incidentes que demandan tiempos y costos considerables de recuperación	Ocasiona pérdidas económicas graves. Ocasiona incumplimientos serios con algunas obligaciones contractuales importantes	Causan incidentes serios relacionados con la seguridad Hay dificultad para realizar el seguimiento o investigación de los incidentes.
3: Medio	Ocasiona interrupciones en las actividades de la empresa generando condiciones operativas negativas que aumentan la carga de trabajo y disminuyen su eficiencia	Ocasiona pérdidas económicas significativas. Ocasiona incumplimientos significativos con algunas obligaciones contractuales	Causan incidentes significativos relacionados con la seguridad Se puede realizar seguimiento o investigación de los incidentes.
2: Bajo	Ocasiona interrupciones en las actividades de la empresa generando algunas interferencias en los servicios, continuando con procedimientos de emergencia	Ocasiona ciertas mermas en los ingresos. Ocasionan incumplimientos leves en las obligaciones contractuales	Causan incidentes de seguridad con poca repercusión en los activos de información.
1: Muy Bajo	Ocasionan interrupciones en las actividades de poca importancia	Ocasionan pérdidas económicas mínimas. Causa incidencias de pequeño valor comercial	Causan incidentes de seguridad de casi nula repercusión en los activos de información.

Fuente: Elaboración propia, tomando como referencia la propuesta de la metodología Magerit

e. Estimación de la probabilidad de ocurrencia

Para estimar de la probabilidad de ocurrencia de una amenaza se utilizó como referencia la siguiente tabla, donde se muestra una escala de valoración en cinco niveles:

Tabla N° 8. Escala de valoración para la probabilidad de ocurrencia

Nivel	Descripción del nivel
5: Muy Alto	Ocurre de manera diaria Los mecanismos de seguridad implantados son inexistentes o ineficientes.
4: Alto	Ocurre de manera semanal Los mecanismos de seguridad implantados poco eficientes.
3: Medio	Ocurre de manera mensual Los mecanismos de seguridad implantados a veces pueden impedir la amenaza
2: Bajo	Ocurre de manera anual Los mecanismos de seguridad implantados son eficientes para impedir una amenaza
1: Muy Bajo	Ocurre más de una vez al año Los mecanismos de seguridad implantados son altamente eficientes que casi siempre impiden una amenaza

Fuente: Elaboración propia

f. Estimación del nivel de exposición al riesgo

La estimación de los niveles de riesgos de TI sirve para determinar qué tan expuesta está la empresa en cada uno de los escenarios de riesgos. El análisis debe considerar las vulnerabilidades y amenazas identificadas para cada activo de TI.

Para realizar este cálculo se utilizará las siguientes fórmulas:

Criticidad del activo = C + I + D (fórmula N° 2)

Riesgo = Criticidad + (Probabilidad * Impacto) (fórmula N° 3)

Se estableció una escala para determinar los niveles de tolerancia a los riesgos. Cada nivel corresponde a un rango de valores de los niveles de riesgo.

Tabla N° 9. Escala para determinar el nivel de tolerancia a los riesgos

Nivel	Descripción del nivel
Totalmente Tolerable o Aceptable (TT)	4 – 15
Con regularidad es Tolerable o Aceptable (RT)	16 – 25
No es Tolerable o No es Aceptable (NT)	26 – 34

Fuente: Elaboración propia

Para los niveles de riesgo que se encuentran fuera de los rangos de tolerancia “Regularmente Tolerable” o “No Tolerable”, deberán ser tratados mediante acciones para redefinir salvaguardas y controles.

Para los niveles de riesgo que se ubiquen en el rango de “Totalmente Tolerable”, son opcionales para ser tratados.

3.3.3. Procedimiento para la construcción del componente: Tratamiento y control del riesgo

a. Identificación de los mecanismos de seguridad para la mitigación de los riesgos no tolerables

En esta tarea se identifican las medidas de seguridad que implantará la organización para la reducción del riesgo. Estas medidas pueden ser tecnológicos o administrativos. Algunos escenarios de riesgo se pueden con los mecanismos de seguridad existentes; sin embargo, otros escenarios de riesgo, requieren de elementos técnicos o tecnológicos.

b. Definición de la estrategia de tratamiento de los mecanismos de seguridad y controles

Las estrategias para el tratamiento de los mecanismos de seguridad y controles han sido clasificadas de la siguiente manera:

a. **Reducción del riesgo (R):** Esta estrategia se aplica generalmente cuando se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas) y la economía suficiente para la implementación de los mecanismos de seguridad y controles.
b. **Aceptar el riesgo (A):** Esta estrategia se aplica generalmente cuando NO se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas) y ni con la economía suficiente para la implementación de los mecanismos de seguridad y controles.
c. **Transferencia del riesgo (T):** Esta estrategia se aplica generalmente cuando se cuenta NO se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas), pero si con la economía suficiente para la implementación de los mecanismos de seguridad y controles transfiriendo a una tercera parte especializada.
d. **Evitar el riesgo (E):** Esta estrategia generalmente se aplica cuando el origen de la amenaza puede ser eliminado, para evitar la presencia del riesgo .

c. Estimación del riesgo residual

El riesgo residual se estima luego de la implementación de los mecanismos de seguridad y los controles, utilizando las mismas relaciones o fórmulas para la estimación del riesgo efectivo.

Riego Residual = Criticidad + (Probabilidad Residual * Impacto Residual)

(fórmula 4)

“Para los riesgos que resulten nuevamente regularmente tolerable o no tolerable se debe redefinir nuevamente salvaguardas. Los riesgos que resulten totalmente tolerables, son considerados riesgos despreciables, y no requieren más acciones, que el monitoreo periódico”.

3.3.4. Procedimiento para la construcción del componente: Plan de tratamiento de riesgos

Luego que se determine la aplicabilidad de los controles, se elaborará un cuadro donde se definan un conjunto de actividades para implementar cada una de las propuestas de control, que permitan superar las debilidades encontradas en cada escenario de riesgo.

IV. RESULTADOS Y DISCUSIÓN

4.1. Diagnóstico de la industria de software en la ciudad de Chiclayo

En la Región Lambayeque, principalmente en la ciudad de Chiclayo, existen un número considerable de PYMES y empresas medianas dedicadas a la fábrica de software, muchas de ellas, debidamente formalizadas como empresa y otras que trabajan casi de manera informal.

Para realizar el diagnóstico de la industria del software en la ciudad de Chiclayo, se seleccionó un grupo de empresas del sector, que cumplieran con un conjunto de criterios y luego aplicar la entrevista como técnica de recogida de la información.

4.1.1. Criterios y selección de las empresas

Las empresas seleccionadas debieron cumplir con características básicas que permitan asegurar la calidad de la información a ser recopilada. Así, las características definidas para la selección de las empresas fueron: su participación en proyectos de tecnología, experiencia en el mercado y reconocimientos en la industria, de acuerdo a los criterios de tabla siguiente:

Tabla N° 10. Criterios para la selección de las empresas

Tamaño de proyectos dirigidos	Para pequeñas, medianas y grandes empresas
Experiencia	Desarrollo de software Arquitectura de software Gerencia de proyectos de software Gerencia de empresa de software
Tipos de proyectos de TI	Proyectos de desarrollo de software
Reconocimiento	Prestigio en la industria

Fuente: Desarrollo propio

Las empresas seleccionadas se muestran en la tabla siguiente.

Tabla N° 11. Empresas seleccionadas de la industria de software en la ciudad de Chiclayo

N°	Empresa
1	Garza Soft
2	AD y L Consulting
3	Audiconsulti S.A.C.
4	Datec Consulting SAC
5	Meraki Software
6	ETI
7	Inticap
8	Grupo ES Consultores
9	Red Chiroque

Fuente: Desarrollo propio

4.1.2. Aplicación de la entrevista de diagnóstico

Para realizar el diagnóstico de la situación actual de las empresas de desarrollo de software en la ciudad de Chiclayo y, en base a ella elaborar un modelo de negocio tipo en este sector, se realizó entrevistas a los responsables de las tecnologías de la información y/o gerentes de sistemas de las empresas seleccionadas, en un total de nueve (09).

Para ello, se elaboró una guía de entrevista (ver Anexo 1), con un cuestionario definido, para respuestas no estructuradas, que abarcaron los siguientes aspectos:

a. Características generales del negocio
b. Producto o servicio ofrecidos
c. Formas de gestión de los proyectos de software
d. Problemas comunes en la gestión de proyectos
e. Perfil del entrevistado

Para la aplicación de las entrevistas, se elaboró un cronograma, que se muestra en la siguiente tabla.

Tabla N° 12. Cronograma de entrevistas a los representantes de las empresas seleccionadas

N°	Empresa	Entrevistado	Cargo	Fecha	Duración (min)
1	Garza Soft	Martín Ampuero Pasco	Gerente General	03.02.20	50
2	AD y L Consulting	Edgar Flores Peña	Desarrollador Senior	03.02.20	55
3	Audiconsulti S.A.C.	Junior Cachay Maco	Gerente general	04.02.20	45
4	Datec Consulting SAC	Marisol Silva	Proyectista	05.02.20	50
5	Meraki Software	Juan José Terry	Proyectista y analista	05.02.20	50
6	ETI	Dolores Toro Seminario	Desarrollador	06.02.20	55
7	Inticap	Edwin Ortega	Desarrollador	10.02.20	50
8	Grupo ES Consultores	Estuardo Ñiquen	Desarrollador Senior	11.02.20	45
9	Red Chiroque	Pablo Pisfil Negra	Desarrollador	13.02.20	50

4.1.3. Síntesis de la información obtenida en las entrevistas

4.1.3.1. Características generales de las empresas

Del análisis de la información obtenida de las entrevistas, de manera general se puede determinar lo siguiente:

1. Las empresas en la ciudad de Chiclayo tienen un enfoque común en cuanto a la oferta de software. La mayoría de las empresas aplica metodologías tradicionales de desarrollo de software. Tan solo 2/9 de las empresas han implementado Software como Servicio (SaaS) dentro de los últimos cuatro años.

2. La oferta está orientada al modelo de distribución de software como producto, generando gran mercado de: desarrollo de software a medida; configuración y parametrización de productos. Adicionalmente es común ofrecer servicios de consultoría y capacitaciones. Debido a esta similitud en los productos y servicios mencionados anteriormente, las empresas de software buscan desarrollar estrategias que les permitan cubrir casi todas las necesidades de los clientes y contar con personal altamente calificado como factor de diferenciación.

3. Sin embargo, el contar con este tipo de estrategias y personal no constituyen en realidad una ventaja competitiva en la industria del software en Chiclayo. Como resultado, los clientes se encuentran con un

mercado que tiene muchos ofertantes, pero con un único esquema de trabajo. Por otro lado, existen empresas que ya están incursionando en el mundo del SaaS ofreciendo una alternativa distinta al modelo de negocios tradicional. Estos emprendimientos están siendo impulsados por la actual tendencia mundial.

4.1.3.2. Productos o servicios ofrecidos

Las empresas de software de la ciudad de Chiclayo ofrecen a sus clientes, tanto del sector público como del privado, un conjunto de productos y servicios con las siguientes características:

a. **Desarrollo de software a medida.** Este servicio se brinda en base a las necesidades que tienen los clientes de las empresas seleccionadas. La empresa de desarrollo de software analiza, desarrolla e implementa aplicaciones informáticas (productos de software) que cumplen con los requerimientos específicos del cliente. En esta modalidad la contratación para brindar el servicio, se puede dar por producto o por horas de desarrollo. Al finalizar el proyecto, el propietario final del código fuente, manuales y aplicativo, es siempre el cliente. Otra de las características de este servicio, es que el cliente debe contar con la infraestructura necesaria para la implementación de las aplicaciones informáticas, además del personal capacitado para dar soporte al aplicativo una vez que este ya se encuentre implementado.
b. **Parametrización de software:** En esta modalidad, las empresas seleccionadas se encargan de vender la licencia de un producto empaquetado acompañado de servicios de análisis, instalación, configuración y parametrización. De acuerdo a la información obtenida, en esta modalidad de servicio, la mayor parte de los ingresos económicos por el desarrollo del proyecto está destinado al pago de la licencia del fabricante.
c. **Servicios de consultoría:** Dentro de este ámbito, las empresas seleccionadas, ofrecen a sus clientes, expertos en áreas específicas, quienes con su experiencia y conocimiento analizan y plantean una solución o mejora a un proceso o problema que se encuentre enfrentando el cliente.
d. **Capacitaciones:** Este es otro servicio que ofrecen las empresas del sector en la ciudad de Chiclayo, aprovechando el nivel de conocimiento y

experiencia que tiene su personal. Se dictan cursos o capacitaciones sobre temas específicos dependiendo del requerimiento del cliente.

e. **Outsourcing:** Es una modalidad de servicio poco aplicada en Chiclayo, y los contratos generalmente son de préstamo de personal para ejecutar tareas específicas y definidas por el cliente. Las empresas cobran mensualmente un valor dependiendo del nivel de experiencia del personal.

Los productos y servicios descritos, representan los principales ingresos económicos de las empresas del sector de desarrollo de software en la ciudad de Chiclayo, y a éstos se debe su subsistencia en el mercado actual. El gráfico siguiente muestra la formas como están distribuidos los productos y servicios que ofrecen las empresas de la industria del software en Chiclayo.

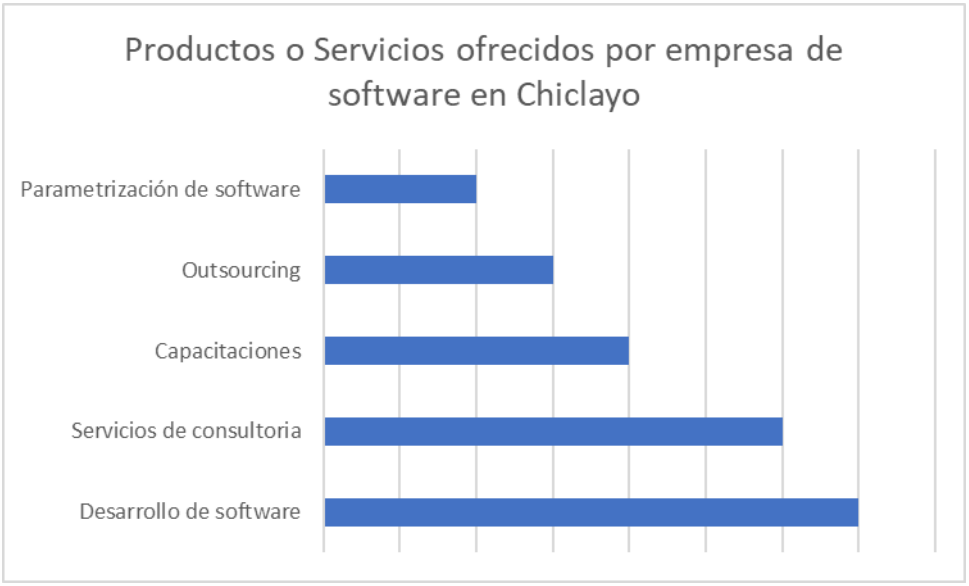


Gráfico N° 4. Productos o servicios ofrecidos por las empresas de software en la ciudad de Chiclayo

4.1.3.3. Diferenciación de los productos o servicios ofrecidos

Las empresas de software en el mercado local, se enmarcan dentro de un modelo de negocio tradicional donde la entrega de productos y servicios va de acuerdo a los aspectos mencionados en el punto anterior. Por lo tanto, la forma en la que buscan generar valor frente a sus competidores es básicamente a través de la calidad del personal con el que cuentan y la calidad de los productos y servicios que entregan al finalizar cada proyecto.

Se puede determinar que no existe un atributo diferenciador predominante en los modelos de negocio de las empresas del sector en la ciudad de Chiclayo actualmente.

El recurso clave que permite generar valor a una empresa se concentra en la calidad del recurso humano con el que cuenta para el desarrollo de sus proyectos.

Adicionalmente, un factor que resulta muy importante es la experiencia con la que cuenta la empresa en el mercado, la cual brinda credibilidad frente a sus clientes.

4.1.3.4. Principales actividades de negocio

Los resultados obtenidos de las entrevistas muestran que las empresas de software en la ciudad de Chiclayo, realizan las siguientes actividades principalmente: operaciones (principalmente desarrollo de software y consultorías), marketing de sus productos y servicios y ventas. Estas actividades representan las actividades Core del negocio en las empresas seleccionadas.

En los proyectos de desarrollo de software, las empresas buscan asegurar que cumplan con las necesidades de sus clientes, aplicando las mejores prácticas en las etapas de construcción de software y en la evaluación de la calidad del mismo. Adicionalmente, se busca ofrecer precios mejorados frente a la competencia.

4.1.3.5. Alianzas con otras empresas

El objetivo de manejar alianzas con otras empresas es cubrir todas las necesidades de los clientes en un solo proyecto. Por lo general, las empresas que no cuentas con la capacidad suficiente para atender un conjunto de requerimientos y necesidades en un contrato, realizan alianzas estratégicas con otras empresas, que, por lo general, es para reforzar su soporte tecnológico y de personal especializado de mayor experiencia.

De este modo, las alianzas permiten acceder a recursos tanto humanos como de hardware.

4.1.3.6. Principales costos en los proyectos

Según los entrevistados, entre los principales costos que las empresas de desarrollo de software enfrentan están: personal, movilización y suscripciones.

f. **Personal.** Este componente de costo en los proyectos, representa el costo más elevado que las empresas tienen que afrontar. Este costo, por lo general, está en función del nivel de conocimientos de las personas que participan en cada proyecto. Adicionalmente, hay empresas que realizan inversiones de tiempo y dinero para la capacitación de su personal. Aquí se puede identificar un escenario de riesgos para las empresas de este sector, que es la salida de personal calificado de la empresa, porque representa una pérdida, en tiempo y dinero, que afecta al negocio de la empresa.
g. **Movilización.** Este componente de costo en los proyectos, representa el segundo costo más elevado. Se ha identificado que, muchos de los proyectos que desarrollan estas empresas, se realizan con clientes fuera de la ciudad de Chiclayo; por tanto, hay un costo relacionado a su movilización, como: pasajes, hoteles, viáticos. De igual manera, dentro de la ciudad la movilización del personal a las oficinas de los clientes es cubiertas por las empresas.
h. **Suscripciones.** Este es un costo, surge cuando las empresas ofrecen productos de terceros, es decir, ofrecen productos ya desarrollados (enlatados). El costo está relacionado con la suscripción que realizan con el fabricante del producto software, y aumenta cuando hay más de una instalación y parametrización.

4.1.3.7. Principales fuentes de ingresos

De acuerdo a la información recogida, las fuentes de ingresos, prácticamente define el modelo de negocio que utilizan las empresas de desarrollo de software en Chiclayo. Las fuentes de ingresos, generalmente está en función del tipo de distribución que realizan de sus productos de software y del segmento de mercado al cual va dirigido.

Encontramos que principalmente son dos tipos de modelo de distribución de productos de software que utilizan las empresas de desarrollo de software en la ciudad de Chiclayo:

a. **Software de prueba (Freemium):** En esta modalidad de distribución, las empresas chiclayanas ofrecen una versión gratuita del servicio, que generalmente es una versión limitada. Para obtener la versión completa del servicio, el cliente debe pagar un precio por acceder a la versión completa.

   La ventaja que se encontró en esta modalidad de distribución de los productos de software, es que permite a los clientes probar las aplicaciones antes de usarlo formalmente.

   De las nueve (09) empresas evaluadas, siete (07) utilizan esta estrategia de distribución, con las siguientes opciones de distribución:
   - Característica del producto (1 empresa): La versión distribuida del producto de software incluyen solo características básicas
   - Capacidad del producto (1 empresa): La versión del producto solo permite registrar un número limitado de transacciones, debido al que el tamaño de la base de datos está parametrizado para un número limitado de registros.
   - Clasificación del producto (4 empresas): Las versiones de los productos de software son clasificadas en categorías como: comercial; no comercial; educación; sin fines de lucro. Dependiendo de ello, de la clase del producto, algunas clases ofrecen versiones free y otras no. En algunos casos, las aplicaciones se habilitan por un tiempo determinado.
   - Soporte (7 empresas): En la mayoría de los contratos analizados, se encontró que el soporte post venta es un ítem que se considera clave. Existen versiones de los productos de software que son distribuidas sin considerar este servicio post venta.

b. Software pagado. En esta modalidad de distribución, las empresas chiclayanas ofrecen sus productos de software utilizando las siguientes estrategias de pago:

- **Pago por uso** (7 empresas). Este modelo de fijación de precios está en función de la adquisición y uso del producto software. El valor del software generalmente está en función de las funcionalidades implementadas, el tipo de cliente y el tipo de tecnología de implementación en algunos casos.

- **Pago por usuario** (8 empresas)**:** La mayoría de las ventas de los productos de software que realizan las empresas chiclayanas evaluadas, aplican esta estrategia. El valor del producto software está en función del número de usuarios o licencias que distribuyen. En varios casos, la facturación se la realiza de manera periódica (mensual usualmente) de acuerdo al número de usuarios registrados.

- **Pago por funcionalidad** (6 empresas)**:** En este modelo de venta de los productos de software, se ofrece primero un servicio con un precio relativamente bajo, para utilizar un software con características o funcionalidades limitadas. Para acceder al resto de funcionalidades el cliente debe pagar un costo por ellas.

4.1.3.8. Recursos para el desarrollo de software

Para las empresas analizadas consideran que sus recursos clave para el desarrollo de sus productos software son: los recursos físicos y los recursos humanos.

La mayoría de empresas (7 empresas) consideran que los recursos de infraestructura física son clave en la estructura del modelo de negocio.

En el caso del equipo humano que debe conformar la empresa, varía de acuerdo a la estrategia de negocio que se adopte. Los roles principales que se han identificado en los proyectos de software son: gerente o responsable de proyecto, analista de procesos y base de datos, desarrollador de interfaces, ingeniero de aseguramiento de calidad, arquitecto de software, equipo de soporte y de mejora continua (post venta) y personal para marketing y ventas.

4.1.3.9. Socios clave

La motivación que debe existir al momento de identificar posibles socios clave para la empresa, debe responder a un análisis de aspectos como: reducción de riesgos, reducción de gastos, optimización y aumento de ventas.
Las actividades clave de las empresas consideradas en el estudio son:

4.1.4. Análisis FODA del sector de la industria del software en la ciudad de Chiclayo

Tomando como base la información recogida en las entrevistas, se realizó un diagnóstico situacional del sector de la industria del software en la ciudad de Chiclayo.

Para ello, se utilizó un modelo descriptivo diagnóstico, como es la técnica FODA, cuyos resultados se muestran a continuación:

Tabla N° 13. FODA del sector de la industria del software en la ciudad de Chiclayo

		Análisis Interno (Empresa)	
		FORTALEZAS: - Experiencia de desarrollo de aplicaciones (programación). - Conocimiento de metodologías de desarrollo de software tradicional - Infraestructura en hardware y software aceptable	**DEBILIDADES:** - Poca experiencia en gestión de proyectos de desarrollo de software. - Incumplimiento de tiempo de desarrollo de proyectos. - Carencia de metodología en la integración de proyectos. - Productos muchas veces incompletos y de calidad no aceptable.
Análisis del Entorno	**OPORTUNIDADES:** - Expansión a otras ciudades o países. - Gran cantidad de proyectos de software requerimientos por instituciones del Estado - Cartera de clientes fidelizados. - Requerimientos de productos de software de diferentes tipos o sectores - Nuevos tipos de productos o servicios, como SaaS	**FO (MAXI-MAXI)** - Ofrecer diversos productos de software con alta calidad que sean únicos en los mercados nacionales y extranjeros. - Realizar marketing focalizando a segmentos de mercados interesantes y poco abordados, resaltando el liderazgo o especialización de la empresa en ese sector del desarrollo de software.	**DO (MINI –MAXI)** - Aplicar y/o certificar estándares en buenas prácticas de gestión y desarrollo de proyectos de software, para posicionarse como una empresa líder. - Implementar estrategias post venta, para hacer seguimiento a los productos distribuidos a los clientes, dando garantía, calidad, mejora continua y reduciendo los defectos.
	AMENAZAS: - Creciente aumento de empresas competidoras. - Alta importación de software.	**FA (MAXI-MINI)** - Aprovechar tecnologías freesoft para abaratar costos y ofrecer productos a precios más bajos que la competencia. - Desarrollar productos con mayor eficiencia y menor costo, que los que se importan.	**DA (MINI MINI)** - Adoptar una metodología de trabajo eficiente que permita el fortalecimiento del trabajo organizacional para hacer frente a las empresas competidoras. - Capacitar al personal para desarrollar sus capacidades y productividad.

A partir de la matriz FODA, se definió las siguientes estrategias, utilizando la perspectiva del Balanced ScoreCard, de Kaplan y Norton.

Tabla N° 14. Estrategias FODA

FINANCIERA (F)	**Objetivo estratégico** Obtener mayor rentabilidad para la empresa reduciendo costos operativos a través de la estandarización de los procesos. **Estrategias** - Impulsar el crecimiento sostenible de la empresa a través del ofrecimiento de productos y servicios de tendencia actual. - Buscar nuevas fuentes de ingresos que agreguen valor a la empresa, a través de servicios postventa o estrategias de tecnología freesoft.
CLIENTES (C)	**Objetivo estratégico** Satisfacción del cliente aumentando la calidad de los productos y servicios. **Estrategias** - Prestar un servicio mejorado al cliente que permita su fidelización a través del seguimiento postventa. - Establecer una cultura de retención de clientes (lealtad).
PROCESOS INTERNOS (PI)	**Objetivo estratégico** Reducción de defectos detectados en producción. **Estrategias** - Incrementar la calidad y estabilidad de los productos. - Estandarizar los procesos de gestión, producción y documentación.
APRENDIZAJE Y CRECIMIENTO (AC)	**Objetivo estratégico** Desarrollar un proceso continuo, integrado y dirigido, buscando mejorar los conocimientos y habilidades de los empleados **Estrategias** - Generar un clima ocupacional que propicie un ambiente laboral satisfactorio. - Mejorar la infraestructura tecnológica buscando el uso de la nube como medio de prestación de los servicios

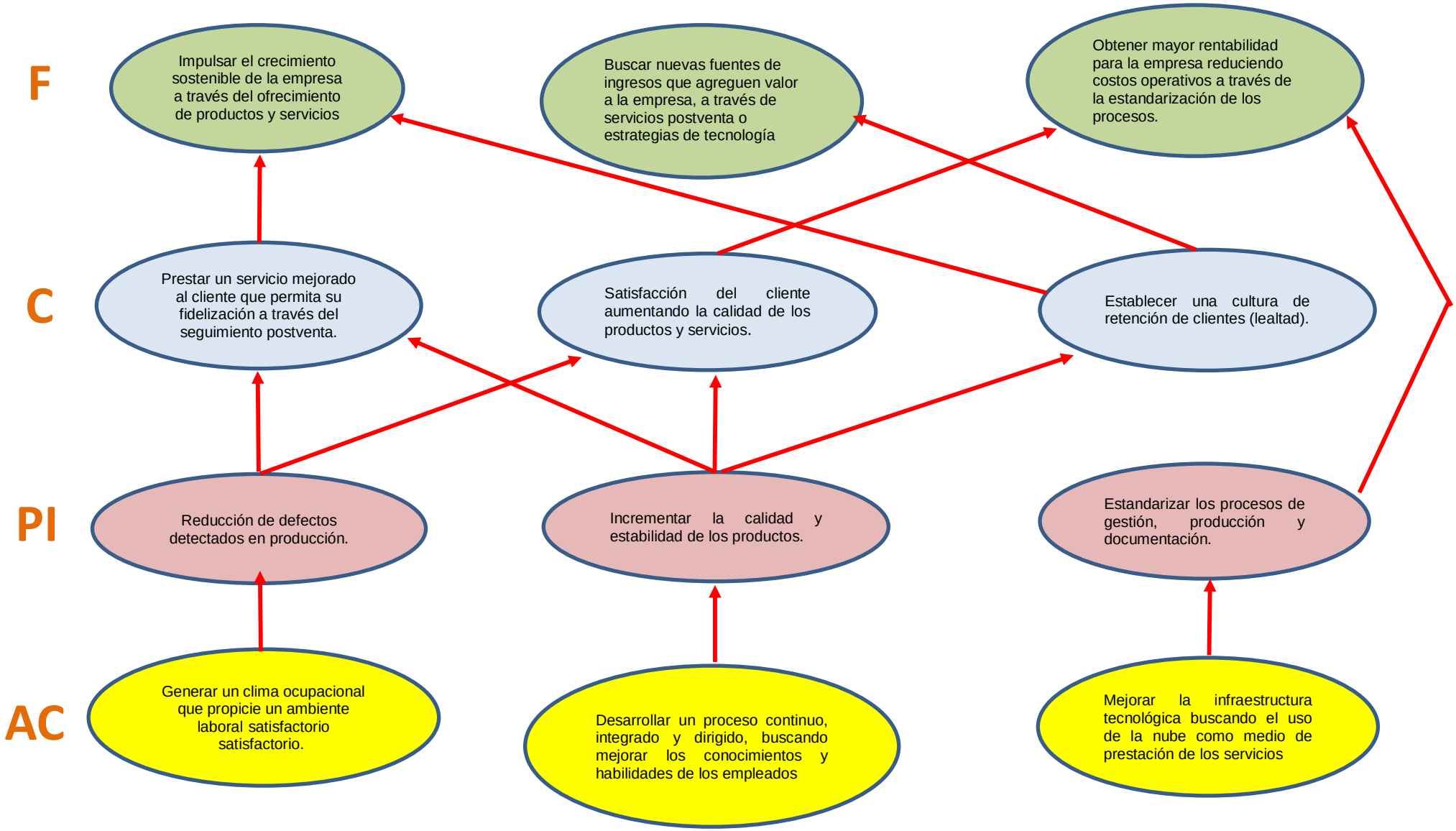


Gráfico N° 5. Mapa estratégico del sector de la industria del software en la ciudad de Chiclayo

4.2. Construcción de la matriz de riesgo integral empresarial

Como parte del diagnóstico del sector empresas dedicadas a la fábrica de software en la ciudad de Chiclayo, se realizó el análisis del riesgo integral empresarial, cuyo propósito fue identificar el entorno de escenarios de riesgo del negocio que pudiesen afectar el no logro de las metas en cada una de las perspectivas del modelo estratégico.

Para ello, se aplicó un método descriptivo analítico, tomando como referencia algunos de los indicadores que se establece en la teoría del Balanced ScoreCard.

4.2.1. Determinación de las metas promedio de un negocio de desarrollo de software

Para la determinación de las metas promedio de un negocio en el sector de la industria del software en la ciudad de Chiclayo, se fijaron, primero las metas de negocio para luego evaluar los escenarios de riesgo que pudiesen influir en que no se alcancen éstas, en cada perspectiva del modelo estratégico (ver tabla Estrategias FODA).

En las siguientes tablas se muestran las metas fijadas para cada indicador considerado en cada una de las perspectivas del modelo estratégico del sector.

Tabla N° 15. Identificación del riesgo en la perspectiva Financiera

Objetivo Estratégico	Indicadores	Valor Actual	Metas		Valorización (Semaforización) Año 2020
			2021	2022	
Obtener mayor rentabilidad para la empresa, reduciendo costos operativos a través de la estandarización de los procesos	**Rentabilidad** Utilidades / total de activos	2.8	4.0	5.5	Rojo: I <= 2.5 Amarillo: 2.5 < I <= 4.0 Verde: I > 4.0
	CLV (Cálculo del valor del cliente) Valor del pedido promedio x Número de ventas x Duración promedio de la relación	27000	30000	50000	Rojo: I <= 22500 Amarillo: 22500 < I <= 35000 Verde: I > 35000

En la tabla se establece que:

a. La *Rentabilidad promedio* de las empresas seleccionadas es del 2.8 actualmente, considerándose un escenario “Regular”.
b. En relación al *Cálculo del valor del cliente el promedio* base es de S/.27000, obtenido de la siguiente manera: S/. 3000 (precio promedio de un producto) x 3 (número de ventas a un cliente promedio) x 3 (años promedio de la relación con el cliente).

Tabla N° 16. Identificación del riesgo en la perspectiva Cliente

Objetivo Estratégico	Indicadores	Valor Actual	Metas		Valorización (Semaforización) Año 2020
			2021	2022	
Satisfacción del cliente aumentando la calidad de los productos y servicios.	NPS (Net Promoter Score) mide la lealtad de los clientes basándose en las recomendaciones	15%	30%	50%	Rojo: I <= 10% Amarillo: 10% < I < =45% Verde: I > 45%
	Porcentaje de incidencias resueltas en los tiempos establecidos	58%	65%	75%	Rojo: I <= 45% Amarillo: 45% < I <= 70% Verde: I > 70%

En la tabla se establece que:

a. Para el valor base del indicador *NPS* se fijó en 15%, considerando que la mayoría de las empresas del medio tiene niveles aceptables de conformidad, pero todavía existen reclamaciones de parte de los clientes.
b. El valor base para el indicador de *Porcentaje de incidencias resueltas en los tiempos establecidos* se ha considerado en 58% del total de incidencias reportadas.

Para calcular el índice NPS, se aplicó una encuesta a 14 clientes de diferentes empresas, quienes respondieron a la siguiente pregunta:
¿Qué posibilidades hay de que recomiende [X empresa] a un amigo o colega?

Las opciones de respuesta fueron una escala del 0 al 10, en la que el 0 es "**nada probable**" y el 10 es "**extremadamente probable**", mientras que el 5 es neutral.

En base a las respuestas dadas por los clientes, éstos fueron categorizados en tres tipos**.** Cada categoría guarda una relación directa entre las respuestas.

- Los clientes que respondieron con un 9 o un 10, mostraron un comportamiento de compra y de recomendación bastante alto. A estos clientes se les llamaron **Promotores**.
- Los que respondieron con un 7 o un 8, mostraron un comportamiento mucho más pasivo, por lo que a estos se les llamaron **Pasivos**.
- Los que dieron puntajes desde el 0 hasta el 6, no mostraron ningún comportamiento positivo para la empresa. Incluso, en muchos casos, sus opiniones hacia otras personas sobre la empresa fueron negativas. A estos se les llamaron **Detractores**.

De esta manera, se estableció la forma de categorizar a los clientes que responden a la encuesta del NPS:

- **Promotores:** quienes responden con 9 o 10. Son clientes muy satisfechos y, por tanto, leales a la marca. Así que están dispuestos a comprar más y a recomendarla.
- **Pasivos:** quienes responden con 7 u 8. Son clientes satisfechos, pero no leales, por lo que son susceptibles de irse con la competencia.
- **Detractores:** quienes responden desde el 0 hasta el 6. Son clientes insatisfechos que pueden ser partícipes de un boca a boca negativo.

Tras reunir las respuestas, el índice NPS se obtiene finalmente al seguir los dos siguientes pasos:

1. Convertir la cantidad de promotores y de detractores en porcentajes, sin tomar en cuenta a los pasivos.
2. Restar al porcentaje de promotores el de los detractores. El resultado es lo que se considera como el porcentaje NPS o el famoso índice NPS.

Tabla N° 17. Escala para la evaluación del indicador NPS

0	1	2	3	4	5	6	7	8	9	10
Detractores							Pasivos		Promotores	
NPS = % Promotores - % Detractores										

Entre los rangos de los posibles resultados NPS, tenemos que:

- Un NPS de 100 indica que todos los clientes son promotores.
- Un resultado de -100, que todos son detractores.
- Uno de 50 es un excelente resultado.
- Uno superior a 0 es un buen resultado.

Tabla N° 18. Identificación del riesgo en la perspectiva Procesos Internos

Objetivo Estratégico	Indicadores	Valor Actual	Metas		Valorización (Semaforización) Año 2020
			2021	2022	
Reducción de defectos detectados en producción.	**Eficiencia función del Help desk** % de eventos atendidos/ % eventos planificados	70%	80%	90%	Rojo: I <= 50% Amarillo: 50% < I <= 75% Verde: I > 75%
	Entrega a tiempo de servicio	60%	75%	90%	Rojo: I <= 60% Amarillo: 60 < I <= 75% Verde: I > 75%

En la tabla se establece que:

a. En relación al indicador de Eficiencia de la función help desk, las entrevistas arrojaron que el valor base para establecer las metas es 70%.
b. En relación al indicador Entrega a tiempo del servicio, referente al cumplimiento de los plazos para entregar el servicio o producto completo, el diagnóstico indica que el valor base es del 60% del total de contratos revisados.

Tabla N° 19. Identificación del riesgo en la perspectiva Desarrollo y Aprendizaje

Objetivo Estratégico	Indicadores	Valor Actual	Metas		Valorización (Semaforización) Año 2020
			2021	2022	
Desarrollar un proceso continuo, integrado y dirigido, buscando mejorar los conocimientos y habilidades de los empleados.	Índice de clima laboral	0.6	0.65	0.70	Rojo: I <= 0.3 Amarillo: 0.30 < I <= 0.6 Verde: I > 0.6
	Porcentaje de personal competente	70%	80%	90%	Rojo: I <= 60% Amarillo: 60 < I <= 70% Verde: I > 70%

En la tabla se establece que:

a. El indicador Índice de clima laboral es tomado en base a el nivel de satisfacción de los trabajadores en su entorno de trabajo, considerándose como base el valor del 0.6 en una escala de 0.0 a 1.0.
b. Del diagnóstico se concluye que el Porcentaje de personal competente, es decir, el porcentaje de personal de desarrollo de software en el nivel senior, es del 70% de toda la planilla de trabajadores en el rubro. No se considera el personal de ventas o marketing.

4.2.2. Análisis de los procesos de negocio típicos de las empresas de desarrollo de software

Se elaboró el mapa de procesos típico, con la finalidad de identificar los de procesos en el rubro, clasificándolos en: operativos, estratégicos, de control y de apoyo. El alcance de la propuesta de construcción del modelo de gestión de riesgos cubrirá solo los procesos operativos o misionales del negocio.

En el gráfico siguiente se visualiza el mapa de procesos de negocio típico de empresas de desarrollo de software.

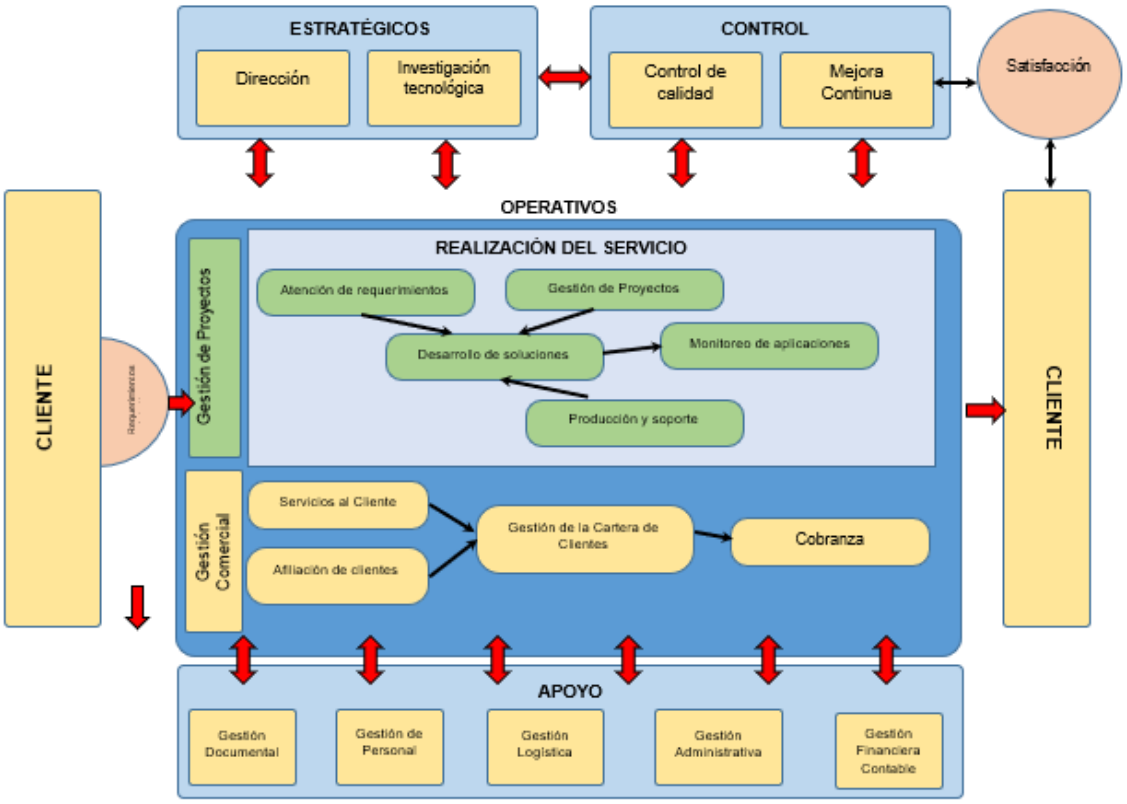


Gráfico N° 6. Mapeado de procesos de la empresa del sector de la industria del software en la ciudad de Chiclayo

Los procesos de TI considerados en el alcance del SGSI son los procesos misionales de Gestión de proyectos y soluciones:

Área de desarrollo:

- Atención de requerimientos
- Gestión de proyectos y soluciones
- Desarrollo de soluciones

Área de producción

- Producción y soporte de TI
- Monitoreo de aplicaciones

A partir de esta delimitación, se elaboraron los subprocesos de las áreas de desarrollo y de producción, las que se muestran a continuación:

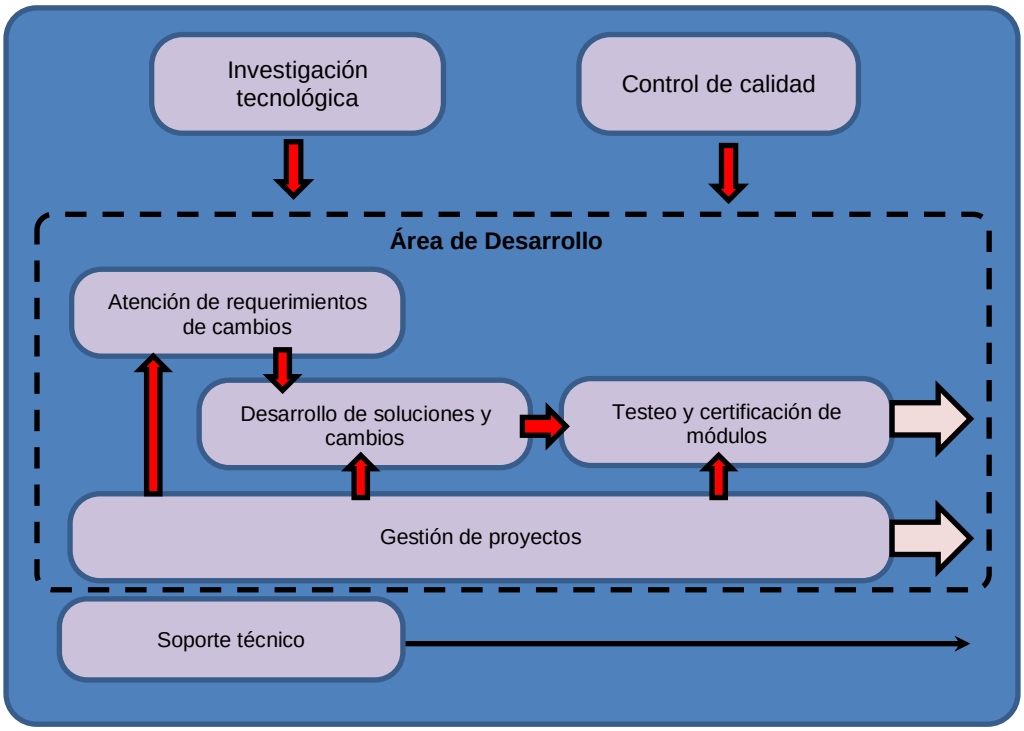


Gráfico N° 7. Mapeado de los procesos del Área de Desarrollo
Fuente: Desarrollo propio

Tabla N° 20. Descripción de los procesos/subprocesos del Área de Desarrollo

	Procesos	Subprocesos	
		Desarrollo	Documento de soporte
AREA OPERATIVA DE DESARROLLO	Investigación tecnológica		Plan de TI
	Atención de requerimientos de cambios	Registro de requerimientos	Ficha de requerimientos
		Autorización de cambio	Ficha de requerimientos
	Desarrollo de soluciones y cambios	Distribución y asignación del trabajo	Plan de trabajo
		Codificación	Librerías de código, estructura de datos, BD
		Gestión de cambios	Ficha de registro de cambios: scripts, datos y carga de datos
		Gestión de versiones	Librería de versiones
		Actualización de manuales y documentación técnica	Manuales
	Testeo y certificación de módulos	Validación funcional Pruebas de integridad	Plan de pruebas Informe de pruebas
	Gestión de proyectos	Gestión de actividades y tiempos Gestión de riesgos	Procedimientos establecidos Documentación de seguimiento
	Soporte técnico	Mantenimiento correctivo Mantenimiento preventivo planificado	Plan de mantenimiento

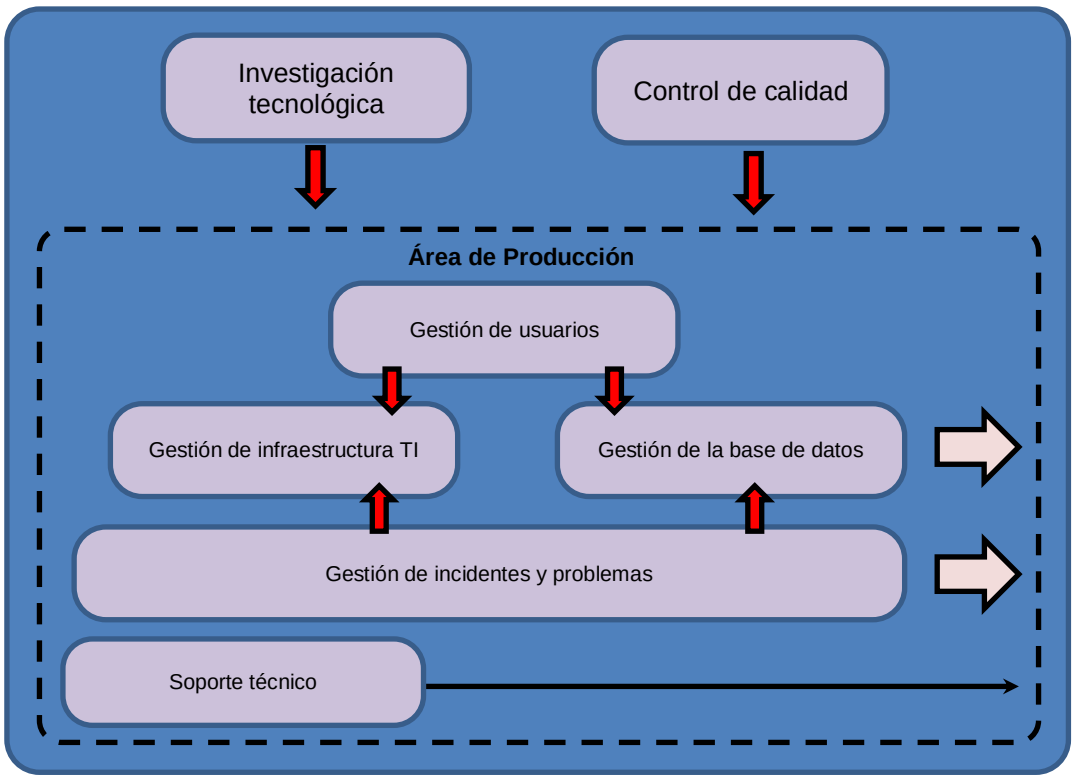


Gráfico N° 8. Mapeado de los procesos de Producción y Soporte
Fuente: Desarrollo propio

Tabla N° 21. Descripción de los procesos/subprocesos del Área de Producción y soporte

	Procesos	Subprocesos	
		Desarrollo	Documento de soporte
AREA OPERATIVA DE PRODUCCIÓN Y SOPORTE DE TI	Investigación tecnológica		Plan de TI
	Gestión de usuarios	Gestión de perfiles de usuario	Procedimiento y reglamento
		Altas, bajas y modificación de cuentas de usuario	Procedimiento y reglamento
	Gestión de infraestructura	Gestión de configuraciones	Procedimiento (no formalizado)
		Gestión antimalware	Procedimiento (no formalizado)
		Gestión de la red	Procedimiento (no formalizado)
		Gestión de página Web	Procedimiento (no formalizado)
		Gestión de telefonía IP	Procedimiento (no formalizado)
	Gestión de base de datos	Gestión de dominios	Procedimiento (no formalizado)
		Gestión de respaldos	Procedimiento y reglamento
	Gestión de incidentes y problemas	Gestión de incidentes Gestión de problemas	Procedimiento (no formalizado)
	Soporte técnico	Mantenimiento correctivo Mantenimiento preventivo planificado	Plan de mantenimiento

a. Catálogo de activos

El catálogo inventariado de los activos de TI se obtuvo del análisis de los procesos en la tarea anterior.

En base a la estructura de catalogación definida en la tabla N° 5, se realizó la catalogación y el inventario de los activos de TI. El inventario se realizó independientemente para cada una de las áreas consideradas en el alcance del SGR y el tipo de activo.

Tabla N° 22. Inventario típico de activos de Información del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Procedimientos y reglamentos de desarrollo	ID		X		X				Carpeta de Documentos de gestión	Personal TI Personal empresa	Jefe TI	Jefe TI		X		X	X	X	X	X
2	Planes de desarrollo (Actividades, tareas, asignación de trabajo)	ID		X			X			Carpeta de proyectos	Personal TI	Jefe TI	Jefe TI		X		X				
3	Cotizaciones y cuadros de evaluación	ID		X					X	Carpeta de Documentos de gestión	Jefe TI	Jefe TI	Jefe TI			X	X	X			X
4	Hojas de requerimientos y cambios aprobadas	ID			X				X	Carpeta de Documentos de gestión	Jefe TI Jefe Desarrollo	Jefe Desarrollo	Jefe Desarrollo	X			X	X			
5	Documentos técnicos de desarrollo (análisis, diseño)	ID		X					X	Carpeta de Documentos de gestión	Jefe Desarrollo Analistas programadores	Jefe Desarrollo	Analistas programadores		X			X	X	X	
6	Registros de Control de Cambios (scripts, BD, carga data)	ID	X				X			Carpeta Control de Cambios	Jefe Desarrollo Analistas programadores Oficial de seguridad	Jefe Desarrollo	Oficial de seguridad	X			X		X		
7	Manuales de usuario	ID			X	X				Carpeta Control de Cambios	Personal empresa	Jefe Desarrollo	Analistas programadores		X			X	X		

8	Informes de las pruebas de testeo y certificación	ID		X					X	Carpeta de Documentos de gestión	Jefe Desarrollo Analistas programadores Jefe de Producción y Soporte	Jefe Desarrollo	Analistas programadores		X			X	X	X	
9	Documentos de versiones de software	ID	X						X	Carpeta Control de Cambios	Jefe TI Jefe Desarrollo	Jefe TI	Jefe Desarrollo	X			X		X		
10	Documentación del personal (HV)	ID			X				X	Carpeta de Documentos de gestión	Administración Jefe de RRHH Jefe TI	Jefe RRHH	Jefe RRHH			X	X				

Fuente: Desarrollo propio

Tabla N° 23. Inventario típico de activos de Software del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Herramientas y entornos de desarrollo	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X					X	X	X
2	Software de ofimática	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X	X	X			
3	Aplicativos para el modelamiento	SWD		X					X	PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte		X		X	X	X		
4	Motores de base de datos	SWD		X		X				Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X					X	X	
5	Herramientas de gestión de proyectos	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte		X		X				
6	Software de virtualización	SWD		X		X				Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
7	Aplicativos	SWD		X		X				PCs/Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte		X		X	X			X

Fuente: Desarrollo propio

Tabla N° 24. Inventario típico de activos de Hardware del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	PC	HWD		X		X				Área de desarrollo	Personal TI	Producción y Soporte	Producción y Soporte		X		X	X	X	X	X
2	Servidor Aplicaciones	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte	X					X	X	
3	Servidor BD	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte	X					X	X	
4	Servidor Respaldo	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte	X					X		
5	Impresora	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte			X	X	X	X	X	X

Tabla N° 25. Inventario típico de servicios del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Internet	SD		X		X				Sala de servidores	Personal	Producción y Soporte	Producción y Soporte			X	X				

Tabla N° 26. Inventario típico de personal del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Jefe de Desarrollo	CD												X				X	X	X	
2	Responsables de proyectos	CD												X				X	X	X	
3	Analistas programadores Senior	CD												X				X	X	X	X
4	Analistas programadores Junior	CD													X			X	X	X	X
5	Practicante de Desarrollo	CD														X					

Fuente: Desarrollo propio

Tabla N° 27. Inventario típico de activos de Información del Área de Producción y Soporte

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Procedimientos y reglamentos de Producción y Soporte	IPS		X		X				Carpeta de Documentos de gestión	Personal TI Personal empresa	Jefe TI	Jefe TI		X		X	X	X	X	X
2	Planes de desarrollo (Actividades, tareas, asignación de trabajo)	IPS		X		X				Carpeta de proyectos	Personal TI	Jefe TI	Jefe TI		X		X				X
3	Plan de Mantenimiento preventivo	IPS		X			X			Carpeta de proyectos	Personal TI Responsable de Soporte	Jefe TI	Jefe TI		X		X				X
4	Registro de incidentes y problemas	IPS	X			X				Carpeta de Documentos de gestión	Servis Desk	Servis Desk	Oficial de seguridad			X	X			X	
5	Hojas de requerimientos y cambios aprobadas	IPS	X						X	Carpeta de Documentos de gestión	Gestor BD Gestor Networking	Gestor Networking	Gestor Networking	X			X		X		
6	Registro de usuarios	IPS	X						X	Carpeta de Documentos de gestión	Gestor BD Gestor	Gestor BD	Gestor BD		X			X			
7	Perfiles de usuario	IPS		X					X	Carpeta Control de Cambios	Gestor BD Gestor	Gestor BD	Jefe TI	X			X	X	X		
8	Estructura de base de datos	IPS	X						X	Carpeta Control de Cambios	Gestor BD	Gestor BD	Jefe TI		X				X		

9	Bitácora de accesos	IPS	X			X				Carpeta de Documentos de gestión	Gestor BD	Gestor BD	Oficial de seguridad		X				X		
10	Informes de las pruebas de testeo y certificación	IPS		X					X	Carpeta de Documentos de gestión	Gestor BD Gestor Networking	Jefe Producción	Gestor Networking		X		X		X		
11	Configuración de equipos	IPS	X					X		Carpeta Control de Cambios	Gestor Networking	Jefe Producción	Gestor Networking	X			X				
12	Inventario de HW y SW	IPS	X					X		Carpeta Control de Cambios	Responsable de Soporte	Jefe Producción	Jefe TI	X			X				X
13	Información de respaldos y copias de seguridad	IPS	X				X			Carpeta de Documentos de gestión	Gestor BD	Jefe Producción	Jefe TI			X	X		X		
14	Documentación del personal (HV)	IPS			X				X	Carpeta de Documentos de gestión	Administración Jefe de RRHH Jefe TI	Jefe RRHH	Jefe RRHH			X	X				

Fuente: Desarrollo propio

Tabla N° 28. Inventario típico de activos de Software de Producción y Soporte

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Herramientas de gestión de usuarios	SWP	X	X		X				PC/Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X			X	X	X	X	X
2	Software de ofimática	SWP		X		X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte			X				X	
3	Software antimalware	SWP		X		X				Servidor	Gestor Networking Gestor BD	Producción y Soporte	Producción y Soporte	X				X	X	X	
4	Motores de base de datos	SWP		X		X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X			X				
5	Herramientas de gestión de proyectos	SWP		X		X				PCs	Personal del área	Producción y Soporte	Producción y Soporte			X	X				
6	Software de virtualización	SWP		X		X				Servidor	Gestor Networking	Producción y Soporte	Producción y Soporte		X		X				
7	Aplicativos Tools	SWP		X		X				PCs	Personal del área	Producción y Soporte	Producción y Soporte			X	X	X	X	X	X
9	Aplicativo – Bitácora	SWP	X				X			PCs	Gestor BD	Producción y Soporte	Producción y Soporte		X			X	X	X	
10	Aplicativo – Control de cambios	SWP	X			X				PCs	Gestor Networking Gestor BD	Producción y Soporte	Producción y Soporte	X			X		X		X
11	Sistema operativo	SWP		X		X				Servidor	Gestor Networking	Producción y Soporte	Producción y Soporte	X			X				

Fuente: Desarrollo propio

Tabla N° 29. Inventario típico de activos de Hardware de Producción y Soporte

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	PCs	HWP		X		X				Área de Producción	Personal Producción y Soporte	Jefe de Producción	Jefe de Producción		X		X	X	X	X	X
2	Servidor Aplicaciones	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X		X		
3	Servidor BD	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X	X	X		
4	Servidor de Dominio	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
5	Servidor Web	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
6	Servidor Antimalware	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
7	Switch Core	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
8	Switch troncales	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
9	Switch de borde	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking		X		X				
10	Router	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking				X				
11	Servidor Pruebas	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking		X		X		X		
12	Impresora	HWP		X		X				Área de Producción	Personal Producción y Soporte	Jefe de Producción	Jefe de Producción			X	X	X	X	X	X

Tabla N° 30. Inventario típico de activos de Servicios de Producción y Soporte

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Internet	SP		X		X				Sala de servidores	Personal	Gestor Networking	Jefe de Producción y Soporte			X	X		X		
2	VPN	SP		X		X				Sala de servidores	Personal	Gestor Networking	Jefe de Producción y Soporte			X	X		X		

Fuente: Desarrollo propio

Tabla N° 31. Inventario típico de Personal del Área de Producción y Soporte

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Jefe de Producción y Soporte	CP												X			X	X	X	X	
2	Gestor Networking	CP												X			X			X	
3	Gestor de BD	CP												X				X	X		
4	Técnico de soporte técnico	CP												X						X	X
5	Practicante de Desarrollo	CP														X					

4.2.3. Componentes del modelo de gestión de riesgos

Para la construcción del modelo de gestión de riesgos en proyectos de software se tomó como base el diseño teórico (capítulo II) de la presente investigación.

Dado que, la necesidad primordial de este tipo de empresas, es mejorar los aspectos de seguridad de la información en sus procesos principales de negocio y sentar las bases para una futura acreditación en esta materia, el diseño teórico, permitió identificar los requisitos más relevantes de la gestión de riesgos, como parte conformante de la seguridad, a partir de los cuales se pudo construir el modelo de gestión de riesgos propuesto.

De la revisión de los marcos de referencia descritos en el diseño teórico, se identificó los componentes mínimos y más relevantes que deberían ser considerados en el modelo propuesto, los mismos que se describen en la siguiente tabla:

Tabla N° 32. Componentes del modelo de gestión de riesgos propuesto

Componente del modelo	Descripción	Normativa o marco de referencia
Evaluación de riesgos	Involucra: – Identificación de los escenarios de riesgo. – Valoración de los escenarios de riesgo. – Cálculo del nivel de riesgo intrínseco.	Norma ISO/IEC 27005:2018. Técnicas de seguridad. Técnicas de seguridad - Gestión de riesgos de seguridad de la información. En los siguientes ítems: – Ítem 8.2.1. Identificación del riesgo – Ítem 8.3.4. Determinación del nivel de riesgo – Ítem 8.4. Evaluación del riesgo – Anexo B: Valoración de activos y evaluación de impacto – Anexo C: Ejemplos de amenazas típicas – Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad Metodología Magerit – Modelo de análisis de riesgos (capítulo 3) – Catálogo de elementos: tipos de activos, dimensiones de valoración de activos, criterios de valoración de activos, amenazas típicas (libro 2)
Tratamiento del riesgo		Norma ISO/IEC 27005:2018. Técnicas de seguridad. Técnicas de seguridad - Gestión de riesgos de seguridad de la información. En los siguientes ítems: – Ítem 9. Tratamiento del riesgo Metodología Magerit – Ítem 4.2.5. Decisión de tratamiento (libro 1)
Plan de tratamiento del riesgo		Norma ISO/IEC 27001:2014. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. En los siguientes ítems: – Ítem 6.1.3. d. declaratoria de aplicabilidad – Anexo A. Objetivos de control y controles

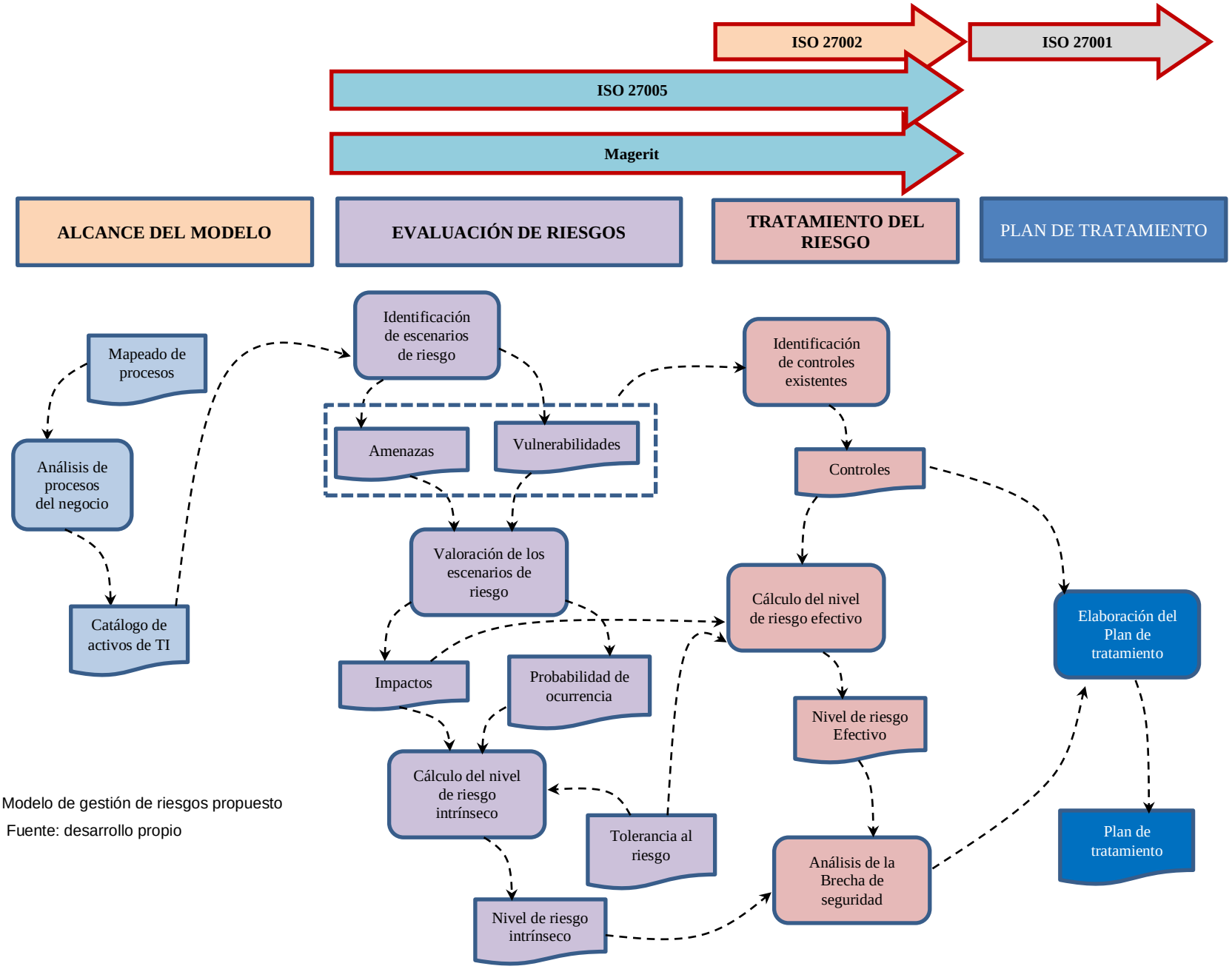


Gráfico N° 9. Modelo de gestión de riesgos propuesto

Fuente: desarrollo propio

4.2.4. Descripción del componente: Evaluación de riesgos

Los elementos considerados para este componente son:

a. Activos. Los activos considerados para el análisis y evaluación de riesgos fueron categorizados de acuerdo a la tabla N° 5.
b. Estimación de la criticidad de los activos de TI. Para esta tarea, se evaluaron las características de aseguramiento de la información (Confidencialidad, Integridad y Disponibilidad) utilizando como referencia la Tabla N° 6. Para esta estimación se aplicó la formula N° 1.
c. Identificación de vulnerabilidades y amenazas. Esta tarea se realizó conjuntamente con el personal de cada una de las áreas de los dos procesos seleccionados en el alcance del SGSI, en un trabajo colaborativo. Se tomó como referencia la clasificación de las amenazas y vulnerabilidades descrita en el ítem 3.6.3.
d. Estimación del impacto. Se utilizó la escala y criterios de la Tabla N° 7. Esta actividad se realizó en trabajo colaborativo con el personal de cada una de las áreas consideradas en el alcance de la investigación.
e. Estimación de la frecuencia de las amenazas. Se utilizó los niveles de probabilidad de ocurrencia definidos en la Tabla N° 8. Esta actividad se realizó en trabajo colaborativo con el personal de cada una de las áreas incluidas en el alcance de la investigación.
f. Estimación del nivel de exposición al riesgo. Para esta estimación se aplicó la formula N° 3.
g. Determinación del nivel de tolerancia al riesgo. Se aplicó los niveles de riesgo definidos en la Tabla N° 9.

El procedimiento metodológico para cumplir con los objetivos de este componente está descrito en el capítulo 3. A continuación se describe la aplicación de este procedimiento metodológico:

Tabla N° 33. Análisis y evaluación de riesgos del Área de Desarrollo – Activos de Información

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de desarrollo	1	2	3	6	No se realizan actualizaciones o revisiones de los procedimientos y reglamentos de manera planificada	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación física y digital relacionada a los procedimientos y normativas de desarrollo, están bajo la custodia del Jefe de Desarrollo. Las normativas y directivas de procedimientos se asignan al personal en base a la función que cumplen. Toda la documentación de procedimientos y normativas tienen copias, resguardadas por el administrador.	5	4	26	NT
							Modificación parcial o total de la información de manera intencional o por error		2	4	14	TT
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	4	10	TT
							Pérdida o sustracción de información		3	4	18	RT
2	Planeamiento del desarrollo de software: actividades, recursos, asignación de trabajo	1	1	3	5	No existe documentación sobre metodologías o procesos o estandarización del desarrollo del software. No se lleva el control de versiones. No se lleva el control de cambios.	Sustracción no autorizada y divulgación de documentación sensible por el personal	Se realizan solo reuniones de coordinación para el desarrollo de los proyectos de software. Se firman actas. El custodio de las versiones es el jefe de desarrollo.	2	3	11	TT
							Modificación parcial o total de la información de manera intencional o por error		3	3	14	TT
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	3	8	TT
							Pérdida o sustracción de información		3	3	14	TT

3	Cotizaciones y cuadros de evaluación	1	1	2	4	No se ha estandarizado el proceso de cotización de los proyectos de software. Las cotizaciones realizadas forman parte de la documentación del proyecto.	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	2	3	10	**TT**
							Modificación parcial o total de la información de manera intencional o por error		3	2	10	**TT**
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	2	6	**TT**
							Pérdida o sustracción de información		2	2	8	**TT**
4	Hojas de requerimientos y cambios aprobadas	2	2	1	5	No existen controles de cambios en los proyectos, por lo que cada desarrollador cumple con la función asignada sin registrar los cambios realizados.	Procesamiento erróneo por parte del personal de Desarrollo	Se tiene un formato establecido para el registro de las peticiones de cambio, las cuales se anexan en el expediente de los proyectos Las peticiones de cambio son aprobadas por el Líder de cada proyecto La documentación de los proyectos de software son gestionadas por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	4	4	21	**RT**
							Información no disponible, en desuso u obsoleta		3	3	14	**TT**
							Modificación parcial o completa de la información, de manera intencional o por error		4	4	21	**RT**
5	Documentos técnicos de desarrollo (análisis, diseño)	2	2	3	7	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No se ha estandarizado el	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	4	5	27	**NT**
							Procesamiento erróneo por parte del personal de Desarrollo		4	5	27	**NT**
							Accesos a los activos de información de manera no autorizada		2	4	15	**TT**
							Sustracción no autorizada de documentación sensible		3	4	19	**RT**

						procedimiento de pruebas No existe un procedimiento estandarizado de control de cambios o versiones	Errores en la ejecución de las pruebas unitarias		4	5	27	NT
							Información no disponible, en desuso u obsoleta		3	3	16	RT
							Modificación parcial o completa de la información, de manera intencional o por error		3	4	19	RT
6	Registros de Control de Cambios (scripts, BD, carga data)	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No se ha estandarizado el procedimiento de pruebas No existe un procedimiento estandarizado de control de cambios o versiones	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionadas por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	3	4	21	RT
							Procesamiento erróneo por parte del usuario		4	5	29	NT
							Información no disponible, en desuso u obsoleta		2	3	15	TT
							Accesos a los activos de información de manera no autorizada		2	3	15	TT
							Sustracción no autorizada de documentación sensible		2	4	17	RT
							Modificación parcial o completa de la información, de manera intencional o por error		3	3	18	RT
7	Manuales de usuario	1	1	2	4	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionadas por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos. Se generan manuales de usuario cuando se realizan cambios sustantivos en las aplicaciones y sistemas	5	3	19	RT
							Información no disponible, en desuso u obsoleta		4	3	16	RT
							Accesos a los activos de información de manera no autorizada		3	2	10	TT
							Sustracción no autorizada de documentación sensible		5	3	19	RT

						de software No existe un procedimiento estandarizado de control de cambios o versiones	Modificación parcial o completa de la información, de manera intencional o por error		2	3	10	TT
8	Informes de las pruebas de testeo y certificación	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No se ha estandarizado el procedimiento de pruebas El ambiente para realizar las pruebas no es independiente de la red	Sustracción no autorizada y divulgación de documentación sensible por el personal	Las pruebas y testeos antes de puesta en producción lo realizan el área de producción con la participación del Jefe de Desarrollo. Los resultados de las pruebas y testeos se documentan y anexan en el expediente de cada proyecto No existen procedimientos de seguridad para protegerlos	3	4	21	RT
							Procesamiento erróneo por parte del usuario		4	5	29	NT
							Información no disponible, en desuso u obsoleta		2	4	17	RT
							Accesos a los activos de información de manera no autorizada		2	3	15	TT
							Sustracción no autorizada de documentación sensible		3	4	21	RT
							Modificación parcial o completa de la información, de manera intencional o por error		3	3	18	RT
9	Documentos de versiones de software	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software	Sustracción no autorizada y divulgación de documentación sensible por el personal	Cuando se cierra un proyecto, toda la documentación se almacena en un armario sin protección bajo la custodia del jefe de Desarrollo	3	4	21	RT
							Información no disponible, en desuso u obsoleta		4	3	21	RT
							Accesos a los activos de información de manera no autorizada		2	3	15	TT
							Sustracción no autorizada de documentación sensible		3	4	21	RT
10	Documentación del personal (HV)	1	2	2	5	La actualización y gestión documentación referida al legajo personal de los empleados no está reglamentada. Por tanto, son fácilmente accesibles, muchas veces están desactualizados	Información no disponible, en desuso u obsoleta	La documentación del legajo de los trabajadores y sus contratos las gestiona el administrador de la empresa.	3	2	11	TT
							Modificación parcial o completa de la información, de manera intencional o por error		2	4	13	TT

Tabla N° 34. Análisis y evaluación de riesgos del Área de Desarrollo – Activos de Software

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	1	3	3	7	No se cuenta con procedimientos formalizados, estandarizados y documentados para la solución de incidentes y problemas de configuraciones	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se lleva un registro de los errores cometidos en relación a las configuraciones e instalaciones de las herramientas y entornos de desarrollo	2	3	13	TT
						Soporte técnico de las actualizaciones de las herramientas tardía	Aplicativos (tools) de desarrollo de software obsoletas, discontinuadas o no vigentes		2	3	13	TT
						No se cuenta con un procedimiento formalizado, aprobado y documentado para cambios de versiones	Puesta en producción de versiones no autorizadas o no probadas o en desuso		2	4	15	TT
						No existen controles para instalaciones de software	Instalación de aplicativos no autorizados o no licenciados		2	4	15	TT
						Incompatibilidad de las versiones de los nuevos sistemas con el software base en las estaciones	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones		2	5	17	RT
						Cantidad de licencias de software de desarrollo limitada	Indisponibilidad, limitaciones o deficiencias en el software de desarrollo		2	3	13	TT
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Pérdida o eliminación de archivos del entorno de desarrollo		2	3	13	TT
2	Software de ofimática	1	1	3	5	Diferentes versiones instaladas de las aplicaciones	Procedimientos de instalación de software con errores	Se trabaja con software de ofimática descargable y se actualiza con parches	2	2	9	TT

							Infección por malware		2	2	9	**TT**
							Baja performance en el funcionamiento del software de ofimática por falta de mantenimiento		2	2	9	**TT**
							Baja performance en el funcionamiento del software de ofimática por configuración incorrecta del software		2	2	9	**TT**
							Daño en los archivos o en su contenido		2	2	9	**TT**
							Pérdida del software de instalación		2	2	9	**TT**
							Posibilidad de uso o modificación de la información de manera no autorizada		2	2	9	**TT**
3	Aplicativos para modelamiento	1	2	3	6	Aplicaciones o herramientas CASE para las fases de análisis y diseño no licenciadas u obsoletas	Procedimientos de instalación de software con errores	Se lleva un registro de los modelamientos desarrollados en carpetas anexadas a cada proyecto	2	1	8	**TT**
							Infección por malware		2	2	10	**TT**
							Baja performance en el funcionamiento de las aplicaciones de modelamiento por configuración incorrecta del software por falta de mantenimiento		3	2	12	**TT**
							Baja performance en el funcionamiento de las aplicaciones de modelamiento por configuración incorrecta del software		3	1	9	**TT**
							Indisponibilidad, limitaciones o deficiencias en el software de desarrollo		3	1	9	**TT**
							Pérdida del software de instalación		2	2	10	**TT**
							Posibilidad de uso o modificación de los archivos de modelamiento de manera no autorizada		2	2	10	**TT**

4	Motores de base de datos	3	3	3	9	No se cuenta con procedimientos formalizados, estandarizados y documentados para la solución de incidentes y problemas de configuraciones	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se generan copias de respaldo de la BD periódicamente. El custodio es el Jefe de Desarrollo Se lleva un registro de los errores en los motores de BD	2	5	19	**RT**
						Sistema antimalware obsoleto	Infección por malware		1	5	14	**TT**
						No se cuenta con procedimientos ni ambientes dedicados a las pruebas del software antes de puesta en producción	Indisponibilidad o inoperatividad de los sistemas por caída de los motores de base de datos o de los servidores que los administran		2	5	19	**RT**
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Deficiencias o caídas de los sistemas o aplicaciones por falta de mantenimiento de los motores de BD		2	5	19	**RT**
						Asignación de privilegios de acceso a los recursos de información mal configurado	Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada		2	5	19	**RT**
						Soporte técnico de las actualizaciones de las herramientas tardía	Aplicativos (tools) de desarrollo de software obsoletas, discontinuadas o no vigentes		2	3	15	**TT**
						No se cuenta con un procedimiento formalizado, aprobado y documentado para cambios de versiones	Puesta en producción de versiones no autorizadas o no probadas o en desuso		2	4	17	**RT**
						No existen controles para instalaciones de software	Instalación de aplicativos no autorizados o no licenciados		2	5	19	**RT**
						Incompatibilidad de las versiones de los nuevos sistemas con el software base en las estaciones	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones		2	5	19	**RT**
						Cantidad de licencias de software de desarrollo limitada	Indisponibilidad, limitaciones o deficiencias en los motores de BD		2	5	19	**RT**
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Pérdida o eliminación de archivos de la BD		2	5	19	**RT**

5	Herramientas de gestión de proyectos	1	1	3	5	Aplicativos de gestión de proyectos no licenciados u obsoletos	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se generan copias de respaldo de los archivos generados con las herramientas de gestión de proyectos. El custodio es el Jefe de cada proyecto	2	2	9	TT
							Infección por malware		3	1	8	TT
							Baja performance en el funcionamiento de las aplicaciones y herramientas de gestión de proyectos por falta de mantenimiento		3	1	8	TT
							Baja performance en el funcionamiento de las aplicaciones y herramientas de gestión de proyectos por configuración incorrecta del software		3	1	8	TT
							Pérdida del software de instalación		2	2	9	TT
							Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada		3	1	8	TT
6	Software de Virtualización	1	2	3	6	Incompatibilidad o poca capacidad de terminales para trabajar en ambientes virtuales	Baja performance de las estaciones de trabajo virtuales	Se lleva un registro de los errores en el funcionamiento del software de virtualización	2	3	12	TT
7	Aplicativos	2	3	3	8	Poca experiencia del personal de soporte para instalar nuevos sistemas	Procedimientos de instalación de software con errores	Se ha definido perfiles de usuario de acuerdo a la función que desempeña. Sin embargo, los procedimientos no están documentados	3	3	17	RT
						No existe procedimientos formalizados, aprobados y documentados de gestión de cambios	Cambio de la versión del software base no controlada con repercusión en los sistemas		3	3	17	RT
						No se cuenta con documentación técnica de los sistemas y aplicaciones en producción	Poco entendimiento de la funcionalidad de los sistemas por parte de los desarrolladores		3	3	17	RT
						No se ha estandarizado la codificación en el proceso de desarrollo	Malas prácticas en el desarrollo de software		3	3	17	RT
						No existe procedimientos de seguridad para el acceso o asignación del código fuente en el proceso de desarrollo	Sustracción parcial /total de los archivos de código fuente de los sistemas o aplicaciones		3	5	23	RT

						No se cuenta con equipos servidores para contingencias en el área de desarrollo Los procedimientos de pruebas y testeo antes de producción se realizan en el mismo servidor de producción	No continuidad de los proyectos de desarrollo de software o de la atención de requerimientos de cambio		3	5	23	**RT**
						Sistema antimalware obsoleto	Infección por malware		2	5	18	**RT**
						No se cuenta con procedimientos de actualización de perfiles de usuario y de asignación de privilegios	Accesos, uso o manipulación de aplicativos de manera no autorizada		3	5	23	**RT**
						Aplicaciones específicas no integradas a los sistemas principales	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración		4	3	20	**RT**
						No se cuenta con un procedimiento para la atención de requerimientos de cambios formalizado, aprobado y documentado	Aplicaciones y sistemas puesos en producción sin pruebas y testeos		4	5	28	**NT**

Tabla N° 35. Análisis y evaluación de riesgos del Área de Desarrollo – Activos de Hardware

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	2	3	3	8	Ausencia de programa de mantenimiento preventivo	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos	El acceso a los equipos terminales es asignado a los empleados de acuerdo al proyecto al que están asignados	2	3	14	TT
						No se cuenta con procedimientos e instructivos de uso adecuado de los equipos terminales	Mal uso de los equipos terminales		3	2	14	TT
						No se cuenta con contactos de proveedores especializados No se programa el mantenimiento de los equipos anualmente Sistema eléctrico antiguo	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos		3	2	14	TT
						No se cuenta con un plan de mantenimiento No se cuenta con catálogo de contacto de proveedores especializados	Fallas técnicas de los equipos terminales		2	3	14	TT
						No se cuenta con contactos de proveedores especializados para repuestos Los equipos no cuenta con garantía	Caída del equipo por obsolescencia		2	3	14	TT
						Sistema antimalware obsoleto	Caída parcial o total del equipo por efecto de malware		2	3	14	TT
						Los equipos no están configurados para prevenir instalaciones de aplicativos o software no autorizado	Instalación de aplicaciones no autorizadas		3	3	17	RT

						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	13	**TT**
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		5	2	18	**RT**
						No se han definido perfiles de usuario. No existen procedimientos para la asignación de privilegios de acceso según el perfil de usuario	Acceso no autorizado a los equipos terminales		5	3	23	**RT**
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		3	1	11	**TT**
						No existe o debilidades en los controles de acceso físico a las áreas seguras	Pérdida o hurto de recursos de tratamiento de datos		5	3	23	**RT**
2	Servidores	2	3	3	8	No se cuenta con un plan de mantenimiento No se cuenta con catálogo de contacto de proveedores especializados Los equipos críticos no cuentan con garantía o está vencida	Fallas técnicas en los equipos críticos	El uso y tratamiento de los equipos críticos (servidores) se realizan por experiencia.	2	5	18	**RT**
						No se cuenta con sistema de alertas de sobrecarga de accesos concurrentes y sobrealmacenamiento	Indisponibilidad de la infraestructura de almacenamiento secundario		3	5	23	**RT**
						El sistema UPS del área de desarrollo no está correctamente dimensionado para soportar toda la carga de abastecimiento de energía de los equipos conectados. Los servidores no cuentan con UPS dedicado	Indisponiblidad del equipo crítico por caída del fluido eléctrico		2	5	18	**RT**
						Sistema antimalware obsoleto	Caída parcial o total del equipo por efecto de malware		3	5	23	**RT**
						No se cuenta con procedimientos e instructivos para el tratamiento de los equipos críticos	Mal uso y tratamiento de los equipos críticos		3	4	20	**RT**

						No se cuenta con equipos o repuestos para equipos de alta disponibilidad	Fallas técnicas en los equipos críticos		2	5	18	**RT**
						No existe un plan de renovación de partes o equipos críticos	Caída del equipo por obsolescencia		2	3	14	**TT**
						Mala configuración por inexperiencia del personal responsable	Caída de los equipos servidores por fallas en la configuración		2	4	16	**RT**
						No se cuenta con mecanismos de seguridad perimetral, específicamente de control de accesos físicos	Manipulación no autorizada del equipo crítico		2	5	18	**RT**
						No se programa el mantenimiento de los equipos anualmente Los servidores no están ubicados en una sala aislada con temperatura controlada	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos		3	4	20	**RT**
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	13	**TT**
						No se han definido áreas seguras No existe o debilidades en los controles de acceso físico a las áreas seguras	Pérdida o hurto de recursos de tratamiento de datos		2	5	18	**RT**

Tabla N° 36. Análisis y evaluación de riesgos del Área de Producción – Activos de Información

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de actividades de producción	2	1	3	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los procedimientos y reglamentos de actividades de producción están documentados, pero no aprobados. El activo de información es entregado a los empleados, cuando firman su contrato. No existe acuerdos de confidencialidad. No existe un procedimiento formal de gestión de cambios	2	3	12	TT
						Poca difusión de las normativas internas y procedimientos	Incumplimiento de las actividades, funciones y responsabilidades		2	3	12	TT
						No existe procedimientos para la generación de copias de respaldo del activo de información	Indisponibilidad del activo de información por eventos sociales o naturales		1	3	9	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Modificación parcial o completa no autorizada del contenido del activo de información		2	2	10	TT

2	Planes de desarrollo en el Área de Producción y Soporte (Actividades, tareas, asignación de trabajo)	3	2	1	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los procedimientos y reglamentos de actividades de producción están documentados, pero no aprobados. El activo de información es entregado a los empleados, cuando firman su contrato. No existe acuerdos de confidencialidad. No existe un procedimiento formal de gestión de cambios	2	2	10	**TT**
						Desconocimiento de los planes por parte de los usuarios y empleados	Incumplimiento de las actividades, funciones y responsabilidades		1	2	8	**TT**
						No existe procedimientos para la generación de copias de respaldo del activo de información	Indisponibilidad del activo de información por eventos sociales o naturales		1	2	8	**TT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Modificación parcial o completa no autorizada del contenido del activo de información		2	2	10	**TT**
3	Plan de mantenimiento preventivo	2	3	1	6	Mala gestión de cambios en los planes No existe difusión ni seguimiento del cumplimiento de los planes	Incumplimiento de actividades, plazos y responsabilidades	La planificación del mantenimiento de equipos se realiza de manera anual Se lleva un registro del cumplimiento de las actividades de mantenimiento	3	3	15	**TT**
						Presupuesto insuficiente para mantenimiento preventivos Planificación de actividades de mantenimiento incoherentes por falta de coordinación entre áreas	Mala planificación de las actividades de mantenimiento preventivo		3	3	15	**TT**
						No existen controles de verificación del cumplimiento de las actividades de los planes de mantenimiento	Incumplimiento o ejecución inoportuna de las actividades de mantenimiento preventivo		4	4	22	**RT**

4	Registros de incidentes y problemas	2	3	3	8	Poca concienciación de los usuarios en materia de seguridad de la información	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	Se realizan capacitaciones programadas de concienciación en materia de seguridad Se lleva un registro de incidentes de TI en una hoja de cálculo, pero no existe un procedimiento formal	4	5	28	**NT**
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un registro de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de incidentes y problemas	Cambios intencionales o no autorizados en el contenido del activo de información		4	4	24	**RT**
						Falta de seguimiento del cumplimiento del procedimiento de gestión de incidentes y problemas	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna		4	3	20	**RT**
5	Hojas de requerimientos y cambios aprobadas	2	2	3	7	Requerimientos de cambios no autorizadas Procedimiento de atención de requerimientos de cambios no formalizado, aprobado, documentado y difundido	Atención de los requerimientos de cambios en las aplicaciones y sistemas en producción incorrectas	Se tiene un formato establecido para el registro de las peticiones de cambio, las cuales se anexan en el expediente de los proyectos Las peticiones de cambio son aprobadas por el Líder de cada proyecto	2	4	15	**TT**
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de atención de requerimientos de cambios en los aplicativos y sistemas en producción No existe un registro de control de cambios	Cambios intencionales o no autorizados en el contenido del activo de información		3	4	19	**RT**
						Poca experiencia de los analistas Falta o deficiencias en el control de autorización de cambios	Mal registro de los requerimientos de cambio de las aplicaciones y sistemas en producción		4	4	23	**RT**

6	Registro de usuarios	3	2	2	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se asigna un usuario y clave de acceso a la red y base de datos a los usuarios, la cual es administrada desde un servidor de dominio	2	5	17	**RT**
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un registro de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de usuarios	Cambios intencionales o no autorizados en el contenido del activo de información		2	5	17	**RT**
7	Perfiles de usuario	3	2	2	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los perfiles de usuario son asignados por el Jefe de producción, a petición de los líderes de los proyectos. Los perfiles de usuario están asociados a la función que cumple el empleado o usuario en la empresa	2	5	17	**RT**
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de perfiles de usuario y asignación de privilegios No existe un registro de control de cambios	Cambios intencionales o no autorizados en el contenido del activo de información		2	4	15	**TT**

						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios Falta o deficiencias en los controles de acceso	Creación de perfiles de usuario o generación de privilegios de acceso a los recursos de información no autorizada		2	5	17	**RT**
8	Manuales de usuario	1	1	2	4	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se generan manuales de usuario cuando se realizan cambios sustantivos en las aplicaciones y sistemas	3	3	13	**TT**
						Poco conocimiento de los procesos del negocio Procedimientos de cambios en los sistemas y aplicaciones no cotenplan capacitación de usuarios o no son oportunas	Incorrecto uso o poco entendimiento de los manuales de usuario		2	3	10	**TT**
9	Estructura de base de datos	2	2	2	6	No se cuenta con un procedimiento ni registros de control de cambios en las estructuras de datos	Errores o inconsistencias en los cambios realizados sobre las estructura de base de datos	Existe un registro de cambios de código, estructuras de datos y carga de datos, en formato excel. El encargado de registrar los cambios es el analista programador que realiza el cambio.	2	5	16	**RT**
						No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible		3	5	21	**RT**
						No existe procedimientos para la gestión de cambios No se registran los cambios en las estructuras de de datos	Inconsistencia en los datos		3	4	18	**RT**

10	Bitacora de accesos	2	2	3	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se lleva un registro bitácora de los accesos a la base de datos, aplicaciones y sistemas desde que el usuario se loguea con su usuario. El acceso a la bitácora está permitido solo al Jefe de producción	2	4	15	**TT**
						Falta o deficiencias en el control de acceso a las bitácoras de seguimiento o auditoría	Acceso y uso no autorizado al contenido de las bitácoras de seguimiento		2	4	15	**TT**
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	4	15	**TT**
11	Informes de las pruebas de testeo y certificación	3	2	1	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Las pruebas y testeos antes de puesta en producción lo realiza el área de producción con la participación del Jefe de Desarrollo. Los resultados de las pruebas y testeos se documentan y anexan en el expediente de cada proyecto No existen procedimientos de seguridad para protegerlos	2	3	13	**TT**
						Procedimiento mal diseñado o poco entendido - testeo y pruebas	Errores en el proceso con generación de datos o resultados incorrectos		2	4	15	**TT**
						Documentación y registros desactualizados o no disponibles - testeo y pruebas de cambios	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	4	18	**RT**
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	3	13	**TT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		3	4	18	**RT**

						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	3	13	**TT**
12	Configuración de equipos	3	2	3	8	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los equipos terminales en el área de producción, tienen las mismas configuraciones de sistemas operativos Las configuraciones de los equipos terminales la realizan los responsables de soporte técnico	2	3	14	**TT**
						Procedimiento mal diseñado o poco entendido - configuración de equipos	Errores en el proceso con generación de datos o resultados incorrectos		3	4	20	**RT**
						Documentación y registros desactualizados o no disponibles - configuración de equipos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	4	20	**RT**
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		3	3	17	**RT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		2	4	16	**RT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	16	**RT**
13	Inventario de HW y SW	1	2	3	6	Documentación y registros desactualizados o no disponibles - gestión de inventarios de HW y SW	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	Se cuenta con un inventario de hardware y software, pero no está actualizado	2	3	13	**TT**

						Procedimiento mal diseñado o poco entendido - gestión de inventarios	Errores en el proceso con generación de datos o resultados incorrectos		2	3	13	**TT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	3	13	**TT**
14	Información de respaldos y copias de seguridad	2	2	3	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se generan copias de seguridad de la base de datos de todas las aplicaciones y sistemas. Una copia se almacena en un disco duro externo que es administrado por el Jefe de Producción, con una frecuencia mensual Se generan respaldos de las aplicaciones y sistemas	2	3	13	**TT**
						Procedimiento mal diseñado o poco entendido - generación de copias de respaldo	Errores en el proceso con generación de datos o resultados incorrectos		3	5	22	**RT**
						Documentación y registros desactualizados o no disponibles - generación de copias de respaldos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	5	22	**RT**
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	3	13	**TT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		2	5	17	**RT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	15	**TT**

15	Documentación del personal (HV)	1	2	2	5	Documentación y registros desactualizados o no disponibles - gestión de legajos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	La documentación de las hojas de vida de los trabajadores y sus contratos las gestiona el administrador de la empresa.	3	2	11	**TT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	13	**TT**

Tabla N° 37. Análisis y evaluación de riesgos del Área de Producción – Activos de Software

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas de gestión	3	3	3	9	Inexistencia de procedimientos o instructivos de instalación de software	Errores en la instalación de software de gestión	Las terminales en el área de producción cuentan con las mismas versiones de sistemas operativos, software base y software de gestión Existen procedimientos establecidos para las instalaciones y configuraciones del software, pero está desactualizado	2	3	15	TT
						Herramientas con versiones desactualizadas	Baja performance de las herramientas de gestión		2	3	15	TT
						No existe procedimientos ni entorno especial para el cambio de versiones	Desconfiguración de las aplicaciones con impacto en los contenidos de los archivos		2	4	17	RT
						Inexistencia o deficiencias de los controles de instalación de software no permitido	Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información		2	4	17	RT
						Falta de documentación de procedimientos e instructivos de configuración o actualizaciones de aplicaciones	Errores en la configuración de las aplicaciones de gestión		2	3	15	TT
2	Software de ofimática	1	1	3	5	Soporte técnico ineficiente en la instalación de software	Errores en la instalación de software de ofimática	Las terminales en el área de producción cuentan con los mismos softwares de ofimática Existen procedimientos establecidos para las instalaciones y configuraciones del software, pero está desactualizado	2	2	9	TT
						Sistema antimalware obsoleto	Infección por malware		2	2	9	TT
						Soporte técnico inexistente o deficiente de los softwares base o de ofimática	Desconfiguración o baja de performance de los softwares base o de ofimática		2	2	9	TT

						Inexistencias de procedimientos o instructivos de instalación y configuración de software	Configuraciones de software que afectan otras aplicaciones o bajan su performance		2	2	9	**TT**
						Inexistencia o debilidades en los controles de acceso a los recursos de información	Sustracción o eliminación intencional o por error de drivers e instaladores		2	2	9	**TT**
						Puertas de conexión expuestas por uso de versiones de sistemas operativos de distintas versiones	Acceso a los recursos de información aprovechando debilidades del sistema operativo		2	2	9	**TT**
3	Motores de base de datos (Oracle, DB2, MySQL)	3	3	3	9	Inexistencia de procedimientos o instructivos de instalación de software	Errores en la instalación de motores de base de datos	Se generan copias de respaldo de la base de datos con una frecuencia semanal. El custodio de las copias en el Jefe de Producción El acceso a las base de datos en producción, solo es permitido con el usuario del Jefe de Producción Los cambios, nuevas versiones de las aplicaciones y sistemas se prueban y revisan antes de la puesta en producción, documentándose los resultados	2	5	19	**RT**
						Sistema antimalware obsoleto	Infección por malware		1	5	14	**TT**
						No se genera una copia de la base de datos para pruebas, testeos y cambios de versiones de la base de datos	Desconfiguración de los motores de base de datos o modificaciones en las estructuras de la base de datos		2	5	19	**RT**
						Soporte técnico inexistente o deficiente de los motores de base de datos	Desconfiguración o baja de performance de los motores de base de datos		2	5	19	**RT**
						Inexistencia o debilidades de controles de acceso a la base de datos Privilegios de acceso a la base de datos mal configurados	Acceso a la base de datos de manera no autorizada		2	5	19	**RT**
						Herramientas con versiones desactualizadas	Baja performance de los motores de base de datos		2	3	15	**TT**
						No existe procedimientos ni entorno especial para el cambio de versiones	Desconfiguración de los motores de base de datos con impacto en las estructura de datos		2	4	17	**RT**
						Inexistencia o deficiencias de los controles de instalación de software no permitido	Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información		2	5	19	**RT**
						Licencias limitadas o vencidas de motores de base de datos	Problemas graves o errores en la instancia de conexión a la base de datos		2	5	19	**RT**

						Falta de documentación de procedimientos e instructivos de configuración o actualizaciones de aplicaciones	Errores en la configuración de los motores de base de datos		2	5	19	**RT**
5	Aplicativos	2	3	3	8	Soporte técnico ineficiente en la instalación de software	Errores en la instalación de aplicaciones	Se tiene un procedimiento para atención de requerimientos de modificaciones de las aplicaciones en producción Se registran los cambios en el código, estructura de datos y carga de datos, en una bitácora en Excel. El acceso a los códigos fuentes solo es permitido al Jefe de Desarrollo	3	3	17	**RT**
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Errores en los cambios de versiones de las aplicaciones o en el software base		3	3	17	**RT**
						No se genera documentación técnica y funcional de las nuevas aplicaciones o sistemas o de sus modificaciones	Errores en los cambios o dificultad para entender las estructuras de las aplicaciones o base de datos en el proceso de desarrollo		3	3	17	**RT**
						Falta de estandarización en el proceso de codificación y programación	Codificación o estructuras de datos no integrada o desorganizada		3	3	17	**RT**
						Inexistencia o debilidades en los controles de acceso a los códigos fuentes	Sustracción o eliminación intencional de los códigos fuente		3	5	23	**RT**
						No existe procedimientos de continuidad para las aplicaciones y sistemas	Indisponibilidad de las aplicaciones por eventos no controlados		3	5	23	**RT**
						Inexistencia y deficiencias en los controles de instalación de software no permitido	Instalación de aplicaciones infectadas con malware		2	5	18	**RT**
						Inexistencia o debilidades de controles de acceso a las aplicaciones Privilegios de acceso a los aplicativos de seguridad mal configurados	Acceso no autorizado a los contenidos de las aplicaciones de seguridad		3	5	23	**RT**
						Software de desarrollo desactualizadas y sin soporte	Aplicaciones no integradas a los sistemas principales		4	3	20	**RT**
						No se realizan pruebas ni testeos de nuevas aplicaciones o cambios antes de la puesta en producción	Errores de integración o procesamiento de las aplicaciones		4	5	28	**NT**

Tabla N° 38. Análisis y evaluación de riesgos del Área de Producción – Activos de Hardware

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Criticidad				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	3	3	3	9	No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	Se ha definido la responsabilidad de la protección de los equipos a los usuarios asignados Se cuenta con un plan de renovación de equipos cada tres años Los equipos terminales están configurados desde un servidor de dominio para evitar instalaciones o desinstalaciones no autorizadas	2	3	15	TT
						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos terminales		3	2	15	TT
						No existe un plan de mantenimiento preventivo No se cuenta con instructivos para el uso adecuado de los equipos terminales	Indisponibilidad o caída de equipo terminal		3	2	15	TT
						No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos terminales		2	3	15	TT
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		2	3	15	TT
						Sistema antimalware obsoleto	Baja performance o caída de los equipos terminales por infección de malware		2	3	15	TT
						Los equipos terminales no están configurados para prevenir la desinstalación de las aplicaciones o software de manera no autorizada	Desistalación de aplicacionesde manera no autorizadas		3	3	18	RT

						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	14	**TT**
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		5	2	19	**RT**
						No se cuenta con un procedimiento formal, aprobado, documentado y conocido de gestión de perfiles usuario	Acceso al equipo con diferentes usuarios		5	3	24	**RT**
						Inexistencia de un procedimiento formal, aprobado, documentado de borrado de la información por baja de equipo	Sustracción o divulgación de información sensible		3	1	12	**TT**
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos No se cuenta con un procedimiento formal para la movilidad de los equipos fuera de las instalaciones de la empresa	Hurto o extravío de equipos terminal		5	3	24	**RT**
2	Servidores (Aplicaciones, BD, Dominio, Antimalware, de pruebas)	2	3	3	8	No se cuenta con servidores alternos listos para puesta en producción No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos críticos, como servidores y switch	Los servidores se ubican en un área de acceso restringido. La llave la administra el Jefe de Producción Se cuenta con un plan de mantenimiento preventivo anual de los equipos de comunicaciones Se cuenta con sistemas UPS con capacidades y autonomías suficientes para mantener funcionando los servidores por 20 minutos	2	5	18	**RT**
						No se cuenta con un sistema de alertas de capacidad de disco	Saturación del espacio de almacenamiento secundario		3	5	23	**RT**
						No se cuenta con un sistema de continuidad alterno para el abastecimiento de energía Los UPS no tienen la autonomía y capacidad necesaria para bastecer de energía a los equipos críticos	Interrupción repentina del fluido eléctrico		2	5	18	**RT**
						Sistema antimalware obsoleto	Baja de performance o mal funcionamiento por infección de malware		3	5	23	**RT**

						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos críticos		3	4	20	**RT**
						No se cuenta con corta fuegos alternos listos para puesta en producción	Falta de capacidad o fallas técnicas del corta fuego		2	5	18	**RT**
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		2	3	14	**TT**
						Errores en la configuración de los equipos críticos	Errores de procesamiento o mal funcionamiento		2	4	16	**RT**
						No se han definido perfiles de usuario. No existen procedimientos para la asignación de privilegios de acceso según el perfil de usuario	Acceso no autorizado a los equipos críticos		2	5	18	**RT**
						No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.		3	4	20	**RT**
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	13	**TT**
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos	Hurto o extravío de equipos críticos		2	5	18	**RT**
3	Equipos de comunicación (switchs, routers)	2	3	3	8	No se cuenta con servidores alternos listos para puesta en producción No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos críticos, como servidores y switch	Los equipos de comunicaciones están protegidos por gabinetes. La llave la administra el Jefe de Producción Se han definido áreas seguras para los equipos de comunicaciones Se cuenta con un plan de mantenimiento preventivo anual de los equipos de comunicaciones	3	5	23	**RT**
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		3	5	23	**RT**

						No se cuenta con un sistema de continuidad alterno para el abastecimiento de energía Los UPS no tienen la autonomía y capacidad necesaria para bastecer de energía a los equipos críticos	Interrupción repentina del fluido eléctrico		3	5	23	**RT**
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos	Hurto o extravío de equipos críticos		3	5	23	**RT**
						No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.		3	4	20	**RT**
						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos críticos		2	5	18	**RT**

4.2.5. Descripción del componente: Tratamiento de los riesgos

Luego de haber determinado el nivel de exposición al riesgo, se debe evaluar la estrategia y mecanismos de seguridad que la empresa ha implementado para la mitigación de los escenarios de riesgo que están fuera de los rangos de tolerancia.

En las tablas siguientes se el procedimiento metodológico para el tratamiento de los riesgos no tolerables.

Tabla N° 39. Tratamiento de riesgos del Área de Desarrollo - Activos de Información

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de desarrollo	6	Sustracción no autorizada y divulgación de documentación sensible por el personal	5	4	26	NT	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	3	4	18	RT
			Pérdida o sustracción de información	3	4	18	RT	La documentación relacionada a procesos de desarrollo de software se difunde sólo a través de capacitaciones e inducciones.	Reducir	2	3	12	TT
4	Hojas de requerimientos y cambios aprobadas	5	Procesamiento erróneo por parte del personal de Desarrollo	4	4	21	RT	Formalizar la metodología de Atención de requerimientos de cambio Capacitar / Concientizar a los usuarios	Reducir	2	3	11	TT

			Modificación parcial o completa de la información, de manera intencional o por error	4	4	21	**RT**	Las hojas de requerimientos de cambios serán aprobadas y firmadas por el Jefe de Desarrollo y el usuario requiriente, y se entregará una copia al analista programador. La validación de los cambios, se cotejará con la Hoja de requerimientos de cambios original	Reducir	1	4	9	**TT**
5	Documentos técnicos de desarrollo (análisis, diseño)	7	Sustracción no autorizada y divulgación de documentación sensible por el personal	4	5	27	**NT**	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	2	5	17	**RT**
			Procesamiento erróneo por parte del personal de Desarrollo	4	5	27	**NT**	Definir un estándar de programación y de estructuración de la base de datos Implementar un procedimiento de revisión de los programas culminados antes de las pruebas y testeo para verificar el cumplimiento del estándar de programación	Reducir	2	3	13	**TT**
			Sustracción no autorizada de documentación sensible	3	4	19	**RT**	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo	Reducir	2	4	15	**TT**
			Errores en la ejecución de las pruebas unitarias	4	5	27	**NT**	Definir un estándar para la ejecución y ducumentación de las pruebas unitarias	Reducir	2	3	13	**TT**
			Información no disponible, en desuso u obsoleta	3	3	16	**RT**	La documentación de referencia para el desarrollo de software (metodología, estándares, protocolos, etc.) será revisada actualizada anualmente.	Reducir	2	3	13	**TT**
			Modificación parcial o completa de la información, de manera intencional o por error	3	4	19	**RT**	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo Se generararán copias de resplado de la documentación crítica del área de Desarrollo, cuyo custodio es el Jefe del área	Reducir	2	4	15	**TT**

6	Registros de Control de Cambios (scripts, BD, carga data)	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	**RT**	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	1	4	13	**TT**
			Procesamiento erróneo por parte del usuario	4	5	29	**NT**	Definir un estándar de programación y de estructuración de la base de datos Implementar un procedimiento de revisión de los programas culminados antes de las pruebas y testeo para verificar el cumplimiento del estándar de programación	Reducir	2	4	17	**RT**
			Sustracción no autorizada de documentación sensible	2	4	17	**RT**	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo	Reducir	1	4	13	**TT**
			Modificación parcial o completa de la información, de manera intencional o por error	3	3	18	**RT**	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo Se generararán copias de resplado de la documentación de control de cambios, cuyo custodio es el Jefe de cada proyecto	Reducir	2	2	13	**TT**
7	Manuales de usuario	4	Sustracción no autorizada y divulgación de documentación sensible por el personal	5	3	19	**RT**	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	3	3	13	**TT**
			Información no disponible, en desuso u obsoleta	4	3	16	**RT**	Los manuales de usuario serán actualizados como parte del proceso de atención a los requerimientos de cambio por el analista programador.	Reducir	3	3	13	**TT**
			Sustracción no autorizada de documentación sensible	5	3	19	**RT**	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo	Reducir	2	3	10	**TT**
8	Informes de las pruebas de testeo y certificación	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	**RT**	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	1	3	12	**TT**

			Procesamiento erróneo por parte del usuario	4	5	29	NT	Definir un estándar de aplicación y documentación del procedimiento de pruebas y testeo del software antes de puesta en producción	Reducir	2	3	15	TT
			Información no disponible, en desuso u obsoleta	2	4	17	RT	La documentación relacionada a las pruebas y testeo del software será revisada por el jefe de cada proyecto.	Reducir	2	3	15	TT
			Sustracción no autorizada de documentación sensible	3	4	21	RT	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo	Reducir	1	2	11	TT
			Modificación parcial o completa de la información, de manera intencional o por error	3	3	18	RT	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo Se generararán copias de resplado de la documentación de control de cambios, cuyo custodio es el Jefe de cada proyecto	Reducir	2	2	13	TT
9	Documentos de versiones de software	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	RT	Incluir en el contrato con los empleados, Actas de confidencialidad con la información que se les asigna. Establecer mecanismos de sanción administrativa y legal en caso de incumplimiento del Acta de confidencialidad	Reducir	1	3	12	TT
			Información no disponible, en desuso u obsoleta	4	3	21	RT	La documentación de las versiones de las aplicaciones y sistemas, será revisada y actualizada por el Jefe de cada proyecto.	Reducir	2	3	15	TT
			Sustracción no autorizada de documentación sensible	3	4	21	RT	Implementar mecanismos de seguridad de acceso a la documentación sensible del área de Desarrollo	Reducir	1	2	11	TT

Tabla N° 40. Tratamiento de riesgos del Área de Desarrollo - Activos de Software

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	7	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	17	**RT**	Estandarizar las versiones de las herramientas y entornos de desarrollo Fijar un presupuesto anual para la renovación o adquisición de licencias nuevas	Reducir	2	5	17	**RT**
4	Motores de base de datos	9	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	2	5	19	**RT**	Elaborar instructivos y procedimientos de actualización y configuración de los motores de base de datos Capacitar al personal de soporte en actualización y configuración de los motores de base de datos	Reducir	1	5	14	**TT**
			Indisponibilidad o inoperatividad de los sistemas por caída de los motores de base de datos o de los servidores que los administran	2	5	19	**RT**	Implementar procedimientos de generación de copias de respaldo de la base de datos con una frecuencia semanal Implementar planes de contingencias para operar con copias de base de datos en servidores alternos	Reducir	1	5	14	**TT**
			Deficiencias o caídas de los sistemas o aplicaciones por falta de mantenimiento de los motores de BD	2	5	19	**RT**	Instalar software de monitoreo de la performance de las BD Elaborar y aplicar un plan de mantenimiento anual de los motores de base de datos	Reducir	1	3	12	**TT**
			Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada	2	5	19	**RT**	Mejorar el procedimiento de gestión de perfiles de usuario Gestionar los privilegios y niveles de acceso a los recursos de información mediante un servidor de dominio	Reducir	1	5	14	**TT**

			Puesta en producción de versiones no autorizadas o no probadas o en desuso	2	4	17	**RT**	Elaborar un procedimiento de gestión y control de versiones de la base de datos Elaborar una biblioteca de versiones de base de datos, con aplicación de su etiquetado	Reducir	2	3	15	**TT**
			Instalación de aplicativos no autorizados o no licenciados	2	5	19	**RT**	Implementar un mecanismo de seguridad para inhabilitar procesos de instalación de software en los terminales de trabajo	Reducir	2	4	17	**RT**
			Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	19	**RT**	Estandarizar las versiones de las herramientas y entornos de desarrollo Fijar un presupuesto anual para la renovación o adquisición de licencias nuevas	Reducir	1	5	14	**TT**
			Indisponibilidad, limitaciones o deficiencias en los motores de BD	2	5	19	**RT**	Instalar software de monitoreo de la performance de las BD, con posibilidades de generar alertas y registro de incidentes en los motores de base de datos	Reducir	1	5	14	**TT**
			Pérdida o eliminación de archivos de la BD	2	5	19	**RT**	Implementar mecanismos de control de acceso y privilegios a la base de datos de acuerdo al perfil de usuario. Generar bitácoras de acceso a la base de datos a través de un servidor de dominio	Reducir	1	3	12	**TT**
7	Aplicativos	8	Procedimientos de instalación de software con errores	3	3	17	**RT**	Elaborar instructivos y procedimientos de instalación y configuración de aplicaciones, considerando pruebas de integridad y funcionalidad	Reducir	1	3	11	**TT**
			Cambio de la versión del software base no controlada con repercusión en los sistemas	3	3	17	**RT**	Aplicar pruebas de integridad en los procedimientos de cambios de versiones de las aplicaciones Elaborar un procedimiento de gestión y control de versiones de las aplicaciones Elaborar una biblioteca de versiones de las aplicaciones	Reducir	1	3	11	**TT**
			Poco entendimiento de la funcionalidad de los sistemas por parte de los desarrolladores	3	3	17	**RT**	Capacitar a los analistas programadores en el entendimiento de los sistemas antes de realizar cambios Elaborar y mantener actualizada la documentación técnica de las aplicaciones desarrolladas	Reducir	2	3	14	**TT**

			Malas prácticas en el desarrollo de software	3	3	17	**RT**	Definir un estándar de programación y de estructuración de la base de datos Implementar un procedimiento de revisión de los programas culminados antes de las pruebas y testeo para verificar el cumplimiento del estándar de programación	Reducir	2	2	12	**TT**
			Sustracción parcial /total de los archivos de código fuente de los sistemas o aplicaciones	3	5	23	**RT**	Implementar un mecanismo de asignación de código fuente a los analistas programadores, de acuerdo a la actividad programada por fechas. Implementar una política de uso restringido de dispositivos de almacenamiento secundario y de acceso a Internet en el área de Desarrollo	Reducir	2	5	18	**RT**
			No continuidad de los proyectos de desarrollo de software o de la atención de requerimientos de cambio	3	5	23	**RT**	Separar los ambientes de producción y desarrollo en dos redes de datos distintas	Reducir	2	4	16	**RT**
			Infección por malware	2	5	18	**RT**	Aplicar procedimientos de revisiones de los códigos fuente en los procesos de pruebas y testeo del software	Reducir	1	5	13	**TT**
			Accesos, uso o manipulación de aplicativos de manera no autorizada	3	5	23	**RT**	Controlar y asignar los privilegios de acceso a las aplicaciones a través de los perfiles de usuario. Generar bitácoras de seguimiento de las acciones de los usuarios en las aplicaciones desde su logueo	Reducir	1	5	13	**TT**
			Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	4	3	20	**RT**	Incluir pruebas de integridad de las aplicaciones antes de su puesta en producción	Reducir	3	3	17	**RT**
			Aplicaciones y sistemas puestos en producción sin pruebas y testeos	4	5	28	**NT**	Implementar un procedimiento de certificación de aplicaciones por parte del área usuario y el Jefe de Producción, antes de su puesta en producción, como parte del proceso de pruebas y testeo	Reducir	2	3	14	**TT**

Tabla N° 41. Tratamiento de riesgos del Área de Desarrollo - Activos de Hardware

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	8	Instalación de aplicaciones no autorizadas	3	3	17	**RT**	Gestionar los puertos, acceso a Internet de cada terminal de trabajo, de acuerdo al perfil del usuario	Reducir	2	3	14	**TT**
			Revelación de información sensible	5	2	18	**RT**	Desarrollar actividades de concientización en materia de seguridad de la información, debidamente planificadas y programas en el plan de trabajo Configurar los equipos terminales de trabajo para el bloqueo de pantalla inactivas	Reducir	2	2	12	**TT**
			Acceso no autorizado a los equipos terminales	5	3	23	**RT**	Asignar el acceso a los terminales desde un solo punto de red Asignar el acceso a los terminales mediante un usuario y clave	Reducir	1	2	10	**TT**
			Pérdida o hurto de recursos de tratamiento de datos	5	3	23	**RT**	Definir áreas seguras para los equipos terminales más críticos Asignar responsabilidades de uso y protección de los equipos terminales a los usuarios, en el inventario de activos Elaborar un procedimiento controlado de movilidad de los equipos fuera de los ambientes de la empresa	Reducir	2	3	14	**TT**
2	Servidores	8	Fallas técnicas en los equipos críticos	2	5	18	**RT**	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	3	11	**TT**

			Indisponibilidad de la infraestructura de almacenamiento secundario	3	5	23	**RT**	Instalar un software de monitoreo y de gestión de alertas de los equipos críticos de la red	Reducir	1	3	11	**TT**
			Indisponiblidad del equipo crítico por caída del fluido eléctrico	2	5	18	**RT**	Instalar UPS independientes, debidamente calculados en su autonomía y capacidad. Implementar un sistema alterno de abastecimiento de energía: motor	Reducir	1	3	11	**TT**
			Caída parcial o total del equipo por efecto de malware	3	5	23	**RT**	Mantener actualizado el sistema antimalware Gestionar el control de acceso a través de puertos	Reducir	1	5	13	**TT**
			Mal uso y tratamiento de los equipos críticos	3	4	20	**RT**	Capacitación permanente al personal que opera los servidores Elaborar instructivos y procedimientos de uso de los servidores	Reducir	1	4	12	**TT**
			Fallas técnicas en los equipos críticos	2	5	18	**RT**	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	5	13	**TT**
			Caída de los equipos servidores por fallas en la configuración	2	4	16	**RT**	Elaborar instructivos y procedimientos para la configuración de los servidores	Reducir	1	4	12	**TT**
			Manipulación no autorizada del equipo crítico	2	5	18	**RT**	Asignar los servidores a una zona considerada como área segura Implementar controles de acceso físico al ambiente de servidores, con registros de entradas y salidas del personal autorizado	Reducir	1	4	12	**TT**
			Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos	3	4	20	**RT**	Instalar sistema de climatización del ambiente de servidores Mantener implementado un servidor de respaldo para casos de contingencias, con la misma configuración del principal	Reducir	1	4	12	**TT**
			Pérdida o hurto de recursos de tratamiento de datos	2	5	18	**RT**	Asignar los servidores a una zona considerada como área segura Implementar controles de acceso físico al ambiente de servidores, con registros de entradas y salidas del personal autorizado	Reducir	1	5	13	**TT**

Tabla N° 42. Tratamiento de riesgos del Área de Producción y Soporte - Activos de Información

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
3	Plan de mantenimiento preventivo	6	Incumplimiento o ejecución inoportuna de las actividades de mantenimiento preventivo	4	4	22	RT	Planificación anual de las actividades de mantenimiento preventivo Revisión periódica del cumplimiento del plan de mantenimiento preventivo	Reducir	2	2	10	TT
4	Registros de incidentes y problemas	8	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	4	5	28	NT	Los incidentes de TI deben ser tipificados y priorizados Desarrollo de actividades de concientización sobre seguridad de la información Evaluaciones del cumplimiento del procedimiento de gestión de incidentes de TI en base a la trazabilidad de la atención de los incidentes de TI	Reducir	1	3	11	TT
			Cambios intencionales o no autorizados en el contenido del activo de información	4	4	24	RT	Evaluaciones periódicas del cumplimiento del procedimiento de atención de incidentes de TI en base a la trazabilidad de la atención de incidentes de TI	Reducir	1	3	11	TT
			Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	4	3	20	RT	Incorporar actividades de mejora continua del procedimiento de gestión de incidentes en base a los registros de atención de incidentes de TI	Reducir	1	3	11	TT

5	Hojas de requerimientos y cambios aprobadas	7	Cambios intencionales o no autorizados en el contenido del activo de información	3	4	19	**RT**	Evaluaciones periódicas del cumplimiento del procedimiento de atención de requerimientos de cambios de los sistemas en producción	Reducir	2	3	13	**TT**
			Mal registro de los requerimientos de cambio de las aplicaciones y sistemas en producción	4	4	23	**RT**	Trazabilidad periódica de los cambios realizados en el procedimiento de atención de requerimientos de cambios de los sistemas en producción	Reducir	2	2	11	**TT**
6	Registro de usuarios	7	Extracción o divulgación no autorizada de la información sensible	2	5	17	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información	Reducir	1	5	12	**TT**
			Cambios intencionales o no autorizados en el contenido del activo de información	2	5	17	**RT**	Evaluaciones periódicas del cumplimiento del procedimiento de gestión de cuentas de usuarios	Reducir	2	3	13	**TT**
7	Perfiles de usuario	7	Extracción o divulgación no autorizada de la información sensible	2	5	17	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información	Reducir	1	5	12	**TT**
			Creación de perfiles de usuario o generación de privilegios de acceso a los recursos de información no autorizada	2	5	17	**RT**	Evaluaciones periódicas del cumplimiento del procedimiento de gestión de cuentas de usuarios	Reducir	1	3	10	**TT**
9	Estructura de base de datos	6	Errores o inconsistencias en los cambios realizados sobre las estructura de base de datos	2	5	16	**RT**	Generación de respaldos periodicos de la BD con procedimientos de restore Trazabilidad periódica a los cambios en la BD	Reducir	1	4	10	**TT**
			Extracción o divulgación no autorizada de la información sensible	3	5	21	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información	Reducir	1	5	11	**TT**

			Inconsistencia en los datos	3	4	18	**RT**	Implementación de un procedimiento de certificación de módulos antes de la puesta en producción	Reducir	2	2	10	**TT**
11	Informes de las pruebas de testeo y certificación	6	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	4	18	**RT**	Implementación de un procedimiento de certificación de módulos antes de la puesta en producción	Reducir	1	2	8	**TT**
			Extravío o hurto del activo de información	3	4	18	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información Implementar controles para protección de documentos	Reducir	1	4	10	**TT**
12	Configuración de equipos	8	Errores en el proceso con generación de datos o resultados incorrectos	3	4	20	**RT**	Definir y establecer una configuración estándar para los equipos de cómputo de acuerdo a la función que cumple el empleado asignado	Reducir	1	2	10	**TT**
			Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	4	20	**RT**	Revisiones periódicas de los cambios en las configuraciones de equipos	Reducir	1	2	10	**TT**
			Accesos y uso al activo de información de manera no autorizados	3	3	17	**RT**	Definir niveles de acceso a los recursos de información en la red de acuerdo a perfiles de usuario Generar bitácoras de seguimiento de las acciones realizadas por los usuarios desde su logueo a la red	Reducir	2	2	12	**TT**
			Extravío o hurto del activo de información	2	4	16	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información	Reducir	1	4	12	**TT**

			Modificación parcial o total de la información	2	4	16	**RT**	Definir niveles de acceso a los recursos de información en la red de acuerdo a perfiles de usuario Generar bitácoras de seguimiento de las acciones realizadas por los usuarios desde su logueo a la red	Reducir	1	3	11	**TT**
14	Información de respaldos y copias de seguridad	7	Errores en el proceso con generación de datos o resultados incorrectos	3	5	22	**RT**	Mejorar el procedimiento de generación de copias de resplado de la base de datos Planificar pruebas de recuperación de la base de datos	Reducir	1	2	9	**TT**
			Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	5	22	**RT**	Revisiones periódicas de las copias de seguridad de la información en base a procesos de restore	Reducir	1	2	9	**TT**
			Extravío o hurto del activo de información	2	5	17	**RT**	Incluir en los contratos de los empleados Actas de confidencialidad de la información Definir y aplicar sanciones administrativas y legales del incumplimiento de las Actas de confidencialidad de la información	Reducir	1	4	11	**TT**

Tabla N° 43. Tratamiento de riesgos del Área de Producción y Soporte - Activos de Software

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas de gestión	9	Desconfiguración de las aplicaciones con impacto en los contenidos de los archivos	2	4	17	RT	Elaborar instructivos para los procedimientos de instalación y configuración de motores de base de datos Utilizar software de monitoreo de los recursos de la red, con alertas de eventos	Reducir	1	4	13	TT
			Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información	2	4	17	RT	Las estaciones de trabajo deben estar protegidas contra instalaciones de software no autorizada, deshabilitando los puertos y dispositivos de lectura. Para la comunicación entre usuarios deberán crearse carpetas compartidas	Reducir	1	4	13	TT
3	Motores de base de datos (Oracle, DB2, MySQL)	9	Errores en la instalación de motores de base de datos	2	5	19	RT	Elaborar instructivos para los procedimientos de instalación de motores de base de datos Desarrollar pruebas de cambios de las versiones de los motores de base de datos	Reducir	1	3	12	TT
			Desconfiguración de los motores de base de datos o modificaciones en las estructuras de la base de datos	2	5	19	RT	Utilizar software de monitoreo de las bases de datos, con generación de alertas de eventos	Reducir	1	5	14	TT
			Desconfiguración o baja de performance de los motores de base de datos	2	5	19	RT	Elaborar instructivos para los procedimientos de instalación y configuración de motores de base de datos Utilizar software de monitoreo de los recursos de la red, con alertas de eventos	Reducir	1	3	12	TT
			Acceso a la base de datos de manera no autorizada	2	5	19	RT	Definir y aplicar perfiles de acceso a los recursos de información en base a las funciones que desempeña el empleado	Reducir	1	5	14	TT

			Desconfiguración de los motores de base de datos con impacto en las estructura de datos	2	4	17	**RT**	Elaborar instructivos para los procedimientos de instalación y configuración de motores de base de datos Utilizar software de monitoreo de los recursos de la red, con alertas de eventos	Reducir	1	4	13	**TT**
			Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información	2	5	19	**RT**	Utilizar software de monitoreo de los recursos de la red, con alertas de eventos	Reducir	1	4	13	**TT**
			Problemas graves o errores en la instancia de conexión a la base de datos	2	5	19	**RT**	Estandarizar las versiones de las herramientas y entornos de desarrollo Fijar un presupuesto anual para la renovación o adquisición de licencias nuevas	Reducir	1	4	13	**TT**
			Errores en la configuración de los motores de base de datos	2	5	19	**RT**	Estandarizar y documentar los procedimientos de configuración de las base de datos en los servidores	Reducir	1	5	14	**TT**
5	Aplicativos	8	Errores en la instalación de aplicaciones	3	3	17	**RT**	Elaborar instructivos y procedimientos de instalación y configuración de aplicaciones, considerando pruebas de integridad y funcionalidad	Reducir	1	4	12	**TT**
			Errores en los cambios de versiones de las aplicaciones o en el software base	3	3	17	**RT**	Elaborar instructivos para los procedimientos de instalación y configuración de motores de base de datos Utilizar software de monitoreo de los recursos de la red, con alertas de eventos	Reducir	1	2	10	**TT**
			Errores en los cambios o dificultad para entender las estructuras de las aplicaciones o base de datos en el proceso de desarrollo	3	3	17	**RT**	Estandarizar la elaboración de la documentación técnica de las aplicaciones desarrolladas La puesta en producción de las aplicaciones o cambios realizados, deben incluir capacitaciones a usuario donde se incluya la aprobación de los manuales de usuario Los analistas programadores deben elaborar o actualizar la documentación técnica de los cambios o desarrollos, los cuales deben ser aprobados por el Jefe del proyecto	Reducir	1	1	9	**TT**

			Codificación o estructuras de datos no integrada o desorganizada	3	3	17	**RT**	Incluir procedimientos de certificación de módulos y aplicativos por parte del área usuaria Incluir en el procedimiento de pruebas del software antes de producción, pruebas funcionales de integración, antes de la puesta en producción	Reducir	1	2	10	**TT**
			Sustracción o eliminación intencional de los códigos fuente	3	5	23	**RT**	Implementar un mecanismo de acceso al código fuente a los responsables del área de Producción. Implementar una política de uso restringido de dispositivos de almacenamiento secundario y de acceso a Internet en el área de Producción	Reducir	1	3	11	**TT**
			Indisponibilidad de las aplicaciones por eventos no controlados	3	5	23	**RT**	Implementar un procedimiento de contingencia en caso de la caída de las aplicaciones principales, mediante procedimientos manuales y registros en software de ofimática	Reducir	1	3	11	**TT**
			Instalación de aplicaciones infectadas con malware	2	5	18	**RT**	Incluir dentro del proceso pruebas y testeo de las aplicaciones antes de la puesta en producción, revisiones de código para detectar código malicioso	Reducir	1	5	13	**TT**
			Acceso no autorizado a los contenidos de las aplicaciones de seguridad	3	5	23	**RT**	Las bitácoras de trazabilidad o de seguimiento solo debe ser accedidas por un perfil de usuario autorizado	Reducir	1	3	11	**TT**
			Aplicaciones no integradas a los sistemas principales	4	3	20	**RT**	Incluir pruebas de integridad de las aplicaciones antes de su puesta en producción	Reducir	2	3	14	**TT**
			Errores de integración o procesamiento de las aplicaciones	4	5	28	**NT**	Incluir pruebas de integridad de las aplicaciones antes de su puesta en producción	Reducir	1	3	11	**TT**

Tabla N° 44. Tratamiento de riesgos de TI del Área de Producción y Soporte - Activos de Hardware

N°	Activo afectado	Criticidad	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
	PCs/Laptops	9	Desistalación de aplicacionesde manera no autorizadas	3	3	18	RT	Gestionar los puertos, acceso a Internet, configuraciones de cada terminal de trabajo, de acuerdo al perfil del usuario	Reducir	2	2	13	TT
			Revelación de información sensible	5	2	19	RT	Desarrollar actividades de concientización en materia de seguridad de la información, debidamente planificadas y programas en el plan de trabajo Configurar los equipos terminales de trabajo para el bloqueo de pantalla inactivas	Reducir	2	2	13	TT
			Acceso al equipo con diferentes usuarios	5	3	24	RT	Asignar el acceso a los terminales desde un solo punto de red Asignar el acceso a los terminales mediante un usuario y clave	Reducir	2	2	13	TT
			Hurto o extravío de equipos terminal	5	3	24	RT	Definir áreas seguras para los equipos terminales más críticos Asignar responsabilidades de uso y protección de los equipos terminales a los usuarios, en el inventario de activos Elaborar un procedimiento controlado de movilidad de los equipos fuera de los ambientes de la empresa	Reducir	2	3	15	TT
2	Servidores (Aplicaciones, BD, Dominio, Antimalware, de pruebas)	8	Fallas técnicas en los equipos críticos, como servidores y switch	2	5	18	RT	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	4	12	TT

			Saturación del espacio de almacenamiento secundario	3	5	23	**RT**	Instalar un software de monitoreo y de gestión de alertas de los equipos críticos de la red	Reducir	1	4	12	**TT**
			Interrupción repentina del fluido eléctrico	2	5	18	**RT**	Instalar UPS independientes, debidamente calculados en su autonomía y capacidad. Implementar un sistema alterno de abastecimiento de energía: motor	Reducir	1	3	11	**TT**
			Baja de performance o mal funcionamiento por infección de malware	3	5	23	**RT**	Mantener actualizado el sistema antimalware Gestionar el control de acceso a través de puertos	Reducir	1	3	11	**TT**
			Manipulación no autorizada de los equipos críticos	3	4	20	**RT**	Asignar los servidores a una zona considerada como área segura Implementar controles de acceso físico al ambiente de servidores, con registros de entradas y salidas del personal autorizado	Reducir	1	2	10	**TT**
			Falta de capacidad o fallas técnicas del corta fuego	2	5	18	**RT**	Contar con corta fuegos alternos listos para puesta en producción	Reducir	1	5	13	**TT**
			Errores de procesamiento o mal funcionamiento	2	4	16	**RT**	Elaborar instructivos y procedimientos para la configuración de los servidores	Reducir	1	4	12	**TT**
			Acceso no autorizado a los equipos críticos	2	5	18	**RT**	Asignar los servidores a una zona considerada como área segura Implementar controles de acceso físico al ambiente de servidores, con registros de entradas y salidas del personal autorizado	Reducir	1	4	12	**TT**
			Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	3	4	20	**RT**	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	3	11	**TT**

			Hurto o extravío de equipos críticos	2	5	18	**RT**	Asignar los servidores a una zona considerada como área segura Implementar controles de acceso físico al ambiente de servidores, con registros de entradas y salidas del personal autorizado	Reducir	1	4	12	**TT**
3	Equipos de comunicación (switchs, routers)	8	Fallas técnicas en los equipos críticos, como servidores y switch	3	5	23	**RT**	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	4	12	**TT**
			Obsolescencia del equipo	3	5	23	**RT**	Incluir este tipo de equipamiento dentro del Plan de renovación tecnológica de la empresa	Reducir	2	4	16	**RT**
			Interrupción repentina del fluido eléctrico	3	5	23	**RT**	Instalar UPS independientes, debidamente calculados en su autonomía y capacidad. Implementar un sistema alterno de abastecimiento de energía: motor	Reducir	1	4	12	**TT**
			Hurto o extravío de equipos críticos	3	5	23	**RT**	Colocar los switch en gabinetes considerados como área segura Implementar controles de acceso físico a los gabinetes	Reducir	2	5	18	**RT**
			Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	3	4	20	**RT**	Mantener actualizado el catálogo de proveedores especializados Incluir en el plan anual de trabajo del área, actividades de mantenimiento preventivo Mantener vigentes las garantías de los equipos	Reducir	1	4	12	**TT**
			Manipulación no autorizada de los equipos críticos	2	5	18	**RT**	Colocar los switch en gabinetes considerados como área segura Implementar controles de acceso físico a los gabinetes	Reducir	1	4	12	**TT**

4.2.6. Descripción del componente: Plan de tratamiento de los riesgos

En la fase de tratamiento de los riesgos, se definió un conjunto mecanismos de seguridad o protección y las actividades relacionadas para su implementación, operación, funcionamiento y continuidad.

Tabla N° 45. Propuesta de controles o mecanismos de seguridad para el tratamiento de riesgos

N°	Controles/Mecanismos de seguridad	Actividades
1	Actualizar los estándares de programación	- Investigar sobre tendencias de programación - Definir entornos de programación: lenguaje, herramientas - Definir un protocolo de programación: estructura - Documentar el protocolo de programación - Capacitar a los analistas programadores
2	Revisiones del código fuente	- Definir un procedimiento de revisión del código fuente para verificar cumplimiento de los estándares de programación - Definir un procedimiento para revisión del código fuente con fines de identificar código malicioso - Documentar los procedimientos - Incluir los procedimientos como parte del proceso de pruebas y testeo de software antes de la puesta en producción
3	Implementar actividades de concienciación y sensibilización en materia de seguridad de información	- Identificar y seleccionar los aspectos de seguridad de la información de interés para la empresa - Identificar buenas prácticas y estándares relacionados a los aspectos de seguridad de la información seleccionados - Elaborar material: documentación, formatos y presentaciones sobre los temas de seguridad seleccionados - Identificar estrategias de concienciación y sensibilización - Elaborar el Plan anual de actividades de concienciación y sensibilización - Desarrollar las actividades consideradas en el Plan - Monitorear el cumplimiento y los resultados de las actividades
4	Diseñar e implementar controles de acceso a la documentación crítica y sensible	- Identificar la documentación producida de cada área de la empresa - Tipificar la documentación de acuerdo a su nivel de uso y divulgación: privada, restringida y pública - Definir estrategias de identificación y protección de la documentación, sobre toda para la crítica - Asignar responsables y funciones para la protección de la documentación en los documentos de gestión de la empresa
5	Implementar un procedimiento de gestión de perfiles de usuario	- Identificar tipos de usuario, funciones, responsabilidades y niveles de acceso a la información en cada área de la empresa - Tipificar los tipos de usuario de acuerdo a las funciones - Definir los niveles y privilegios de acceso a la información de cada perfil de usuario - Configurar los niveles y privilegios de acceso a la información en el software de gestión de perfiles de usuario en el servidor de dominio - Elaborar un procedimiento para cambios, altas y bajas de perfiles de usuario - Elaborar un procedimiento para los cambios, altas y bajas de cuentas de usuario
6	Actas de confidencialidad con el personal de la empresa	- Identificar la documentación e información entregada al personal en cada puesto de trabajo - Tipificar la documentación entregada al personal, en base a su uso y divulgación: privada, restringida, pública

		- Incluir cláusulas de confidencialidad de la documentación e información en los contratos con cada personal - Elaborar y firmar actas de confidencialidad con cada empleado en base lo estipulado en los contratos
7	Actas de confidencialidad con los proveedores	- Identificar la documentación e información compartida entre ITnovate Lab S.R.L y sus proveedores de servicios - Tipificar la documentación compartida con los proveedores en base a su uso y divulgación: privada, restringida, pública - Incluir cláusulas de confidencialidad de la documentación e información en los contratos con los proveedores - Elaborar y firmar actas de confidencialidad con los proveedores en base lo estipulado en los contratos
8	Establecer formas, canales y protocolos de comunicación ágil y oportuna con los proveedores de servicios	- Definir el canal formal de comunicación entre ITnovate Lab S.R.L y sus proveedores de servicios tipo IaaS para reportar incidencias en producción.
9	Implementar mecanismos de control de acceso a las aplicaciones	- Identificar las funcionalidades implementadas en cada aplicación en producción - Identificar los usuarios con privilegios de acceso a cada funcionalidad de las aplicaciones, según su rol o función - Elaborar el mapa de privilegios de accesos por aplicación - Implementar los niveles y privilegios de acceso a las aplicaciones en software de gestión de usuarios en el servidor de dominio - Mantener actualizado el mapa de privilegios de accesos por aplicación y el software de gestión de usuarios
10	Elaborar documentación técnica de los desarrollos	- Definir la documentación técnica obligatoria que se debe generar en el proceso de desarrollo o en la gestión de cambios - Definir una estructura estándar para cada documento técnico - Asignar responsabilidades de la generación o actualización de la documentación técnica en el proceso de desarrollo o cambios en las aplicaciones y sistemas
11	Implementar un proceso de gestión de licencias de software	- Identificar las necesidades de licenciamiento de software actual en la empresa - Estimar las necesidades de licencias de software a futuro - Elaborar un presupuesto fijo para la adquisición de licencias de software e incluir en el Plan anual de adquisiciones - Elaborar el inventario de licencias de software - Definir y elaborar un procedimiento de revisión de licencias de software
12	Entrenamiento de personal en protocolo de comunicaciones	- Definir un protocolo de comunicación en materia de seguridad de la información entre el personal y áreas de la empresa - Definir los formatos y canales de comunicación - Capacitar y sensibilizar al personal en el protocolo de comunicación en materia de seguridad de la información
13	Actualizar normativas de gestión con aspectos de seguridad de la información	- Identificar los aspectos de seguridad de la información que deben ser consideradas como funciones y responsabilidades del personal de la empresa - Identificar y definir responsabilidades y funciones de seguridad de la información de cada puesto de trabajo de la empresa - Actualizar el MOF con las definir responsabilidades y funciones de seguridad de la información de cada puesto de trabajo de la empresa
14	Implementar el protocolo y procedimiento de pruebas funcionales del software antes de puesta en producción	- Definir el protocolo y procedimiento para la realización de pruebas unitarias - Definir el protocolo y procedimiento para la realización de pruebas de integridad - Documentar los protocolos y procedimientos - Asignar responsabilidades de la ejecución de pruebas

		funcionales - Capacitar al personal responsable de las pruebas funcionales
15	Implementar el procedimiento de atención de requerimientos de cambios de las aplicaciones en producción	- Diseñar los formatos de registro de requerimientos de cambio y de aceptación del cambio - Definir el procedimiento de recogida de la información y su registro - Definir el protocolo de autorización de los cambios - Definir el protocolo de asignación de la responsabilidad del cambio - Establecer los criterios de aceptación de los cambios en el área de desarrollo: revisión de estructuras de programación, documentación generada - Definir el procedimiento de entrega al área de Producción para la realización de pruebas y testeos - Capacitar a los usuarios finales
16	Formalizar la metodología de Ingeniería de Software	- Definir el (los) modelo(s) de ciclo de vida que utilizará la empresa para el desarrollo de software - Definir la metodología base que empleará la empresa para el desarrollo del software, identificando actividades, tareas, entradas y salidas - Documentar la metodología
17	Elaborar instructivos de instalación de software	- Definir los procedimientos de instalación de los diferentes softwares - Elaborar instructivos de instalación
18	Elaborar manuales de usuario	- Definir una estructura estandarizada de los manuales de usuario - Actualizar los manuales de usuario de cada aplicación - Asignar la responsabilidad de actualización de los manuales de usuario a los analistas programadores como parte del proceso de gestión de cambios y atención de los requerimientos de cambios
19	Definir las condiciones necesarias para la ejecución de pruebas de cambios de versiones del software	- Definir el procedimiento para configuración del laboratorio de prueba - Elaborar el procedimiento para la obtención de datos de prueba - Elaborar los formatos para el seguimiento y registro de resultados
20	Implementar un sistema de gestión de versiones de software	- Identificar las herramientas de software que necesitan licenciamiento - Identificar los tipos de licencias por cada tipo de software que utiliza la empresa - Instalar una aplicación de control de versiones que facilite la administración de las distintas versiones de cada producto desarrollado en la empresa
21	Separar los entornos de trabajo de Desarrollo, Producción y Pruebas	- Cada ambiente de trabajo (Desarrollo, Producción y Pruebas) debe tener su propia base de datos y su copia de las aplicaciones de forma que no haya interferencias en los ambientes y entre los diferentes participantes en la construcción del software. - Implementar redes de computadoras distintas para cada una de las áreas.
22	Planificar revisiones permanentes de la documentación de los proyectos de desarrollo de software	- Identificar los documentos que debe anexarse al expediente documental de cada proyecto de desarrollo de software - Definir parámetros y criterios de revisión de documentos de proyectos - Definir fechas de revisión de documentos para cada proyecto
23	Implementar un proceso de gestión de cambios	- Definir un protocolo de cambios de las aplicaciones en producción: estructura de datos, carga de datos y código - Definir un protocolo de cambios de versiones de las aplicaciones en producción - Definir un protocolo de cambios en las actualizaciones de versiones de las herramientas de software: sistema

		operativo, motores de base de datos, herramientas de gestión, antivirus, etc.
24	Implantar un control de monitoreo del servicio de base de datos	- Identificar los servicios críticos del servidor de base de datos - Identificar los eventos que requieren atención técnica en los servicios del servidor de base de datos - Instalar una herramienta de monitoreo de los servicios de base de datos - Configurar y programar reportería del monitoreo del servicio de base de datos
25	Implementar un procedimiento para altas, bajas y cambios de usuarios	- Definir perfiles de usuario de acuerdo a la función que desempeña el personal - Identificar niveles y privilegios de acceso a los recursos de información de cada perfil de usuario - Configurar los niveles y privilegios de acceso de cada usuario en el aplicativo de gestión de usuarios en el servidor de dominio - Definir un protocolo y procedimiento documentado para las altas, bajas y cambios de usuarios -
26	Implementar un procedimiento de control de accesos a las aplicaciones, base de datos y recursos informáticos	- Elaborar un inventario usuarios de TI - Elaborar el mapa de accesos por usuario - Configurar los niveles y privilegios de acceso de cada usuario a las aplicaciones, base de datos y recursos informáticos, en el aplicativo de gestión de usuarios en el servidor de dominio - Elaborar una bitácora de registro y seguimiento de las acciones del usuario desde su logueo
27	Elaborar instructivos de buen uso de los equipos terminales	- Definir procedimientos de encendido, apagado y mantenimiento de preventivo de equipos - Elaborar instructivos - Sensibilizar a los usuarios
28	Planificar el mantenimiento preventivo de equipos	- Realizar coordinaciones con las diferentes áreas para programar el mantenimiento de equipos de manera periódica - Definir lineamientos para el procedimiento del mantenimiento de computadoras/laptops, impresoras, etc. - Elaborar el programa anual de mantenimiento de equipos terminales
29	Elaborar instructivos para la manipulación de servidores	- Elaborar instructivos y procedimientos técnicos para la revisión y manipulación de los servidores
30	Elaborar un catálogo de proveedores especializados de servicios y repuestos de equipos críticos	- Elaborar el inventario de equipos críticos y sus repuestos - Identificar y coordinar con proveedores especializados - Definir un presupuesto de contingencia para imprevistos con los equipos críticos
31	Evaluar y mejorar instalaciones eléctricas	- Mapear el sistema de instalaciones eléctricas - Identificar puntos críticos de consumo de energía y evaluar su capacidad actual - Identificar debilidades, vulnerabilidades - Identificar zonas peligrosas en el sistema de cableado eléctrico - Corregir, cambiar o mejorar las debilidades y vulnerabilidades del cableado eléctrico
32	Mejorar el sistema antimalware	- Identificar alternativas de sistemas antimalware - Implementar y configurar un servidor dedicado antimalware - Configurar el sistema antimalware para realizar diagnósticos programados
33	Configurar el servidor de dominio para controlar la instalación de aplicaciones no autorizadas	- Identificar perfiles de usuario con privilegios de instalación/desinstalación de aplicaciones - Configurar restricciones de acceso a puertos y lectoras a usuarios sin privilegios de instalación/desinstalación de aplicaciones

34	Implementar mecanismos de control para evitar divulgación de información sensible	- Configurar terminales de trabajo para la activación automática de protectores de pantalla - Sensibilizar al personal en la aplicación de la política de escritorio limpio
35	Implementar un proceso de gestión de cuentas de usuarios y claves	- Definir una política de uso de claves de acceso a los recursos de información - Configurar el control de acceso en el servidor de dominio, para solicitar al usuario el cambio de clave de acceso, con una frecuencia trimestral
36	Elaborar un procedimiento para el inventario de hardware	- Elaborar el inventario de los equipos de cada área - Definir las características técnicas de los equipos inventariados - Asignar responsabilidades de uso, mantenimiento y seguridad de los equipos inventariados - Estimar la vida útil de los equipos inventariados - Definir el procedimiento de actualización del inventario - Elaborar un Plan de renovación de equipos
37	Implementar controles de acceso físico a zonas seguras y restringidas	- Identificar zonas seguras y de acceso restringido - Identificar al personal con privilegios de acceso a zonas seguras y restringidas, asignándoles los permisos correspondientes - Generar una bitácora de registro de las entradas a las zonas seguras y restringidas - Elaborar el protocolo de autorización a zonas seguras y restringidas del personal no autorizado
38	Mejorar el sistema de protección contra incendios	- Planificar la adquisición de extintores - Evaluar el estado de los extintores existentes: presión, rajaduras, etc. con la finalidad de certificarlos - Instalar los extintores y rotular su ubicación en zonas de fácil acceso - Capacitar al personal en el uso de extintores - Asignar responsabilidades del uso de extintores en caso de un evento de incendio no controlado
39	Mejorar el sistema de climatización del área de servidores	- Evaluar la capacidad del sistema de aire acondicionado actual - Evaluar la posibilidad de adquirir un sistema de aire acondicionado de precisión
40	Mejorar los sistemas UPS	- Calcular la capacidad de los UPS en base a la identificación de los equipos y servicios que deben ser abastecidos de energía en caso de caída del fluido eléctrico principal - Evaluar los UPS existentes en relación a su autonomía y capacidad - Identificar los UPS que no cumplen con los requerimientos de autonomía y capacidad - Planificar la adquisición de 3 UPS

Fuente: Desarrollo propio

4.2.7. Evaluación del modelo de gestión de riesgos

Objetivo del juicio de expertos

Verificar la validez del modelo de gestión de riesgos propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los criterios de cumplimiento de las normas ISO/IEC 27005, la metodología Magerit.

Selección de expertos

Para la selección de los expertos se establecieron los siguientes criterios:

a. Tener formación en áreas afines al tema de investigación
b. Tener experiencia en el tema de gestión de riesgos o en gestión de proyectos de desarrollo de software
c. Tener mínimo cinco (05) años de experiencia profesional

El número de expertos seleccionados fueron dos (02), los que fueron seleccionados. Los expertos externos se detallan a continuación:

Tabla N° 46. Identificación de expertos para la evaluación del modelo de gestión de riesgos propuesto

	Experto 1	**Experto 2**
Nombres y Apellidos	Martín Ampuero Pasco	Oscar Zocón Alva
Formación académica	- Ingeniería en Computación e Informática - Maestro en ciencias con mención en Informática y Sistemas	- Ingeniero de Computación y Sistemas - Maestro en Ingeniería de Sistemas
Área de experiencia profesional	- Especialización en Gestión de Proyectos - Consultor Senior en Desarrollo de Software	- Certificación ITIL - Auditor Interno ISO 27001:2007 - Especialización en Dirección de Proyectos y Calidad PMI
Tiempo de experiencia	18 años	22 años
Cargo actual	- Gerente General de la empresa de desarrollo de software GarzaSoft - Docente Universitario - Proyectista de software	- Docente Universitario - Consultor en seguridad de la información - Consultor en gestión de proyectos PMI
Institución	- Universidad Nacional Pedro Ruiz Gallo - GarzaSoft SAC	- Universidad Nacional de Cajamarca - Independiente

Elaboración y aplicación de cuestionarios

Para la evaluación del modelo se utilizó como instrumento un cuestionario diseñado para recoger la valoración de los expertos a cada uno de los componentes que integran el modelo de gestión de riesgos.

Los componentes evaluados fueron:

Tabla N° 47. Componentes y subcomponentes evaluados en el modelo de gestión de riesgos

Componente	Subcomponente
	Desarrollo del mapeado de los procesos para identificar el alcance del modelo de gestión de riesgos
	Análisis de los procesos del negocio seleccionados en el alcance del modelo de gestión de riesgos
	Identificación y clasificación de los activos de TI en cada proceso de negocio
Evaluación de riesgos	Procedimiento para determinar la criticidad de los activos de TI
	Identificación de las amenazas para cada activo de TI
	Identificación de las vulnerabilidades relacionada a cada amenaza
	Procedimiento y criterios para valorar el impacto de los escenarios de riesgo
	Procedimiento y criterios para valorar la probabilidad de ocurrencia de los escenarios de riesgo
	Cálculo del nivel de riesgo intrínseco
	Establece criterio para definir los rangos de tolerancia o no tolerancia de los niveles de exposición al riesgo
Tratamiento del riesgo	Identificación de los controles existentes para cada escenario de riesgo
	Procedimiento para la estimación de los niveles de riesgo efectivos
	Selección de las estrategias de tratamiento de riesgos
Plan de tratamiento de los riesgos	Definición de actividades de seguridad para cada control o mecanismo de seguridad propuesto

Los criterios de valoración de los componentes del modelo propuesto fueron:

- Suficiencia
- Claridad
- Coherencia y
- Relevancia

El sistema de valoración fue una escala cualitativa ordinal de cinco (5) ítems, donde:

- (1) = Muy Malo
- (2) = Malo
- (3) = Regular
- (4) = Bueno
- (5) = Muy Bueno

La siguiente tabla muestra los criterios y el sistema de valoración que se utilizó como referencia para la evaluación del modelo de gestión de seguridad de la información, propuesto.

Tabla N° 48. Criterios y sistema de valoración del modelo de gestión de riesgos

Criterio	Indicador	Valoración				
		Muy malo	Malo	Regular	Bueno	Muy bueno
SUFICIENCIA	Grado de suficiencia del componente para cumplir con sus objetivos como parte de la gestión de la seguridad de la información en la empresa	1	2	3	4	5
CLARIDAD	Nivel de claridad del lenguaje utilizado para describir el componente y que permite su comprensión y entendimiento.	1	2	3	4	5
COHERENCIA	Nivel de coherencia de la(s) relación(es) del componente con otros componentes del modelo, para lograr una gestión de la seguridad de la información de manera integrada.	1	2	3	4	5
RELEVANCIA	Grado de relevancia del componente en el proceso de gestión de seguridad de la información en la empresa.	1	2	3	4	5

Procedimiento para la aplicación de cuestionarios

El procedimiento para la aplicación del cuestionario de evaluación del modelo de gestión de riesgos fue:

a. Contacto y compromiso de los evaluadores. Se estableció contacto con los dos expertos considerados, a través de correo electrónico y luego, vía telefónicamente se coordinó para explicar el procedimiento de aplicación del cuestionario. En el caso del personal de la empresa, el contacto se realizó vía la administración de la empresa, por contar con la autorización para realizar la investigación.
b. Envío del modelo y del instrumento de evaluación. Se seleccionó las partes del informe de tesis que son pertinentes para que los

evaluadores conozcan el modelo propuesto, generándose un archivo pdf, denominado “modelo.pdf”. Luego se envió vía correo electrónico el modelo, conjuntamente con el instrumento de evaluación (cuestionario). Los evaluadores tuvieron dos (2) semanas para leer el modelo y evaluarlo.

c. Finalmente, se consolidó los resultados de los dos cuestionarios recibidos en cuadro, con la finalidad de obtener el promedio de las valoraciones en cada componente.

Resultados de la evaluación del modelo

Tabla N° 49. Resultados de la evaluación del modelo de gestión de riesgos, por juicio de expertos

Componente	Subcomponente	Experto	Criterios			
			Suficiencia	Claridad	Coherencia	Relevancia
Alcance del modelo	Descripción del contexto para identificar necesidades de la seguridad de la información en la empresa	Experto 1	4	4	5	5
		Experto 2	4	5	5	5
		Promedio	**4.0**	**4.5**	**5.0**	**5.0**
	Desarrollo del mapeado de los procesos para identificar el alcance del modelo de gestión de riesgos	Experto 1	3	4	4	4
		Experto 2	4	5	4	5
		Promedio	**3.5**	**4.5**	**4.0**	**4.5**
	Análisis de los procesos del negocio seleccionados en el alcance del modelo de gestión de riesgos	Experto 1	4	4	4	4
		Experto 2	5	4	4	5
		Promedio	**4.5**	**4.0**	**4.0**	**4.5**
	Identificación y clasificación de los activos de TI en cada proceso de negocio	Experto 1	4	5	4	5
		Experto 2	5	5	5	5
		Promedio	**4.5**	**5.0**	**4.5**	**5.0**
Evaluación de riesgos	Procedimiento para determinar la criticidad de los activos de TI	Experto 1	5	5	4	5
		Experto 2	5	5	5	5
		Promedio	**5.0**	**5.0**	**4.5**	**5.0**

	Identificación de las amenazas para cada activo	Experto 1	4	4	4	4
		Experto 2	4	4	5	5
		Promedio	**4.0**	**4.0**	**4.5**	**4.5**
	Identificación de las vulnerabilidades relacionada a cada amenaza	Experto 1	4	4	4	4
		Experto 2	4	4	5	5
		Promedio	**4.0**	**4.0**	**4.5**	**4.5**
	Procedimiento y criterios para valorar el impacto de los escenarios de riesgo	Experto 1	5	5	5	5
		Experto 2	5	5	5	5
		Promedio	**5.0**	**5.0**	**5.0**	**5.0**
	Procedimiento y criterios para valorar la probabilidad de ocurrencia de los escenarios de riesgo	Experto 1	5	5	5	5
		Experto 2	5	5	5	5
		Promedio	**5.0**	**5.0**	**5.0**	**5.0**
	Cálculo del nivel de riesgo intrínseco	Experto 1	5	5	5	4
		Experto 2	5	5	5	5
		Promedio	**5.0**	**5.0**	**5.0**	**4.5**
	Establece criterio para definir los rangos de tolerancia o no tolerancia de los niveles de exposición al riesgo	Experto 1	5	5	5	5
		Experto 2	5	5	5	5
		Promedio	**5.0**	**5.0**	**5.0**	**5.0**
Tratamiento del riesgo	Identificación de los controles existentes para cada escenario de riesgo	Experto 1	4	4	3	4
		Experto 2	4	4	4	4
		Promedio	**4.0**	**4.0**	**3.5**	**4.0**
	Procedimiento para la estimación de los niveles de riesgo efectivos	Experto 1	4	4	4	4
		Experto 2	5	5	4	4
		Promedio	**4.5**	**4.5**	**4.0**	**4.0**
	Selección de las estrategias de tratamiento de riesgos	Experto 1	4	4	4	4
		Experto 2	5	5	4	4
		Promedio	**4.5**	**4.5**	**4.0**	**4.0**

Plan de tratamiento de riesgos	Definición de actividades de seguridad para cada control o mecanismo de seguridad propuesto	Experto 1	5	4	5	4
		Experto 2	5	5	5	5
		Promedio	**5.0**	**4.5**	**5.0**	**4.5**
Promedio General			**4.5**	**4.6**	**4.5**	**4.7**

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El diagnóstico de la industria del software en la ciudad de Chiclayo, antes de del desarrollo de la propuesta del modelo de gestión de riesgos, es una actividad esencial e importante en el logro de los objetivos, por cuanto permite identificar las reales debilidades de las empresas del rubro en relación a la gestión de la seguridad de TI, variable importante para generar ventaja competitiva. Los resultados del diagnóstico realizado nos permitieron evidenciar que es lo que se tiene que mejorar, específicamente en los aspectos de gestión de los problemas de seguridad, como: accesos lógicos a las aplicaciones, sobre todo cuando son concurrentes, las malas estimaciones de las capacidades asignadas, caídas de los servicios, desconfiguración del software de gestión y errores de conexión a la base de datos; debido a que esta situación podría provocar en el futuro problemas en la prestación de los servicios, aumento de las reclamaciones por la caída de la imagen de la empresa y la huida de clientes, que repercutiría directamente en la economía del negocio

2. De acuerdo a los requisitos de la norma ISO/IEC 27001, la definición del alcance del SGR es importante porque identifica los procesos que serán considerados en la implementación del nuevo SGR. Debe tenerse en cuenta que, la norma no certifica a toda la empresa, si no a ciertos procesos claves del negocio, que están directamente relacionados con el giro del negocio. La estrategia utilizada para identificar los procesos clave del negocio, mediante el mapeado de procesos, permitió identificar, que los procesos considerados en el alcance del SGR son los que están directamente relacionados con el desarrollo de software, como son los procesos de las áreas de Desarrollo de Software y la de Producción y Soporte. Para cada uno de estos procesos se identificaron los activos de información y los activos de TI clave, que deberán ser protegidos, clasificándolos en: Información, Hardware y Software.

3. Se propuso un marco metodológico para el análisis y tratamiento de los riesgos identificados para cada activo de TI. Esta metodología se elaboró considerando las buenas prácticas de la ISO/IEC 27005 y la metodología Magerit, lográndose construir una secuencia lógica de pasos que permitieron identificar el nivel de criticidad de los activos, definir los escenarios de riesgos para cada activo a través

de la identificación de sus amenazas y vulnerabilidades, valorar su nivel de exposición al riesgo con la estimación de sus impactos y probabilidades de ocurrencia; así como su correspondiente niveles de riesgo; y por último, la estrategia de implementación de los controles utilizando como referencia la norma ISO/IEC 27002 para la etapa de tratamiento de los niveles de riesgo no tolerables.

4. Para la implementación de los controles se propusieron un conjunto de procedimientos como mecanismos de seguridad o controles, con sus correspondientes actividades para su implementación. Esta propuesta de mecanismos de control se realizó previo análisis de aplicabilidad de los controles para evitar el desgaste de esfuerzos o gastos innecesarios en la implementación de controles que no son necesarios.

5. El modelo de gestión de riesgos propuesto fue puesto a consideración de dos expertos, los cuales, mediante sus valoraciones de los cuatro criterios evaluados, como son: Suficiencia, Claridad, Coherencia y Relevancia, determinaron que la propuesta cumple los criterios mencionados, por lo tanto, podría pasar a la fase de su implementación en la empresa.

Recomendaciones

1. La metodología para el análisis y tratamiento de riesgos abarca los componentes principales de la gestión de riesgos, como son: activos de TI, amenazas, vulnerabilidades, impactos, probabilidad de ocurrencia y niveles de riesgos. Sin embargo, existen marcos de referencia que proponen otros componentes que podrían ser considerados en otros estudios para mejorar el modelo propuesto.

2. Esta investigación no abarca los aspectos de ciber riesgos. La gestión de ciber riesgos utiliza otras estrategias de análisis e implementación de controles. Por ello, se recomienda otros estudios para reforzar el modelo propuesto.

BIBLIOGRAFÍA

Alexander, A., & AMBCI. (2012). *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012.* Recuperado el Agosto de 2019, de http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

Avison, D., & Fitzgerald, G. (1995). *Information Systems Development: Methodologies, Techniques and Tools* (2da ed. ed.). Maidenhead, England: McGraw Hill.

Ballefín, S. (2017). Métodos de gestión de riesgos en proyectos de software. *Tesis de maestría*. Uruguay: Universidad de la República Oriental del Uruguay.

Benavides, R. A. (2012). Curso a distancia sobre el gobierno de tecnologías de información y continuidad del negocio. México.

BSI GROUP. (2015). *Lineamientos para la implementación de las Normas ISO 9001 y ISO 22301 en las organizaciones.* Recuperado el Agosto de 2019, de Sitio Web oficial de BSI: http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

Business Continuity Institute. (2018). BCI continuity and resilience report. Everbridge.

Cardoza, A., & Guerrero, D. (2016). Comparación de cuatro sistemas de certificación del ámbito de la Dirección de Proyectos. *XV Congreso Internacional de Ingeniería de Proyectos*, (págs. 411 - 428 pp). Huesca, España.

Carrillo, J. (2013). *Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones.* Recuperado el Agosto de 2019, de http://oaji.net/articles/2015/1783-1426290171.pdf

Centro de Coordinación de ITIL UTN FRBA. (s.f.). *Sobre ITIL: Centro de Coordinación de ITIL UTN FRBA*. Obtenido de Centro de Coordinación de ITIL UTN FRBA web site: http://www.cursositil.com.ar/index.php?option=com_content&view=article&id=44&Itemid=53

Chamoun, Y. (2017). *Administración Profesional de Proyectos.* México DF: Mc Graw Hill.

Chavarry Sandoval, C. J. (2012). *Propuesta de modelo ajustado a la gestión de TI/SI Orientado a los servicios basado en el marco de trabajo ITIL, caso de estudio aplicado al departamento de TI/SI de la Universidad de Lambayeque - Perú.* Chiclayo.

de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., & van Bon, J. (2008). *Estrategia del Servicio Basada en ITIL® V3 - Guía de Gestión.* Amersfoort, Holanda: Van Haren Publishing.

De la Cruz Ramírez, A., & Rosas Miguel, R. (2012). Implementación de un sistema service desk basado en ITIL. *Tesis*. México: Universidad Nacional Autónoma de México.

Dewar, W. R. (2011). Mejores Prácticas de Gestión. *Gerenc. Tecnol. Inform.* |, 11.

Ferrer, R. (2011). *Metodología para el diseño de un Plan de recuperación ante desastres O DRP.* Recuperado el Agosto de 2019, de http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_PLAN_RECUPERACION_ANTE_DESASTRES_DRP.pdf

Figuerola, N. (2008). Introducción a ITIL. *Serie Artículos sobre Gestión de IT y Calidad.*, pp. 2.

Gómez Alvarez, J. R. (2012). Implantación de los procesos de gestión de incidentes y gestión de problemas según ITIL v3.0 en el área de tecnologías de información de una entidad financiera. *Tesis*. Lima, Perú: Pontificia Universidad Católica del Perú.

González, J. (2015). Elaboración de un plan de auditoría para evaluación de cumplimiento en sistemas para gestión de la continuidad del negocio basado en la normativa ISO 22301. Costa Rica: Universidad de Costa Rica.

Group APM. (2015). Guía de Análisis y Gestión de Riesgos de Proyectos. Gran Bretaña: Association for Project Management.

Guerrero, G. (2016). Metodología para la gestión de proyectos bajo los lineamientos del Project Management Institute en una empresa del sector eléctrico. Bogotá, Colombia: Universidad Nacional de Colombia.

Harrington, H. (1992). *Mejoramiento de los procesos de la empresa.* Bogotá: McGraw-Hill.

ICONTEC. (2017). NTC- ISO 31000 Gestión del Riesgo, Principios y Directrices. Bogotá, Colombia: Insituto Colombiano de Normas Tecnicas y Certificación.

INDECOPI. (2008). NTP-ISO/IEC 27001. EDI. . Tecnología de la Informacion.Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. *Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual*. Obtenido de Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

Info Q Con. (Febrero de 2019). *Standish Group 2015 Chaos Report*. Obtenido de https://www.infoq.com/articles/standish-chaos-2015

ISACA. (2009). Guía del usuario de COBIT para Gerentes de Servicios. 1.

ISO. (2016). International Standard ISO 21500 Guidance on project management. Suiza: ISO Copyright.

ISO International organization for Standardization. (2016). ISO Guide 73:2009 Risk management -- Vocabulary.

Lozano Sandova, F., & Rodríguez Mejía, K. (2011). Modelo para la implementación de ITIL en una institución universitaria. *Tesis*. Santiago de Cali: Universidad ICESI.

Lucio Nieto, T. d. (2013). *Marco para la definición y adecuación de una service management office en el contexto de los servicios de tecnologías de la información.* Legenés.

Magerit - Libro 1. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciónes Públicas.

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Ministerio de Hacienda y Administraciones Públicas de España.

Martinez, J. (2016). El plan de continuidad de negocio. España: Diaz de Santos.

Medina Cárdenas, Y. C., & Rico Bautista, D. W. (2011). Mejores Prácticas de Gestión. 11.

Muñoz, D., & Cuadros, A. (2017). Comparación de metodologías para la gestión de riesgos en los proyectos de las Pymes. *Revista Ciencias Estratégicas, 25*(38), 319-338 pp.

NTP-ISO/IEC 27001. (2014). *EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.* Lima.

OSI. (2010). *Seguridad de la Sociedad: Sistemas de Continuidad del Negocio – Requisitos.* Obtenido de International Organization for Standardization: https://www.pea.co.th/BCM/DocLib/ISO_22301_2012.pdf

Project Management Institute, Inc. (2016). Guía de los fundamentos para la dirección de proyectos (guía del PMBOK®). *Quinta Ed.* Pensilvania.

Project Management Institute, Inc. (2017). *La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK)* (Sexta edición ed.). Pennsylvania, EEUU.

Ramírez, T., Calderas, R., & Benavides, A. (2012). Curso a distancia sobre el gobierno de tecnologías de información y continuidad del negocio. México.

Ruiz Carreira, M., & Toro Bonilla, M. (2010). *Simulación aplicada a la mejora de los procesos de gestión de servicios ti.* Cadíz, España.

SAE International Group. (2018). AS9100C. Aerospace standard. USA.

Salgueiro, A. (2004). *Como mejorar los procesos y la productividad.* (A. E. Certificación, Ed.) Madrid, España: AENOR.

Sandhusen, R. (2002). *Mercadotecnia* (ISBN 9789702402473 ed.). CECSA (Compañía Editorial CONTINEN).

SISTESEG. (2016). *Business Impact Analysis.* Recuperado el Junio de 2019, de http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.pdf

Spiñeira, Sheldon y Asociados. (2015). *Desarrollo de un plan de continuidad del Negocio: Aplicando un enfoque rápido, económica y efectivo.* Recuperado el julio de 2019, de https://www.pwc.com/ve/es/asesoriagerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf

Stanton, W. J., Etzel, M. J., & Walker, B. J. (2007). *Fundamentos de Marketing* (14 ava edición ed.). Mexico DF, Mexico: McGraw-Hill / Interamericana Editores, S.A.

Thejendra, B. (2014). *thejendra.com*. Recuperado el 2014, de thejendra.com: http://www.thejendra.com/ARTICLES/ITIL.htm

Trischler, W. (2008). *Mejora del valor añadido en los procesos.* Ediciones Gestión 2000.

Ureña, M. (2011). *Sistema de Gestión de Continuidad del Negocio de acuerdo con BS 25999 e ISO 22301.* Recuperado el Agosto de 2019, de http://sasorigin.onstreammedia.com/origin/isaca/LatinCACS/cacslat/forSystemUse/papers/133.pdf

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (. (2008 b). *Diseño del Servicio Basada en ITIL® V3 - Guía de Gestión* (Primera edición ed.). Zaltbommel, Holanda: Van Haren Publishing.

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2008 a). *Estrategia del servicio basada en ITIL v3 - Guia de Gestión* (1 era edición ed.). Amersfoort, Holanda: Van Haren Publishing.

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2008 d). *Operación del Servicio Basada en ITIL® V3 - Guía de Gestión* (Primera edición ed.). Zaltbommel, Holanda: Van Haren Publishing.

Vásquez O., A. (2014). Uso del ciclo de vida de ITIL para la adopción de servicios en la nube para PYMES mexicanas. *Tesis de maestría en administración de servicios de tecnologías de la información*. México: Universidad Iberoamericana.

ANEXOS

ANEXO 1. Guía de entrevista

Introducción de la investigación

La presente entrevista se realiza a responsables de las tecnologías de la información y/o gerentes de sistemas para obtener un diagnóstico de la situación actual de las empresas de desarrollo de software en la ciudad de Chiclayo, a partir de la cual se poder elaborar un modelo de negocio tipo en este sector.

Saludo al entrevistado

Agradecimiento por el tiempo brindado para la entrevista

Explicar el ¿por qué? de la entrevista, y comentar sobre el tema de tesis

Explicar que se investiga sobre la forma actual para llevar el negocio

Introducción del entrevistado

Se menciona el nombre, el título y las razones porque se lo ha considerado para la investigación.

Preguntas

Características generales del negocio

a.1. ¿Qué productos o servicios de software ofrece su empresa?

Nombre	
Descripción rápida de funcionalidad	
En qué empresa está implementado	
Metodología	
Tecnología	

a.2. ¿A qué industria ofrece estos productos o servicios?

a.3. ¿Cuál es el perfil de sus clientes?

a. Pequeñas empresas
b. Medianas empresas
c. Grandes empresas
d. Empresas Internacionales

a.4. ¿Cuáles son las necesidades de sus clientes?

a.5. ¿Qué tan rentable resulta su actual modelo de negocio? ¿Cómo era el negocio en los primeros años?

a.6. ¿Quiénes son sus socios y clientes estratégicos?

a.7. ¿Cuál es el mecanismo de cobro que maneja con sus clientes?

a.8. ¿Qué le haría cambiar su forma de trabajar?

a.9. ¿Cómo mide el nivel de satisfacción de sus clientes?

Producto o servicio ofrecidos

b.1. ¿Cuáles son las características de sus productos?

b.2. ¿Qué tipo de licenciamiento ofrecen? ¿Qué sucede con el código fuente?

b.3. ¿Cuál es la propuesta de valor por la que sus clientes están dispuestos a pagar?

b.4. ¿Cuáles son los recursos que utiliza para generar valor?

b.5. ¿Su empresa ha incursionado en SAAS? ¿Cuáles de sus productos podrían ser ofrecidos como servicio? ¿Ha sido solicitado este tipo de distribución por sus clientes?

Formas de gestión de los proyectos de software

e.1. ¿Cuál es la forma de cobranza? ¿Qué estrategias de comercialización aplica?

e.2. ¿Cuál cree que es la ventaja de sus productos frente a la competencia?

e.3. ¿Es rentable este modelo de negocio?

e.4. ¿Mantiene socios estratégicos?

e.5. ¿Con qué infraestructura tecnológica cuenta, en relación al hardware y al software?

e.6. ¿Con qué personal cuenta? ¡cómo es su modalidad de trabajo en la empresa?¡De qué manera mejora las capacidades de su RRHH dedicado al desarrollo de software, en la empresa?

Problemas comunes en la gestión de proyectos

c.1. ¿Cuáles son los principales gastos de su forma de trabajar y cuales implican mayor inversión?

c.2. ¿Cuáles son los problemas más comunes o riesgo que enfrenta en el desarrollo de sus actividades?

Perfil del entrevistado

f.1. ¿Años de experiencia?

f.2. ¿Cargos desempeñados?

f.3. ¿Cargo en la empresa actual?

ANEXO N° 2: Encuesta para la validación del modelo de gestión de riesgos propuesto

Componente	Subcomponente	Criterios			
		Suficiencia	Claridad	Coherencia	Relevancia
Alcance del modelo	Descripción del contexto para identificar necesidades de la seguridad de la información en la empresa				
	Desarrollo del mapeado de los procesos para identificar el alcance del modelo de gestión de riesgos				
	Análisis de los procesos del negocio seleccionados en el alcance del modelo de gestión de riesgos				
	Identificación y clasificación de los activos de TI en cada proceso de negocio				
Evaluación de riesgos	Procedimiento para determinar la criticidad de los activos de TI				
	Identificación de las amenazas para cada activo				
	Identificación de las vulnerabilidades relacionada a cada amenaza				
	Procedimiento y criterios para valorar el impacto de los escenarios de riesgo				
	Procedimiento y criterios para valorar la probabilidad de ocurrencia de los escenarios de riesgo				
	Cálculo del nivel de riesgo intrínseco				
	Establece criterio para definir los rangos de tolerancia o no tolerancia de los niveles de exposición al riesgo				
Tratamiento del riesgo	Identificación de los controles existentes para cada escenario de riesgo				
	Procedimiento para la estimación de los niveles de riesgo efectivos				
	Selección de las estrategias de tratamiento de riesgos				
Plan de tratamiento de riesgos	Definición de actividades de seguridad para cada control o mecanismo de seguridad propuesto				

ANEXO N° 3: Formato para el análisis de riesgos operativos de TI

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los activos tecnológicos.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado		
Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje		
Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)		
Errores de configuración		
Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)		
Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)		
Mantenimiento		
Robo		
Afectación por virus		

II. BASE DE DATOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Copia no autorizada de o a un medio de datos externos		
Errores de software (motor y contenedor de base de datos)		
Falta de espacio de almacenamiento		
Pérdida o falla de backups		
Pérdida de confidencialidad en datos privados y de sistema		
Directorios compartidos		
Sabotaje		
Afectación de virus		

III. SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Aplicaciones sin licencias		
Error de configuración		
Mala Administración de control de accesos		
Pérdida de datos		
Afectación de virus		

IV. BACKUP (SISTEMA DE RESPALDO)

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Copia no autorizada del backup		
Errores de software para recuperación de información de backup (restore)		
Falla o deterioro del medio de almacenamiento externo del backup		
Falta de espacio de almacenamiento		
Mala integridad de los datos resguardados al recuperar la información de un backup		
Medios de datos no están disponibles cuando son necesarios		
Pérdida o robo de backups		
Sabotaje		

V. CABLEADO Y CONCENTRADORES

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)		
Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros)		
Factores ambientales		
Accesos no autorizados.		
Longitud de los cables de red excedidos a las normas		

VI. RED

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)		
Configuración inadecuada de componentes de red		
Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)		
Mal uso de servicios de red		

VII. USUARIOS

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado a datos		
Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida		
Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)		
Destrucción negligente de datos por parte de los usuarios		
Documentación deficiente (manual de usuario)		
Entrada sin autorización a ambientes		
Entrenamiento de usuarios inadecuado		
Falta de controles y log de las transacciones realizadas por los usuarios.		
No cumplimiento con las medidas de seguridad del sistema		
Desvinculación del personal con la institución		

VIII. DOCUMENTACIÓN DE LOS SISTEMAS EN PRODUCCIÓN

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Acceso no autorizado a datos de documentación		
Borrado, modificación o revelación desautorizada de información		
Copia no autorizada de un medio de documentación del sistema		
Descripción de archivos y programas inadecuado		
Documentación insuficiente o faltante, en relación a seguridad de la información		
Mantenimiento y actualización inadecuado o ausente de la documentación		

X. SISTEMAS O APLICACIONES INFORMÁTICAS EN PRODUCCIÓN

Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Inadecuada gestión de cambios		
Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)		
Acceso a los programas fuentes no controlado		
Validación en los procesos de captura y registro de transacciones		
Sabotaje (eliminación de programas)		

ANEXO N° 4: Tablas de referencia para la valoración de la criticidad de los activos de TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Fuente: (Magerit, 2012)

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia

	de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración seria del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización
1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

Fuente: (Magerit, 2012)

INFORME DE ORIGINALIDAD DE TESIS

Para	:	**Dra. Tomasa Vallejos Sosa** Directora (e) de la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo
De	:	**Nora Noelia Sernaque Zapata** Alumna de la Maestría en Ingeniería de Sistemas con mención en Gerencia de Tecnología de Información y Gestión del Software.
Asunto	:	**Informe de Originalidad de Tesis**
Fecha	:	**08 de Setiembre de 2021**

Me es grato dirigirme a Usted para saludarle cordialmente y a la vez hacerle llegar el informe de originalidad de la tesis, lo siguiente:

Tesis: **"MODELO PARA LA GESTIÓN DE RIESGOS DE DESARROLLO DE SOFTWARE BAJO LA PERSPECTIVA DE LA GESTIÓN DE PROYECTOS"**

Autora: **Nora Noelia Sernaque Zapata**

Informe de originalidad de Turnitin

Procesado el : 08-sep-2021 21:54 p.m.

Similitud permitida por la Universidad: Hasta el 20%

Plagio permitido por la Universidad: 0.0% de plagio

La presente tesis tiene un margen de similitud de 18%

Adjunto Informe Turnitin de Originalidad

En caso que se demuestre lo contrario, asumo cualquier responsabilidad administrativa sin perjuicio de que se anule este informe y se anule el grado emitido por la Universidad.

FIRMA-TESISTA

Nora Noelia Sernaque Zapata

FIRMA-ASESOR

Dr. Alberto Enrique Samillán Ayala

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Nora Sernaqué
Assignment title:	Informes finales de tesis
Submission title:	Informe final de tesis de maestría
File name:	DesarrolloTesisNoraSernaque.docx
File size:	708.81K
Page count:	148
Word count:	39,079
Character count:	206,276
Submission date:	08-Sep-2021 11:53AM (UTC-0500)
Submission ID:	1643846006

TESIS

Informe final de tesis de maestría

INFORME DE ORIGINALIDAD

18%	17%	2%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

2%

★ repository.udistrital.edu.co

Fuente de Internet

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado