República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil - UTEG

Facultad de Estudios de Postgrado

Tesis en opción al título de Magíster en:

Sistemas de Información Gerencial

Tema de Tesis:

Modelo de Gestión de Seguridad de la Información para Proyectos de TI Basado en ISO 27000 Y Scrum para Entidades de Registro Civil en el Ecuador

Autor:
Ing. Wilmer Germán Sánchez González

Director de Tesis:

Ing. Diana López Armendáriz, Msc.

Junio 2020

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este trabajo de investigación le corresponde exclusivamente al autor; y el patrimonio intelectual del mismo a la “UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL”.

…….

Ing. Wilmer Sánchez González

C.C. 0921770632

DEDICATORIA

Quiero dedicar este trabajo de investigación a mi esposa, mi hija y a mis padres, sin ellos, hoy no sería nada, cultivaron en mí, el deseo de superación y me enseñaron a trabajar y no desmayar ante las adversidades.

AGRADECIMIENTO

Quiero agradecer a Jehová Dios por la oportunidad de estar aquí con vida cumpliendo mi objetivo de desarrollo profesional; a mi madre, por ser un buen ejemplo de que con esfuerzo todo es posible; a mi esposa, por su paciencia y apoyo durante todo este tiempo de estudio.

RESUMEN

Las organizaciones dependen en gran medida de la información digital por eso es importante usar procedimientos que en su aplicación permita resultados favorables de seguridad. Este tema de investigación se basa en el estándar ISO 27000 que permite dar seguridad en la información, siendo de gran utilidad en los últimos años. El uso de esta herramienta ha sido necesario ya que presenta normativas adaptables a todos los procesos internos del área de TI.

La gestión proyectos en las entidades de registro civil en el Ecuador es proceso interno que utiliza información muy importante, tomar a la ligera este proceso sin considerar aplicación de metodologías de seguridad en la información, ocasiona muchos problemas entre ellos el de aspecto monetario.

Acoplar las fases de los proyectos con desarrollo ágil Scrum y los controles de seguridad en la metodología ISO 27000 es una buena práctica que logra dar protección la información utilizada. Mediante revisiones literarias se propone un modelo con variables, dimensiones e indicadores adecuados que permiten mantener la seguridad de la información en todo el ciclo de vida de los proyectos del área de TI.

En el desarrollo de este tema de investigación se usó la técnica de investigación documental que a través de medios como tesis, libros, artículos de metodologías y la ayuda de la técnica de campo que mediante el uso de la herramienta SPSS se analizaron los datos recolectados de las encuestas enviadas a funcionarios de las entidades de registro civil en el Ecuador.

En el resultado de esta investigación, se visualizan falencias que ocurren en la mala gestión de desarrollo de los proyectos y sus fases, así mismo los problemas y riesgos que se presentan por omitir controles de seguridad en la información que fluye dentro de cada proyecto.

Palabras claves: Seguridad en la información, ISO 27000, Gestión de proyectos, desarrollo ágil Scrum, fases del proyecto.

ABSTRACT

Organizations rely heavily on digital information so it is important to use procedures that allow favorable security results in their application. This research topic is based on the ISO 27000 standard that allows information security, being very useful in recent years. The use of this tool has been necessary as it presents regulations adaptable to all internal processes in the IT area.

The management of projects in the civil registry entities in Ecuador is an internal process that uses very important information, taking this process lightly without considering the application of information security methodologies, causing many problems among them the monetary aspect.

Engaging the phases of projects with agile Scrum development and security controls in the ISO 27000 methodology is a good practice that manages to protect the information used. Through literary revisions, a model with appropriate variables, dimensions and indicators is proposed that allow the information security to be maintained throughout the life cycle of IT projects.

In the development of this research topic, the documentary research technique was used that, through media such as these, books, methodologies articles and the help of the field technique that, through the use of the SPSS tool, the data collected from Surveys sent to officials of civil registration entities in Ecuador.

In the result of this investigation, flaws that occur in the mismanagement of project development and its phases are visualized, as well as the problems and risks that arise from omitting security controls on the information that flows within each project.

Keywords: Information security, ISO 27000, Project management, agile Scrum development, phases of the project.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

GLOSARIO DE TÉRMINOS

Sistemas de Información.- Agrupación de datos que se interrelacionan con un objetivo en sí, se los puede administrar, procesar, almacenar, rescatar y distribuir para algún fin en común.

TICs.- Sus siglas corresponden a Tecnología de la información y comunicación, es un conjunto de herramientas que permiten transmitir, procesar y almacenar la información digitalizada.

Vulnerabilidad.- Es la condición de la debilidad en los sistemas informáticos.

Amenazas.- Son aquellas anomalías que pueden afectar el correcto funcionamiento de los sistemas de información tales como spyware, troyanos, gusanos, etc.

Riesgos.- Combinación de circunstancias del entorno organizacional donde hay posibilidad de pérdida de información por descuidos de seguridad, estas pueden ser amenazas o atentados en los sistemas de información.

Gestión de riesgos.- Es una metodología que permite conocer, analizar, valorar, clasificar y mitigar mediante mecanismos de control aquellos posibles sucesos que pongan en peligro la estabilidad de la información.

Seguridad de la información.- En un conjunto de medidas que contribuyen a la prevención y protección de la información para mantener el principio de seguridad de la información.

SGSI.- Sistema de gestión de seguridad de la información, concepto principal que lo conforma la ISO 27001 contribuye a la protección de la información mediante procesos documentados y que son conocidos por todos los integrantes de una organización para ponerlos en práctica.

EGSI.- Es el Esquema Gubernamental de Seguridad de la Información, basado en la norma técnica Ecuatoriana INEN ISO/IEC 27002 y que establece un conjunto de directrices para el SGSI de una organización para una mejora continua.

CID.- Es el acrónimo del principio de seguridad que implica Confidencialidad, Integridad y Disponibilidad en la información organizacional.

ISO 27000.- Es un conjunto de estándares internacionales creadas por un grupo de expertos profesionales que permite asignar seguridad en la información a través de un conjunto de buenas prácticas.

Controles de Seguridad.- Es la supervisión recursiva del cumplimiento de parámetros establecidos mediante las políticas de seguridad de una organización para salvaguardar la información.

Gestión de Proyectos.- Es un conjunto de procedimientos sistemáticos que permite planificar, ejecutar y finalizar de manera ordenada y efectiva un proyecto organizacional.

PMBoK.- Es un instrumento guía desarrollado por el PMI (Project Management Institute) y contiene criterios de buenas prácticas para la gestión o dirección de los proyectos.

SCRUM.- Es una metodología de trabajo ágil que, mediante buenas practicas minimizan los riesgos en el desarrollo de los proyectos organizacionales.

Fases del Proyecto.- Son etapas que contienen un conjunto de tareas y/o actividades su estructura empieza desde el inicio, planificación, ejecución supervisión y cierre del proyecto y que son efectuadas por un conjunto de profesionales.

Políticas de Seguridad.- Son un conjunto de normas documentadas basadas en el apartado ISO 27002 su aplicación contribuye a la seguridad de la información.

Criptografía.- Es una técnica que permite generar claves secretas para proteger accesos a la información de personas no autorizadas.

Modelo.- Es la representación de algo u objeto; es decir, un punto de referencia o muestra que guía a la persona para su imitación.

INTRODUCCIÓN

Como un activo valioso así se ha convertido la información a través del tiempo y en vista de su importancia es necesario asignar procedimientos que contribuyan en protegerla de cualquier peligro o amenaza dentro o fuera del perímetro local.

Toda organización de cualquier naturaleza requiere proteger su información, para lograrlo, es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI), que ayudará a establecer políticas y procedimientos adecuados en relación a los objetivos de la organización (Rienzo A.& Bustamente M, 2018). La existencia de procedimientos que gestionen la seguridad de la información es de gran utilidad en las organizaciones, de hecho se requiere que estén actualizados y bajo constante supervisión, tal forma permitirá que la información mantenga un alto nivel de seguridad.

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. (Francisco Valencia & Mauricio Orozco, 2017) La seguridad no es una responsabilidad netamente del departamento de tecnologías, es un asunto que involucra a todo el personal organizacional y más que todo a aquellos que tienen acceso a dispositivos que procesan tal información.

Las organizaciones deben de brindar el apoyo necesario al departamento de tecnologías para fortalecer las medidas de seguridad en todos los procesos del área, así como los que se efectúan en los demás departamentos. No se debe tomar a la ligera el tema de seguridad de la información, ya que esto implicaría poner en riesgo la información y una mayor probabilidad de que ocurra algún tipo de desastre.

Los riesgos, están presentes en todas las actividades organizacionales, pero cuando algún evento que amenace el logro de los objetivos de la organización se manifiesta, no se debe improvisar posibles soluciones. (Aranguri & Iman & Leon, 2016). Es importante la presencia de mecanismos que ayude a localizar y gestionar riesgos en cada proceso que realice la organización, no es de mucha ayuda que los responsables de la seguridad posean conocimiento parcial de seguridad de la información, el mantener segura la información depende de conocimiento y procedimientos basados en las metodologías propiamente diseñadas para estos fines.

La continuidad de labores de una organización depende de una correcta implementación de un sistema de gestión de seguridad de información que implique políticas y lineamientos basados en una identificación, evaluación y tratamiento de los riesgos tecnológicos respaldado en la aplicación de las ISO 27001:2013 (Indecopi, 2015). El uso de metodologías para evaluar el nivel de seguridad existente en la información de la organización, contribuye a que a futuro se emprendan correctivos necesarios de acuerdo los resultados dados, esto debe ser considerado como una práctica común que no debe de hacerse pasar por alto.

Las amenazas existentes tanto dentro como fuera de las organizaciones, este trabajo de investigación tiene como finalidad presentar un modelo de evaluación de la seguridad de la información en el proceso de gestión de proyectos de TI basándose en la experiencia del uso de metodología realizadas por establecimientos públicos y privados. A la vez para lograrlo es necesario el uso de un procedimiento o marco de trabajo que permita llevar a cabo la elaboración del modelo que se propone en el desarrollo de esta tesis y dar recomendaciones que se adapten al caso.

CAPÍTULO I. MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes de la investigación

La seguridad de la información es una cuestión que preocupa a todas las organizaciones a nivel mundial y con el paso del tiempo, se hace necesario tener al alcance las herramientas que ayuden a dar protección. La presencia de factores que ponen en riesgo la información, es inevitable en todo lugar, de la misma forma debe de existir procedimientos para contrarrestar tales riesgos.

Desde el punto de vista de la seguridad de la información, es imposible garantizar la protección absoluta, cada organización debe definir el nivel necesario de protección en los activos e implementaría controles de gestión de seguridad, que garanticen el nivel de protección. (Dmitrij Olife & Nikolaj Goranin & Arnas Kaceniauskas & Antanas Cenys, 2017). Una organización sin problemas de seguridad, no existe, siempre habrá elementos nocivos que pongan en peligro la información, por eso se debe de mantener procedimientos que gestionen la mejora continua de seguridad.

Mantener segura la información es también un asunto importante en el Ecuador, de hecho un estudio realizado en el año 2017 a 50 organizaciones de diferentes sectores en nuestro país y menciona que hay que trabajar mucho para mantener niveles de seguridad de la información de manera óptima. El 55% falta de presupuesto y/o recursos, un 42% no poseen visibilidad en cuanto a seguridad, un 34% falta de recursos capacitados y competentes, 30% falta de claridad sobre el ámbito de gestión funciones y responsabilidades, 28% falta de apoyo ejecutivo o del negocio, 26% falta de estrategia de seguridad de información, 19% impacto de las nuevas tecnologías y amenazas. (Doloite, 2017). Los resultados muestran que aún existen inconvenientes en establecer una metodología de seguridad para la información, es más estos datos evidencian el desconocimiento que aún persiste en las organizaciones en cuanto a la gestión de la seguridad de la información de

sus procesos, la alta gerencia debe de considerar entre sus prioridades, dar apoyo a este respecto.

De hecho, para las organizaciones en el Ecuador se ha impulsado la adopción procedimientos para proteger la información. Es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva. (Acuerdo Ministerial 166 Registro Oficial, 2013) El gobierno Ecuatoriano ha impulsado a las organizaciones públicas y a las privadas al uso de políticas de seguridad que garanticen control y eficacia en la administración pública, los negocios y comercio electrónico. En vista de aquello se debe de implementar medidas de seguridad en todos los sistemas de información actuales y en los que se pretenden iniciar mediante futuros proyectos.

La información en los servicios que proveen las organizaciones de gobierno a la ciudadanía, dependen de la disponibilidad en los medios tecnológicos y su forma de gestionarlos. La innovación tecnológica a través de los proyectos de TI, permiten una mejor administración de la información en beneficio de los interesados, por eso los proyectos que se emprende deben de contar con procedimientos que contribuyan a la conclusión satisfactoria y que minimicen los riesgos de fracasos.

Las principales causas de fracaso de proyectos según el PMI fueron: 37% falta de objetivos e hitos no definidos o alcanzables para medir el progreso, el 19% mala comunicación entre los que desarrollan el proyecto, 18% falta de comunicación de la gerencia sénior, 14% resistencia de los empleados, 4% otras razones (Project Manangement Institute, 2017). Estos factores conllevan al fracaso de proyectos en su periodo de realización, la presencia de uno o varios de estos elementos, pone en amenaza la estabilidad, la fluidez y atenta en la seguridad y disponibilidad de la información.

Las organizaciones de Registro Civil para mejorar el servicio brindado a la ciudadanía han realizado con el paso del tiempo modernización de la infraestructura tecnológica y la suscripción de convenios interinstitucionales de cooperación.

Y en años recientes, se ha consolidado una imagen de atención ágil y oportuna. El servicio de cedulación, inscripción de nacimiento, matrimonio y defunción, así como la entrega de partidas de nacimiento son los más demandados por el usuario dentro de un amplio abanico de productos y servicios principales que ofrecen estas organizaciones.

La innovación tecnológica en las organizaciones de registro civil es necesaria debido a la criticidad de la información que se administra y vez tras vez se la realiza mediante el desarrollo y funcionamiento de los proyectos realizados en el área de TI.

Tabla 1 Proyectos de TI en los últimos 5 años

Inversión	Descripción
Tipos de Proyectos de TI	• Infraestructura • Seguridad Informática • Desarrollo de software • Mejoras de los procesos • Diseño e implementación de redes informáticas • Otros proyectos de TI

Fuente:https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/buscarProceso.cpe?sg=1#
Elaborado por: El autor

En la **tabla 1** se describen las inversiones en los tipos de proyectos de TI que han realizado en los últimos 5 años las organizaciones de Registro Civil, esta información constan de acuerdo al portal de compras públicas del Ecuador.

1.2. Planteamiento del problema de investigación

La ausencia de normas de seguridad de la información en cualquier tipo de organización, se convierte en una debilidad que puede ser aprovechada por personas mal intencionadas dentro o fuera del perímetro local y como resultado termina en perdida de información valiosa que podría poner en riesgo la estabilidad organizacional.

La Seguridad de la Información en Ecuador todavía no consigue los niveles de reconocimiento a nivel organizacional que tienen otras normas de la misma familia, ISO 9001 y 14001 (Mahecha & Coello, 2016). Nuestro país debe de trabajar mucho para adoptar medidas de protección en la información, la norma ISO 27001:2013 como una metodología para adoptar niveles de seguridad, contribuye a mantener la información a buen recaudo.

Los procedimientos rutinarios que se gestionan en las organizaciones son importantes para la sostenibilidad, el departamento de TI administra aquellos que tienen que ver con la parte tecnológica, uno de estos es la gestión de proyectos que tiene como enfoque la presentación de soluciones en ciclo de desarrollo. Para emprenderlos hay que considerar claramente los objetivos y el impacto que va a tener frente las estrategias de la organización.

Los proyectos de TI se realizan por la necesidad de aprovechar una oportunidad de negocio o para corregir procesos mal gestionados, si se los emprende y finalizan satisfactoriamente se convierten en una ventaja que puede ser aprovechada, de lo contrario la mala gestión o un desempeño deficiente encaminará a pérdidas de todos los recursos que se utilizan.

En encuestas recientes sobre el desempeño de los proyectos realizados, el PMI mostró un 24% termina a tiempo, un 25% concluye dentro del presupuesto, un 33% logran la intención del negocio, un 68% tienen errores en el alcance, 24% considerados un rotundo fracaso (Project Manangement Institute, 2017). Las cifran muestran porcentajes bajos de proyectos que finalizan acorde al tiempo, presupuesto y objetivos, en contraste con aquellos que inician con una mala planificación ocasionando que un porcentaje considerable concluya en fracaso.

La información ha sido un elemento clave en el éxito de los negocios y los proyectos tecnológicos son necesarios para contribuir en el procesamiento y administración de dicha información. Cuando se requiere emprender un proyecto, hay que considerar cuidadosamente la fases de inicio, preparación ejecución y cierre (PMBOK, 2017). Para que los proyectos se desarrollen con desempeño eficiente hay que considerar el uso de procedimientos o metodologías actuales que permitan en el avance de cada entregable, exista la seguridad y se cumpla con los requerimientos establecidos.

La definición de los límites del sistema de una organización para la gestión de la seguridad exige un manejo responsable de los riesgos que persiguen la confidencialidad, integridad y disponibilidad de la información (Flowerday & Tuyikeze, 2016). Los proyectos tecnológicos enfrentan al igual que otros procesos de TI, riesgos en cuanto a la seguridad de la información, este principio debe de plasmarse desde que se planifica y se debe dar seguimiento hasta la etapa de conclusión, para que al final de todo, se mantenga el principio de seguridad de la información.

Síntomas

- Falta de compromiso por parte del equipo de trabajo, personal no dedica esfuerzos para el desarrollo del proyecto (Arteaga & Pazmiño, 2018).

- Falta de recurso humano y personal idóneo, en la realización del proyecto. El número de personas que integran el equipo no es suficiente, o éstos no cuentan con las habilidades que se requieren (Unemi, 2017).

- Falta de seguimiento y control. Los proyectos de TI por lo general significarán grandes cambios a la empresa, y el no darle la debida atención provocara que en una de las instancias, pierda su rumbo y si concluye, se visualizarán los errores (Juan Brito & Jorje Bermeo, 2017).

- Errónea definición del alcance y objetivos, arriesgando la estabilidad de factores importantes el desarrollo del proyecto y sus costos establecidos (Smail, 2017).

Causas

- Desarrollo de requisitos con errores además de las ausencias constantes y poco interés para la realización del proyecto.

- Malestar entre miembros del proyecto debido a la sobreasignación de tareas y/o actividades propias del proyecto.

- Cambios inesperados y forzosos en el transcurso del proyecto, conllevando a volver a trabajar en tareas ya realizadas.

- Extensión o mayor tiempo para la culminación del proyecto, costos nos programados adicionales en cuanto a operativos, monetarios y de tiempo.

Pronóstico

- Producto final con alta probabilidad de fallas de operatividad, sanciones a personal interno o proveedores que participaron en el desarrollo, riesgos de confidencialidad de la información.

- Retrasos en la entrega del proyecto debido a que se editan las actividades ya terminada, así mismo retrasos en el periodo de pruebas.

- Riesgos en el esquema del principio de seguridad de la información en cuanto a disponibilidad e integridad ya que los proyectos no tienen un cierre a tiempo y presentan problemas de funcionalidad.

- Fracaso total del proyecto conllevando a la Intervención forzosa por parte de otros proveedores y adicionando más recursos para su replanteamiento.

1.2.1. Formulación del problema

¿Cómo la norma ISO 27001 permite mejorar la Seguridad de la Información en el proceso de Gestión de Proyectos del Departamento de tecnologías de la información en una organización de Registro Civil en el Ecuador?

1.2.2. Sistematización del problema

- ¿Cómo afecta en el ciclo de vida de cada proyecto la falta de políticas y normas de seguridad de la información?

- ¿Qué impacto genera en los proyectos la falta de seguimiento y control durante el desarrollo del mismo?

- ¿Qué efecto tendría la falta de personal profesional competente para llevar a cabo los proyectos de TI?

- ¿Qué modelo o metodología contribuye a mitigar los problemas existentes de seguridad de la información en los proyectos organizacionales?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar un modelo de seguridad de la información basado en la metodología ISO 27001:2013 en el proceso de gestión de proyectos del departamento de TI siguiendo los lineamientos del marco de trabajo SCRUM para las organizaciones de registro civil en el Ecuador.

1.3.2. Objetivos específicos

- Plantear un esquema de aseguramiento de la información aplicado a las fases del ciclo de vida en los proyectos de TI.

- Describir los problemas que ocasionan la falta de seguimiento y control en los proyectos y cómo afecta a la seguridad de la información.
- Seleccionar adecuadamente los controles ISO 27002:2013 para aplicarlos en cada uno de las fases del proyecto.
- Conocer aquellos factores que entorpecen la fluidez de un proyecto y tomar medidas de seguridad para evadirlos posteriormente.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

La investigación presentada en este documento ayuda a recopilar elementos importantes para realizar un esquema que permita la seguridad en la información cuando se gestionan proyectos en departamento de TI, mediante el uso de la norma internacional ISO 27001:2013, además de presentar las recomendaciones a usar y mitigar los problemas que obstaculizan la fluidez del desarrollo de los proyectos.

Es importante que el sistema de gestión de seguridad de la información sea parte de y se integre con el proceso y gestión general de la estructura de organización además de preservar la confidencialidad, integridad y disponibilidad de la información mediante el proceso de gestión de riesgos dando confianza a las partes interesadas (Norma Tecnica Ecuatoriana INEN, 2017). Esta norma internacional puede ser adaptada las necesidades en cuanto a seguridad que presenten las organizaciones, el estándar ISO/IEC 27001 contribuye a mejorar los procedimientos para gestionar la información y corregir falencias en la administración u operación.

El funcionamiento de cualquier tipo de organización, depende de la disponibilidad de la información, el nivel de protección y de las constantes mejoras de los medios de gestión, para eso los proyectos mediante una adecuada planificación, desarrollo y culminación efectiva, ayudan a mantener tal información a disposición. Establecer niveles de seguridad de la información en la gestión de los

proyectos de TI, es el motivo de este tema de investigación además de conocer las medidas a tomar para una conclusión adecuada.

Los conceptos y teorías expuestos en el marco teórico de este documento identifican las variables cruciales de la investigación, partiendo de la metodología técnica de la ISO 27001:2013 y que pondrá al descubierto en qué y cómo se debe de mejorar como organización.

.

1.4.2. Justificación práctica

Cada organización persigue metas y objetivos mediante las actividades que realizan a su vez el establecimiento de procedimientos de mejora continua contribuye al bienestar y continuidad de todos los procesos internos. El uso de nuevas herramientas tecnológicas sea en equipamiento o mediante nuevos métodos de gestión se convierten en factores de apoyo para la permanencia en un mundo que cada vez se torna más competitivo.

Mediante la misión, como instrumento de la planificación estratégica y la visión como las aspiraciones que tienen las organizaciones, el planteamiento y desarrollo de los proyectos son una forma poner en marcha estos elementos para alcanzar los objetivos propuestos.

La gestión de proyectos es un proceso que ayuda a las organizaciones a efectuar con precisión proyectos que se efectúan en el departamento de TI. El no contar con las suficientes herramientas tecnológicas, conocimiento e insumos claves, conlleva a complicaciones durante todo el proceso de ejecución. Abandonos, replanteamientos de los objetivos, pérdida de tiempo, recursos y poner en riesgos la información que interviene, son situaciones que debe de impulsar a la alta gerencia a no descuidar cuando se tengan proyectos en desarrollo.

Disponer de un modelo que permita encaminar cada proyecto al éxito mediante el análisis de los riesgos y la seguridad de la información, usando metodologías y procedimientos estandarizados, es la base de creación de este tema de

investigación presentando un guía para gestionar proyectos en organizaciones públicas de registro civil cedulación e identificación.

1.5. Marco de referencia de la investigación

1.5.1. Marco teórico

1.5.1.1. Seguridad de la información

Ayuda a dar protección a los sistemas de información de las organizaciones, el tipo de información puede ser de propiedad intelectual, financiera, detalles de empleados o información de terceros (ISO/IEC 27001, 2018). Una organización con un sistema de protección para la información basado en estándares internacionales estará saludable y con estabilidad, sus procesos funcionaran correctamente por el aseguramiento aplicado de forma previa.

El aumento de uso de los sistemas de información ha permitido satisfacer las necesidades de las organizaciones y personas, así mismo aumentó la importancia de la seguridad de la información mediante procedimientos de alto nivel para garantizar la seguridad de la información (Yilmaz & Rustu & Yildiray Yalman, 2016).

Las tecnologías de información, con el paso del tiempo han establecido facilidades de comunicación para todas las personas en los diferentes medios, en vista de aquello es importante que las organizaciones cuiden de la información de los peligros que constantemente están al acecho sea de forma mal intencionada o sin intención.

1.5.1.2. Principios de la seguridad de la información

Cuando se habla de seguridad de la información, es importante conocer el término CID (Confidencialidad, Integridad, Disponibilidad), si no se realiza una correcta gestión de la seguridad con los tres elementos mencionados lo más probable es no

exista una seguridad plena (Cardenas, 2019). Una organización que efectúe procedimientos de seguridad basándose en el principio en mención, tendrá como resultado, una información optima, en buen estado y disponible estará cuando se la requiera. Los principios de la seguridad se describen a continuación:

- **Confidencialidad**: (divulgación no autorizada)

  Privacidad de la información almacenada y procesada en los sistemas informáticos, las herramientas de seguridad deben de proteger de entes no autorizados.

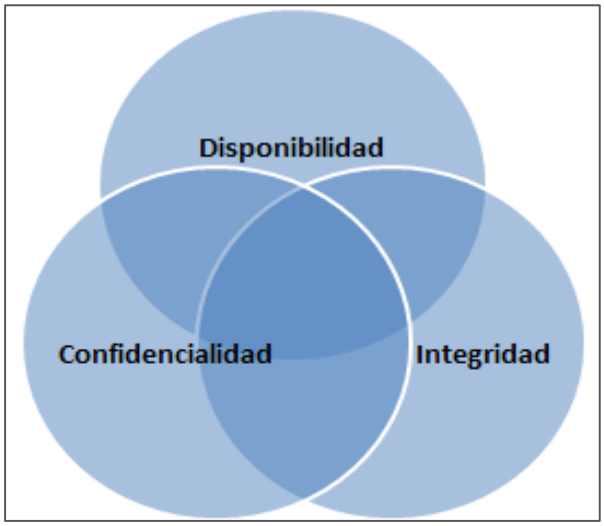
- **Integridad** (modificación o uso indebido no autorizado)

  Validez y consistencia de la información, las medidas de seguridad deben de establecer que los procesos de actualización estén sincronizados y que no se manipulen de forma inadecuada.

- **Disponibilidad** (destrucción o pérdida)

  La información debe de estar siempre accesible y permanente en condiciones adecuadas con estrictas medidas de seguridad para aquellos que desean utilizarla.

Figura 1 Principios de la seguridad de la información



Fuente: *(Cárdenas, 2019)*
Elaborado por: El a*utor*

- **Responsabilidad**
  Asignación de responsables en materia de la información y los sistemas contenedores.

- **Confiabilidad**
  La información que se utiliza debe de ser confiable.

- **Autenticidad**
  La información debe de ser accedida y usada por aquellos que tengan las respectivas credenciales de acceso.

- **No Repudio**
  Nivel de aceptación de una acción cometida entre emisor y receptor.

Para mantener segura la información organizacional, hay que considerar las propiedades fundamentales que debe de cumplir todo sistema (Guamán, 20147). Analizar como interviene cada una de estas propiedades en los sistemas de información, permitirá una mejor gestión de la seguridad con óptimos niveles de protección.

1.5.1.3. Riesgos, amenazas y vulnerabilidades

Riesgos

Las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externas e internas denominados riesgos que surgen durante la consecución de los objetivos (ISO.ORG, 2018). La permanencia y no tratamiento de los riesgos en una organización obstaculizan las actividades comunes, el no gestionarlos debidamente se convertirán en un grave problema y malestar para la organización.

El riesgo es siempre evaluado acorde al impacto adverso en los objetivos organizacionales y la interrupción de las operaciones de la organización (Elizalde,

2018). La verificación de los riesgos, estimar el efecto que puede causar y eliminación total, no permitirá el entorpecimiento de las gestiones organizacionales, más bien ayudara a conocer como se originan, a su vez como mitigarlos.

Vulnerabilidades

Los conceptos de vulnerabilidad y amenaza tienen una relación entre sí haciendo parte de la concepción de la seguridad en distintos ámbitos, las vulnerabilidades son debilidades del sistema o activo informático (Solarte & Enriquez & Benavidez). Las vulnerabilidades se dan en el entorno, con características que propician a que se vuelven susceptibles a una amenaza (Sanchez, 2019). Las vulnerabilidades de un sistema que se perciban y no se atiendan son una puerta abierta para ataques externos, desencadenando en incidentes potencialmente dañinos, afectando la estabilidad de las organizaciones.

Tabla 2 Vulnerabilidades presentes

Área/Lugar	Personas	Medios
• Interna (organización) • Externa (medio ambiente) • Dependencia de partes externas	• Personal interno(empleados) • Personal externo (proveedores)	• Procesos • Rutinas de gestión • Equipos de computo • Software

Fuente: *ISO27001.org*
Elaborado: *Por autor.*

Amenazas

Las amenazas informáticas se refieren a la posibilidad de ocurrencia de algún evento con propiedades anómalas que provoque daño tangible o intangible en cualquier momento sobre los activos de información (Sanchez, 2019). Si se materializan pueden destruir la información o dejar a los sistemas fuera de línea

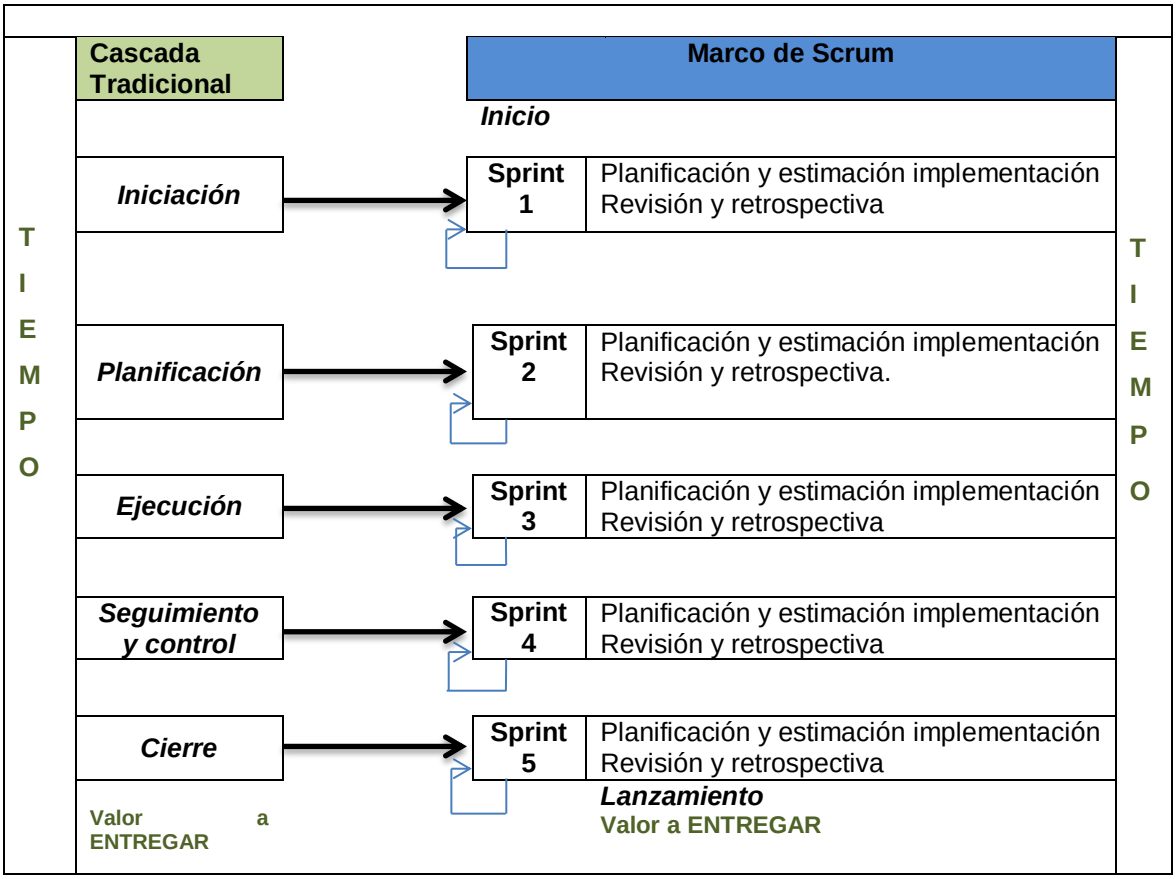
(Mahecha & Coello, 2016). Como son eventos que pueden ocurrir y con desenlace catastrófico, estos males que están al acecho deben de ser vigilados constantemente, los encargados de supervisar el estado de la seguridad de la información harían uso de las herramientas de hardware y software para combatirlas.

1.5.1.4. Los Proyectos en la gestión de TI

Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único, puede involucrar a una persona o a un grupo, así como una sola organización o varias (Guía SBOK, 2016).Los proyectos se han convertido en herramientas claves que surgen para alcanzar los objetivos propuestos de una organización, se los desarrolla acorde a los requerimientos o necesidades y como resultado se obtiene un producto terminado que por lo general tendrá beneficios de la gestión en todo el proceso.
Actualmente han surgido metodologías ágiles para una gestión certera en el desarrollo de los proyectos.

Los proyectos en el campo informático sufrirán ciertas modificaciones enfocadas en la utilización de diferentes metodologías en las fases de: análisis, diseño, desarrollo, implementación y pruebas teniendo como resultado final un producto único (Unemi, 2017). Los proyectos tienen diferentes formas o estados para su desarrollo, debemos de reconocer que cada uno maneja diferente procedimiento en todo el ciclo de vida. En la actualidad existen metodologías de gestión de proyectos como la Guía del PMBOK y SCRUM como un marco de trabajo ágil, presentando pasos que encaminan a cada proyecto a su objetivo.

Figura 2 Ciclo de vida de un proyecto tradicional con Scrum



Fuente: *Scrum study-sbok, (2016), Guía del PMBoK (2017).*
Elaborado por: *El Autor*

El beneficio del desarrollo iterativo (**figura 2)** es que permite la corrección a medida que todas las personas involucradas obtengan una mejor comprensión de lo que se debe entregar como parte del proyecto, e incorporar lo aprendido de manera iterativa, produciendo entregables que se adapten al entorno organizacional (Guía SBOK, 2016). El modelo iterativo permite adaptar cualquier cambio que surja de manera improvisada por parte del o los interesados del proyecto, logrando flexibilidad en el desarrollo y cumpliendo con los entregables de cada fase.

1.5.1.5. Herramientas y elementos para gestionar proyectos

La Gestión de Proyectos se refiere a una serie de conocimientos, habilidades, elementos y técnicas a las tareas necesarias para lograr los objetivos de un

proyecto, facilitan el diseño, estructura, transigencia y la verificación o supervisión necesaria en los integrantes del equipo de trabajo para conseguir resultados extraordinarios a tiempo y que estén dentro del presupuesto.

Las buenas prácticas en la gestión de proyectos, ayuda al éxito de los proyectos organizacionales. Puede llegar a convertirse en una herramienta de trabajo común para el desarrollo donde exista control en tiempo y recursos (Arteaga & Pazmiño, 2018). Utilizar las buenas prácticas para la gestión de proyectos ayuda a que las comunicaciones sean de bilateral entre desarrolladores e interesados, así como la realización de las actividades de forma distribuida o trabajo en equipo. Actualmente existen herramientas que se usan en la gestión de proyectos, saber cuál de estas es la adecuada para la administración y adaptarla a las necesidades, es una tarea a evaluar.

PMBOK

El PMI define los fundamentos para la dirección de proyectos como un término que describe los conocimientos de la profesión de dirección de proyectos. Los fundamentos para la dirección de proyectos incluyen prácticas tradicionales comprobadas y ampliamente utilizadas, así como prácticas innovadoras emergentes para la profesión (PMBOK, 2017). Esta guía es un estándar que recoge una serie de factores y buenas prácticas que permitirán la hacer de la gestión de un proyecto sea más llevadera. Fue creado tras décadas de recopilar experiencias previas de profesionales, limando detalles y añadiendo experiencias aprendidas.

Los proyectos se llevan a cabo en todos los niveles de una organización. Un proyecto puede involucrar a una única persona o a un grupo. Un proyecto puede involucrar a una única unidad de la organización o a múltiples unidades de múltiples organizaciones (PMBOK, 2017). La administración de un proyecto no es sencilla, y dependiendo de las necesidades de la organización se torna aún más compleja, esta guía contiene una serie de pasos a seguir que contribuyen a la gestión de cualquier tipo de proyecto.

Componentes

Los proyectos comprenden varios componentes clave que, cuando se gestionan de forma eficaz, conducen a su conclusión exitosa. Los diversos componentes se interrelacionan unos con otros durante la dirección de un proyecto (PMBOK, 2017). Un proyecto para que se administre de manera eficiente, se debe de utilizar una serie de procesos puntuales para cada una de las fases o etapas: inicio, planificación, ejecución, control y cierre, la aplicación estricta de los procesos del proyecto, lograra encaminar al éxito.

Tabla 3 Componentes de la gestión de proyectos

Componentes claves	Breve descripción
Ciclo de vida del proyecto	Serie de fases que atraviesa un proyecto desde su inicio hasta su conclusión.
Fase del proyecto	Conjunto de actividades del proyecto relacionadas lógicamente que culmina con la finalización de uno o más entregables.
Punto de revisión de fase	Revisión al final de una fase en la que se toma una decisión de continuar a la siguiente fase, continuar con modificaciones o dar por concluido un programa o proyecto
Procesos de la dirección de proyectos	Serie sistemática de actividades dirigidas a producir un resultado final de forma tal que se actuará sobre una o más entradas para crear una o más salidas.
Grupo de procesos de la dirección de proyectos	Agrupamiento lógico de las entradas, herramientas, técnicas y salidas relacionadas con la dirección de proyectos. Los grupos de procesos de la dirección de proyectos incluyen procesos de inicio, planificación, ejecución, monitoreo y control, y cierre. Los grupos de procesos de la dirección de proyectos no son fases del proyecto.
Area de conocimiento de la dirección de proyectos	Area identificada de la dirección de proyectos definida por sus requisitos de conocimientos y que se describe en términos de sus procesos, prácticas, datos iniciales, resultados, herramientas y técnicas que los componen.

Fuente: *PMBOK, 2017*
Elaborado por*: El autor*

Elementos

Los elementos permiten llevar a cabo que se efectúen los trabajos en el tiempo, costos y recursos necesarios, generando productos entregables (PMBOK, 2017). Hay que tener presente que en todo proyecto aparecen cambios inesperados,

desde sus objetivos hasta las especificaciones de producto, saber darles seguimiento mediante los elementos del estándar contribuye a una mejor gestión.

Tabla 4 Elementos de la gestión de proyectos

Elementos	Descripción
Actividades	Es el proceso que consiste en identificar las acciones específicas a ser realizadas para elaborar los entregables del proyecto
Cronograma	Es definir cómo se va a realizar esta gestión de proyecto, lo que incluye la metodología que se usará para planificar los márgenes que se incluirán, el tamaño mínimo y máximo de las tareas, así como las acciones que se va a llevar a cabo para seguir, controlar y corregir posibles desviaciones del objetivo.
Roles	**Interesados del proyecto**: Cliente o la misma organización solicitante **Director del proyecto:** Encargado de la dirección y éxito del proyecto **Equipo del proyecto:** Integrantes que desarrollan el proyecto junto con el Director del proyecto.

Fuente: *PMBOK, 2017*
Elaborado por: *El autor*

Estos cambios deberán retroalimentarse a los procesos de planificación de tal manera que los resultados, sean estos productos o servicios, se vayan dando acorde al plan actualizado y que, al final de la ejecución, tanto el plan como los productos o servicios ofrezcan un resultado homogéneo en su configuración y atributos de calidad.

SCRUM

Desarrollada por Ken Schwaber, Jeff Sutherland y Mike Beedle Es una metodología de adaptación, iterativa, rápida, flexible y eficaz, diseñada para ofrecer un valor significativo de forma rápida en todo el proyecto, garantiza transparencia en la comunicación y crea un ambiente de responsabilidad colectiva y de progreso continuo (Guía SBOK, 2016). Scrum es un marco de trabajo incremental para la elaboración y control de proyectos de cualquier índole, se lo utiliza mucho en la gestión de proyectos de TI, debido a que promueve la creación de entregables e incrementos de un producto en desarrollo.

Roles y Responsabilidades Scrum

Entender los roles y responsabilidades definidos en un proyecto Scrum es muy importante a fin de asegurar la implementación exitosa del método de Scrum (Guía SBOK, 2016). Los roles centrales son elementos directos y necesarios para la elaboración del proyecto, están comprometidos en el desarrollo del mismo ya que se cooperan entre sí para encaminar una culminación exitosa.

Tabla 5 Términos y actividades SCRUM

Categorías-Roles	Funciones
Centrales	• **Propietario del Producto:** Es el profesional que da la cara y toma decisiones para el bienestar del proyecto, emite las ideas junto con el cliente y las coloca en el Product Backlog. • **Scrum Master:** Comprueba que el modelo y metodología funciona, está pendiente que no existan interrupciones. • **Equipo de desarrollo:** Número limitado de personas 5 a 9 que organizan y toman decisiones para lograr el objetivo de cada sprint y las tareas del Backlog.
No centrales	• **Los Socio(s):** Son clientes, usuarios y patrocinadores que interactúan con el equipo Scrum. • **Cuerpo asesoramiento Scrum:** Documentos y/o expertos que definen los objetivos de calidad, seguridad y parámetros claves de la organización. • **Vendedores:** Entes externos que ofertan productos y/o servicios • **Jefe propietario del producto:** Encargado de dirigir varios equipos Scrum. • **Jefe Scrum Master:** Coordina actividades Scrum en proyectos grandes con varios equipos Scrum.

Fuente: *SCRUM Guía-SBOK*
Elaborado por: *El autor*

Bloques de tiempo Scrum

Scrum trata al tiempo como uno de los limitantes más importantes en la gestión de un proyecto, propone la fijación de una cierta cantidad de tiempo para cada proceso y actividad, garantizando que los miembros del Equipo Scrum no ocupen demasiado o muy poco tiempo para un trabajo determinado (Guía SBOK, 2016).

Son las reuniones que se realizan para la asignación de bloques de tiempos en los procesos Scrum, se los estima de acuerdo a tipo de proceso que se vaya a realizar. El propósito de los bloques de tiempo es para no dedicar tiempo en demasía hacia un elemento, o todo el producto proyecto en sí.

Tabla 6 Bloques SCRUM

Bloques y Tiempos	
Bloques de tiempo	• **Sprint**: iteración que dura 6 semanas máximo para la realización de entregables o partes del proyecto. • **Reunión diaria:** espacio de tiempo de 15 minutos para informar el avance del proyecto y considerar lo que se continúa haciendo. • **Planificación del Sprint**: Reuniones para programar cada tarea. • **Seguimiento del Sprint:** Son las reuniones diarias, en las que se evalúa el avance de cada tarea. • **Revisión del Sprint**: Revisión de las agregaciones o los incrementos realizados. • **Reunión de retrospectiva de Sprint**: duración de 4 horas para sprint de un mes, se analiza el sprint anterior y todo lo que conllevo para su realización.

Fuente: *SCRUM Guía-SBOK*
Elaborado por: *El autor*

Lista de pendientes Scrum

El listado de pendiente, son parte de las herramientas elementales para la realización de cualquier proyecto, las iteraciones mediante el Product Backlog, los Sprint y la debida supervisión o seguimiento en todas las fases permite la obtención de los entregables debidamente culminados para la finalización de un proyecto de manera satisfactoria. **Ver tabla 6.**

Tabla 7 Artefactos SCRUM

Artefactos	
Lista de Pendientes	• **Product Backlog:** Lista de Ítems que representa los trabajos que están pendientes, se lo actualiza de forma constante, el propietario del producto determina su desarrollo. • **Sprint Backlog:** Tablero de tareas en donde se ubican de manera física los trabajos a desarrollar en el sprint y su estado. • **Burndown del Sprint:** verificación del progreso total de un sprint y el tiempo restante para finalizar con el sprint, se lo representa mediante gráficas. • **Burndown del producto:** El propietario del producto verifica la velocidad del equipo Scrum en el desarrollo del producto, además constata las entregas de funcionalidades ya probadas.

Fuente: *SCRUM Guía-SBOK*
Elaborado por: *El autor*

Buenas prácticas del PMI y Desarrollo Ágil

PMBOK 6ta edición como una guía de buenas prácticas y SCRUM edición 2016, como un marco de trabajo permiten la gestión eficiente de cualquier tipo de proyecto. El PMI es quien manifiesta que procesos se debe aplicar y con qué nivel de detalle, a la vez que Scrum, es una metodología para el desarrollo ágil de los proyectos.

A continuación se presenta una comparación de la elaboración progresiva del PMI (PMBOK) el desarrollo ágil de Scrum.

Tabla 8 Comparativa de PMBoK y SCRUM

Desarrollo tradicional(PMI)			Scrum (Desarrollo Ágil)		
Fase	**Actividad**	**Herramienta**	**Fase**	**Actividad**	**Herramienta**
Planificación	Definición de Alcance Elaboración de Estructura Desagregada de Trabajo	Definición de Alcance Estructura Desagregada de Trabajo	Product Backlog Review	Revisión del alcance del producto y descomposición en sus partes	Backlog con las características (Features) del producto desagregadas.
Planificación	Definición de actividades	Lista de actividades	Planificación de la Iteración	Revisión del Backlog	Backlog de Producto
	Secuencia de actividades	Diagrama de Precedencia	Planificación de la Iteración	Seleccionar los componentes del Backlog que formarán parte de la iteración.	Backlog de Producto
	Estimación de duración de actividades	Estimaciones de duración de actividades	Planificación de la Iteración	Estimación de esfuerzo para fabricar componentes.	Plan de la iteración
Ejecución	Dirección y Ejecución del Trabajo	Sistema de asignación de tareas	Ejecución de la Iteración	Ejecución de la iteración	El equipo usa el Radiador para seleccionar el trabajo a realizar
Monitoreo y Control	Control de Calidad	Inspecciones	Ejecución de la Iteración	Ejecución de la iteración	El QA trabaja de la mano con desarrollo, construyendo la calidad en el producto.
	Monitoreo y Control (Tiempo y Costo)	Reportes y mediciones de desempeño	Ejecución de la Iteración	Reunión diaria	Burndown
	Control de Riesgos	Registro de Riesgos	Ejecución de la Iteración	Reunión diaria	Lista de Impedimentos
	Verificación de Alcance	Inspecciones	Revisión de la Iteración	Revisión de Producto	Backlog de Producto
	Control de Alcance	Estructura Desagregada de Trabajo	Revisión de la Iteración	Reorganización del Backlog	Backlog de Producto
Cierre de Fase	Cierre de Fase	Lecciones Aprendidas	Retrospectiva	Reunión de Equipo	Lecciones Aprendidas
	Autorizar cierre de fase	Aprobación	Cierre de iteración	Revisión del Backlog	Backlog de Producto.

Fuente: *SCRUM Guía-SBOK*
Elaborado por*: El autor*

Estas herramientas no pueden ser opciones excluyentes, más bien, se complementan gestionando un proyecto y teniendo en cuenta el marco definido en el PMBOK pero aplicando metodologías ágiles para su ejecución.

1.5.1.6. Factores de éxito de los proyectos de TI

Los proyectos se inician para aprovechar oportunidades en la organización que están alineadas con las metas estratégicas. Antes de iniciarlo, a menudo se desarrolla un caso de negocio para definir los objetivos, la inversión requerida, y los criterios financieros y cualitativos para el éxito del proyecto (PMBOK, 2017). Los proyectos aportan beneficios a las organizaciones mediante acciones estratégicas dando cumplimiento a su visión y misión. Estas estrategias impulsan a la creación de proyectos que se ajustaran en cubrir las necesidades que surgen, por eso se debe de considerar los factores que encaminen al éxito y que favorecerán en todo ciclo de vida.

Figura 3 Factores de éxito de proyectos TI

Fuente: *Gestión de proyectos informáticos, UNEMI, 2017*
Elaborado por*: El autor*

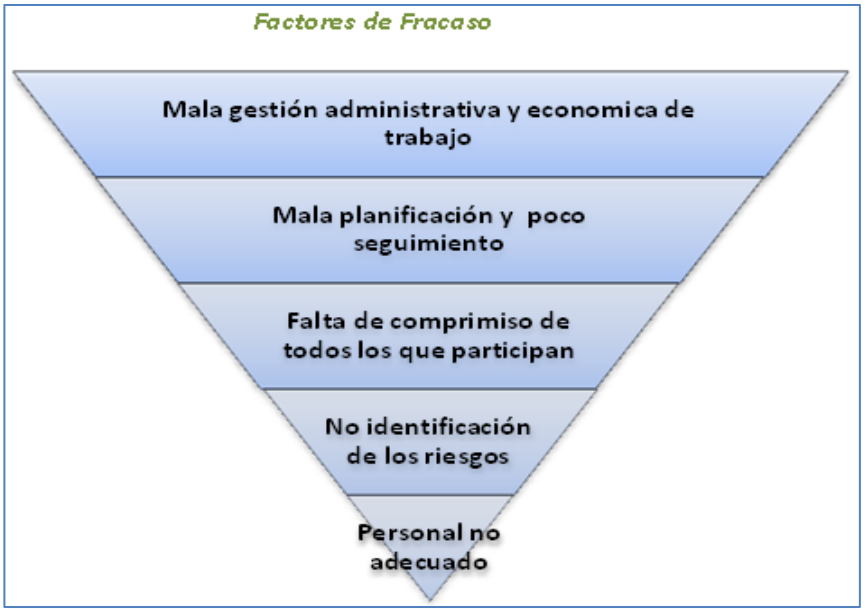
La **figura 3** muestra cada factor para el desarrollo efectivo de los proyectos de TI, desde la supervisión hasta el apoyo de la alta gerencia, son elementos claves a considerar para la culminación eficiente.

1.5.1.7. Factores de fracaso de los proyectos de TI

Un proyecto no puede manejarse a la ligera, necesita de una buena dirección y de personas capaces de resolver problemas que entorpezcan tal gestión. Antes de

comenzar cualquier movimiento dentro de un proyecto es indispensable poner énfasis las posibles actividades críticas y tener preparado un plan ante posibles riesgos o de emergencia (Unemi, 2017). Desde la fase de inicio hasta su conclusión debe existir la responsabilidad de generar un buen desarrollo, todo esto se logra con la cooperación de la organización y que provea constante apoyo para no lidiar con obstáculos durante el tiempo de vida de los proyectos de TI.

Figura 4 Factores de fracaso en proyectos TI



Fuente: *Gestión de proyectos informáticos, UNEMI, 2017*
Elaborado por*: El autor*

Gestionar los proyectos de TI es mucho más complejo que lo tradicional, se necesita un nivel de exigencia respecto al tiempo, costo, equipo humano y calidad (**figura 4**). Su desarrollo genera riesgos mayores en cuanto a factores técnicos y tecnológicos respecto al uso de metodologías, estándares y software cada cierto tiempo.

1.5.1.8. Gestión de la seguridad en los proyectos de TI

El propósito de la gestión de seguridad en proyectos es establecer, identificar, planificar, gestionar las actividades relacionadas en todo el ciclo de vida del

proyecto y gestionar los riesgos de seguridad del producto (De la Cámara, 2015). La identificación y tratamiento oportuna de los riesgos permitirá que no incidan en de forma adversa en cada una de las fases del proyecto, así mismo logrará mantener el esquema de seguridad en la información durante el desarrollo, sin importar el tipo de proyecto que se efectúe.

Los proyectos como parte de la gestión de las TI se los considera elementos claves para la estabilidad y crecimiento de una organización, por tal motivo incluir la seguridad de la información desde la etapa de planificación mediante la gestión de los riesgos, ayudará a que prevalezca el principio de seguridad a todo nivel.

Dado que los riesgos no tienen el mismo origen ni la misma naturaleza, existen varias estrategias para su gestión. Sin embargo, otros factores que inciden significativamente son el tamaño de las organizaciones, su número de integrantes, su estructura, la actividad de producción y el sector en el que operan (ISO.ORG, 2018). La misión de los líderes de proyectos es culminar cada proyecto a su cargo de forma satisfactoria, cumpliendo con el alcance, costo y tiempos definidos y los estándares de calidad necesarios, previamente se tuvo que haber llevado a cabo el proceso de gestión de riesgos.

El proceso de gestión de riesgos en proyectos de TI es:

Tabla 9 Proceso de gestión de riesgos en los proyectos

.	Fases	Acciones
1	**Planificación**	• Definición de las actividades a realizar en el proyecto
2	**Identificación**	Identificación de los riesgos a través de reuniones: • ¿Cómo afecta en el proyecto de TI, al departamento y a la organización? • ¿Cuáles son las fuentes? • Documentación de las características.
3	**Análisis cualitativo**	Priorización de los riesgos individuales para análisis y acción posterior en base a: • Probabilidad de ocurrencia • Impacto
4	**Análisis cuantitativo**	Análisis numérico de cada riesgo identificado. • Efecto que produce en cada proceso • Efecto en los objetivos generales
5	**Planificación de respuesta**	Desarrollo de opciones, selección de estrategias y acciones que se tomaran: • Desaparición de los riesgos

		• Transferencia del riesgo a otra dependencia. • Mitigación: reduce la probabilidad del impacto. • Explotación del riesgo si no tiene efectos adversos. • Aceptación: convivencia si no supone mayor impedimento en los objetivos.
6	**Implementación de respuesta**	Planes acordados para combatir los riesgos.
7	**Monitoreo**	Seguimiento a los riesgos identificados, verificar la existencia de nuevos y gestionarlos.

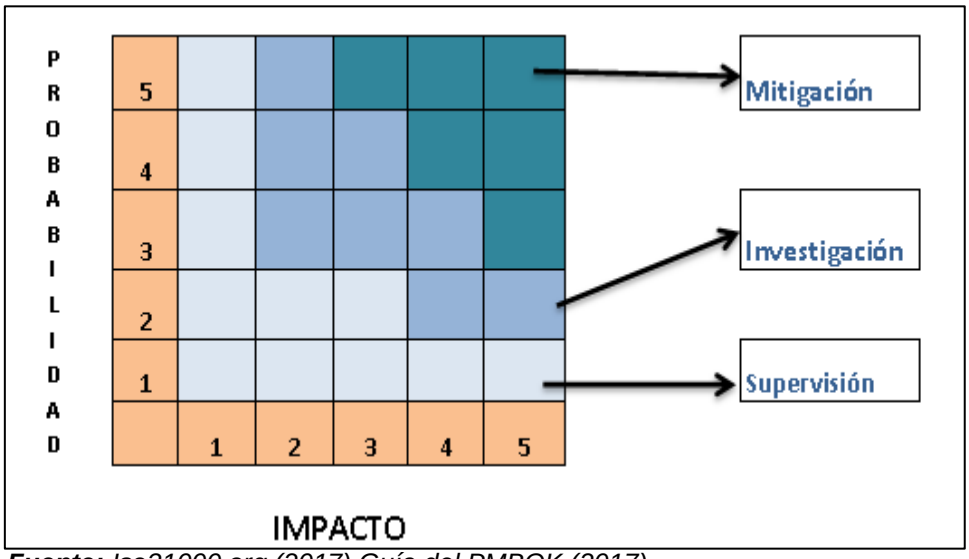
***Elaborado por**: El autor*
***Fuente:** Iso31000.org (2017), guía del PMBoK (2017)*

La **tabla 9** muestra las fases de cómo se debe de efectuar el proceso de gestión de riesgos en los proyectos, este procedimiento basado en la guía del PMBOK contribuye a la realización efectiva de los proyectos, además de darle protección a la información.

Cuando se identifican los riesgos en la fase de análisis, se debe de evaluarlos mediante la valoración a fin de clasificarlos a través de las dos categorías:

- Probabilidad de ocurrencia.
- Nivel de impacto.

Figura 5 Matriz de probabilidad e impacto



***Fuente:** Iso31000.org (2017) Guía del PMBOK (2017)*
***Elaborado por**: El autor*

Al realizar la valoración de la probabilidad y el impacto pueden surgir variaciones según sea la naturaleza del proyecto, los procesos y procedimientos existentes en

la organización, la utilización de esta matriz (**figura 5**) permite verificar, supervisar y mitigar los riesgos inherentes que se localizan en primera instancia.

1.5.1.9. Sistema de Gestión de Seguridad de la Información

El SGSI se lo define como un sistema general aplicable a todos los procesos de una organización para que se cumpla y prevalezca la confidencialidad, integridad y disponibilidad en la información, mediante el planteamiento, análisis y tratamiento de los riesgos (Guamán, 20147). Este sistema debe de estar bajo estricta supervisión de uno o varios responsables expertos en cuanto a seguridad de la información, un SGSI se fundamenta a partir de elementos que contribuyen a la protección contra amenazas.

En la actualidad existen varias herramientas que contribuyen en asegurar la información, la metodología y funcionalidad que poseen están orientadas a la protección a la información, a continuación se describen algunas:

Norma ISO 27000

Es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (ISO/IEC 27000, 2018). Es una norma internacional comúnmente usada debido a lo adaptable que es su aplicación en las organizaciones, ayuda a evaluar e implementar un sistema de seguridad mediante una serie de procedimientos que tienen como fin, proteger la información.

Ventajas de la Norma ISO 27000:

- La norma ISO/IEC 27000 contiene términos y definiciones.
- Para su aplicación de sus estándares, se lo hace con vocabulario definido.

- Describe una visión y vocabulario del SGSI organizacional, haciendo referencia a la familia de la norma.
- Mejores prácticas para la seguridad de la información basado en ISO 27002.
- Especificaciones para desarrollar, implementar y mantener el sistema de gestión de seguridad de la información SGSI basado en la ISO 27001.
- Es adaptable a cualquier tipo de organización.
- Dentro de la familia posee un apartado para la revisión de los riegos en los sistemas de información.

Tabla 10 Estándares ISO 27000

Estándar	Descripción
ISO 27001	• Es la norma principal de la serie • Contiene requisitos para el SGSI • Es certificable • Anexo A, enumera los objetivos de control y controles
ISO 27002	• Es una guía de buenas prácticas • No es certificable • 39 objetivos de control y 133 controles, en 11 dominios
ISO 27003	• Guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI • Especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación. • Describe el proceso de obtención de aprobación por la dirección para implementar un SGSI
ISO 27004	• No es certificable • Es una guía para el desarrollo y utilización de métricas y técnicas de medida. • Determina la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
ISO 27005	• No es certificable • Proporciona directrices para la gestión del riesgo en SI • Aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos
ISO 27006	• Requisitos para los organismos que certifican y registran un SGSI (ISO27001).
ISO 27007	• No es certificable • Guía de Auditoría para un SGSI, basada en ISO 19011
ISO 27008	• No es certificable • Guía de auditoría en el marco de implantación de un SGSI

Fuente: *https://www.iso.org/isoiec-27001-information-security.html*
Elaborado por: *El autor*

La **tabla 10** describe de forma breve cada estándar que compone la familia de la ISO27000, todos tienen como objetivo estructurar un sistema de gestión de seguridad de la información, abarcando todas las etapas para un SGSI.

1.5.1.10. Análisis de riesgos en la Seguridad de la Información

Metodología OCTAVE

Se centra en la evaluación de riesgos ofrece un enfoque alternativo que está específicamente dirigido a los activos de información y su capacidad de recuperación. OCTAVE es auto dirigido en el sentido de que un pequeño equipo de personas de las unidades de negocios y el departamento de TI trabajen juntos para abordar el problema (Tsung-Han Yang & Cheng-Yuan Ku & Man-Nung Liu, 2016). Es un proceso que a través de los activos de información busca conocer los riesgos presenta la organización y que daños ocasionaría si no se los gestiona, es un proceso secuencial ordenado que puede ser administrador por un pequeño grupo de especialista mejorar la seguridad de la información.

Esta metodología posee características que ayudan al análisis de riesgos para la seguridad de TI (ISACA, 2015):

- Identifica riesgos de seguridad que pueden impedir la consecución de los objetivos de la organización
- Define riesgos y amenazas basadas en los activos críticos
- Dirige, gestiona y permite la toma de decisiones de acuerdo a la evaluación de los riesgos
- Protege los activos de información claves
- Contribuye al aseguramiento de la continuidad del negocio
- Permite establecer estrategias de protección para mitigar los riesgos basados en practicas
- Ayuda a la organización a cumplir regulaciones de la seguridad de la información.

Tabla 11 Proceso OCTAVE

	Fase 1	Fase 2	Fase 3
	Vista de la Organización	**Vista Tecnológica**	**Desarrollo del plan y de la Estrategia**
Planificación	• Activos • Amenazas • Practicas actuales • Vulnerabilidades de la organización • Cumplimiento	• Identificación de las vulnerabilidades tecnológicas	• Riesgos • Estrategias de protección • Planes de atenuación

Fuente: *(ISACA.org)*
Elaborado por: *El autor*

La **tabla 11** muestra el proceso OCTAVE en 3 fases para combatir los riesgos comienza, la identificación de los activos que contengan o gestionen la información, sus áreas, el análisis de los riesgos encontrados y por último, planes de mitigación para contrarrestar los riesgos y no afecten a la organización.

Metodología Magerit

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI (Magerit V3, 2015). Esta norma generaliza el uso de las tecnologías de la información, permitiendo realizar un adecuado análisis y evaluación de los riesgos que pueden presentar o presentan, mediante un proceso sistemático de revisión.

MAGERIT persigue los siguientes objetivos (administración electrónica de España (Magerit V3, 2015):

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

El análisis de riesgos propuesto por MAGERIT es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos (Magerit V3, 2015):

Figura 6 Pasos para determinación de riesgos en activos

Fuente: *(Magerit V. 3)*
Elaborado por: *El autor*

Esta metodología (**Figura 6)** se centra primordialmente en los riesgos, posee un enfoque similar al proceso OCTAVE, su procedimiento está basado de manera sistemática para localizar y dar la debida atención a los riesgos existentes y que no se han percibido comúnmente, es usada por varios organismos españoles debido a su facilidad de administración.

Metodología NIST 800-53 R.4

El Laboratorio de Tecnología de la Información (ITL) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía y el bienestar público de los EE. UU. Las responsabilidades de ITL incluyen el desarrollo de normas y

pautas técnicas, físicas, administrativas y de gestión para la seguridad y privacidad rentables de la información confidencial no clasificada en los sistemas informáticos federales (NIST 800-53 R4, 2015). Un modelo de gestión de seguridad de la información basada en procedimientos y procesos técnicos para áreas de tecnologías de la información propiamente, direccionada a las organizaciones estatales y posee lineamientos para proteger la información del uso indebido, no es común el uso de esta metodología por las organizaciones privadas.

Tabla 12 Áreas de Control del NIST 800-53 v.4

Control de Gestión	Control Operacional	Control Técnico
• **Gestión de Riesgos** • **Revisión de controles de seguridad** • **Autorización de trasmisión** • **Ciclo vital**	• Controles de producción • Plan de seguridad del sistema • Personal de seguridad • Seguridad física • Entrada/salida • Planificación y contingencia • Entrenamiento • Conciencia de Seguridad • Integridad de Datos.	• Mantenimiento de Hardware/Software y sistemas • Documentación • Entrenamiento y educación • Capacidad de respuesta a incidentes • Controles de acceso lógico. • Pistas y auditorias.

***Fuente**: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
***Elaborado por**: El autor*

El marco establece las bases para la estandarización en cinco niveles de estado de seguridad, y los adoptantes pueden usarlo para determinar si los cinco niveles están adecuadamente implementados (NIST 800-53 R4, 2015).

- **Nivel 1** - Objetivo de control documentado en una política de seguridad.
- **Nivel 2** - Controles de seguridad documentados como procedimientos.
- **Nivel 3** - Se han implementado procedimientos
- **Nivel 4** - Procedimientos y controles de seguridad se prueban y revisan
- **Nivel 5** - Procedimientos y controles de seguridad están completamente integrados en un programa integral.

Siendo una metodología para la medición de la seguridad de la información, se enfoca en la parte operativa y técnica, de acuerdo a la revisión, se limita a la evaluación de los activos de la organización.

1.5.1.11. Comparativo de Metodologías para la seguridad de la información

A continuación, se presenta una tabla comparativa de metodologías que contribuyen a la seguridad de la información mencionados en el literal anterior. Mediante parámetros de comparación se puede observar que solo la metodología ISO 27001 cumple con todos los parámetros de medición.

Tabla 13 Comparativos de metodologías para gestionar la seguridad en la información

Modelo	Fecha creación de Metodología	Breve descripción del modelo	Parámetros de comparación					
			¿Gestión de riesgos?	¿Permite certificación?	¿Se adapta a cualquier tipo de organización?	¿Permite la evaluación de procesos?	Controles de seguridad a la información	Resultados parámetros
1. ISO 27000	1995	Metodología que permite la implementación de un sistema de gestión de seguridad de la información.	X	X	X	X	X	5
2. OCTAVE	2001	Centrada en la evaluación de riesgos en los activos de información.	X	-	X	-	-	2
3. MAGERIT	2004	Metodología que analiza y gestiona los riesgos y el uso de las tecnologías.	X	-	X	-	-	2
4. NIST 800-53 r4.	2002	Posee normas pautas técnicas para gestionar la seguridad en los sistemas informáticos.	X	-	-	X	X	3

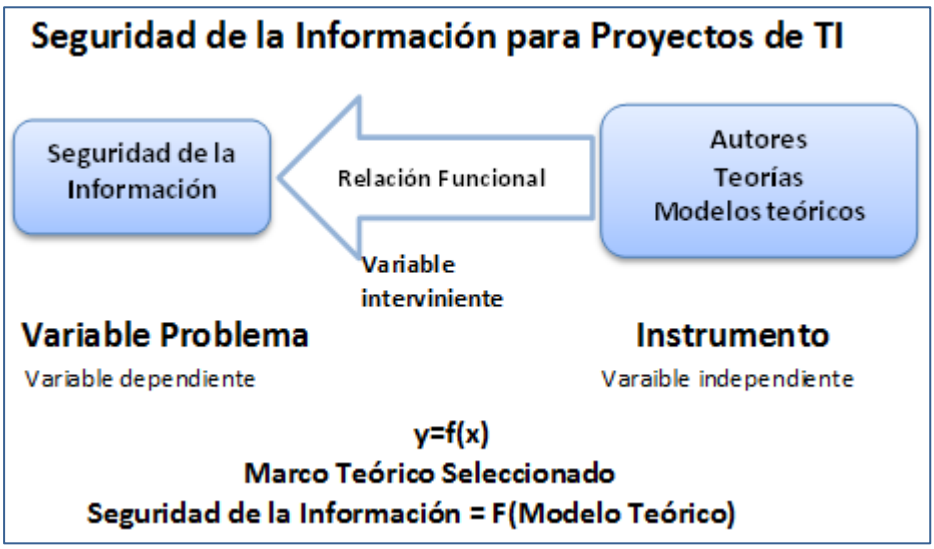
***Fuente**: Marco Teórico*
***Elaborado por**: El autor*

1.5.1.12. Selección de la Metodología para la Seguridad de la Información

De las metodologías en la sección anterior, se ha seleccionado la mejor calificación, en este caso fue en la ISO 27001, que obtuvo la mayor calificación “5 puntos” puesto que cumple con los parámetros de comparación.

Definición del problema de Seguridad de la Información a partir de la utilización de la metodología Seleccionada.

Figura 7 Problemática planteada en el trabajo de investigación



Fuente: *Marco Teórico*
Elaborado por: *El autor*

La expectativa de la ISO 27000 es asegurar que las normas que desarrolla ofrezcan una gran flexibilidad para su aplicación en las organizaciones y éstas mantengan la capacidad para afinar los sistemas de gestión incluso de una forma superior a la norma propiamente dicha (Cardenas, 2019). La normativa describe un enfoque para gestionar la seguridad en la información, debido a la adaptabilidad para aplicarlo en cualquier proceso organizacional, permitiendo una mejor protección a diferencia del uso de la experiencia o procesos rudimentarios.

Se selecciona esta metodología en este tema de investigación debido a que posee un esquema estructurado para establecer un sistema de seguridad para la

información, además de procedimientos para la supervisión, control y cumplimiento de requisitos necesarios para la permanencia de un SGSI.

1.5.1.13. ISO 27000

ISO 27001:2013

Esta Norma Internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización, requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptada a las necesidades de la organización (ISO 27001:2013, 2018). Esta metodología presenta un conjunto de políticas y procedimientos cuyo objetivo es diseñar, implementar y mantener la seguridad de la información, proporcionando una metodología sistemática, documentada y fuertemente enfocada en los riesgos que pueda enfrentar una organización

Es importante que el sistema de gestión de seguridad de la información forme parte de los procesos y la estructura de gestión general de la organización y esté integrado con ellos, y que la seguridad de la información se tenga en cuenta en el diseño de procesos, sistemas de información y controles (ISO/IEC 27001, 2018). La existencia de procesos con finalidades diferentes en la organización permite el funcionamiento de las operaciones o actividades, en vista del uso de información en cada uno de tales procesos, debe de existir la garantía en que la información que fluya sea gestionada con niveles de seguridad.

Controles ISO 27002:2013

Proporciona pautas para los estándares de seguridad de la información organizacional y las prácticas de SGSI, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización (ISO/IEC 27002:2013, 2018). Esta guía conformada

por 14 dominios, 35 objetivos y 114 controles sirve como referencia para la gestión de mejoras en la seguridad de información organizacional.

Tabla 14 Lista de dominios ISO 27002:2013

ID	Dominios
5	Políticas de seguridad
6	Aspectos Organizativos de la seguridad de la información
7	Seguridad ligada a los recursos humanos
8	Gestión de activos
9	Control de acceso
10	Cifrado
11	Seguridad física y ambiental
12	Seguridad de las operaciones
13	Seguridad de las telecomunicaciones
14	Adquisición, desarrollo y mantenimientos de sistemas de información.
15	Relaciones con los proveedores
16	Gestión de incidentes de seguridad de la información
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio
18	Cumplimiento

Fuente: (*ISO27002.org)*
Elaborado por: *Autor*

Este apartado es una herramienta que se debe de usar para ajustar la seguridad de la información en la gestión de proyectos del departamento de TI, luego del análisis y evaluación de los riesgos, se procede con la verificación de que control del grupo de dominios, se debe de aplicar para mitigar los riesgos que se presenten en el desarrollo.

1.5.1.14. Identificación de variables dimensiones e indicadores

Variables

Definir un patrón para procesos de seguridad que facilite la gestión de seguridad en proyectos y que incluya una guía que ayude al usuario a seleccionar los activos

adecuados para la gestión de la seguridad de un determinado proyecto y estructurarlos en el proceso a través del patrón definido (De la Cámara, 2015) .Es importante comprender que factores de seguridad de la información deben de intervenir en las fases del desarrollo de los proyectos de TI, tal conocimiento contribuirá a que la gestión sea segura desde sus inicios hasta la etapa de cierre. Considerar el nivel de protección adecuado para cada tipo de proyecto hará que el ciclo de vida tenga un desenlace con buenos resultados.

Tabla 15 Variables seguridad de la información en proyectos de TI

Variable	Descripción de la Variable
Gobernanza	Conlleva el proceso de controlar y supervisar las políticas de seguridad junto con aquellos procedimientos para poder llevar a cabo la gestión de proyectos de TI mediante sus fases como el Inicio, planificación, ejecución, control y cierre.
Recursos de TI	Son elementos importantes para la organización ya que se los utiliza la realización de los proyectos, se los adquiere con el propósito de la innovación, en el desarrollo para nuevos productos o servicios.
Gestión de Riesgos	Se refiere al proceso de evaluar, analizar y ponderar los riesgos localizados en el desarrollo del proyecto, realizados o efectuados por personal experto y con la debida experiencia en la gestión de proyectos.
Liderazgo	Es la responsabilidad de que cada proyecto en ejecución, inicie y finalice con éxito y que en el ciclo de vida tenga un nivel de desempeño muy eficiente.
Gestión de calidad	Se refiere al soporte económico que asigna la organización para que la gestión de los proyectos cumpla con todos los niveles de calidad, asignando los recursos necesarios como profesionales y la adquisición de equipamiento tecnológico.

Fuente: *Mercedes de la Cámara Delgado, (2015).*
Elaborado por: *El autor*

Dimensiones

La gestión eficaz de la seguridad de los sistemas de información no es una actividad independiente, sino que debe basarse en una estrategia de seguridad bien desarrollada (A. Barton & G. Tejay & M. Lane & S. Terrel, 2016). Para que la seguridad de la información se establezca en los proyectos de TI, debe de estar involucrada toda la organización, siguiendo los lineamientos para robustecer todos los procesos y subprocesos fundamentales de la organización de Registro Civil.

Tabla 16 Dimensiones en la seguridad de la información de proyectos de TI

Criterios	Descripción
Políticas, normas y procedimientos	Se refiere a cumplir y hacer cumplir las reglas o normas de seguridad de la información establecidas para que los proyectos de TI tengan un desarrollo adecuado.
Tecnología	Es el uso de la tecnología de informática disponible, por adquirir y herramientas metodológicas que se van a usar para realizar los proyectos de TI.
Experiencia	Se refiere a la experiencia que poseen los que participan en el desarrollo del proyecto para identificar, analizar, evaluar y mitigar adecuadamente los riesgos en el ciclo de vida.
Responsabilidad	Se trata de que el personal comprenda, acepte y se responsabilice de las acciones efectuadas en el marco de la seguridad de la información.
Desempeño	Como se muestra el personal al efectuar las funciones y tareas principales que exige su cargo en el contexto laboral específico de actuación, lo cual permite demostrar su idoneidad
Financiera	Se enfoca en los requerimientos económicos y financieros de la organización, de tal manera que permita gestionar de forma óptima el uso de recursos asignados en cada proyecto y que al finalizar existan mejoras de la rentabilidad.
Cumplimiento	Se refiere a la medición de los resultados con los objetivos, estándares y normas de la seguridad de la información establecidos al principio del proyecto de TI. A la vez que permite obtener la satisfacción y conformidad de los interesados una vez concluido el proyecto.

Fuente: *Mercedes de la Cámara Delgado, (2015).*
Elaborado por: *El autor*

Indicadores

Lo que se requiere obtener en el modelo propuesto es el uso y aplicación de seguridad en la información para cada proyecto que se gestione, desde su inicio hasta el cierre del mismo, que se han determinado algunos indicadores que coinciden con la problemática de investigación tomados de los artículos científicos relacionados al modelo. A continuación, se enlistan:

Tabla 17 Indicadores de la toma de decisión

Indicadores	
1	Documentación de políticas de seguridad
2	Revisión y actualización de las políticas de seguridad
3	Adquisición de herramientas de TI
4	Metodologías y técnicas de gestión
5	Evaluación de riesgos.
6	Aceptación de funciones
7	Actuación e idoneidad
8	Capacidad financiera
9	Conformidad y satisfacción

Fuente: *Marco Teórico*
Elaborado por*: El autor*

1.5.1.15. Modelo de seguridad de la información en la gestión de proyectos de TI.

Para el desarrollo de este trabajo de investigación, se plantea un modelo de seguridad de la información basado en la metodología ISO 27001 y los controles de 27002, que fusione las variables, dimensiones e indicadores de los artículos seleccionados y que contribuirá a sobrellevar de una mejor forma los proyectos del departamento de TI, el modelo queda de la siguiente manera:

Tabla 18 Modelo de seguridad de la información en proyectos de TI

Variable Dependiente	Variables Independiente	Dimensiones	Indicadores	Ítems
Seguridad de la información	Gobernanza	• Política, normas y procedimientos	• Documentación de políticas de seguridad • Revisión y actualización de las políticas de seguridad	• Se usa documentación de procedimientos y normas de seguridad de la información para todos los procesos y subprocesos de la organización • Se documenta y se usa medidas de seguridad documentadas para la gestión de los proyectos de TI de forma particular • Se revisan y actualizan las normas y procedimientos de seguridad de la información respecto a cada tipo de proyecto de TI gestionado • Las normas y procedimientos de seguridad de la información se basan en reglamentos, normas de gobierno y/o estándares internacionales.
	Recursos de TI	• Tecnología	• Adquisición de Recursos de TI • Metodologías y técnicas de gestión	• Se mejora/innova los procesos de negocio y/o servicios de la organización mediante el uso de tecnología de la actualidad. • La organización cuenta con herramientas para planificar los proyectos de TI • La organización cuenta con metodologías agiles o estándares internacionales para la gestión de los proyectos de TI.
	Gestión de Riesgos	• Experiencia	• Evaluación de los riesgos	• Los participantes cuentan con la suficiente experiencia, capacidad y nivel académico para el desarrollo de los proyectos de TI • Se supervisa el uso de políticas y controles de seguridad de la información cuando se están desarrollando los proyectos de TI. • Se establecen niveles de responsabilidad en base a políticas de seguridad en la información a todos los que

		• Responsabilidad	• Aceptación de funciones	participan en el desarrollo del proyecto de TI. • Los participantes en el desarrollo de proyectos de TI conocen de las responsabilidades que implica el uso de la información de la organización.
	Liderazgo	• Desempeño	• Actuación e idoneidad	• Existe nivel de liderazgo y compromiso en el equipo para gestión de desarrollo de los proyectos de TI. • Se asignan las tareas y/o actividades de los proyectos de TI acorde al nivel de conocimiento de cada empleado participante. • Existe personal externo o proveedores que participan en el desarrollo de los proyectos
	Gestión de la calidad	• Financiera • Cumplimiento	• Capacidad financiera • Conformidad y satisfacción	• El departamento financiero brinda todas las facilidades y apoyo para desarrollar proyectos de TI. • El éxito de cada proyecto de TI depende del departamento financiero • Por lo general, los proyectos de TI culminan acorde a los objetivos y alcance que se plantearon • Se realizan pruebas de funcionamiento y endurecimiento (hardening) en los proyectos de TI culminados antes de su entrega. • Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados.

***Fuente**: Propia*

***Elaborado por:** Autor*

CAPÍTULO II. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de la investigación

2.1.1. Tipo de diseño

En este capítulo se presenta el diseño de la estrategia de la tesis cualitativa, la cual está basada en la recolección de datos a través de herramientas tales como entrevistas y observaciones realizadas con el apoyo de propio investigador como instrumento principal.

El tipo de diseño usado en este tema de investigación es No Experimental, de acuerdo al enfoque se escogió los siguientes tipos de estudio:

- Exploratorio.- Se recopiló información variada teórica para lograr obtener un modelo adecuado y ajustarlo al modelo de seguridad de la información en los proyectos de TI con variables, dimensiones, indicadores e ítems necesarios para analizar el problema de investigación.
- Descriptivo.- Se describen las características de las variables que forman parte de la investigación.

De la misma forma se correlacionó las variables a fin de identificar si existe relación entre ellas, para lo cual se ejecutó la prueba de Chi cuadrado la cual fue contrastada mediante la prueba no paramétrica de Análisis de Correspondencia Simple.

2.1.2. Alcance de la investigación

Este tema de investigación tiene como alcance el análisis y evaluación de aquellos factores que afectan en el éxito de los proyectos que se gestionan en el departamento de TI, debido a la ausencia de un modelo de seguridad de la

información en las organizaciones de registro civil del sector público. En este modelo se han considerado variables, dimensiones indicadores e ítems.

En este tema de investigación no incluye análisis de otros sectores de negocio del Ecuador, ni pretende hacer un estudio de caso de alguna otro tipo de organización en particular.

2.1.3. Enfoque

En este tema de investigación posee un enfoque de carácter cualitativo y cuantitativo. Una combinación que pretender obtener una perspectiva de la realidad de las organizaciones de registro civil cedulación e identificación del Ecuador, en vista de la falta de un modelo de seguridad de la información para gestionar proyectos del departamento de TI y a su vez tengan un desarrollo exitoso.

2.2. Métodos de investigación

Para este tema de investigación se utilizó los siguientes métodos:

- ✓ **Método Cuantitativo.-** Se seleccionó este método para la obtención de datos, con respecto a en la medición numérica y el análisis estadístico de las organizaciones del sector público que permitió conocer su comportamiento.
- ✓ **Método Cualitativo.**- De la misma forma se optó por este método para conocer cuáles son los puntos de vista de los entrevistados, efectuados durante la investigación.
- ✓ **Método Analítico.-** Finalmente se escogió este método para descomponer el objeto de investigación y poder analizarlos en partes, logrando comprender y conocer la problemática de estudio.

2.3. Unidad de Análisis, población y muestra

2.3.1. Unidad de Análisis

Para poder realizar esta investigación y recabar información pertinente y útil, se seleccionó como unidad de análisis a las organizaciones públicas de registro civil cedulación e identificación del Ecuador que están distribuidas a nivel nacional, así como en la ciudad de Guayaquil que en total fueron 224 puntos de atención, en base a este dato se puntualizó la investigación para 142 sitios, de acuerdo al cálculo de la muestra que se verá posteriormente.

2.3.2. Población de estudio

De acuerdo a lo anterior aquellos "puntos de atención" fueron debidamente verificados en cada uno de los sitios de gobierno del Ecuador y gobierno seccional de Guayaquil acerca de entidades de registro civil en el Ecuador existentes.

2.3.3. Tamaño de la muestra

Para el cálculo probabilístico de la muestra se utilizará la fórmula de la población finita que a continuación se indica:

$$\boldsymbol{n = \frac{z^2 Npq}{(N-1)e^2 + z^2 pq}}$$

Dónde:

N- Población total = 224

z- nivel de confianza = 95% coeficiente tabla estadística =1,96

p- Probabilidad de ocurrencia = (0,5)

q- Probabilidad de no ocurrencia (1 – p) = (1 – 0,5) = 0,5

e- Error de muestreo = 5% (0,05)

n- Tamaño de la muestra = ¿?

Tabla 19 Cálculo del tamaño de la muestra

Variable	Resultado
N	224
Z	1,96
p	0,5
q	0,5
e	0,05
n	**142**

Fuente: *Propia*
Elaborado por*: El autor*

2.4. Variables de investigación, operacionalización

Variable dependiente (VP)

Seguridad de la información: Esta variable en la investigación nos ayudará a determinar el nivel de protección de información.

Variable independiente (VI)

- **Gobernanza (VI01)** Variable para ponderar el estado de las políticas, estándares y procedimientos, a través de la ISO27000.
- **Recursos de TI (VI02)** variable que describe el uso de tecnología disponible para el desarrollo de los proyectos, hardware, software y metodologías de gestión.
- **Gestión de riesgos (VI03)** variable que permite medir los riesgos de la organización, supervisión constante para verificar el estado de la seguridad de la información.
- **Liderazgo (VI04)** Variable que permite medir el grado éxito o fracaso en un proyecto de TI, tal medición sirve para conocer las mayores incidencias de los proyectos.
- **Gestión de calidad (VI05)** Variable que contribuye a conocer Se refiere al soporte económico que asigna la organización para que la gestión del proyecto a desarrollar cumpla con los niveles de calidad grupo de personas constituido para el desarrollo del proyecto, con nivel de experticia, conocimientos acorde a la situación.

Variables Empíricas de la variable Independiente (VEVI)

- Gobernanza (VI01)
  - Políticas, normas y procedimientos (VEVI01)
- Recursos de TI (VI02)
  - Tecnología (VEVI02)
- Gestión de riesgos (VI03)
  - Experiencia (VEVI03)
  - Responsabilidad (VEVI04)
- Liderazgo (VI04)
  - Desempeño (VEVI05)
- Gestión de calidad (VI05)
  - Financiera(VEVI06)
  - Cumplimiento (VEVI07)

2.5. Fuentes, técnicas e instrumentos para la recolección de información

Esta investigación es de tipo documental y por este motivo se hace uso de fuentes para el análisis primario de documentos y segundario de organizaciones públicas que posean información similar.

2.5.1. Fuentes

- **Fuente Primaria.-** Información original tomada de medios públicos y que ha sido usada por la persona que investiga, el contenido de la misma no ha sido ni manipulada ni alterada.
- Información de análisis de los proyectos del departamento de TI ejecutados a lo largo de los últimos 3 años.
- Modelos de evaluación de seguridad de la información

- **Fuente Secundaria.-** Información estadística, documental de otros orígenes, diferentes a las fuentes primarias.

- Información de artículos científicos consultados en revistas de alto impacto.
- Información de tesis de maestría y doctorales con temas que han abarcado una problemática similar.
- Información de metodologías y marcos de trabajo para poder realizar este proyecto de investigación.

2.5.2. Técnicas

Las técnicas de recolección de información que se utilizaron para este trabajo de investigación serán:

Técnica Estadística.- Se optó esta técnica en la investigación para poder recabar información del problema presente, para ello, se tomó la información de las páginas de registro civil en el Ecuador, así mismo información de los organismos públicos que poseen información de interés en cuanto al tema de investigación.

Técnica Documental.- Se optó por esta técnica de investigación para obtener información relacionada al tema de investigación con las fuentes primarias y secundarias de las variables independientes: Gobernanza, Recursos, Gestión de Riesgos, Liderazgo y Gestión de calidad.

Técnica de Campo.- En esta investigación se empleó la entrevista como técnica para recabar información acerca del objeto de estudio, en cuanto a la seguridad de la información en el proceso de gestión de proyectos de TI, realizada a un grupo de expertos en el tema a fin con los cargos de: "Directora de Gestión de TI", "Coordinador de Tecnologías de la información", "Consultor de Gestión de Proyectos de TI". Así mismo se realizó encuestas a aquellos profesionales que son miembros de las organizaciones públicas de registro civil y que hayan participado en la gestión de proyectos del departamento de TI.

2.5.3. Instrumentos

Se utilizó como instrumento de recolección de datos:

Investigación Documental.- En esta investigación se utilizó el instrumento documental para la recolección de datos de escritos que guardan relación con el problema presente.

Entrevistas.- Se realizaron entrevistas a varios profesionales con alta experiencia en el desempeño de gestión de proyectos de TI con preguntas para recabar información acerca de la problemática en este tema de investigación.

Encuestas.- Se realizó un formulario con varias preguntas y usando la cuenta personal de formularios Google, donde se ingresaron los ítems y se envió el enlace respectivo a cada profesional a su correo electrónico, en base a la información que está disponible en el sitio web y ubicado en el link de nombre “transparencia”.

Escala aplicada para la evaluación de las variables

Al respecto, (Souza & Porcile, 2009), mencionan que para la evaluación de las variables obtenidas en el modelo se aplicó la Escala de Likert, la cual fue ponderada a través de la escala Fuzzy que permite convertir variables lingüísticas a una escala continua, cuyo fundamento estadístico se establece a través de restricciones difusas que contiene números funcionales soportadas por el índice de Gini-Simpson (H. Vite, 2019).

Tabla 20 Criterios de la escala de Likert

ESCALA	CRITERIO	RANGO		VALORACIÓN
1	Nunca	0%	20%	BAJA
2	Raramente	30%	40%	
3	Ocasionalmente	50%	60%	MEDIA
4	Frecuentemente	70%	80%	MEDIA – ALTA
5	Muy Frecuentemente	90%	100%	ALTA

Fuente: *Vite, 2019*
Elaborado por*: El autor*

Esta valoración permite convertir las 5 categorías de Escala de Likert en datos de tipo cuantitativo, se presenta en la **tabla 20** el rango con las mediciones respectivas.

2.6. Tratamiento de la información

Para el tratamiento de la información obtenida en la investigación, se utilizaron las siguientes herramientas:

- Para el tratamiento de la información de esta investigación, se aplicó la herramienta de IBM SPSS, software en la versión 24(versión de prueba) se usó con el objetivo de conseguir resultados estadísticos, gráficos y tablas que posteriormente permitirá el análisis de las variables que son objeto de investigación.
- Se usó herramientas procesadoras de texto.
- Hojas de cálculo para la creación de gráficos y tablas.

2.7. Aplicabilidad de Seguridad de la Información en Proyectos TI

Las fases de un proyecto representan la evolución de cómo va el producto, desde el concepto hasta la entrega, el crecimiento, la madurez y el retiro, una fase es un conjunto de actividades del proyecto, relacionadas de manera lógica, que culmina

con la finalización de uno o más entregables (PMBOK, 2017). Los proyectos se componen de partes, que pueden ser denominadas subcomponentes, el objetivo de la separación es abarcar un grupo de actividades para su realización en un tiempo estimado y se pueda tener una mejor dirección del mismo, además del análisis, desempeño y como se va desarrollando el proyecto.

Para este modelo de gestión de proyectos de TI aplicando seguridad de la información contiene 5 fases y son:

- Fase 1: Inicio del proyecto.
- Fase 2: Definición y planificación del proyecto de TI.
- Fase 3: Ejecución del proyecto de TI.
- Fase 4: Monitoreo y control del proyecto de TI.
- Fase 5: Cierre del proyecto de TI.

En cada fase se adaptó de forma adecuada los controles ISO 27002:2013, a su vez siguiendo el modelo del estándar de la guía del PMBOK y con la ayuda de la metodología ágil de SCRUM.

2.7.1. Fase 1: Inicio del proyecto.

En esta fase se alienan los objetivos estratégicos de la organización con el propósito del proyecto a desarrollar, además se expone el alcance y el beneficio la participación de los interesados durante el tiempo de vida del proyecto.

Tabla 21 Inicio del Proyecto de TI

Participantes	
Stakeholders (Interesados Claves) **Propietario del Producto(Director del proyecto)**	
Objetivo/Product Backlog_1	**Descripción**
• Presentación de las necesidades y requerimientos (Visión del producto). **(Sprint1_PB1)** • Exposición y alineamiento de los objetivos y el alcance. **(Sprint2_PB1)** • Compromiso de apoyo por parte de la alta gerencia. **(Sprint3_PB1)** • Asignación y gestión del presupuesto**(Sprint4_PB1)** • Presentación y ajustes de la propuesta **(Sprint5_PB1)** • Seleccionar los que intervienen en el desarrollo. **(Sprint6_PB1)**	Autorización formal del inicio del proyecto una vez analizada y documentada, la información con respecto a: participación, influencia, uso de medios/recursos y cómo impactará en la organización el éxito del proyecto.
Controles ISO 27002:2013	
A.5.1.1 Políticas de la seguridad de la información. **A.6.1.5 Seguridad de la información en la gestión de proyectos.** **A.7.1.1 Antecedentes en la contratación** **A.7.1.2 Términos y condiciones de empleo** **A.14.1.1 Análisis de especificaciones de los requisitos de seguridad**	
Consideraciones	
• Como fase de inicio, se deben de realizar reuniones entre los interesados del proyecto y el director para establecer parámetros necesarios en el inicio de cada proyecto que se desee establecer. • De ser necesario comunicar a toda la organización que se va a inicializar un nuevo proyecto ya que puede involucrar uno o varios departamentos. • Plantear y aplicar las políticas internas de seguridad en la información. • Se necesita la colaboración del departamento de RRHH para la revisión de los perfiles profesionales según se requiera.	

Fuente: *Guía del PMBOK, ISO27002.org, SCRUM Guía-SBOK.*
Elaborado por: *El autor*

Desarrollo de la fase I

En esta etapa los **Stakeholders** y el **Propietario del producto** (Profesional con alto nivel de liderazgo y que comanda el proyecto), se reúnen para establecer lo que abarcará el proyecto y como beneficiará a la organización, así como los recursos, instrumentos, herramientas y demás elementos a usarse.

Objetivos/Product Backlog_1 se refiere a las actividades pendientes a realizarse, este elemento cuenta con varios **Sprint [1] hasta [6]** que son todas las tareas que deben de ser revisadas de manera exhaustiva y que permitirán que se complete de todo el **Product Backlog_1**. Cada **Sprint** dependerá de tipo de tarea a completar

y de la agilidad de los que intervienen para concluirla y proveer los **entregables** o partes del proyecto**.**

En el apartado **Controles ISO27002:2013 del cuadro** se encuentra un listado de los controles necesarios para establecer medidas de seguridad en la información, además de puntos importantes a tomar en cuenta durante el desarrollo de esta etapa y que están ubicados en el apartado final de la **tabla 21** con nombre **Consideraciones.**

2.7.1.1. Aplicación de controles ISO 27002 en Fase I

- **A.5.1.1 Políticas de la seguridad de la información**.

  El objetivo de este control es orientar y dar apoyo desde la directiva para asegurar la información, según las reglas del negocio y de acuerdo a las normas locales o leyes pertinentes.
  En este control es necesario que la alta directiva lo apruebe, y debe de socializarse hacia los empleados internos o personal externo como proveedores.

  La política de seguridad debe de contener la siguiente estructura:

  1. Nombre de la organización, información referente al tiempo de creación, actividad económica.
  2. Importancia de la creación del documento y por qué hay que seguir las pautas de seguridad de la información.
  3. Mencionar las medidas correctivas como sanciones o llamados de atención en caso de hacer caso omiso en prestar atención a cumplir con las políticas de seguridad.
  4. De entre los parámetros orientados a los usuarios o personas que tengan acceso a la información se debe de considerar lo siguiente:

     - ✓ Asignación de los activos que operen con información.
     - ✓ Uso solamente de aplicativos con licenciamiento.
     - ✓ Plan de actualización de software, parches de sistemas operativos y herramientas de protección contra amenazas como virus, malware, etc.

- ✓ Uso de herramientas de planificación y software para el desarrollo de los proyectos.
- ✓ Uso de criptografía y generación de claves en todos los medios de TI.
- ✓ Uso de los recursos de TI solamente para asuntos de la organización.
- ✓ Accesos de credenciales tanto físicas como lógicas de acuerdo al cargo y permisos según el rol.
- ✓ Asignación de correo corporativo asignado y uso de forma exclusiva por temas profesionales.
- ✓ Contingencia para salvaguardar la información, tales como medidas de respaldos y sistemas de redundancia eléctrica UPS.
- ✓ Plan de formación y capacitación al personal interno.
- ✓ Un programa de auditorías, como mínimo una vez cada año.
- ✓ Firma de acuerdos de confidencialidad y no divulgación para empleados internos y/o proveedores.
- ✓ Sanciones respectivas por incumplimiento de la aplicación de las políticas de seguridad.

(Referencia. 01 Anexos) posee un modelo de políticas de seguridad que deben de ser revisadas y aprobadas por la alta gerencia para su posterior publicación a empleados y/o proveedores.

- **A.6.1.5 Seguridad de la información en la gestión de proyectos.**

  La seguridad de la información debe de abordarse independientemente del tipo de proyecto que se efectúe, se establece el siguiente proceso:

  - ✓ **Paso 1:** Plantear la necesidad de aplicar mecanismos de seguridad en toda la información que se vaya a utilizar en todas las fases de desarrollo del proyecto.
  - ✓ **Paso 2:** Evaluar los riesgos y su mitigación mediante controles: Identificar y asignar valores a los riesgos asociados mediante el uso de Matrices, tablas y cuadros:
    - Matriz de riesgo básica contiene la siguiente estructura: mención del **proceso,** indagar en los **factores de riesgo** que se pueden suscitar, **origen del riesgo**, **la consecuencia**, **el impacto ("A"=Alto, "M"= Medio, "B"= Bajo)**, **probabilidad de ocurrencia ("A"=Alto, "M"= Medio, "B"= Bajo)**, **y nivel de riesgo inherente** de acuerdo a la ponderación dada entre impacto vs probabilidad de ocurrencia (**Referencia. 02a Anexos**).
    - La matriz de riesgos completa se retroalimenta de la matriz básica permitiendo profundizar en los riesgos evaluados, mediante un mayor análisis hecho con mapas de ponderación entre el impacto y la

probabilidad de que ocurrencia de cada riesgo, a la vez que permite dar seguimiento mediante controles estrictos para su mitigación (**Referencia. 02b Anexos**).

- ✓ **Paso 3** Documentar la integración de la seguridad de la información del **Paso 1 y Paso 2** en el proceso de gestión de proyectos de TI.

De entre los participantes de cada proyecto debe de existir expertos en la gestión de integrar los proyectos con lineamiento de Seguridad en la información.

- **A.71.1. Selección del personal (Empleado / Proveedor)**

Se debe de asegurar que tanto los empleados como los proveedores que vayan a participar en el desarrollo del o los proyectos de TI, sean capaces y confiables en cuanto a asumir sus responsabilidades así como la capacidad de estar aptos para desempeñar los roles asignados:

- ✓ Comprobar de referencias tanto personal como profesional.
- ✓ Comprobar la veracidad de la hoja de vida del postulante.
- ✓ Verificar la autenticidad del nivel académico y de las capacitaciones declaradas.
- ✓ Verificaciones de antecedentes penales, etc.
- ✓ Verificación y comprobar la experiencia y conocimientos declarados.

El personal de Talento humano así como el encargado del departamento de TI o el que ejerza directriz sobre los proyectos de TI de la organización deben de tomar en cuenta lo siguiente:

- **A 7.1.2 Términos y condiciones de empleo**

En este apartado se debe de incluir los contratos realizados para los empleados seleccionados y/o proveedores participantes en el o los proyectos de TI, teniendo en cuenta lo siguiente:

- ✓ Deben de firmar acuerdos de confidencialidad o de no divulgación para acceder a la información requerida y que tiene la siguiente estructura:
  - o El objetivo del acuerdo de confidencialidad y no divulgación.
  - o Las obligaciones del empleado o proveedor.
  - o Vigencia del deber o sigilo profesional.
  - o Las sanciones por el no cumplir con el acuerdo firmado.
  - o Protección de los datos.

- ✓ Deben de estar debidamente informados de las responsabilidades asignadas en cuanto a:
  - Uso de activos.
  - Uso y accesos de instalaciones de procesamiento de la información.
  - Los servicios de información a los que accede.

Tanto a los empleados como los proveedores deben de aplicar los ítems mencionados, en (**Referencia. 06 Anexos**) se encuentra un modelo de documento para este objetivo.

- **A.14.1.1 Análisis de especificaciones de los requisitos de seguridad**

En este apartado se establecen parámetros de seguridad en la etapa de especificaciones y condiciones del sistema a desarrollarse, hay que tener en cuenta las debidas valoraciones de impacto que pueden generar daños potenciales. En cada proyecto se tiene que especificar siguiente:

- ✓ Nombre de la organización.
- ✓ Tipo de proyecto a efectuarse y la razón de su creación.
- ✓ Importancia de cumplir con las medidas de seguridad.
- ✓ Mecanismos para evaluar los riesgos.
- ✓ Gestión de registro de documentos y las responsabilidades de su uso.
- ✓ Seguridad en el control de versión.
- ✓ Repositorio seguro del desarrollo.
- ✓ Validez y gestión de documentos.

Tomar en cuenta estas medidas de seguridad de la información antes del desarrollo del proyecto, mediante valoraciones de impacto ante posibles daños o fallos, logrará ahorro de costes de rediseño (**Referencia. 07 Anexos)**.

Dentro de la documentación que se genera durante esta etapa es importante y necesaria la existencia del Acta de constitución del proyecto, lo cual se lo elabora tomando en cuenta lo siguiente:

- ✓ A partir de las políticas de seguridad previamente planteadas
- ✓ Participantes con sus roles y responsabilidades
- ✓ Los riesgos iniciales percibidos
- ✓ Las necesidades del proyecto a desarrollar
- ✓ Personal encargado que todo el trayecto del proyecto.

En los anexos se encuentra un modelo de acta de constitución del proyecto. (**Referencia**. **08 Anexos).**

2.7.2. Fase 2: Definición y planificación del proyecto de TI

Se definen parámetros encajados a la gestión del proyecto antes de su ejecución, mediante reuniones se concreta el alcance y objetivos, la planificación del desarrollo, exposición y gestión de los riesgos que se podrían presentar procurando tener un menor impacto en el desarrollo del proyecto.

Tabla 22 Definición y planificación del proyecto de TI

Participantes	
Propietario del Producto(Director del proyecto) **Scrum Master(Jefe del proyecto)** **Stakeholders (Interesados del proyecto)**	
Objetivo/ Product Backlog_2	**Descripción**
• Descomposición de las tareas **(Sprint1_PB2)** • Revisión de las dependencias de las tareas**(Sprint2_PB2)** • Asignación de recursos humanos y comunicación del proyecto. **(Sprint3_PB2)** • Estimación y asignación de tiempos**(Sprint4_PB2)** • Gestión de riesgos **(Sprint5_PB2)** • Evaluación e implementación de metodologías técnicas para potenciar la gestión de los proyectos. **(Sprint6_PB2)**	Proporciona un enfoque general de la planificación y definición además contribuye a la creación de una estructura de gestión para todo el proceso de desarrollo usando los recursos y materiales disponibles.
Control ISO 27002:2013	
A.5.1.2 Actualización de las políticas de seguridad de la información. **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.** **A.10.1.1 Política del uso de controles criptográficos.** **A.14.2.1 Política del programa de desarrollo seguro.**	
Consideraciones	
• La gestión de proyecto dependerá mucho del nivel de complejidad en el desarrollo y de todo lo que implique en su realización. • Así mismo un proyecto es un documento formal aprobado por la dirección o alta gerencia, en el cual ya se han definido los objetivos, alcance, acciones necesarias para constituirlo y ordenarlo. • Se debe de documentar detalles de relevancia todos aquellos términos del proyecto, objetivos, requisitos, entregables, limitaciones, asunciones, riesgos e hitos.	

Fuente: *Guía del PMBOK, ISO27002.org, SCRUM Guía-SBOK*
Elaborado por: *El autor*

Descripción de la fase II

En esta etapa Los **Stakeholders**, el **Propietario del producto** y el **Scrum Master**, se reúnen para planificar el proyecto y considerar lo necesario en cuanto desarrollo y el uso de controles de seguridad en la información en las etapas posteriores, permitiendo de esta forma la obtención de resultados favorables en relación a los objetivos del proyecto.

Objetivos/Product Backlog_2 se refiere a las actividades pendientes a realizarse, este elemento cuenta con varios **Sprint [1] hasta [6]** que son todas las tareas que deben de ser revisadas de manera exhaustiva y que permitirán que se complete de todo el **Product Backlog_2**. Cada **Sprint** dependerá de tipo de tarea a completar y de la agilidad de los que intervienen para concluirla y proveer los **entregables** o partes del proyecto**.**

En el apartado **Controles ISO27002:2013 del cuadro** se encuentra un listado de los controles necesarios para establecer medidas de seguridad en la información, además de puntos importantes a tomar en cuenta durante el desarrollo de esta etapa y que están ubicados en el apartado final de la **tabla 22** con nombre **Consideraciones.**

2.7.2.1. Aplicación de controles ISO 27002 en Fase II

- **A.5.1.2 Actualización de las políticas de seguridad de la información.**

  La documentación de políticas de seguridad debe de ser revisada constantemente, es responsabilidad de la organización y de los encargados realizar la actualización considerando lo siguiente:

  - ✓ Plan de actualización establecido por la organización
  - ✓ Las políticas deben de poseer una estructura jerárquica.
  - ✓ Las actualizaciones deben de adaptarse continuamente a las necesidades.
  - ✓ Retroalimentarse de acuerdo a las experiencias de los procesos utilizados o efectuados.

- ✓ Si es necesario la definición de otras políticas departamentales.

En cada proyecto realizado se genera nueva información asociada con hechos positivos o negativos, sirviendo para la retroalimentación de las políticas de seguridad y a su vez experiencias para proyectos futuros.

- **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.**

  Definir, actualizar y comunicar responsabilidades asignadas a los participantes del proyecto siendo estos empleados internos, externos y proveedores. Para cumplir con este requisito de seguridad se debe de considerar lo siguiente:

  - ✓ Poseer un formato o matriz en donde se constate la asignación y aceptación de este requisito.
  - ✓ La herramienta debe de contener un responsable, un aprobador, a quien se consulta y a quien se le informa.
  - ✓ Una sección donde contenga ocupación/actividad para realizar las asignaciones.
  - ✓ Un listado ya definido de los que se van involucrar o participar en el proyecto.

  Una buena gestión de las funciones y las responsabilidades para cada proyecto, contribuye al fortalecimiento de medidas de seguridad en la información que interviene. (**Referencia. 03 Anexos**).

- **A.10.1.1 Política del uso de controles criptográficos.**

  Enfocados en dar protección en el proceso de desarrollo del proyecto, se debe de implementar un sistema de cifrado para bloquear accesos no autorizados permite mantener la integridad de la información.

  La política debe de poseer los siguientes parámetros:

  - ✓ Objetivos y el alcance
  - ✓ Los participantes y sus responsabilidades
  - ✓ Documentación de referencia ISO 27001 y políticas
  - ✓ Tipo de protección basado en una gestión de riesgos.
  - ✓ Métodos de recuperación en caso de pérdida o daño
  - ✓ Se debe de incluir todos los medios o dispositivos móviles.
  - ✓ Consecuencias de no aplicar la política.

En los anexos se encuentra una guía y un modelo de documento con las consideraciones a tomar para cumplir con este control. (**Referencia. 04 Anexos).**

- **A.14.2.1 Política del programa de desarrollo seguro.**

  Las reglas para el desarrollo de software y de los sistemas deben ser establecidas y aplicadas dentro de la organización.

  Estas reglas deben de ser estructuradas de la siguiente forma:

  - ✓ Nombre de la organización.
  - ✓ Versión del documento y fecha de creación.
  - ✓ Objetivos, importancia y alcance del documento.
  - ✓ Documentación de referencia a utilizar.
  - ✓ Listado de participantes con sus responsabilidades asignadas.
  - ✓ La política debe de contener al menos:
    - Seguridad en el entorno de desarrollo.
    - Seguridad en cada fase.
    - Seguridad en el control de versión.
    - Plan de solución para evitar, encontrar y solucionar vulnerabilidades.
    - Verificación de seguridad en los hitos.
    - Seguridad en la metodología de desarrollo y la codificación del software.
  - ✓ Implementación de la política
  - ✓ Difusión de la política de desarrollo a los participantes.

  En los anexos se encuentra una guía de documento que especifica la estructura de la política de desarrollo seguro. (**Referencia. 09 Anexos).**

2.7.3. Fase 3: Ejecución del proyecto de TI

El planteamiento correcto y sistemático de toda la planificación del proyecto de TI, considerando aquellos elementos y documentación clave para la ejecución de esta fase, permite una elaboración eficaz de todos los entregables cumpliendo de tal manera con los interesados y los objetivos.

Tabla 23 Ejecución del proyecto de TI

Participantes	
Propietario del Producto(Director del proyecto) **Scrum Master (Jefe del Proyecto)** **Equipo Scrum (Equipo de desarrollo)**	
Objetivo/Product Backlog_3	**Descripción**
• Gestionar el desarrollo del proyecto de acuerdo a lo establecido**(Sprint1_PB3)** • Dar seguimiento al equipo de desarrollo**(Sprint2_PB3)** • Administrar los elementos que se usan tales como insumos. **(Sprint3_PB3)** • Asegurar que se cumpla con los niveles de calidad**(Sprint4_PB3)** • Dar seguimiento a que se cumpla la seguridad de la información**(Sprint5_PB3)**	Enfoque general de la ejecución de los proyectos de TI, se efectúan las tareas previamente programadas en la fase de Planificación. La finalidad de esta fase es ajustar todo tipo de trabajo para cumplir con los requisitos y objetivos de acuerdo a lo planificado.
Control ISO 27002:2013	
A.5.1.1 Políticas de seguridad de la información. **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.** **A.12.6.1 Gestión de vulnerabilidades técnicas.** **A.14.2.6 Ambiente de desarrollo seguro** **A.14.2.7 Programa de desarrollo sub-contratado**	
Consideraciones	
• La comunicación bidireccional en esta etapa es fundamental tanto para la gestión eficaz de los entregables, hay que considerar el principio de Scrum, reuniones constantes en espacios y tiempos adecuados. • La distribución de las actividades del proyecto de TI debe de considerarse al inicio de esta fase, se logrará efectuar un desarrollo eficaz y eficiente. • La revisión de los entregables es fundamental, considerando una pregunta clave, ¿Esta acorde con lo que requiere el cliente?, si la respuesta en negativa, hay que revisar y proceder con una restructuración del mismo hasta encajar el entregable con la necesidad del Stakeholders.	

Fuente: *Guía del PMBOK, ISO27002.org, SCRUM Guía-SBOK*
Elaborado por: *El autor*

Descripción de la fase III

En esta etapa el **Propietario del producto**, el **Scrum Master** y el **Equipo de desarrollo Scrum** Trabajan con toda la información que se consideró en las dos fases anteriores, así mismo mediante una serie de reuniones se realiza el control para que el desarrollo mantenga los niveles de calidad y seguridad, considerados en los acuerdos establecidos previamente.

Objetivos/Product Backlog_3 se refiere a las actividades pendientes a realizarse, este elemento cuenta con varios **Sprint [1] hasta [5]** que son todas las tareas que deben de ser revisadas de manera exhaustiva y que permitirán que se complete de todo el **Product Backlog_3**. Cada **Sprint** dependerá de tipo de tarea a completar y de la agilidad de los que intervienen para concluirla y proveer los **entregables** o partes del proyecto**.**

En el apartado **Controles ISO27002:2013 del cuadro** se encuentra un listado de los controles necesarios para establecer medidas de seguridad en la información, además de puntos importantes a tomar en cuenta durante el desarrollo de esta etapa y que están ubicados en el apartado final de la **tabla 23** con nombre **Consideraciones.**

2.7.3.1. Aplicación de controles ISO 27002 en Fase III

- **A.5.1.1 Políticas de seguridad de la información.**

  En esta fase los participantes ya conocen las políticas de seguridad de manera general y los parámetros de desarrollo para trabajar en el proyecto:

  - ✓ Las políticas de seguridad deben de estar disponibles para cuando se requiera.
  - ✓ Las políticas de desarrollo seguro de proyectos de igual manera estarán disponibles para la respectiva consulta.

- **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.**

  Cada componente o entregable de esta fase, tiene su respectivo responsable por lo que hay que tener presente lo siguiente:

  - ✓ Socializar las tareas asignadas al grupo para el desarrollo en equipo.
  - ✓ Deben de estar disponibles en caso de algún cambio imprevisto.
  - ✓ Los cambios realizados deben de ser socializados.

.

- **A.12.6.1 Gestión de vulnerabilidades técnicas.**

  El uso de software sin licenciamiento, programas de origen desconocido y técnicas de desarrollo, producen un alto riesgo durante y al concluir todo el proyecto, para ello hay que tomar en consideración lo siguiente:

  - ✓ Identificación de posibles vulnerabilidades analizando todas las herramientas.
  - ✓ Consultar foros especializados en el desarrollo de proyectos.
  - ✓ Búsqueda de vulnerabilidades mediante escaneos.
  - ✓ Prueba de ataques simulados.
  - ✓ Política de control de uso e instalación de software.

  En virtud de las constantes amenazas, es necesario tomar en consideración este control, existe una guía técnica recomendable para aplicar seguridad en la información. (**Referencia. 05 Anexos**).

- **A.14.2.6 Seguridad en entornos de desarrollo**

  En la instancia de evaluación de los riesgos, los ítems que también se consideran para proteger la información son: el entorno de desarrollo del proyecto, los participantes, proceso de desarrollo y las tecnologías. Para aplicar medidas de seguridad se debe de tener en cuenta lo siguiente:

  - ✓ Qué nivel de seguridad se debe aplicar.
  - ✓ Nivel de sensibilidad de la información usada.
  - ✓ Si es confiable el personal que participa (revisar **control A.7.1.1**)
  - ✓ Es crítico no separar los entornos desarrollo y pruebas.
  - ✓ Un plan de backups de la información.
  - ✓ Tipificar la información el nivel de seguridad para cada uno.
  - ✓ La debida seguridad en el hardware.

  Se debe de determinar un alto nivel de protección para los entornos de desarrollo, documentarlo y hacerlo conocer a todos los implicados. (**Referencia. 011 Anexos**)

- **A.14.2.7 Programa de desarrollo sub-contratado.**

Cuando el desarrollo del proyecto es netamente realizado por los proveedores, hay que tener en cuenta lo siguiente:

- ✓ Fiscalización por parte de la organización.
- ✓ Estricto control al cumplimiento de las políticas de seguridad establecidas.
- ✓ Controlar todas las fases del desarrollo en aspectos como licencias de software y la codificación que se usa.
- ✓ Supervisión en los tipos de metodología y/o herramientas de desarrollo de proyectos.
- ✓ Todo lo anterior tuvo que haberse tratado con el proveedor y su equipo de trabajo.

La creación de un documento y firmarlo por ambas partes (Organización-Proveedor) es muy importante para mantener la seguridad de la información. (**Referencia. 012 Anexos**)

2.7.4. Fase 4: Monitoreo y control del proyecto de TI

En esta fase se recolectan datos del rendimiento de los trabajos realizados en el proyecto, se recomiendan procedimientos de mejoras para efectuar los trabajos o las tareas en base a las mediciones de los resultados sobre el desempeño y se controla la duración de todo el proyecto para no extender el tiempo de entrega.

Tabla 24 Monitoreo y control del proyecto de TI

Participantes	
Propietario del Producto(Director del proyecto) **Scrum Master (Jefe del Proyecto)** **Equipo Scrum (Equipo de desarrollo)**	
Objetivo/Product Backlog_4	**Descripción**
• Supervisar y controlar el rendimiento**(Sprint1_PB4)** • Supervisión y control el cumplimiento del alcance**(Sprint2_PB4)** • Seguimiento de los cambios **(Sprint3_PB4)** • Controlar las asignaciones de recursos económicos **(Sprint4_PB4)** • Controlar toda la planificación del proyecto**(Sprint5_PB4)** • Supervisar y controlar los riesgos **(Sprint6_PB4)** • Seguimiento al equipo humano participante**. (Sprint7_PB4)**	Análisis y supervisión de cada parte del proyecto desarrollada, para identificar cualquier desvío realizado no planteado, esta fase es de suma importancia porque se pueden corregir actividades y/o tareas que puedan dificultar la terminación exitosa del proyecto.
Control ISO 27002:2013	
A.5.1.1 Políticas de seguridad de la información. **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.** **A.14.2.1 Política del programa de desarrollo seguro** **A.14.2.5 Principios del sistema de seguridad para la ingeniería.** **A.14.2.7 Programa de desarrollo sub-contratado.** **A.14.2.8 Revisión de la seguridad del sistema.**	
Consideraciones	
• El seguimiento a las actividades dentro de la dirección del proyecto de TI, se recolecta, analiza y mide la información relacionada con su desempeño. • La información usada en el proyecto gestionado por el departamento de TI debe ser supervisada y controlada por los responsables y encargados de acuerdo a sus roles, esto va a permitir identificar anomalías que requerirán una atención específica. • Seguimiento de las fases del proyecto de TI para corroborar que los objetivos se cumplan, así mismo las expectativas planteadas en su respectiva planificación.	

Fuente: *Guía del PMBOK, ISO27002.org, SCRUM Guía-SBOK*
Elaborado por: *El autor*

Descripción de la fase IV

En esta etapa el **Propietario del producto**, el **Scrum Master** y el **Equipo Scrum** de manera constante establecen comunicación bilateral acerca del estado del desarrollo del proyecto y se pone atención en cualquier desviación que ocasione problemas en la entrega del producto final.

Objetivos/Product Backlog_4 se refiere a las actividades pendientes a realizarse, este elemento cuenta con varios **Sprint [1] hasta [7]** que son todas las tareas que deben de ser revisadas de manera exhaustiva y que permitirán que se complete de todo el **Product Backlog_4**. Cada **Sprint** dependerá de tipo de tarea a completar y de la agilidad de los que intervienen para concluirla y proveer los **entregables** o partes del proyecto**.**

En el apartado **Controles ISO27002:2013 del cuadro** se encuentra un listado de los controles necesarios para establecer medidas de seguridad en la información, además de puntos importantes a tomar en cuenta durante el desarrollo de esta etapa y que están ubicados en el apartado final de la **tabla 24** con nombre **Consideraciones.**

2.7.4.1. Aplicación de controles ISO 27002 en Fase IV

- **A.5.1.1 Políticas de seguridad de la información.**

  Para cumplir con el debido control y supervisión en esta fase las políticas de seguridad son una herramienta a consultar, para ello hay estar pendiente de lo siguiente:

  - ✓ Los avances de cada actividad
  - ✓ Ser parte de las sesiones de reuniones
  - ✓ Dar seguimientos a los cambios inesperados
  - ✓ Dar seguimiento del manejo y administración de los tiempos.

- **A.6.1.1 Funciones y responsabilidades para la seguridad de la información.**

  Es necesario supervisar al personal de desarrollo si se está cumpliendo con este control, para lograrlo hay que tomar en cuenta lo siguiente:

  - ✓ Verificar que cada participante esté realizado sus actividades de acuerdo a las funciones dadas.
  - ✓ Cada componente o subcomponente tenga su respectivo responsable.
  - ✓ Instar al personal a realizar consultas en caso de desconocer procedimientos.

- **A.14.2.1 Política del programa de desarrollo seguro**

  La documentación considerada en el **control A.14.2.1** es de utilidad durante esta fase del proyecto, permite hacer una verificación del cumplimiento de los puntos tratados en la fase II, para constatar lo anterior se podría hacer un checklist referentes a:

  - ✓ Seguridad en cada fase del proyecto.
  - ✓ Las versiones trabajadas.
  - ✓ Los participantes y sus asignaciones.
  - ✓ De las herramientas y metodologías.

- **A.14.2.5. Uso de principios de ingeniería en la protección de sistemas.**

  En esta fase de elaboración de los proyectos se la aplica de la siguiente manera:

  - ✓ Elaborar procedimientos de Ingeniería en los sistemas de información.
  - ✓ Elaborar documentación de ingeniería de seguridad y como se lo aplica.
  - ✓ Aplicar niveles de seguridad en refuerzo a la arquitectura.
  - ✓ Análisis de hardware y software a usarse en el proyecto y conocer los riesgos de seguridad.
  - ✓ Realizar una revisión periódica en comparación con la documentación de los **controles A.5.1.1** y **A.14.2.1.**

  Es fundamental mejorar el proceso de uso de ingeniería en el desarrollo de los proyectos, vea las recomendaciones en (**Referencia. 010 Anexos**)

- **A.14.2.7 Programa de desarrollo sub-contratado.**

  La supervisión al talento humano externo participes del desarrollo es importante para desempeño del proyecto, se debe de controlar lo siguiente:

  - ✓ Existencia de al menos un profesional adicional de parte de la organización para reemplazar al principal.
  - ✓ La existencia del personal externo de acuerdo a los términos y condiciones del proyecto.
  - ✓ Monitorear las técnicas de desarrollo y sus funcionalidades.
  - ✓ Se revisa el cumplimiento de los términos del **control A.14.2.1**

Para cumplir con este control se debe de tomar en consideración los puntos dados en **(Referencia. 012 Anexos).**

- **A.14.2.8 Pruebas de seguridad durante el desarrollo de los sistemas.**

  Realizar pruebas de seguridad en trayecto del desarrollo es tan importante como las pruebas de funcionamiento operativo. Para cumplir con este control hay que tomar en cuenta lo siguiente:

  - ✓ Se tiene que realizar pruebas de hardening (endurecimiento).
  - ✓ Tomar en consideración el **control A.12.6.1**.
  - ✓ Revisión del software y hardware que se utilizó en el desarrollo.
  - ✓ Asegurar que no se haya afectado algún proceso interno organizacional.
  - ✓ Planes de contingencia listos en caso de siniestros.
  - ✓ Lo anterior tiene que realizarse en un programa de actividades bajo diversas condiciones definidas previamente.

  Estas pruebas, sellan posibles huecos de seguridad que amenacen la integridad de la información, de ahí su importancia de efectuar este control. En **(Referencia. 013 Anexos)** existe un listado de cómo realizar esta actividad.

2.7.5. Fase 5: Cierre del proyecto de TI

Es la parte en donde el proyecto culmina, previo a la revisión del cumplimiento de todas aquellas formalidades pactadas al inicio del proyecto de TI que incluye los objetivos, alcance y además la aplicación de controles de seguridad en la información planteadas para su ejecución en las actividades.

Tabla 25 Fase de cierre del proyecto de TI

Participantes	
Stakeholders (Interesados Claves) **Propietario del Producto(Director del proyecto)**	
Objetivo/Product Backlog_5	**Descripción**
• Verificación de pruebas del proyecto**(Sprint1_PB5)** • Análisis de las expectativas con la finalización del proyecto en sus fases. **(Sprint2_PB5)** • Reporte y registro de los riesgos gestionados **(Sprint3_PB5)** • Cierre del contrato del proyecto de TI. **(Sprint4_PB5)**	Actualización de los documentos del proyecto, retroalimentación de todas las novedades presentadas de las fases y de lo que implico su desarrollo, además del informe del resultado final.
Control ISO 27002:2013	
A.12.6.1 Gestión de Vulnerabilidades Técnicas **A.14.2.9 Revisión de la aceptación del sistema.**	
Consideraciones	
• Revisión del cumplimiento de acuerdos pactados en la entrega del proyecto de TI. • Entrega del producto probado y certificado que cumplió con los lineamientos de seguridad de la información establecidos en las referencias Ref. 01 hasta Ref. 014. • Evaluación del impacto generado por los riesgos en el trayecto del desarrollo del proyecto de TI. • Cierre del contrato y acta de finiquito del proyecto de TI en donde se demuestra el cumplimiento de los objetivos y alcance del proyecto.	

Fuente: *Guía del PMBOK, ISO27002.org, SCRUM Guía-SBOK*
Elaborado por: *El autor*

Descripción de la fase V

En esta etapa los **Stakeholders** y el **Propietario del producto** Analizan todas las novedades presentadas durante el trayecto de las fases anteriores, evalúan el cumplimiento de los acuerdos establecidos y se procede con la entrega formal del producto final.

Objetivos/Product Backlog_5 se refiere a las actividades pendientes a realizarse, este elemento cuenta con varios **Sprint [1] hasta [5]** que son todas las tareas que deben de ser revisadas de manera exhaustiva y que permitirán que se complete de todo el **Product Backlog_5**. Cada **Sprint** dependerá de tipo de tarea a completar y de la agilidad de los que intervienen para concluirla y proveer los **entregables** o partes del proyecto**.**

En el apartado **Controles ISO27002:2013 del cuadro** se encuentra un listado de los controles necesarios para establecer medidas de seguridad en la información, además de puntos importantes a tomar en cuenta durante el desarrollo de esta etapa y que están ubicados en el apartado final de la **tabla 25** con nombre **Consideraciones.**

2.7.5.1. Aplicación de controles ISO 27002 en Fase V

- **A.12.6.1 Gestión de Vulnerabilidades Técnicas.**

  La gestión de vulnerabilidades durante el desarrollo del proyecto, permite la entrega de un producto final seguro de acuerdo a las necesidades solicitas del o los interesados, según sea necesario se realiza lo siguiente:

  - ✓ Entrega de un informe acerca de las vulnerabilidades encontradas, origen nivel de riesgos y mitigación.
  - ✓ Sugerencias para el tratamiento y reducción del impacto.
  - ✓ Recomendaciones a seguir para futuros proyectos.

- **A.14.2.9 Revisión de la aceptación del sistema.**

  Antes de la puesta en producción del producto final se debe de establecer una política de desarrollo y prueba de aceptación para todos los sistemas que adquiera la organización y se debe de establecer lo siguiente:

  - ✓ Los requisitos de seguridad deben de seguirse de acuerdo a lo tratado en el **control A.14.2.1.**
  - ✓ También las pruebas deben de hacerse en componentes y sistemas integrados.
  - ✓ Las pruebas deben de simular entornos y casos reales.
  - ✓ Las pruebas deben de basarse en el **control A.12.6.1** y su documentación.
    - ✓ Establecer lineamientos de pruebas mediante protocolos y normas de la organización.

El cumplimiento de este control permite conformidad y nivel de satisfacción para el cliente u organización. En los anexos existen los pasos a seguir, de acuerdo a **(Referencia. 014 Anexos).**

2.8. Enfoque del modelo de seguridad en la información

El modelo propuesto tiene dos enfoques: el primer enfoque concierne en recomendar el uso de la guía de buenas prácticas PMBOK complementando con metodología de desarrollo ágil SCRUM para la óptima gestión de los proyectos de TI y el segundo enfoque tiene que ver con la aplicación de medidas de seguridad basados en los controles y dominios de la metodología ISO27002 en las cinco fases que se componen.

Estos dos enfoques contribuyen a que cada proyecto llegue a su etapa de conclusión constando con tanto niveles de calidad, funcionamiento y más que todo posea lineamientos de seguridad en la información que fluye durante y en la entrega final de un proyecto gestionado.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual

En este capítulo se muestran los resultados del trabajo de investigación, se empieza realizando el análisis de las variables con sus dimensiones así como la presentación de las entrevistas y encuestas con su respectivo diagnóstico y desenlace.

3.1.1. Análisis de las Variables y sus Dimensiones

3.1.1.1. Variable # 1 Gobernanza

La variable independiente **Gobernanza,** consiste en una modalidad de trabajo estructurado que entre otras beneficios alinea los objetivos de la organización con los objetivos de TI enfocando la atención en la seguridad de la información en los proyectos de TI, contribuye a la realización de control y supervisión del cumplimiento del uso de las políticas de seguridad cuando se están desarrollando los proyectos de la organización, así mismo dando seguimiento ordenado mediante estándares y metodologías de gestión, tal forma contribuye al éxito de los proyectos y la seguridad de la información en los mismo.

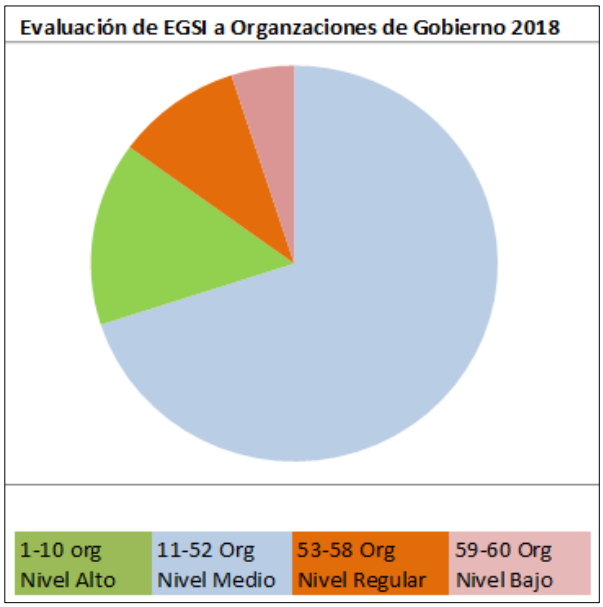
- **Dimensión Políticas, normas y procedimientos**

Documentación imprescindible que debe de tener la organización para usarse como una guía de buenas prácticas con el fin de supervisar y mantener la seguridad de la información en todos sus procesos, esto también incluye en el proceso de Gestión de Proyectos de TI. La aplicación de este procedimiento permitirá obtener resultados satisfactoriamente deseables en todos los procesos internos.

Para el año 2018 en el Ecuador, existieron 60 organizaciones del sector público que fueron evaluadas para verificar el cumplimiento del EGSI

(Esquema Gubernamental de Seguridad de la Información), en base a la norma ISO 27002, esto significa que luego de una revisión y supervisión de todas las políticas de seguridad y documentación, existe un porcentaje no considerable que mantienen actualizadas la documentación de las políticas de la organización aunque aún falta algunas que deben mejorar sobre este asunto.

Figura 8 Cumplimiento del EGSI Ecuador 2018



Fuente:https://www.gobiernoelectronico.gob.ec/ranking-esquema-gubernamental-de-seguridad-de-la-informacion-egsi/
***Elaborado por**: El autor*

Se ha localizado indicadores relacionados a la dimensión descrita para el objetivo de esta investigación, se seleccionaron de organizaciones del sector público de Registro Civil en el Ecuador para evaluar el nivel de aplicación de las Políticas, normas y procedimientos internamente de sus organizaciones y la revisión y/o actualización de las políticas de seguridad.

A continuación, se detallan junto con los respectivos ítems:

Tabla 26 Indicadores para la dimensión Políticas, normas y procedimientos

Indicadores	Ítems
• **Documentación** • **Revisión y actualización de las políticas de seguridad**	• Documentación de procedimientos y normas de seguridad de la información para todos los procesos y subprocesos de la organización • De forma particular se documenta y se aplica medidas de seguridad para la gestión de los proyectos de TI. • Se revisan y actualizan las normas y procedimientos de seguridad de la información respecto a cada tipo de proyecto de TI gestionado. • Las normas y procedimientos de seguridad de la información se basan en reglamentos, normas de gobierno y/o estándares internacionales.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

3.1.1.2. Variable # 2 Recursos de TI

Se seleccionó **Recursos de TI** como variable debido la importancia que generan en el desarrollo de los proyectos. Se debe de escoger recursos de TI adecuados para cada proyecto, acorde a las necesidades evaluadas, si se recure por equipamiento y/o herramientas inadecuadas para la gestión de desarrollo, el resultado final de los proyectos no serán los esperados por los interesados.

La infraestructura tecnológica considerada como hardware y los elementos intangibles considerados como software se deben de gestionar de manera que produzca una fusión positiva y que contribuya la innovación y/o mejoras de los servicios que imparten las organizaciones de Registro Civil en el Ecuador. En resumen las herramientas y elementos de tecnología deben de ser las adecuadas para la construcción de los proyectos.

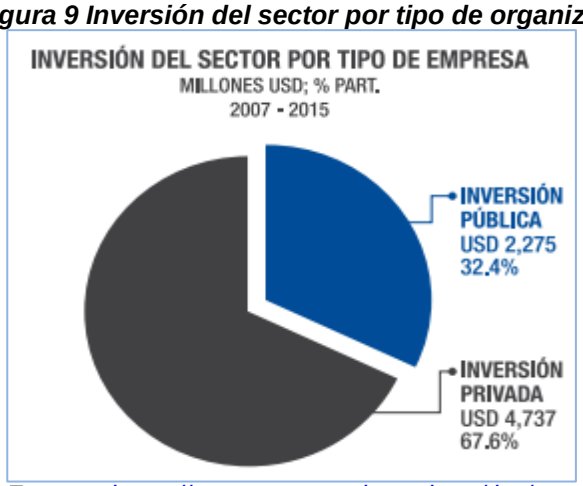
- **Dimensión Tecnología**

Las inversiones en cuanto a la adquisición de recursos de Tics para innovar o mejorar procesos claves mediante los proyectos a cargo del departamento

de TI, también es realizado en otros tipos de organizaciones en el Ecuador por ejemplo, según datos de la página gubernamental proecuador, existe inversión tanto de organizaciones públicas como privadas.

Desde el 2007 al 2015 se ha invertido más de USD 7,000 millones en telecomunicaciones, donde el 67.1 % del capital invertido pertenece a la empresa privada, demostrando confianza en el país. Solo en el 2015 la inversión pública fue de USD 243.5 millones.

Figura 9 Inversión del sector por tipo de organización



Fuente: *https://www.proecuador.gob.ec/tics/*
Elaborado por*: El autor*

El **figura 9** muestra que las inversiones realizadas en el sector privado es alto en comparación con las organizaciones públicas, no quiere decir que son menos importantes, antes bien hay que recalcar que el sector privado es mucho más grande, además las inversiones que realiza las organizaciones de estado se focalizan directamente en la administración de información y servicios públicos.

Tabla 27 Indicadores para la dimensión Tecnología

Indicadores	Ítems
• **Adquisición de recursos de TI** • **Metodologías y técnicas de gestión**	• Se mejora/innova los procesos de negocio y/o servicios de la organización mediante el uso de tecnología de la actualidad. • La organización cuenta con herramientas para planificar los proyectos de TI • Se utilizan metodologías agiles o estándares internacionales para la gestión de los proyectos de TI.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

3.1.1.3. Variable # 3 Gestión de riesgos

Se optó por esta variable porque permite conocer clasificar y valorar los riesgos de la organización, ayuda a monitorear el estado de la seguridad de la información, a través de las responsabilidades asignadas al empleado o grupo de empleados, este procedimiento debe de ser realizado por profesionales con la debida experiencia en el tema.

La gestión de riesgos es iterativa y asiste a las organizaciones a establecer sus estrategias, lograr sus objetivos y tomar decisiones informadas, permitiendo a las mejoras de los sistemas de gestión (ISO.ORG, 2018). Es un elemento clave que deben de utilizar todas las organizaciones para alcanzar sus objetivos planteados, un buen tratamiento estructurado de los riesgos en los procesos permite mejorar el desempeño y la reducción de pérdidas en factores económicos, de tiempo y recursos.

Existe una variedad de herramientas para la gestión de los riesgos, es muy importante usar la adecuada para este fin, aunque la experiencia de un profesional contribuye mucho, este proceso bien trabajado con todos los elementos necesario ayudará a ahorrarse problemas en el desarrollo de los proyectos de TI.

- **Dimensión Experiencia**

En la gestión de riesgos es de gran ayuda cuando se requiere planificar, desarrollar y culminar un proyecto de TI, se convierte en una herramienta de utilidad imprescindible cuando se la gestiona de la forma correcta y para que surta efecto, debe de ser realizado por profesionales con la experiencia y nivel académico.

De acuerdo a información de la Secretaría de Educación Superior, Ciencia, Tecnología e Investigación (SENECYT), en el país existen 86,409 profesionales en el área de Informática debidamente formados y reconocidos por dicha Secretaría. La existencia de profesionales es una cantidad grande, las organizaciones cuando realicen el proceso de selección de talento humano para el departamento de Tics y/o la selección del proveedor junto con su equipo de trabajo para proyectos, hay que considerar su nivel, académico y la experiencia en la gestión de riesgos y en el desarrollo de proyectos tecnológicos propiamente.

A continuación se muestra el indicador y sus respectivos ítems basados en la dimensión de gestión de riesgos:

Tabla 28 Indicador para la dimensión Experiencia

Indicadores	Ítems
• **Evaluación de los riesgos**	• Los participantes cuentan con la suficiente experiencia, capacidad y nivel académico para el desarrollo de los proyectos de TI • Se supervisa el uso de políticas y controles de seguridad de la información cuando se están desarrollando los proyectos de TI.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

- **Dimensión Responsabilidad**

La responsabilidad de cada funcionario, empleado y /o proveedor(es) usar las políticas de seguridad establecidas, cumplir con su utilización es muy importante para mantener la información que se utiliza de manera protegida. Cada organización debe controlar la aplicación de las políticas de seguridad, previamente haberlas dado a conocer a todos los miembros internos y externos.

En el desarrollo de los proyectos de TI la consideración y aplicación del uso de las políticas de seguridad en todo el proceso de gestión, no solo se logrará un desarrollo de proyecto que finalice a tiempo ajustado al alcance, sino un producto seguro y confiable.

A continuación se describen los indicadores con los ítems respectivos:

Tabla 29 Indicador para la dimensión responsabilidad

Indicadores	Ítems
• **Aceptación de funciones**	• Se establecen niveles de responsabilidad en base a políticas de seguridad en la información a todos los que participan en el desarrollo del proyecto de TI. • Los participantes en el desarrollo de proyectos de TI conocen de las responsabilidades que implica el uso de la información de la organización.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

3.1.1.4. Variable # 4 Liderazgo

La variable **Liderazgo** de buen nivel es muy importante considerarla ya que una parcial existencia de la misma no será de utilidad para dar seguimiento a los proyectos y puedan seguir hacia un cierre exitoso. El resultado bueno o malo de un proyecto dependerá del tipo de liderazgo y diligencia que posea el responsable profesional que esta adelante en el desarrollo.

Es importante la selección de profesionales con habilidades en la materia para la supervisión del equipo del proyecto, su experiencia contribuirá a establecer buenas relaciones de negocio, aceptación y seguimiento de la aplicación de la seguridad y privacidad de la información. La presencia de un alto nivel de liderazgo en los responsables de la dirección los proyectos de TI, ayuda a la existencia de una buena comunicación con los interesados.

El liderazgo puede ser representado por una persona o un grupo de personas encargadas de hacer cumplir los objetivos trazados por los contratantes o empleadores de una organización. El líder está a la expectativa de la coordinación y del seguimiento de los problemas que se pueden presentar en el transcurso del proyecto, su gestión logrará que cada proyecto finalice exitosamente en cuanto al alcance y objetivos, así como la aplicación y supervisión de las políticas de seguridad para proteger la información.

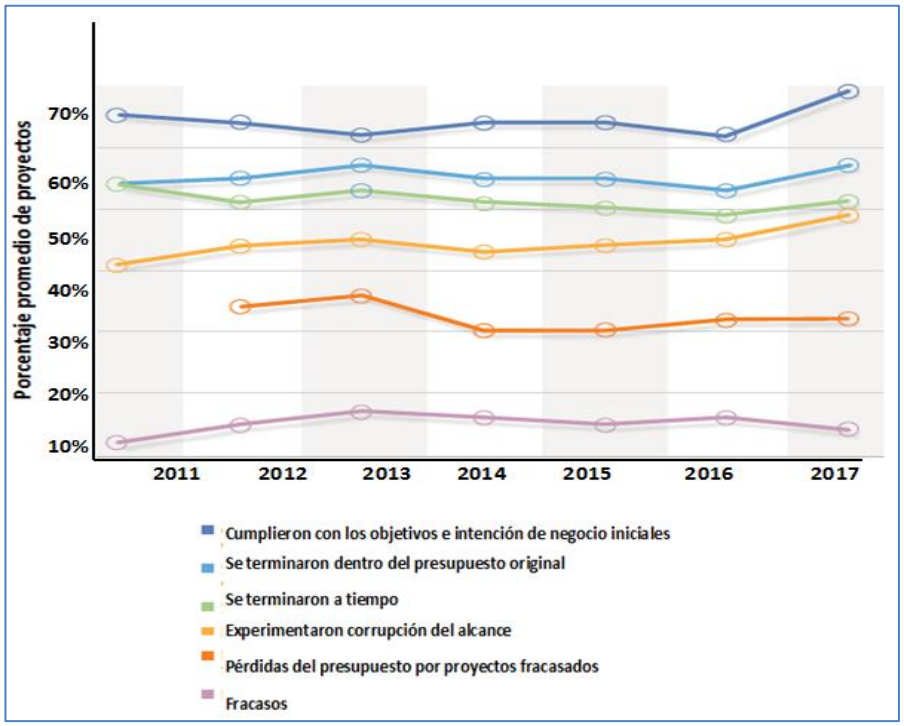
- **Dimensión Desempeño**

El desempeño permite medir, supervisar y ponderar el rendimiento de las actividades del equipo, de los interesados y de la condición del proyecto, además del rendimiento del propio líder del proyecto. Si existe buena dirección y gestión de las fases que componen el proyecto se podrá conocer cómo se encuentra, funciona el equipo y saber el estado de las labores asignadas.

Esta dimensión tiene dos enfoques, por un lado se revisa los por menores el estado final del proyecto y por otro se verifica el accionar de cada integrante o participante. Se puede decir que es una actividad recurrente cada vez que se gestionen proyectos de cualquier tipo. Esta revisión sirve de información histórica para futuros proyectos a emprender.

Por otro lado, el PMI menciona que cuando existe un buen desempeño en la gestión de los proyectos, el éxito de los mismos es notorio. Pues finalizan a tiempo dentro del presupuesto y cumplen con los objetivos e intenciones del negocio.

Figura 10 Métricas de desempeño de los proyectos



Fuente: *PMI, 2017*
Elaborado por*: El autor*

Se puede apreciar según la figura 10 que el desempeño en todo el ciclo de vida del proyecto ayuda a la obtención de resultados comprobables y aplicables para futuras gestiones, la existencia de un buen liderazgo, ocasiona un buen rendimiento y resultados esperados.

A continuación, se detalla los indicadores con sus respectivos ítems:

Tabla 30 Indicador para la dimensión desempeño

Indicador	Ítems
• **Actuación e idoneidad**	• Existe nivel de liderazgo y compromiso en el equipo para gestión de desarrollo de los proyectos de TI. • Se asignan las tareas y/o actividades de los proyectos de TI acorde al nivel de conocimiento de cada empleado participante. • Existe personal externo o proveedores que participan en el desarrollo de los proyectos

Fuente: *Marco Teórico*
Elaborado por*: El autor*

3.1.1.5. Variable # 5 Gestión de la calidad

Aquí se involucra la creación de procesos para asegurar que un proyecto alcance los requisitos para lo cual va a ser desarrollado. Debe de ser incluido desde sus inicios en el plan de gestión y debe de ser controlado por los encargados del desarrollo para que al final se obtenga un producto acorde a lo solicitado.

Gestionar la calidad es un factor importante para poder catalogar a un proyecto como exitoso. Establecer lineamientos de calidad en la planificación, aplicarlos en el desarrollo y verificarlos en cada entregable, así como en la finalización de todo el proyecto, se estaría cumpliendo con los requerimientos solicitado por el cliente u organización.

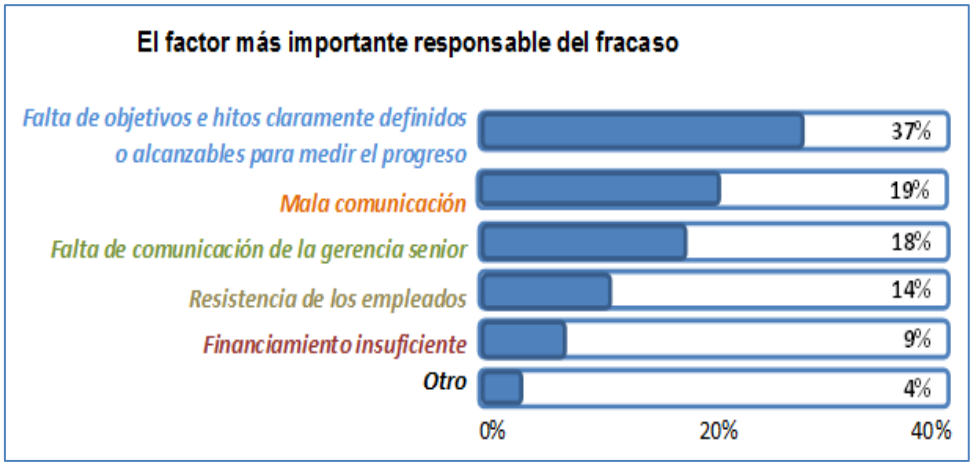
- **Dimensión Financiera**

Cada organización tiene como finalidad mantenerse en el mundo competitivo y crecer de manera paulatina, la distribución eficaz de los recursos monetarios dentro de un establecimiento, asegura el bienestar para su estabilidad y crecimiento.

El financiamiento necesario es importante para que se gestionen los proyectos de manera óptima y no se fracase. El PMI de acuerdo a un

sondeo a 3234 profesionales en la dirección de proyectos, menciona uno de los factores de fracaso es el insuficiente financiamiento (Project Manangement Institute, 2017). El apoyo en términos monetarios en todas las fases de la gestión de los proyectos, contribuye junto con otros factores, a encaminar exitosamente la culminación de todos los entregables.

Figura 11 Fracaso debido financiamiento insuficiente



Fuente: *PMI, 2017*
Elaborado por*: El autor*

Según los resultados presentados en la **Figura 11** muestran que entre los factores que obstaculizan el éxito de los proyectos, es el poco apoyo por parte del área financiera.

Del financiamiento se deriva la adquisición de los recursos tanto tecnológicos; hardware y software, las capacitaciones al talento humano interno, así como la contratación de profesionales externos para el desarrollo de los proyectos.

A continuación, se detalla el indicador con su respectivo ítem:

Tabla 31 Indicador para la dimensión financiera

Indicador	Ítems
• **Financiera**	• El departamento financiero brinda todas las facilidades y apoyo para desarrollar proyectos de TI. • El éxito de cada proyecto de TI depende del departamento financiero.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

- **Dimensión Cumplimiento**

Se refiere a la ejecución de todo lo que el o los interesados plantearon en los requerimientos y necesidades cuando se fundamentó el proyecto. La verificación del cumplimiento con las normas y procedimientos exigidos por la organización, permite la obtención de un proyecto bien desarrollado.

Tiene dos enfoques: el primero está relacionado con la ejecución de los parámetros establecidos en los requisitos, alcance y objetivos del proyecto. El segundo es el aplicar todos los lineamientos de las políticas, normas y procedimientos de seguridad en la información en las fases de desarrollo del proyecto.

Para que se cumpla con los requisitos de seguridad en las fases del desarrollo del proyecto debe de existir activos de seguridad tales como: Roles, procedimientos de desarrollo, técnicas, herramientas y métricas (De la Cámara, 2015). La presencia de esta documentación previamente creada, es de utilidad para aquellos que participan en la gestión de proyectos, los lineamientos descritos permiten asegurar la información utilizada en todo el proyecto.

A continuación se detallan los indicadores con sus respectivos ítems:

Tabla 32 Indicador para la dimensión cumplimiento

Indicador	Ítems
• **Conformidad y satisfacción**	• Por lo general, los proyectos de TI culminan acorde a los objetivos y alcance que se plantearon • Se realizan pruebas de funcionamiento y endurecimiento (Hardening) en los proyectos de TI culminados antes de su entrega. • Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados.

Fuente: *Marco Teórico*
Elaborado por*: El autor*

3.2. Presentación de resultados y discusión

3.2.1. Resultado de la matriz de riesgos

En esta investigación se estableció una matriz para el análisis de los riesgos en el proceso de gestión de proyectos de TI, se pudo constatar y conocer una variedad con resultados en donde la organización debe de poner en acción un plan de tratamiento para su respectiva mitigación cada vez que se vaya a poner en marcha un proyecto.

A continuación se presenta en una tabla los factores de riesgos localizados con sus respectivos valores y tratamiento a realizar:

Tabla 33 Resultados de matriz de riesgos del proceso gestión de TI

Ítem	Factor de Riesgo	Valor del Riesgo inherente	Tratamiento
1	Planificación mal realizada de proyectos	3	Lo asume la organización y establece controles propios.
2	Indisponibilidad de medios de TI o equipos tecnológicos	3	Lo asume la organización y busca una solución para la mitigación
3	Vulnerabilidad de la información	5	Plan de acción inmediato mediante empleados expertos o contratación con proveedores
4	Producto/Servicio sin niveles de seguridad	5	Plan de acción inmediato mediante empleados expertos o contratación con proveedores
5	Problemas de operatividad y comprensión del proyecto	4	Plan de acción inmediato mediante empleados expertos o contratación con proveedores
6	Problemas de funcionamiento del producto	4	Plan de acción inmediato mediante empleados expertos o contratación con proveedores
7	Cambios en los requisitos	4	Plan de acción inmediato mediante empleados expertos o contratación con proveedores

Fuente: *Anexo # 7*
Elaborado por*: El autor*

3.2.2. Resultado de las entrevistas

Se realizó tres entrevistas para abordar el tema de la gestión de proyecto en el área TI en las entidades de Registro Civil, la primera a una Directora de gestión de TI que cuenta con 10 años de experiencia (Ver anexo # 3); otra, al Coordinador de Tecnología de la información de otra entidad de registro civil con 11 años de experiencia (Ver anexo # 4); y por último, a un Consultor de gestión de proyectos de TI con experiencia de 15 años en el desarrollo y administración de todo tipo de proyectos de diferentes sectores empresariales (Ver anexo # 5).

3.2.2.1. Entrevista al Coordinador de Proyectos

Se reconoce que en la organización constantemente se desarrollan proyectos en el área de TI para mejorar los procesos y en su mayoría no se está trabajando con seguridad para la información, si bien es cierto que las organizaciones del sector publico deben de operar e implementar seguridad en la información en todos sus procesos, de acuerdo al EGSI (Esquema Gubernamental de Seguridad de la Información), no se está utilizando medidas de seguridad al respecto en las fases o actividades que concierne cada proyecto.

Se determinó que en la organización existen proyectos que no terminan a tiempo, abarcan más recursos a nivel económico y humano, esto ha ocasionado inconvenientes en presupuesto a la vez, hay que esperar que el proyecto concluya debidamente para poner en marcha el servicio que funcionará. Además en ocasiones surgen interferencias en la fluidez del proyecto debido a indisponibilidad del recurso humano, sea por salud o por inconformidades hacia la institución.

3.2.2.2. Entrevista a la Directora Gestión Tecnológica

En esta entrevista se observó que en la gestión de proyectos hay inconvenientes de nivel medio en cuanto a la planificación no ordenada, en vista de aquello hay que reprogramar las actividades y las tareas. Además no existe una correcta gestión de los riesgos y en vista de aquello los cierres de los mismos no son a tiempo, se descuida mucho la documentación de las lecciones aprendidas en cada proyecto. A lo anterior se reconoce el problema de la rotación del personal sea interno o proveedores del cual afecta la planificación y el cumplimiento de los objetivos organizacionales.

Aunque si se está trabajando con los procedimientos que recomienda ISO 27001, la aplicación de medidas de seguridad en la información no se está llevando a cabo en la gestión de proyectos, no se existe una documentación

guía de trabajo para aplicar controles seguridad en la información en este proceso.

3.2.2.3. Entrevista a Consultor en Gestión de Proyectos TI

De acuerdo a los años de experiencia laborando en una empresa de soluciones informáticas en la ciudad de Guayaquil y administrando proyectos en organizaciones del sector público y privado, se visualizó que uno de los principales problemas es la presión de culminar el proyecto a tiempo, pero el apoyo financiero es limitado para casos emergentes cuando se presentan algún imprevisto de cualquier tipo, esto ocasiona que se retrase en la entrega, hasta adquirir lo que se necesita. Otro de los problemas es debido a la falta de conocimiento técnico y experiencia por parte de los empleados que trabajan junto al equipo de desarrollo del proveedor, esto se debe a los cambios políticos en el país que ocasiona rotación de personal, indisponibilidades por salud, ausencias y hasta renuncias inesperadas.

Respecto al uso de medidas de seguridad de la información, las organizaciones están orientadas a que el proyecto se entregue funcionando y que no genere costos adicionales, aunque en ciertos casos existen acuerdos de confidencialidad en la contratación en otros no existe tal documentación. También se reconoce que en desarrollo no se está trabajando bajo ninguna metodología de seguridad en la información en las fases del proyecto, el entrevistado considera y enfatiza que si es una buena decisión desarrollar los proyectos mediante controles y niveles de seguridad.

3.2.3. Discusión de las entrevistas

De las tres entrevistas se pudo constatar que los encargados de mejorar los procesos están conscientes que no se está usando parámetros de seguridad en la información utilizada en los proyectos, su enfoque está

centrado principalmente en la conclusión del proyecto, aunque según las entrevista se está teniendo problemas en cuanto al control y seguimiento, lo que está generando atrasos en la entrega del producto.

Además se observa falta apoyo económico, debido a las restricciones del presupuesto, hay que esperar mucho tiempo para la asignación de nuevos recursos y se pueda completar el proyecto. No se está realizando una gestión oportuna de los riesgos lo que conlleva al entorpecimiento de fluidez debido a problemas comunes como: la presencia de personal con poca experiencia, poco conocimiento técnico, falta de compromiso durante la gestión de desarrollo e inclusive falta de liderazgo y también riesgos de perdida de información sensible que interviene en todo el ciclo de vida.

3.2.4. Resultados de las encuestas

Se efectuó una encuesta a 142 funcionarios del área de tecnología, mismos que fueron tomados de la base de datos de las organizaciones de registro civil en el ecuador para el año 2017.

Los datos proporcionados por los 142 participantes en los 19 ítems de la encuesta, fueron procesados en la herramienta SPSS para efectuar un análisis de fiabilidad de Alfa de Cron Bach; siendo su resultado satisfactorio obteniendo 0,842.

Tabla 34 Estadísticas de fiabilidad

Alfa de Cron Bach	N de elementos
0,842	19

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 1

Se usa documentación de procedimientos y normas de seguridad de la información para todos los procesos y subprocesos de la organización.

El 8.5% de los encuestados confirmaron el uso con frecuencia de documentos de políticas de seguridad en la organización, el 53.5% confirmó el uso de la documentación con frecuencia, mientras que el 29.26% respondió que en ocasiones, el 7.7% respondió que es raro el uso, 0.7% mencionó que nunca.

Tabla 35 Existencia de normas de seguridad en la organización

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	11	7,7	7,7	8,5
	Ocasionalmente	42	29,6	29,6	38,0
	Frecuentemente	76	53,5	53,5	91,5
	Muy frecuentemente	12	8,5	8,5	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 2

Se documenta y se usa medidas de seguridad para la gestión de los proyectos de TI de forma particular.

El 7.0% menciona que con frecuencia se documentan medidas de seguridad para los proyectos, el 27,5% mencionó que si es frecuente, mientras el 20.4% afirmó que en ocasiones se documenta y el 42.3% mencionó que es rara la ocasión y un 2.8% respondió que nunca. Con estos resultados muestra que aproximadamente un 45.1% de los profesionales mencionan que no es común la documentación de medidas de seguridad para proteger la información en los proyectos de TI.

Tabla 36 Se trabaja con medidas de seguridad en los proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	2,8	2,8	2,8
	Raramente	60	42,3	42,3	45,1
	Ocasionalmente	29	20,4	20,4	65,5
	Frecuentemente	39	27,5	27,5	93,0
	Muy frecuentemente	10	7,0	7,0	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 3

Se revisan y actualizan las normas y procedimientos de seguridad de la información respecto a cada tipo de proyecto de TI gestionado.

Se puede visualizar que entre el 5.6% y el 26.8% mencionó que se actualiza documentación en los proyectos, mientras que el 24.6% se lo realiza en ocasiones, el 40.1% se lo hace muy raramente y el 2.8% menciona que nunca se ha realizado documentación al respecto. Existe una brecha de aproximadamente de un 42.9% que no es regular o común la actualización de los documentos donde se utilizó seguridad en la información al finalizar cada proyecto para utilizarlo como historial de lecciones aprendidas, esta cantidad da con la suma de “Raramente” y “nunca”, es algo que se debe de considerar.

Tabla 37 Actualización de documentación de SI en cada fin de proyecto

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	2,8	2,8	2,8
	Raramente	57	40,1	40,1	43,0
	Ocasionalmente	35	24,6	24,6	67,6
	Frecuentemente	38	26,8	26,8	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 4

Las normas y procedimientos de seguridad de la información se basan en reglamentos, normas de gobierno y/o estándares internacionales.

Un 8.5% afirma que con mucha frecuencia la organización utiliza los estándares y acuerdos de gobierno referente a la seguridad de la información, un 59.2% también afirma el uso frecuente, mientras que el 26.8% menciona que lo hace en ocasiones, un 4.9% lo realiza raras veces y solo un 0.7% menciona que nunca se lo realiza.

Estos resultados indican que existe aproximadamente un 32% que no se está utilizando estándares comunes para gestionar seguridad en la información organizacional.

Tabla 38 Políticas de seguridad basadas en normas de gobierno

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	7	4,9	4,9	5,6
	Ocasionalmente	38	26,8	26,8	32,4
	Frecuentemente	84	59,2	59,2	91,5
	Muy frecuentemente	12	8,5	8,5	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 5

Se mejora/innova los procesos de negocio y/o servicios de la organización mediante proyectos gestionados en el departamento de TI con el uso de la última tecnología.

Un 10.6% y el 59.2% respondieron que se realiza con frecuencia la gestión de proyectos en el departamento de TI, un 26.8% mencionó que en ocasiones, mientras que el 3.5% respondió que es raro el desarrollo de proyectos.

Los resultados anteriores muestran que si se están desarrollando proyectos con frecuencia.

Tabla 39 Frecuencia de proyectos en la organización

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	5	3,5	3,5	3,5
	Ocasionalmente	38	26,8	26,8	30,3
	Frecuentemente	84	59,2	59,2	89,4
	Muy frecuentemente	15	10,6	10,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 6

La organización cuenta con herramientas para planificar los proyectos de TI.

Un 12% respondió que es muy frecuente el uso de herramientas para la planificación de los proyectos, un 47.9% mencionó que es frecuente, mientras que un 34.5 afirmó que en ocasiones se usan este tipo de herramientas y un 5.6 afirmo que es raro.

Tabla 40 Uso de herramientas de planificación de proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	8	5,6	5,6	5,6
	Ocasionalmente	49	34,5	34,5	40,1
	Frecuentemente	68	47,9	47,9	88,0
	Muy frecuentemente	17	12,0	12,0	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 7

Se utilizan metodologías agiles o estándares internacionales para la gestión de los proyectos de TI.

Un 8.5% de los encuestados declaró que usan estándar y metodología ágil para la gestión de los proyectos, un 31.7% de la misma manera lo afirmó, un 47.2% respondió que esto se realiza en ocasiones, mientras que un 12% manifestaron que es raro el uso 0.7 % mencionaron que es raro no se trabaje con las metodologías.

Los resultados anteriores muestran que un 59.9 % no es muy frecuente el uso de metodologías o estándares para la gestión de proyectos, se percibe que se valen más de la poca experiencia en el tema.

Tabla 41 Uso de metodología ágil para proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	17	12,0	12,0	12,7
	Ocasionalmente	67	47,2	47,2	59,9
	Frecuentemente	45	31,7	31,7	91,5
	Muy frecuentemente	12	8,5	8,5	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 8

Los participantes cuentan con la suficiente experiencia, capacidad y nivel académico para el desarrollo de los proyectos de TI.

Una cantidad baja del 8.5% de los encuestados respondieron que los desarrolladores de proyectos de TI cuentan con suficiente experiencia, un 41.5% menciono algo similar que si es frecuente, un 43.7% declaró que en ocasiones se cuenta con experiencia y un 6.3% mencionó que es raro que los participantes tengan experiencia.

Los resultados están ligados con el Ítem 7 debido que un 50% de los que desarrollan no cuentan con la experiencia debida para la gestión de los proyectos, de ahí el inconveniente en los cierres y entregables.

Tabla 42 Desarrolladores con experiencia, capacidad y nivel académico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	9	6,3	6,3	6,3
	Ocasionalmente	62	43,7	43,7	50,0
	Frecuentemente	59	41,5	41,5	91,5
	Muy frecuentemente	12	8,5	8,5	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 9

Se supervisa el uso de políticas y controles de seguridad de la información cuando se están desarrollando los proyectos de TI.

Una cantidad pequeña de 7.7% manifestó que sí se supervisa el uso de controles proyectos seguridad en la información cuando se desarrollan los proyectos, de la misma forma un 21.1% respondió que es frecuente, un 29.6% respondió que en ocasiones se realiza esta inspección, y un 41.5% mencionó que es raro que se realice esta tarea.

Según los resultados últimos entre raramente y en ocasionalmente existe un 41.5% poco menos de la mitad de los encuestados manifiestan que no se está llevando un control estricto para la seguridad en la información en la gestión de proyectos.

Tabla 43 Control de uso controles de seguridad en proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	59	41,5	41,5	41,5
	Ocasionalmente	42	29,6	29,6	71,1
	Frecuentemente	30	21,1	21,1	92,3
	Muy frecuentemente	11	7,7	7,7	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 10

Se establecen niveles de responsabilidad en base a políticas de seguridad en la información a todos los que participan en el desarrollo del proyecto de TI.

Un 5.6% de los encuestados respondió que si se está estableciendo niveles de responsabilidad de seguridad en los proyectos, también un 38% manifestó que es frecuente esta actividad, un 45.8% manifestó que se lo realiza en ocasiones, y un 10.6% declaró que raro la realización de esta actividad.

Los dos últimos datos de esta pregunta, el 45.8% y el 10.6% declaran que es necesario realizar con más frecuencia los niveles de responsabilidad para los que desarrollan los proyectos.

Tabla 44 Asignación de responsabilidades en SI a desarrolladores

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	15	10,6	10,6	10,6
	Ocasionalmente	65	45,8	45,8	56,3
	Frecuentemente	54	38,0	38,0	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 11

Los participantes en el desarrollo de proyectos de TI conocen de las responsabilidades que implica el uso de la información de la organización.

Un 6.3% de los encuestados mencionaron que conocen las responsabilidades del uso de información que fluye en el desarrollo de los proyectos, un 32.4% menciono algo similar que es frecuente este tipo de conocimiento, un 40.8% acotó que en ocasiones se les hace conocer este tema, mientras que un 15.5% manifestó que raramente se lo hace y un 4.9% declaró que nunca se enteran de este tema.

Tabla 45 Conocimiento de uso de información en proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	7	4,9	4,9	4,9
	Raramente	22	15,5	15,5	20,4
	Ocasionalmente	58	40,8	40,8	61,3
	Frecuentemente	46	32,4	32,4	93,7
	Muy frecuentemente	9	6,3	6,3	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 12

Existe nivel de liderazgo y compromiso en el equipo para gestión de desarrollo de los proyectos de TI.

Un 5.6% de los encuestados manifestó que si existe liderazgo y compromiso en los miembros del equipo de desarrollo, un 45.1% afirmó que también es frecuente esta actitud, un 37.3% declaró que en ocasiones se evidencia, un 11.3% dijo que es raro estas actitudes y un 0.7 recalcó que nunca existe liderazgo al respecto.

Tabla 46 Existencia de liderazgo y compromiso en los proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	16	11,3	11,3	12,0
	Ocasionalmente	53	37,3	37,3	49,3
	Frecuentemente	64	45,1	45,1	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 13

Se asignan las tareas y/o actividades de los proyectos de TI acorde al nivel de conocimiento de cada empleado y/o participante

Un 14.1% de los encuestados respondió que si se asignan tareas de acuerdo al perfil de cada colaborador, un 46.5% dijo que si es frecuente la asignación al respecto, un 32.4 declaró que en ocasiones se lo realiza, un 6.3% manifestó que es raro que ocurra esto y un 0.7% expresó que nunca sucede esta asignación.

Tabla 47 Asignación de tareas de acuerdo a perfil

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	9	6,3	6,3	7,0
	Ocasionalmente	46	32,4	32,4	39,4
	Frecuentemente	66	46,5	46,5	85,9
	Muy frecuentemente	20	14,1	14,1	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 14

Existe personal externo o proveedores que participan en el desarrollo de los proyectos.

Un 24.5% de los encuestados respondió que sí existe la presencia de personal externo en el desarrollo de los proyectos, un 47.2% dijo que también es frecuente la participación de los proveedores y un 28.2% declaró que en ocasiones si se desarrollan proyectos junto a los proveedores.

Tabla 48 Asignación de tareas de acuerdo a perfil

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalmente	40	28,2	28,2	28,2
	Frecuentemente	67	47,2	47,2	75,4
	Muy Frecuentemente	35	24,6	24,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 15

El departamento financiero brinda todas las facilidades y apoyo para desarrollar proyectos de TI.

Un 5.6% de los encuestados expresó que es muy frecuente que el departamento financiero dé el apoyo necesario para la gestión de proyectos de TI, un 43.7% manifestó que es frecuente tal apoyo, un 45.1% mencionó que en ocasiones ocurre este suceso, un 4.2% dijo que es raro las facilidades de tal departamento y un 1.4% dijo que nunca ve apoyo.

Tabla 49 Apoyo financiero para el desarrollo de proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	1,4	1,4	1,4
	Raramente	6	4,2	4,2	5,6
	Ocasionalmente	64	45,1	45,1	50,7
	Frecuentemente	62	43,7	43,7	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 16

El éxito de cada proyecto de TI depende del departamento financiero

Un 6.3% de los encuestados dijo que el éxito de la culminación de los proyectos también proviene del apoyo del departamento financiero, un 52.8 manifestó que es frecuente, un 31% declaró que en ocasiones esto puede ocurrir, un 9.2% expresó que es raro que el éxito dependa de tal departamento y el 0.7 dijo que nunca sucede así.

Tabla 50 Éxito de los proyectos depende de apoyo financiero

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	,7	,7	,7
	Raramente	13	9,2	9,2	9,9
	Ocasionalmente	44	31,0	31,0	40,8
	Frecuentemente	75	52,8	52,8	93,7
	Muy frecuentemente	9	6,3	6,3	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 17

Por lo general, los proyectos de TI culminan acorde a los objetivos y alcance que se plantearon.

Un 4.9% de los encuestados dijo que es muy frecuente que los proyectos culminan según los objetivos y el alcance, un 51.4 manifestó que es frecuente que ocurra así, un 37.3% declaró que en ocasiones sucede y un 6.3% expresó que es raro que ocurra este tipo de culminación.

Tabla 51 Cumplimiento de objetivos y alcance en los proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	9	6,3	6,3	6,3
	Ocasionalmente	53	37,3	37,3	43,7
	Frecuentemente	73	51,4	51,4	95,1
	Muy frecuentemente	7	4,9	4,9	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 18

Se realizan pruebas de funcionamiento y endurecimiento (hardening) en los proyectos de TI culminados antes de su entrega.

Un 5.6% de los encuestados declaró que si es muy frecuente que se haga un hardening en los proyectos antes de la entrega, un 19.7% expresó que si es frecuente, un 31.7 % dijo que no se realizan este tipo de pruebas, un 39.4% manifestó que es raro realizar esta tarea y un 3.5% dijo que nunca se realiza estas pruebas.

Tabla 52 Realización de hardening al final de los proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	3,5	3,5	3,5
	Raramente	56	39,4	39,4	43,0
	Ocasionalmente	45	31,7	31,7	74,6
	Frecuentemente	28	19,7	19,7	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Ítem # 19

Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados.

Según los encuestados, el 5.6% respondió que sí es muy frecuente que los proyectos no ocupen más tiempo y recursos de lo asignado, el 43% manifestó algo similar que si es frecuente este suceso, el 47.9 dijo que en ocasiones abarcan los proyectos más de lo que se planteó y un 3.5% expresó que es raro que los proyectos terminen según lo asignado y programado.

Tabla 53 Finalización de proyectos con tiempo y recursos asignados

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raramente	5	3,5	3,5	3,5
	Ocasionalmente	68	47,9	47,9	51,4
	Frecuentemente	61	43,0	43,0	94,4
	Muy frecuentemente	8	5,6	5,6	100,0
	Total	142	100,0	100,0	

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

3.2.5. Discusión de los resultados de las encuestas

Resultados de medidas de tendencia central

Al efectuar el cálculo de las medidas de tendencia central en la herramienta SPSS, se observa aquellos ítems que obtuvieron puntuaciones repetitivas más bajas “2” en la moda, y sus medias y medianas entre “3”, fueron:

1. Problemas en la generación de medidas y controles de seguridad en la información para los proyectos de TI.
2. Descuidos en la actualización de documentación de historial respecto a normas y procedimientos de seguridad de la información luego de cada proyecto concluido
3. Presencia de parcial conocimiento y experiencia para gestionar los proyectos.
4. Falta control o supervisión de la aplicación de políticas y/o controles de seguridad en el proyecto en curso.
5. Problemas en la asignación de responsabilidades en el uso de la información utilizada.
6. Parcial apoyo del área financiera ya que es necesario para la fluidez de los proyectos.
7. Problemas en la definición del alcance y objetivos en los proyectos.
8. Descuidos en las pruebas de endurecimiento antes de la entrega final de los proyectos.
9. No se está cumpliendo con la entrega a tiempo y se está abarcando más recursos.

Los literales anteriores muestran lo que se deben de mejorar, una de las ayudas que contribuirá a este respecto es el uso de un modelo de seguridad en la información para la gestión de proyectos en el departamento de TI.

Tabla 54 Medidas de Tendencia central

		Documentación y normas de seguridad	Aplicación de seguridad en proyectos de TI	Actualización de procedimientos de seguridad en proyectos TI	Procedimientos de seguridad basados en normas de gobierno	Frecuencia de innovación de servicios mediante proyectos de TI	Presencia de herramientas para planificar proyectos TI	Uso de metodologías y estándares en gestión de proyectos TI	Suficiencia de experiencia en la participación de proyectos TI	Supervisión en aplicación de medidas de seguridad en proyectos TI	Asignación de responsabilidades en estándares para la seguridad en la información	Conocimiento de lo que implica la seguridad de la información en proyectos TI	Nivel de liderazgo y compromiso en gestionar proyectos de TI	Asignación de tarea en base nivel de conocimientos	Presencia de proveedores en la gestión de proyectos de TI	Apoyo del departamento financiero en los proyectos	Dependencia de éxito de proyectos de TI con departamento financiero	Culminación de proyectos acorde con objetivos y alcance	Aplicación de Hardening en proyectos de TI	Culminación de proyectos TI en tiempo programado.
N	***Válido***	142	142	142	142	142	142	142	142	142	142	142	142	142	142	142	142	142	142	142
	Perdidos	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media		3,61	2,94	2,92	3,70	3,77	3,66	3,35	3,52	3,39	2,95	3,20	3,36	3,67	3,96	3,48	3,55	3,55	2,85	3,51
Mediana		4,00	3,00	3,00	4,00	4,00	4,00	3,00	3,50	3,00	3,00	3,00	3,00	4,00	4,00	3,00	4,00	4,00	3,00	3,00
Moda		4	2	2	4	4	4	3	3	3	2	3	3	4	4	3	4	4	2	3

***Fuente**: Resultado encuesta a profesionales de TI*
***Elaborado por:** Autor, en herramienta SPSS*

Correlación de variables cualitativas

Se realiza la asociación aplicando tablas cruzadas para las variables cualitativas entre la utilización de medidas de seguridad en la información para los proyectos y la finalización satisfactoria de los proyectos de TI en tiempo y recursos asignados. A continuación se muestra los resultados:

Tabla 55 Nivel de asociación entre variable

Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados*Se documenta y se usa medidas de seguridad para la gestión de los proyectos de TI de forma particular tabulación cruzada								
			Se documenta y se usa medidas de seguridad para la gestión de los proyectos de TI de forma particular					Total
			Nunca	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente	
	Raramente	Recuento	0	3	1	1	0	5
		Finalización de proyectos satisfactoriamente	0,0%	60,0%	20,0%	20,0%	0,0%	100,0 %
	Ocasionalmente	Recuento	1	29	21	17	0	68
		Finalización de proyectos satisfactoriamente	1,5%	42,6%	30,9%	25,0%	0,0%	100,0 %
	Frecuentemente	Recuento	3	26	5	19	8	61
		Finalización de proyectos satisfactoriamente	4,9%	42,6%	8,2%	31,1%	13,1%	100,0 %
	Muy frecuentemente	Recuento	0	2	2	2	2	8
		Finalización de proyectos satisfactoriamente	0,0%	25,0%	25,0%	25,0%	25,0%	100,0 %
Total		Recuento	4	60	29	39	10	142
		Finalización de proyectos satisfactoriamente	2,8%	42,3%	20,4%	27,5%	7,0%	100,0 %

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

La **tabla 55** determina el grado de asociación entre la aplicación de medidas de seguridad en la información en los proyectos de TI y la conclusión satisfactoria de los mismos. Cabe recalcar que de acuerdo a los valores de las tabla 36 y 53 si **"Raramente"** se usa medidas de seguridad y documentación en los proyectos **"Raramente"** producirá una culminación de forma satisfactoria.

CHI cuadrado

El estadístico observado 23.46 tiene una distribución de 12 grado de libertad (gl=12) haciendo uso del coeficiente de confianza del 95% con una probabilidad de asociación de significancia de 0.024 menor a 0.05 existe una relación entre las variables de uso de controles de seguridad en la gestión de proyectos y la conclusión de los mismos con tiempo y recursos asignados.

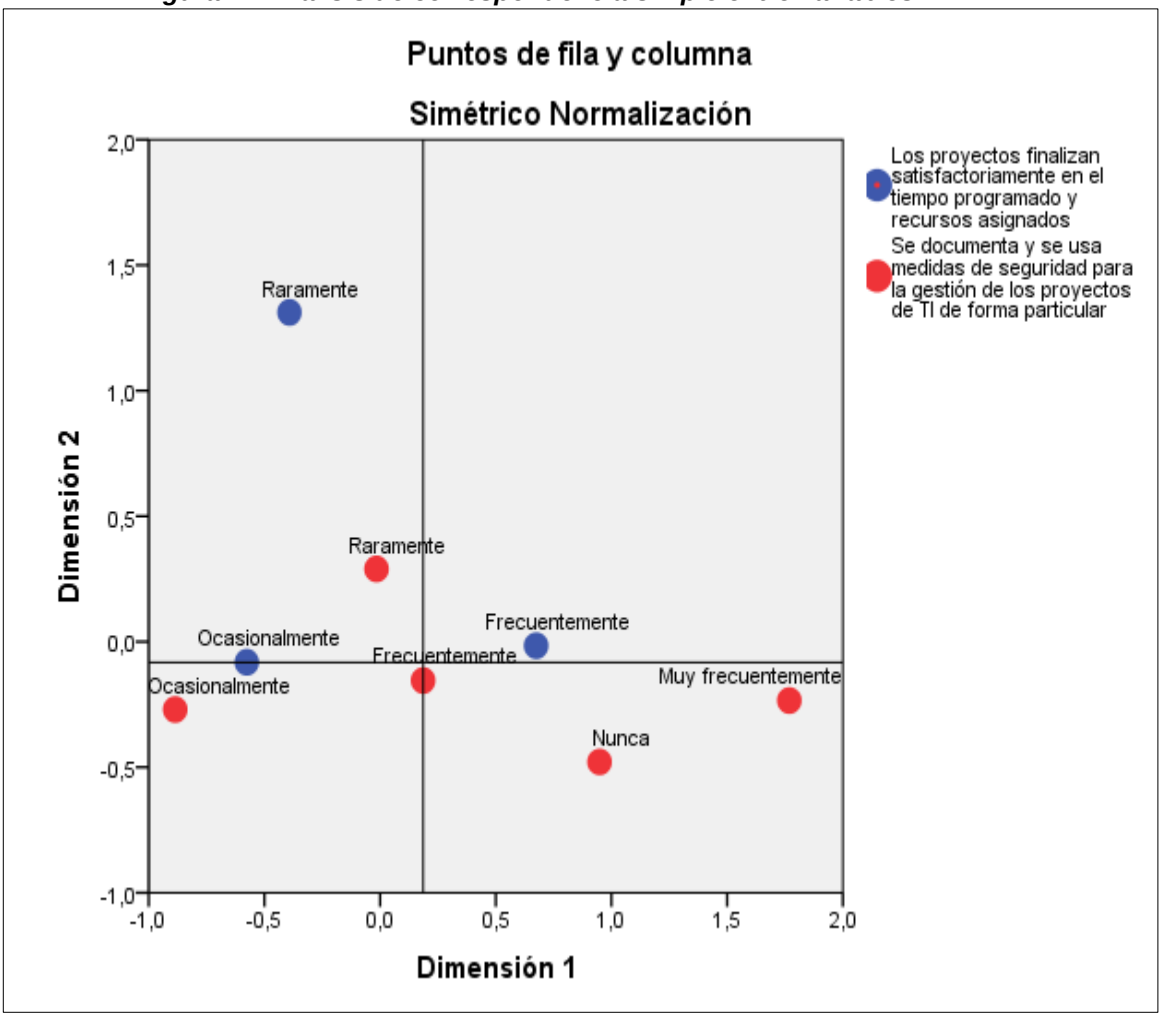
Tabla 56 Prueba de Chi Cuadrado sobre datos cualitativos

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	23,460[a]	12	,024
Razón de verosimilitud	27,637	12	,006
Asociación lineal por lineal	4,580	1	,032
N de casos válidos	142		
a. 14 casillas (70,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,14.			

***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

Para corroborar el nivel de significancia realizado en Chi Cuadrado, se realizó un análisis de correspondencia simple que se muestra de la siguiente manera.

Figura 12 Análisis de correspondencia simple entre variables



***Fuente**: Resultado encuesta a Profesionales*
***Elaborado por**: Autor, en herramienta SPSS*

La **figura 12** evidencia la relación entre las variables, mientras se utilice con frecuencia medidas de controles de seguridad en la información, los proyectos finalizaran satisfactoriamente con el tiempo y recursos asignados de manera frecuente.

3.3. Resultados del estudio y discusión

Los resultados de la investigación se detallan en la tabla siguiente:

Tabla 57 Semáforo de valoración por rango

RANGO		VALORACIÓN
0%	20%	BAJA
30%	40%	
50%	60%	MEDIA
70%	80%	MEDIA – ALTA
90%	100%	ALTA

Fuente: *Escala Likert del marco metodológico*
Elaborado por*: Autor*

Tabla 58 Resultados del estudio

VARIABLE INDEPENDIENTE	DIMENSIÓN	RESULTADO	CALIFICACIÓN / 100	PONDERACION
Gobernanza	*Políticas, normas y procedimientos*	Documentación de seguridad de la información	80	MEDIA-ALTA
		7% Muy frecuentemente 27.5 frecuentemente 20.4% Ocasionalmente 42.3% Raramente 2.8 Nunca	40	BAJA
		5.6 %Muy frecuentemente 26.8% frecuentemente 24.6 Ocasionalmente 40.1% Raramente 2.8 Nunca	40	BAJA
		La documentación basada en normas de gobierno.	100	ALTA
Recursos	*Tecnología*	Frecuencia de proyectos de TI en la organización	80	MEDIA-ALTA
		Herramientas de Planificación proyectos	80	MEDIA-ALTA
		Uso de Metodologías ágiles	80	MEDIA-ALTA
Gestión de Riesgos	*Experiencia*	8.5% Muy frecuentemente 41.5% Frecuentemente 43.7% Ocasionalmente 6.3% Raramente	60	MEDIA
		7.7% Muy frecuentemente 21% frecuentemente 29.6% Ocasionalmente 41.5 Raramente	40	BAJA
	Responsabilidad	5.6% Muy frecuentemente 38% Frecuentemente 45.8% Ocasionalmente	60	MEDIA

		10.5% Raramente		
		6.3 % Muy frecuentemente 32.4% Frecuentemente 40.8% Ocasionalmente 15.5% Raramente 4.9% Nunca	60	MEDIA
Liderazgo	*Desempeño*	5.6 % Muy frecuentemente 41.5% Frecuentemente 37.3% Ocasionalmente 11.3% Raramente 0.7% Nunca	60	MEDIA
		Asignación de tareas acorde a perfil	80	MEDIA-ALTA
		Presencia de proveedores en el desarrollo de proyectos	80	MEDIA-ALTA
Gestión de la calidad	*Financiera*	5.6 % Muy frecuentemente 43.7% Frecuentemente 45.1% Ocasionalmente 4.2% Raramente 1.4% Nunca	60	MEDIA
		El existo del proyecto depende del apoyo financiero	100	ALTA
	Cumplimiento	4.9 % Muy frecuentemente 51.4% Frecuentemente 37.3% Ocasionalmente 6.3% Raramente	60	MEDIA
		5.6 % Muy frecuentemente 19.7% Frecuentemente 31.7% Ocasionalmente 39.4% Raramente	40	BAJA
		5.6 % Muy frecuentemente 43% Frecuentemente 47.9% Ocasionalmente 3.5% Raramente	60	MEDIA

Fuente *El autor*

La ponderación obtenida en la tabla anterior establece que en la parte de las políticas, normas y procedimientos de seguridad de la información, no se están utilizando en la gestión de proyectos, no existe supervisión o el debido control en las fases de desarrollo, por lo que afecta la calidad de los proyectos o también llamado producto final. Sin embargo el conocimiento de herramientas y metodologías agiles permiten que el modelo presentado

se pueda implementar, debido a que está basado en estos elementos de desarrollo.

El modelo propuesto permite identificar y cuantificar las variables que forman parte de su estructura, en las cuales las variables con una ponderación ALTA, MEDIA-ALTA no afectarían a la implementación del modelo propuesto, ya que se están cumpliendo de forma equilibrada, lo que se puede considerar como una contribución dentro del proceso de gestión de proyectos.

En cuanto las variables con calificación MEDIA y BAJA son aquellas cuyas dimensiones permite la implementación del modelo en vista de la frecuencia de la presencia de proyectos a gestionar en la organización.

Desde una perspectiva técnica el modelo promueve resultados positivos en el proceso de gestión de proyectos, su utilización permite llevar un desarrollo seguro manteniendo niveles de seguridad en la información y contribuyendo a un producto de calidad para las organizaciones de Registro Civil Cedulación e Identificación.

CONCLUSIONES

Los proyectos realizados en el área de TI son de gran utilidad, ya que permiten mejoras en los procesos internos, por lo que gestionarlos debidamente en cooperación con toda la organización logran cumplir con los objetivos planteados.

No se debe de eximir dentro de la gestión de proyectos de TI lineamientos para la protección de la información ya que debido a los resultados de la investigación, a mayor aplicación de protocolos de aseguramiento o protección, mayor satisfacción de cierre tendrá cada proyecto culminado.

Otro de los datos obtenidos en la investigación pone de relieve que el desconocimiento de la no aplicación y supervisión de medidas de seguridad en los proyectos, entorpece la fluidez del proceso, poniendo en peligro factores o recursos claves de la organización.

Es importante considerar el recurso humano altamente capaz para tomar las riendas y para la gestión conjunta de cada proyecto de TI a realizarse, disponer de personal interno y/o externo de este tipo es un factor clave para la creación de actividades o tareas que logren cumplir con el alcance de cada proyecto.

El modelo propuesto establece seguridad a la información a través de normas de control debidamente seleccionadas y aplicadas según cada una de las fases, así mismo con la aplicación de una herramienta de trabajo para un seguimiento ágil, contribuye al desarrollo seguro, eficaz y eficiente en los proyectos de TI.

Cada una de las variables de la investigación permite tener una mejor perspectiva para la gestión de los proyectos, proveyendo una mejor visualización de los factores a considerar para obtención de entregables en donde se evidenciará un alto nivel de calidad del producto final.

Este trabajo realizado se basa en las metodologías ISO 27000 (2013) y Scrum (basado en la Guía del PMBoK 6ta edición) lo cual son herramientas usadas y recomendadas a nivel internacional debido a las bondades que presentan cada una de ellas para una óptima gestión de procesos organizacionales.

En virtud de lo anterior la investigación presentada en este documento ofrece a las entidades de registro civil del Ecuador un modelo que combina seguridad en la información y desarrollo ágil que, por un lado ayuda a asignar protección a la información que fluye, y por otro lado permite cuidar de los intereses de la organización.

RECOMENDACIONES

La alta gerencia o directiva tiene como responsabilidad que se efectúe la utilización de las políticas, normas y procedimientos de seguridad en la información para todos los procesos internos de la organización, así mismo es la encargada de supervisar el cumplimiento de las mismas.

En vista de la criticidad de la información se debe de actualizar constantemente la documentación referente a la seguridad de la información y aquella que se utiliza en el proceso de gestión de proyectos, la existencia de este procedimiento permitirá una mejor administración y bienestar para la organización.

La información organizacional que fluye dentro de un proyecto, tiene que ser protegida, no se debe de tomar a la ligera, por eso tanto los empleados así como los proveedores y otros participantes interventores deben de conocer y aplicar medidas de seguridad impartidas por la organización.

Es necesario que la organización de facilidades para que los funcionarios se capaciten en temas relacionados a la gestión de proyectos y así mismo en cuanto a mecanismos de seguridad en la información. Igualmente debe de analizar los perfiles de aquellos quienes vayan participar en el desarrollo de los proyectos tanto al personal interno como a los proveedores.

Es responsabilidad de todos los miembros que están involucrados de forma directa e indirecta a que los proyectos, en primer lugar, cumplan con las medidas y controles de seguridad y en segundo lugar que exista un compromiso de gestión estricto para que cada proyecto concluya satisfactoriamente.

No hacer uso de la mera experiencia que posean los participantes para la gestión de proyectos, se debe recordar que cada uno tiene un objetivo y

alcance distinto por lo que llevará más o menos tiempo, igualmente más o menos recursos a utilizarse.

El uso del modelo propuesto contribuirá a mejorar la gestión de proyectos en dos direcciones, primero en establecer, utilizar y hacer cumplir las medidas/controles de seguridad para proteger la información que interviene y segundo promoverá un desarrollo efectivo y satisfactorio beneficiando a la organización de forma directa.

Además, de acuerdo a los resultados que genere este modelo propuesto de gestión, será revisado respectivamente en el futuro lo que permitirá mejorarlo para proveer una herramienta de uso constante y conseguir los objetivos establecidos.

Bibliografía

A. Barton & G. Tejay & M. Lane & S. Terrel. (2016). Information system security commitment. Recuperado el 2019, de https://dl.acm.org/doi/10.1016/j.cose.2016.02.007

Acuerdo Ministerial 166 Registro Oficial. (25 de 09 de 2013). ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI. Quito, Pichincha, Ecuador: Gobierno Electronico.

Aranguri & Iman & Leon. (2016). MODELO DE GESTIÓN DE RIESGOS DE TI BASADOS EN ESTÁNDARES ADAPTADOS A LAS TI QUE SOPORTAN LOS PROCESOS PARA CONTRIBUIR A LA GENERACIÓN DE VALOR EN LAS UNIVERSIDADES PRIVADAS DE LA REGIÓN LAMBAYEQUE. En M. A. Leon.

Arteaga & Pazmiño. (2018). Use of Good Practices in TI Project Management. En M. A. Castro.

Cardenas. (2019). Implementación de un marco de cumplimiento de la Norma ISO 27001:2013 para el proceso de Gestión de TI en una empresa familiar dedicada a la comercialización de productos para el hogar. En D. Cardenas. Guayaquil: Fiec:Espol.

De la Cámara. (2015). GPS-PYMEs: Marco de gestión de proyectos para el desarrollo seguro en PYMEs. En M. d. Delgado. Madrid: Universidad Politecnica de Madrid.

Dmitrij Olife & Nikolaj Goranin & Arnas Kaceniauskas & Antanas Cenys. (2017). Controls-based approach for evaluation of information security standards implementation costs. Technological and Economic Development of Economy, 196-219.

Doloite. (2017). Seguridad de la información en el Ecuador. Recuperado el 20 de 9 de 2019, de Seguridad de la información en el Ecuador: https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

Elizalde. (2018). Diseño E Implementación De Un Esquema De Seguridad De La Información Basado En La Norma Iso/Iec 27001 – 2013 Para El Servicio De Directorio De Una Empresa De Venta Al Detalle. En A. Elizalde, Trabajo final para la obtención del título de Magister en Seguridad Informática Aplicada (pág. 156). Guayaquil: Fiec:Espol.

Flowerday & Tuyikeze. (2016). Information security policy development and implementation. En S. V. Tuyikeze.

Francisco Valencia & Mauricio Orozco. (2017). Metodología para la implementación de un sistema de gestión de seguridad de la información

basado en la familia de la norma ISO 27000. Revista ibérica de sistemas de tecnologías de la información. Recuperado el 15 de 12 de 2019, de http://dx.doi.org/10.17013/risti.22.73-88

Guamán. (20147). Diseño De Un Sistema De Gestión De Seguridad De La Información Para El Departamento De Informática De La Dirección De Tecnologías De La Información Y Comunicaciones Del Comando Conjunto De Las FFAA. En J. Guamán, Trabajo final para la obtención del título Magíster en Seguridad Informática aplicada (pág. 207). Guayaquil: Espol:Fiec.

Guía SBOK. (2016). SCRUM Study. Una guía para el cuerpo de conocimiento de SCRM. En T. Satpathy. Guía SBOK.

H. Vite. (2019). Modelo de Big Data para la aplicación de internet de las cosas en la gestión de la producción de banano orgánico en la provincia del Oro. En H. Vite. Guayaquil: UTEG.

Indecopi. (2015). Norma Técnica Peruana NTP - ISO/ IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. En Indecopi. Lima: R.0129-2014/ CNB - INDECOPI.

ISACA. (2015). Metodologías y normas para el análisis de riesgos, ¿Cuál debo aplicar? . Recuperado el 08 de 10 de 2019, de https://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%

ISO 27001:2013. (2018). Information technology — Security techniques — Information security management systems — Requirements . Recuperado el 12 de 10 de 2019, de Information technology — Security techniques — Information security management systems — Requirements : https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1:en

ISO.ORG. (2018). Gestión de riesgos. Recuperado el 05 de 10 de 2019, de Gestión de riesgos: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO/IEC 27000. (2018). Information security management systems. Recuperado el 6 de 10 de 2019, de Information security management systems: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27001. (2018). Information security management. Recuperado el 04 de 10 de 2019, de https://www.iso.org/isoiec-27001-information-security.html.

ISO/IEC 27002:2013. (2018). 2013 Information technology -- Security techniques -- Code of practice for information security controls. Recuperado el 15 de 10 de 2019, de 2013 Information technology -- Security techniques -- Code of practice for information security controls: https://www.iso.org/standard/54533.html

Juan Brito & Jorje Bermeo. (2017). publicaciones.ucuenca.edu.ec. Recuperado el 01 de 10 de 2019, de https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1470/1143.

Magerit V3. (2015). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Ministerio de Hacienda y Administración Públicas, Secretaria General Tecnica, Subdireccion General de información. Madrid: Magerit.

Mahecha & Coello. (2016). DESARROLLO DE UN SISTEMA DE INFORMACIÓN PARA GESTIONAR LA IMPLANTACIÓN, MANTENIMIENTO YMEJORA CONTINUA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013. En M. M. Coello. Guayaquil: Espol:Fiec.

NIST 800-53 R4. (2015). Security and Privacy Controls for Federal Information Systems and Organizations. Recuperado el 10 de 10 de 2019, de Security and Privacy Controls for Federal Information Systems and Organizations.: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

Norma Tecnica Ecuatoriana INEN. (2017). Tecnologias de la información-Tecnicas de seguridad – Sistemas de gestion de gestión de seguridad de la información – Requisitos (ISO/IEC 27001:2013 Cor. 2015, IDT). Recuperado el 03 de 10 de 2019, de https://181.112.149.204/buzon/normas/nte_inen_iso_iec_27001.pdf

PMBOK. (2017). Guia de los fundamentos para la gestion de proyectos. En PMI. Chicago, EEUU: PMI.

Project Manangement Institute. (2017). Recuperado el 22 de 09 de 2019, de https://www.pmi.org/learning/thought-leadership/pulse/pulse-of-the-profession-2017.

Rienzo A.& Bustamente M. (2018). Evaluation of the Degree of Knowledge and Implementation of Information Security Management Systems, based of the NCh-ISO 27001 Standard, in Health Institutions. Evaluation of the Degree of Knowledge and Implementation of Information Security Management Systems, based of the NCh-ISO 27001 Standard, in Health Institutions (págs. 1-6). Chile: ICA-ACCA.

Rienzo A.& Bustamente M. (2018). Evaluation of the Degree of Knowledge and Implementation of Information Security Management Systems, based of the NCh-ISO 27001 Standard, in Health Institutions. 1-6.

Sanchez. (2019). Planificación De La Implementación De Un Esquema De Seguridad Basada En La Norma Iso 27001:2013, Para El Proceso De Administración Del Sistema De Información Geográfica En El Gobierno Autónomo Descentralizado Del Cantón Samborondón. En V. Sanchez. Guayaquil: Repositorio Dspace Espol.

Smail, N. (2017). UK wasting £37 billion a year on failed agile IT projects. Recuperado el 01 de 10 de 2019, de UK wasting £37 billion a year on failed agile IT projects: https://www.information-age.com/uk-wasting-37-billion-year-failed-agile-it-projects-123466089/.

Solarte & Enriquez & Benavidez. (s.f.). Francisco Solarte, Edgar Enriquez, Mirian Benavidez. En a. a. Metodología de analisis y evaluación de riesgos. Guayaquil: Revista Tecnologica Espol.

Tsung-Han Yang & Cheng-Yuan Ku & Man-Nung Liu. (2016). An integrated system for information security management with the unified framework. Journal of Risk Research, 21-41.

Unemi. (2017). Gestion de proyectos Informaticos. En U. d. Milagro, Gestion de proyectos Informaticos. Milagro: Unemi.

Yilmaz & Rustu & Yildiray Yalman. (2016). A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. TEM JOURNAL-TECHNOLOGY EDUCATION MANAGEMENT INFORMATICS 5 (2). HILMA ROZAJCA 15, NOVI PAZAR, 36300, SERBIA: ASSOC INFORMATION COMMUNICATION TECHNOLOGY EDUCATION & SCIENCE, 181-190.

ANEXO # 1 CUADRO DETALLADO DE INDICADORES POR PREGUNTA, TÉCNICA DE INVESTIGACIÓN, TIPO DE INSTRUMENTO Y FUENTE

VARIABLE	DIMENSIÓN	INDICADORES	PREGUNTAS	TÉCNICAS	INSTRUMENTOS	FUENTES
Gobernanza	Políticas, normas y procedimientos	Documentación de políticas de seguridad	¿Se usa documentación de procedimientos y normas de seguridad de la información para todos los procesos y subprocesos de la organización?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿Se documenta y se usa medidas de seguridad documentadas para la gestión de los proyectos de TI de forma particular?	documental y de campo	inv. Bibliográfica, encuesta y entrevista	primaria y secundaria
		Revisión y actualización de las políticas de seguridad	¿Se revisan y actualizan las normas y procedimientos de seguridad de la información respecto a cada tipo de proyecto de TI gestionado?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿Las normas y procedimientos de seguridad de la información se basan en reglamentos, normas de gobierno y/o estándares internacionales?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
Recursos de TI	Tecnología	Adquisición de Recursos de TI	¿Se mejora/innova los procesos de negocio y/o servicios de la organización mediante el uso de tecnología de la actualidad?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿La organización cuenta con herramientas para planificar los proyectos de TI?	documental y de campo	inv. Bibliográfica, encuesta y entrevista	primaria y secundaria

		Metodologías y técnicas de gestión	¿La organización cuenta con metodologías agiles o estándares internacionales para la gestión de los proyectos de TI?	documental y de campo	inv. bibliográfica, encuesta y entrevista	primaria y secundaria
Gestión de Riesgos	Experiencia	Evaluación de los riesgos	¿Los participantes cuentan con la suficiente experiencia, capacidad y nivel académico para el desarrollo de los proyectos de TI?	documental y de campo	inv. Bibliográfica, encuesta y entrevista	primaria y secundaria
			¿Se supervisa el uso de políticas y controles de seguridad de la información cuando se están desarrollando los proyectos de TI?	documental y de campo	inv. Bibliográfica, encuesta y entrevista	primaria y secundaria
	Responsabilidad	Aceptación de funciones	¿Se establecen niveles de responsabilidad en base a políticas de seguridad en la información a todos los que participan en el desarrollo del proyecto de TI?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿Los participantes en el desarrollo de proyectos de TI conocen de las responsabilidades que implica el uso de la información de la organización?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
Liderazgo	Desempeño	Actuación e idoneidad	¿Existe nivel de liderazgo y compromiso en el equipo para gestión de desarrollo de los proyectos de TI?	documental y de campo	inv. Bibliográfica, encuesta y entrevista	primaria y secundaria

			¿Se asignan las tareas y/o actividades de los proyectos de TI acorde al nivel de conocimiento de cada empleado participante?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿Existe personal externo o proveedores que participan en el desarrollo de los proyectos?	documental y de campo	inv. Bibliográfica, encuesta y entrevista.	primaria y secundaria
Gestión de la calidad	Financiera	Capacidad financiera	El departamento financiero brinda todas las facilidades y apoyo para desarrollar proyectos de TI	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿El éxito de cada proyecto de TI depende del departamento financiero?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			¿Por lo general, los proyectos de TI culminan acorde a los objetivos y alcance que se plantearon?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
	Cumplimiento	Conformidad y satisfacción	¿Se realizan pruebas de funcionamiento y endurecimiento (Hardening) en los proyectos de TI culminados antes de su entrega?	documental y de campo	inv. bibliográfica y encuesta	primaria y secundaria
			Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados	documental y de campo	inv. Bibliográfica, encuesta y entrevista.	primaria y secundaria

ANEXO # 2 FORMATO DE LA ENCUESTA

ENCUESTA DE OPINIÓN SOBRE LA SEGURIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS DE TI A LAS ORGANIZACIONES DEL SECTOR PÚBLICO.

Este formato de encuesta esta direccionada a las organizaciones del sector público en la ciudad de Guayaquil, para conocer la opinión acerca del nivel de gestión, frecuencia, incidencias, y demás factores que influyen en el desarrollo de proyectos cuando se aplica seguridad de la información, por lo tanto, solicitamos que usted responda con sinceridad a todas las preguntas formuladas.

PREGUNTAS DE LA ENCUESTA

Responda las preguntas de acuerdo al nivel de escala que se presenta a continuación:
5: Muy frecuentemente
4 frecuentemente
3: Ocasionalmente
2: Raramente
1: Nunca

DIMENSION	PREGUNTAS	5	4	3	2	1
POLÍTICAS, NORMAS Y PROCEDIMIENTOS	¿Se usa documentación de procedimientos y normas de seguridad de la información para todos los procesos y subprocesos de la organización?					
	¿Se documenta y se usa medidas de seguridad documentadas para la gestión de los proyectos de TI de forma particular?					
	¿Se documenta y se usa medidas de seguridad documentadas para la gestión de los proyectos de TI de forma particular?					
	¿Las normas y procedimientos de seguridad de la información se basan en reglamentos, normas de gobierno y/o estándares internacionales?					
TECNOLOGÍA	¿Se mejora/innova los procesos de negocio y/o servicios de la organización mediante el uso de tecnología de la actualidad?					
	¿La organización cuenta con herramientas para planificar los proyectos de TI?					
	¿La organización cuenta con metodologías o estándares internacionales para la gestión de los proyectos de TI?					
EXPERIENCIA	¿Los participantes cuentan con la suficiente experiencia, capacidad y nivel académico para el desarrollo de los proyectos de TI?					
RESPONSABILIDAD	¿Se supervisa el uso de políticas de seguridad de la información cuando se están desarrollando los proyectos de TI?					
	¿Se establecen niveles de responsabilidad en base a políticas de seguridad en la información a todos los que participan en el desarrollo del proyecto de TI?					

	¿Los participantes en el desarrollo de los proyectos de TI conocen de las responsabilidades del uso de información de la organización?					
DESEMPEÑO	¿Existe nivel de liderazgo y compromiso para gestión eficiente de cada proyecto de TI?					
	¿Se asignan las tareas y/o actividades de los proyectos de TI acorde al nivel de conocimiento de cada empleado participante?					
	¿Existe personal externo o proveedores que participen en el desarrollo de los proyectos?					
FINANCIERA	¿El departamento financiero brinda todas las facilidades y apoyo para desarrollar proyectos de TI?					
	¿El éxito de cada proyecto de TI depende del departamento financiero?					
CALIDAD	¿Por lo general, los proyectos de TI culminan acorde a los objetivos y alcance que se plantearon?					
	¿Se realizan pruebas de funcionamiento y endurecimiento (hardening) en los proyectos de TI culminados antes de su entrega?					
	¿Los proyectos finalizan satisfactoriamente en el tiempo programado y recursos asignados?					

Se refiere a la conformidad de los resultados con los objetivos y estándares establecidos al principio del proyecto de TI. La calidad tiene una dimensión objetiva (conformidad con las normas) y una dimensión subjetiva (la satisfacción del cliente y usuario, o calidad percibida).

ANEXO # 3 ENTREVISTA DIRECTORA DE GESTIÓN DE PROYECTOS

Entrevista a Profesionales de Gestión de Proyectos de TI

Objetivo: Recopilar información para conocer cómo influye la seguridad de la información en la gestión de los proyectos de TI y su culminación satisfactoria.

Sector empresarial: _____Gobierno_____

Años de experiencia: _____10 años_____

Cargo en la organización: __Directora Gestión de T. I.

Preguntas:

1) **Cuente su experiencia en la gestión de proyectos realizados en el departamento o área.**
   La gestión de proyectos requiere asignar tiempo para la planificación y cierre, en el sector gobierno no se realiza una planificación ordenada y en forma adecuada, eso se evidencia en las diferentes reprogramaciones que se deben realizar, tampoco hay una adecuada gestión de riesgos, y el no hay un cierre adecuado para la gestión de lecciones aprendidas que permiten mejorar el proceso de gestión de proyectos.
   Adicionalmente la rotación de personal es considerable, lo cual afecta a toda planificación de proyectos.

2) **¿Por qué cree usted que es importante conocer el proceso de gestión de proyectos para la llevarlos a cabo?**
   Es importante para una adecuada gestión de proyectos y para documentar las actividades que se realiza, para tomar en cuenta todos los procesos que se deben considerar en la planificación, seguimiento, ejecución y cierre de proyectos.

3) **En los proyectos que ha participado: ¿Cuáles serían los elementos que han contribuido para que un proyecto finalice con éxito?**

   Una adecuada planificación considerar los riesgos a los que está expuesto, mantener el equipo del proyecto, realizar una adecuada comunicación con los interesados, definir bien el alcance considerando los recursos disponibles y el tiempo que se dispone para la finalización del proyecto.

4) **¿Cuáles son los errores más comunes que ud ha percibido al llevar a cabo proyectos dentro de la organización?**

Alcances no definidos adecuadamente, con el detalle necesario. No definir claramente las restricciones y las suposiciones.
Realizar cambio de prioridades de proyectos y cambio a los recursos de los proyectos.

5) **Según su opinión: ¿Cuáles con las principales causas de fracaso en los proyectos de TI?**

No definir un alcance adecuado.
No realizar una planificación considerando las restricciones de alcance, tiempo, costos y calidad.
No se tiene la autorización y apoyo de las autoridades o interesados del proyecto.

6) **¿Cuáles son las herramientas técnicas y/o metodologías que le han ayudado a la gestión eficaz de proyectos, y por qué?**

El Juicio de Expertos es la herramienta que más se utiliza. Conocimiento de PMI para conocer las diferentes herramientas y procesos que se deben realizar, con ello permite la formalidad de la gestión de proyectos.

7) **Según su opinión ¿Cuáles son los principales factores de riesgos que se asocian al buen desempeño de un proyecto? Y ¿Cómo los mitigaría?**
Realizar una buena planificación de los riesgos, permite realizar la planificación para la mitigación, y eso difiere en cada proyecto, por lo cual antes de ejecutar se debe establecer bien los riesgos.
El principal factor es el cambio de prioridades, el cual es más frecuente por el aspecto político que tienen las entidades de gobierno.
Otro factor es no considerar o no formalizar las restricciones y supuestos, para el proyecto.

8) **¿Cree usted que es necesario aplicar medidas de seguridad de la información en los proyectos de TI y que mejoraría el desarrollo de los mismos?**

Pienso que si sería importante aplicar medidas de seguridad, lamentablemente debido a muchos factores, incluidos el tiempo, se pasa por alto trabajar con las medidas adecuadas para salvaguardar la información organizacional.

Inclusive es importante tener un apartado dirigido a temas de proyectos de TI con metodologías de gestión de riesgos en la información.

ANEXO # 4 ENTREVISTA AL COORDINADOR DE TECNOLOGÍA

Entrevista a Profesionales de Gestión de Proyectos de TI

Objetivo: Recopilar información para conocer cómo influye la seguridad de la información en la gestión de los proyectos de TI y su culminación satisfactoria.

Sector empresarial: _____Gobierno_____

Años de experiencia: _____11 años_____

Cargo en la organización: __COORDINADOR DE TECNIOLIGIAS DE LA INFORMACION.

Preguntas:

1) **Cuente su experiencia en la gestión de proyectos realizados en el departamento o área.**
   Como funcionario público poseo 11 años, participando en diferentes tipos de proyectos de TI, siendo líder de proyecto, gerente de proyecto, líder técnico, con diferentes responsabilidades en cada uno de los proyectos realizados, en virtud de los diferentes proyectos sucede que existen diferentes formas de administrarlos y en vista de aquello hay proyectos que no finalizan como se lo espera, más bien hay que darle una serie de seguimiento para que puedan culminarse.

2) **¿Por qué cree usted que es importante conocer el proceso de gestión de proyectos para llevarlos a cabo?**
   Porque un proyecto posee una serie de etapas para en las que hay que saber cómo encaminarlas para que disminuir los riesgos. Desde que inicia el proyecto hay que darle el debido seguimiento para saber el estado de las actividades asignadas al proyecto. Aquí existen participantes de la institución, así como los que son de un prestador de servicios externo. El conocer y saber realizar la planificación del proyecto, conlleva a que finalice como se espera, de no ser así, cae en incumplimiento, que desemboca en penalidades para el prestador de servicios (proveedor).

3) **En los proyectos que ha participado: ¿Cuáles serían los elementos que han contribuido para que un proyecto finalice con éxito?**
   El recurso humano es un elemento primordial, tanto de la organización como del prestador de servicios, siempre y cuando esté debidamente capacitado para estar al frente del proyecto.
   La definición correcta de los objetivos del proyecto, el alcance del proyecto y el planteamiento del cronograma de trabajo del proyecto, son elementos fundamentales. Así como lo fundamental del tiempo de implementación y la fase de pruebas con factores que contribuyen a la

efectividad del proyecto, esto último es importante pues se corre el riesgo de que no se concluya el proyecto en el tiempo acordado y conlleve a la asignación de más tiempo agregando un incremento adicional del costo de proyecto.

4) **¿Cuáles son los errores más comunes que usted ha percibido al llevar a cabo proyectos dentro de la organización?**

Cálculos de tiempo mal establecidos, en la parte del proceso de compras/adquisición de bienes por parte del proveedor para la realización del proyecto. Esto conlleva a que la planificación del proyecto sufra y se tarde más en la entrega del mismo.

Riesgos:
Demora en entrega/recepción de bienes genera atrasos en el cumplimiento de entrega del proyecto.
Plazo de cumplimiento
Establecimiento de *contrato entre el proveedor* y organización para la fabricación o adquisición de los equipos para el proyecto.

5) **Según su opinión: ¿Cuáles con las principales causas de fracaso en los proyectos de TI?**

-Deficiencia en la definición del alcance (alto)
-Deficiencia en el planteamiento de los objetivos (alto)
-Cálculos de tiempo mal planteados (cronograma) (alto)

-Falta de *Recurso humano* (alto)
-Falta de liderazgo (medio)
-Falta de experiencia en los participantes del proyecto (medio)
-Falta de compromiso de los integrantes del proyecto (medio)
-Seguimiento del proyecto (líder técnico) (medio)
-fase de pruebas, implementación

6) **¿Cuáles son las herramientas técnicas y/o metodologías que le han ayudado a la gestión eficaz de proyectos, y por qué?**
-Planificación detallada por experto
-conocer ruta crítica del proyecto (implica más dinero, tiempo, recurso)
-Scrum
-PMBOOK
-Experiencia en variedad de proyectos de TI.

7) **Según su opinión ¿Cuáles son los principales factores de riesgos que se asocian al buen desempeño de un proyecto? Y ¿Cómo los mitigaría?**

-Adquisición de bienes (entrega de) ---------- > establecer plazos de entregas
-recursos humanos no especializado
-Recurso humano limitado (multitarea).
-planteamiento de cronograma personal sin experiencia
-Falta de planificación
-sobre asignación de tareas al personal.
-disponibilidad del servicio al no finalizar el proyecto.

Otros datos
Capacitación al personal interno
Proveedores o personal capacitado para los servicios.
Documentación de procedimientos, falta de
Centro alterno, muy caro, falta de apoyo financiero.
Faltad documentación al concluir el proyecto.

8) **¿Cree usted que es necesario aplicar medidas de seguridad de la información en los proyectos de TI y que mejoraría el desarrollo de los mismos?**

Para esto la organización debe de tener o estar trabajando con lineamientos de seguridad en la información, el esquema que presenta la ISO 27001 es una herramienta valiosa. En vista que esta metodología es aplicable a cualquier proceso de una empresa, se la puede usar en la gestión de los proyectos de TI. Pienso que si ayuda mucho a una buena conclusión en donde interviene el tiempo, recursos y objetivos.

ANEXO # 5 ENTREVISTA CONSULTOR DE GESTIÓN DE PROYECTOS TI

Entrevista a Profesionales de Gestión de Proyectos de TI

Objetivo: Recopilar información para conocer cómo influye la seguridad de la información en la gestión de los proyectos de TI y su culminación satisfactoria.

Sector empresarial: _____Privado_____

Años de experiencia: _____15 años_____

Cargo en la organización: __Consultor de Gestión de Proyectos de TI.

Preguntas:

1) **Cuente su experiencia en la gestión de proyectos realizados en el departamento o área.**

   Como administrador o gerente de proyectos de TI tengo 5 años y siendo participante 10 años, en total 15 años estando delante de todo tipo de proyectos tanto en empresas privadas como públicas. La verdad cada una maneja procedimientos diferentes para gestionarlos, en cuanto a recursos financieros, tecnología, recursos humanos y herramientas. En algunos casos unas quieren llevar a cabo sus proyectos con un mínimo de inversión y que a su vez abarquen una gran cantidad de funcionalidades lo cual conlleva a varias sesiones de reuniones en donde se consideran acuerdos mutuos.

2) **¿Por qué cree usted que es importante conocer el proceso de gestión de proyectos para la llevarlos a cabo?**

   El empirismo no es una técnica buena a utilizar para gestionar proyectos de TI, para estar delante de los proyectos hay que tener conocimientos de la rama y usar las herramientas adecuadas, acorde a la necesidad que presente cada uno y esto a su vez va de la mano con la experiencia del, de tal forma se puede encaminar de manera óptima un proyecto.

3) **En los proyectos que ha participado: ¿Cuáles serían los elementos que han contribuido para que un proyecto finalice con éxito?**

Los listo:

- Recurso monetario
- Recurso humano para el desarrollo
- La tecnología y equipos actualizados
- Software y herramientas adecuadas
- Correcta definición del alcance y objetivos
- Seguimiento del estado del proyecto.

4) ¿Cuáles son los errores más comunes que usted ha percibido al llevar a cabo proyectos dentro de la organización?

Depende del tipo de organización, por ejemplo en las empresas privadas no se consideran seriamente los riesgos que conllevan la elaboración de un proyecto. En las empresas públicas a veces asignan a personal con poca experiencia en la gestión y desarrollo, lo cual entorpece la fluidez del proyecto en el tiempo asignado por cada actividad o grupo de tareas.

5) Según su opinión: ¿Cuáles con las principales causas de fracaso en los proyectos de TI?

Según mi experiencia los siguientes:

- Inexperiencia en el desarrollo o gestión
- Poca supervisión o control de los tiempos de cada fase
- Falta de compromiso de los funcionarios
- Pobre gestión de los riesgos
- Plan de desarrollo de proyectos mal estructurado

6) ¿Cuáles son las herramientas técnicas y/o metodologías que le han ayudado a la gestión eficaz de proyectos, y por qué?

- Framework Scrum y sus buenas practicas
- Guía del PMBoK
- Herramientas de seguimiento como MS Project
- Reuniones constantes con el equipo de desarrollo

Son metodologías y herramientas muy utilizadas por profesionales en materia ya que seguir los lineamientos que contienen, permite un buen desarrollo de los proyectos por experiencia he hecho uso de los ya mencionados por su contribución a formarme como consultor.

7) Según su opinión ¿Cuáles son los principales factores de riesgos que se asocian al buen desempeño de un proyecto? Y ¿Cómo los mitigaría?

De parte del cliente:

- Falta de capacitación
- Falta de experiencia en gestión de proyectos
- Mala planificación
- Falta de personal técnico
- Falta de contingencia en equipos hardware

De parte del proveedor

- Rotación de personal
- Falta de control y seguimiento

8) **¿Cree usted que es necesario aplicar medidas de seguridad de la información en los proyectos de TI y que mejoraría el desarrollo de los mismos?**

Muchas organizaciones o por decir la mayoría consideran de poca importancia el uso de medidas de seguridad para la información, pienso que si es importante este asunto, ya que está en juego la información de la organización, si no hay control puede existir fuga de información o inclusive perdida de la misma, por no tomar medidas preventivas en la gestión de los riesgos.

ANEXO # 6 MATRIZ DE RIESGO DE LA INVESTIGACIÓN

PROCESOS	FACTORES DE RIESGO	ORIGEN DEL RIESGO	POTENCIAL CONSECUENCIA	IMPACTO	PROBABILIDAD DE OCURRENCIA	NIVEL DE RIESGO INHERENT
Gestión Proyectos TI	Problemas de operatividad y comprensión del proyecto	Falta de compromiso,capacitaciones de ultima hora, falta de presupuesto, falta de conocimiento tecnico, incumplimiento de acuerdos por parte de empleados como proveedores.	Atrasos en la entrega del proyecto, perdidas económicas, reasignación de tareas, reasingación de responsabilidades, capacitación de involucramiento en el desarrollo.	A	B	4
	Planificación del proyecto mal realizada	Falta de conocimiento técnico, falta de presupuesto,falta de experiencia, falta de apoyo de autoridades, falta de comprencion de proyecto, fallas en calculos de tiempos de las actividades	Improductividad, reasignacion de tareas, Perdidas para la institución, perdida de credibilidad, reclamos e inconformidad, cambios o sobre carga de trabajo al personal, repogramacion de actividades.	M	M	3
	Indisponibilidad de medios de TI o equipos tecnológicos	Falta de presupuesto, falta de apoyo por parte de las autoridades. Incumplimiento de políticas, cambios politicos,	Reclamos e inconformidad de la institucion, retraso en la puesta a produccion del servicio, retrasos en la inicializacion y conclusion del proyecto, perdidas economicas para la institución, culminacion forzosa del proyecto, multas o penalidades a terceros.	M	M	3
	Vulnerabilidad de la información en el proyecto TI	Falta de comprension de la naturaleza del proyecto,inadecuado metodo de recopilacion de informacion, falta de presupuesto, falta de experiencia, falta de controles y politicas de seguridad en la información, falta de actualizacion de politicas de seguridad, falta de herramientas de protección de amenazas informáticas.	Ataques externos de software mal intencionados, uso de información robada para fines ajenos a la institución, desconfianza de usuarios hacia la institución, reprogramacion de actvidades, inconformidad institucional, reprogramacion de tareas, perdidas economicas para la institucion, atrasos en la entrega del proyecto.	A	M	5

	Producto/Servicio sin niveles de seguridad informática	Falta de politicas de seguridad, falta de actualizacion de las politicas y niveles de seguridad, desconocimiento de tecnicas de hardening para Tics, falta de capacitación, falta de prosupuesto, falta de apoyo de las autoridaddes	Ataques externos de software mal intencionados, indisponibilidad de o los servicios institucionales, perdidas para la institución, fallas operativas, contratación de personal especialista en seguridad informática, problemas con organismos de control o auditorías.	A	M	5
	Problemas de funcionalidades del proyecto	Falta de politicas de seguridad, falta de capacitación, falta de prosupuesto, falta de apoyo de las autoridaddes, falta de conocimiento tecnico para en la gestión de proyectos TI	Perdidas económicas para la institución, desconfianza de los usuarios por el servicio brindado, perdida de información, adquisición de nuevo equipamiento tecnológico, recontratación de otros proveedores y/o especialistas.	A	B	4
	Cambios en los requisitos	Incumplimiento de acuerdos o contratos, falta de presupuesto, falta de liderazgo, falta de experiencia, falta de conocimiento técnico	Baja calidad del producto o proyecto, reclamos e inconformidad por la organización, retrasos en la culminacion del proyecto, perdidas para la organización, suspension temporal de las actividades del proyecto, rotacion de personal.	A	B	4

Anexo # 7: Referencias del 1 al 14: Controles de Seguridad

Referencia. 01 POLÍTICA DE SEGURIDAD

NOTA: se muestra un esquema de política de seguridad, aplicado en la gestión de proyectos de TI. Si es necesario, este documento debe de ser revisado y editado de acuerdo a las novedades que se presenten luego de cada proyecto culminado.

POLÍTICA DE SEGURIDAD

La organización ha experimentado un crecimiento notable desde su fundación en <AÑO EN QUE SE FUNDÓ>. Los clientes/usuarios confían en nosotros. Por lo tanto, nosotros tenemos el deber de proporcionar la seguridad con la que gestionamos su información.

Este documento presenta la política de seguridad de la información que debe ser implantada en toda la organización. Dispone del total soporte de la dirección y toda la compañía está obligada a seguir los preceptos que aquí se presentan incluyendo terceras partes con las que se tenga relación en el ejercicio de las actividades en la organización.

La política será revisada una vez al año para confirmar que la confidencialidad, integridad y disponibilidad de la información no se vea afectada. Esta política permitirá el cumplimiento con las regulaciones actuales a las que se ve sujeta la organización.

Derecho del cliente

- Se debe garantizar la confidencialidad de la información en todo momento
- La información personal almacenada tendrá un carácter temporal. En todo momento, la persona a la cual se realice un tratamiento de los datos, tendrá el derecho de rectificación, supresión o limitación de tratamiento de los datos.

Uso de las aplicaciones

- No se permite el uso de aplicaciones que no dispongan de licencia.
- El borrado de aplicaciones software sólo lo podrá realizar el administrador de sistemas o en su defecto el responsable tecnológico.
- No se permite la instalación de programas software sin la previa autorización del responsable. El administrador delos sistemas es el encargado de la instalación.
- En caso de instalación de software con licencia pública, siempre se tendrán en cuenta los derechos de propiedad intelectual.
- Se restringe el acceso a redes sociales, aplicaciones de almacenamiento en la "nube" y aplicaciones de intercambio de ficheros "Punto a Punto".
- La Dirección exigirá el uso de software propietario o, en su defecto, utilización de software de licencia pública adquirido en lugares seguros cuyas páginas web sean oficiales.

Es obligatorio realizar las actualizaciones de software que se reciban de forma automática.

- Todos los datos informáticos deberán tener una copia de seguridad que se realizará de forma diaria incremental.

Desarrollo software

- Todos los desarrollos software deben considerar requisitos de seguridad desde el inicio de los proyectos.
- Los datos que se utilicen para realizar pruebas deben ser son siempre simulados para evitar utilizar datos sensibles que identifiquen a la persona.

Aplicación criptografica y gestión de claves

- Considerando la confidencialidad se utiliza cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.
- Considerando la integridad/autenticidad se utiliza firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.
- Considerando el no repudio se utiliza técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.
- En cuanto a la gestión de claves, ver el apartado "**Del acceso**" para la consideración de la gestión de claves

Uso de los equipos

- No se permite inactivar los sistemas de seguridad de los equipos corporativos que se utilizan en la organización (p.ej. antivirus)
- Es obligatorio que todos los equipos informáticos dispongan de antivirus actualizados.
- No se permite sacar aquellos recursos informáticos de la compañía sin previa autorización del responsable tecnológico o director general.
- Todos los recursos informáticos a disposición del personal deberán ser utilizados exclusivamente para las actividades inherentes al negocio de la compañía.
- Se deberán utilizar candados de seguridad en aquellos equipos portátiles que la compañía ha puesto a disposición del empleado.
- No se permite la utilización de equipos personales en la compañía para el desempeño de las actividades de negocio.
- No se permite utilizar los equipos portátiles de la compañía fuera de las instalaciones.
- Se deberán bloquear los computadores de sobremesa o portátiles cuando no se utilicen o bien pasada 1 hora de inactividad. Se desbloquearán mediante el usuario y contraseña del empleado.

Acceso

- El administrador de sistemas es el encargado de proporcionar los accesos a los recursos informáticos.
- Se realizará un control de las personas que accedan a las instalaciones sin excepción.
- Todas las personas dispondrán de una tarjeta identificativa que permitirá el acceso a determinadas áreas de las instalaciones.
- Los empleados tendrán acceso a aquellas aplicaciones corporativas a las que hayan sido específicamente autorizados por los responsables de área o el director general.
- Las contraseñas deberán tener un mínimo de 8 caracteres incluyendo letras,

números, mayúsculas, minúsculas y signos especiales.
- Las contraseñas deben ser difíciles de adivinar. Se pueden utilizar reglas nemotécnicas para evitar que se olviden.
- Se ofrecerá una contraseña inicial al crear el usuario. Una vez se acceda por primera vez a los sistemas corporativos, el usuario deberá cambiar esta contraseña.
- Las contraseñas se deberán cambiar una vez cada 3 meses.
- Las contraseñas no deben guardarse en papeles fácilmente accesibles como post-it, no almacenarse en ficheros no encriptados, etc.
- Los usuarios no deben distribuir la información de su autenticación ni siquiera a sus responsables. Debe considerarse como información personal.
- El administrador de sistemas puede crear listas de distribución siempre que haya recibido la aprobación del responsable tecnológico o del director general.
- El control de acceso al código fuente del software sólo está disponible para los empleados directamente relacionados con el desarrollo.

Comunicación y conexión al exterior

- Toda comunicación deberá realizarse de forma encriptada para evitar su manipulación.
- Cada empleado dispondrá de un correo corporativo que únicamente podrá ser utilizado para aquellos fines profesionales relacionados con las actividades de la compañía y no para uso privado.
- La conexión a Internet se realizará siempre a través de la red corporativa. Se dispone de WiFi para invitados con limitado acceso a ciertas aplicaciones.
- Siempre se debe realizar una conexión exterior a través del proxy.

Los incidentes

- En caso de producirse cualquier tipo de incidencia, es obligatorio notificar al responsable tecnológico y al administrador de los sistemas.
- Los incidentes deben ser siempre clasificados y registrados como evidencia.
- Los incidentes deben ser tratados como lecciones aprendidas.
- Se deben notificar aquellas debilidades encontradas en el sistema como medida de prevención de posibles incidentes.

Clasificación de la información

- Cada uno de los activos de la compañía dispondrá de un responsable. Por lo tanto, será el encargado de realizar un buen uso de los mismos.
- Aquellos documentos que la compañía emita o reciba deberán ser clasificados como uso interno (sólo accesibles al personal), públicos (podrán ser accesibles por todo el mundo) y confidenciales (únicamente accesibles por la Dirección).

Gestión de los dispositivos móviles

- Todos los dispositivos móviles que contienen información sensible (p.ej. pen drives o HDD externos), deben ser almacenados en armarios con llave si no se utilizan en ese momento.
- Aquellos dispositivos móviles que contengan información sensible y dejen de ser útiles para la organización deberán ser completamente destruidos. Previamente se

deberá realizar un registro de la información que contienen.
- Todos los dispositivos móviles deberán utilizar criptografía para almacenar información sensible.

Propiedad intelectual

- Todos los desarrollos informáticos creados en la compañía formarán parte de los activos de la misma la cual dispondrá de los derechos de propiedad intelectual.

Formación y capacitaciones

- El personal deberá participar en aquellos cursos de seguridad de la información que se realizaran de forma periódica.

Auditorias

- La Dirección establecerá un programa de auditoria con el fin de, como mínimo, llevar a cabo una auditoria al año sea interna o externa.

Política de "escritorio y pantallas limpios"

- Los escritorios deben estar limpios de forma que no haya documentos con información sensible encima de la mesa a no ser que sean estrictamente necesarios para el desarrollo de las actividades de negocio.

Acuerdos de confidencialidad

- Documentación establecida por la alta dirección en donde se establezca directrices para mantener seguridad entre la organización, sus miembros y entre los proveedores. Estos acuerdos deben de ser en secreto y firmados por los que van a intervenir en el proyecto.

    - La naturaleza de la información
    - La duración del acuerdo
    - Los procedimientos de rescisión
    - Las responsabilidades y las propiedades,
    - El uso permitido de la información
    - El derecho de auditoría
    - Los procesos a llevar a cabo en caso de una infracción
    - Cláusulas que obliguen a mantener el deber de secreto debe incluso más allá de la relación profesional entre las dos entidades

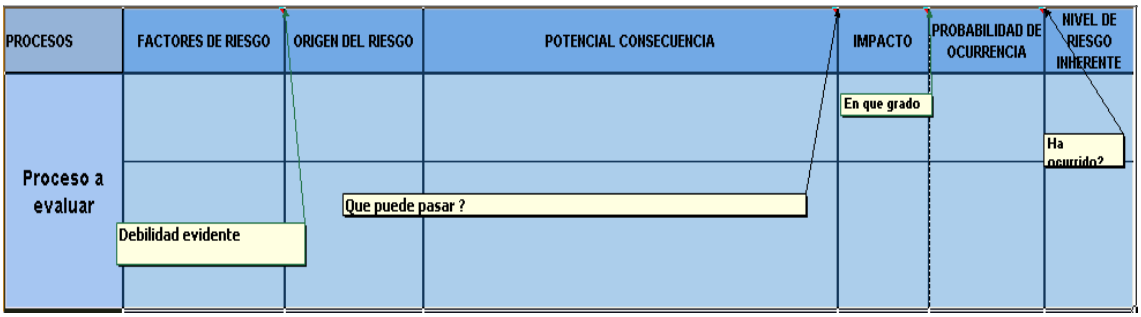
Sanciones por incumplimiento

- En caso de incumplimiento de esta política de seguridad, el personal se verá sujeto a sanciones según lo dispuesto en la normativa del departamento de RR.HH.

Referencia. 02a Matriz de Riesgos y tablas de evaluación.

El uso de esta matriz básica, sirve para hacer un análisis preliminar de los riesgos del proceso de gestión de proyectos de TI.

Matriz de riesgos preliminar



En la matriz de gestión de riesgos completa se analizara profundamente el proceso de Gestión de proyectos de TI para luego de la evaluación, asignar medidas de tratamiento adecuado para cada riesgo, de acuerdo a los controles ISO 27002:2013.

Matriz de riesgos completa

Matriz de riesgos y controles

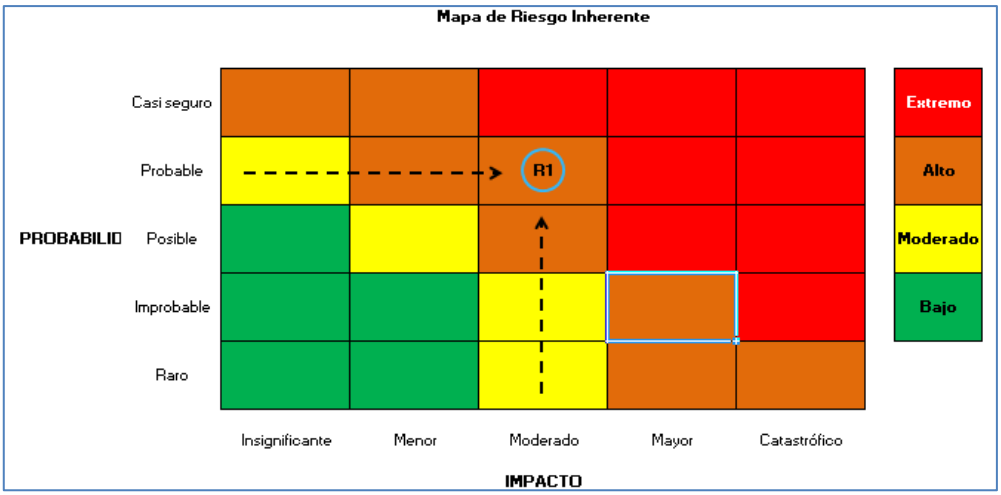
No.	Macroproceso / Servicio	Proceso / Producto	Riesgo	Tipo de Riesgo	Causas	Factor del Riesgo Externo	Factor del Riesgo Interno	Consecuencias	Tipo de Impacto	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Tipo de Control	Clase de Control	Frecuencia	Responsable del Control

Matriz de riesgos y controles

Clase de Control	Frecuencia	Responsable del Control	Documentación del Control	Evaluación Efectividad del Control	Afecta Probabilidad	Afecta Impacto	Riesgo Residual	Política de Manejo	Requiere Plan de Mejoramiento

Mapa de medición riesgos inherentes

Esta tabla de medición sirve para la evaluación de los riesgos que salen a flote de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior, surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un choque negativo afecte la rentabilidad y el capital de la organización frente a la gestión de un proyecto de TI



Mapa de medición riesgos residual

En vista que el riesgo residual continua después de que la dirección desarrolle sus respuestas a los riesgos en los proyectos de TI. El riesgo residual refleja el riesgo remanente una vez que se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente, esta tabla es elemental en la evaluación de los riesgos, contribuye en la tabla general de análisis y gestión de riesgos.

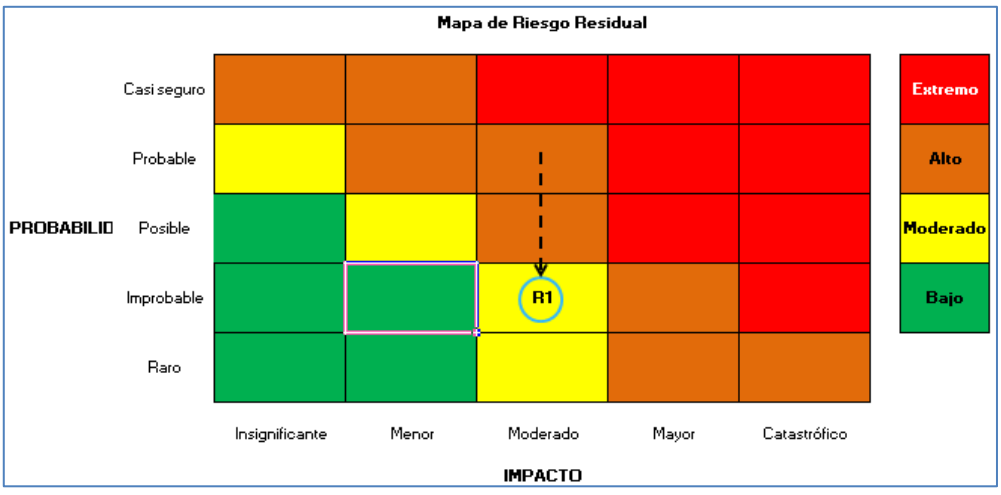


Tabla para evaluación de riesgos

Referencia. 02b Tablas de asignación

Esta da una guía para clasificar, asignar y tipificar los riesgos gestionados en todo proceso, su uso va de la mano con la matriz de gestión de riesgos completa.

tipo de riesgo	factor de riesgo externo	factor de riesgo interno	tipo de impacto	probabilidad	impacto	riesgo inherente	tipo de control
Estratégico	Social	Estructura	1.1.Confidencialidad de información/Personal	Casi seguro	Catastrófico	Extremo	Preventivo
Operativo	Cultural	Cultura organizacional	1.2.Confidencialidad de información/Grupo de trabajo	Probable	Mayor	Alto	Detectivo
Cumplimiento	Económico	Modelo de operación	1.3.Confidencialidad de información/Relativa al proceso	Posible	Moderado	Moderado	Correctivo
Imagen	Tecnológico	Cumplimiento de planes y programas	1.4.Confidencialidad de información/Institucional	Improbable	Menor	Bajo	
Financiero	Político	Sistemas de información	1.5.Confidencialidad de información/Estratégica	Raro	Insignificante		
Tecnológico	Legal	Procesos y procedimientos	2.1.Credibilidad o imagen/Grupo de funcionarios				
Corrupción	Ambiental	Recursos humanos	2.2.Credibilidad o imagen/Todos los funcionarios				
	N.A.	Recursos económicos	2.3.Credibilidad o imagen/Usuarios ciudad				
		N.A.	2.4.Credibilidad o imagen/Usuarios región				
			2.5.Credibilidad o imagen/Usuariso país				
			3.1.Legal/Multas				
			3.2.Legal/Demandas				
			3.3.Legal/Investigación disciplina				
			3.4.Legal/Investigación fiscal				
			3.5.Legal/Intervención-sanción				
			4.1.Operativo/Ajustes a una actividad concreta				
			4.2.Operativo/Cambios en procedimientos				
			4.3.Operativo/Cambios en la interacción de los procesos				
			4.4.Operativo/Intermitencia en el servicio				
			4.5.Operativo/Paro total del proceso				

clase de control	frecuencia	documentación del control	efectividad del control	Probabilidad	Impacto	riesgo residual	política de manejo	requiere plan de mejoramiento
Manual	Diario	Documentado	1.No se aplica	Si	Si	Extremo	Reducir la probabilidad	Si
Automático	Semanal	No documentado	2.Se aplica pero no efectivo	No	No	Alto	Reducir el impacto	No
	Bimensual		3.Se aplica y es efectivo			Moderado	Transferir el riesgo	
	Quincenal					Bajo	Aceptar el riesgo	
	Mensual						Evitar el riesgo	
	Bimestral							
	Trimestral							
	Semestral							
	Anual							
	Permanente							
	Esporádico/Sorpresivo							
	Cuando se requiera							

Referencia. 03 Roles y responsabilidades R.A.C.I. (Control A.6.1.1)

La matriz RACI es una forma de realizar la asignación de responsabilidades, y lleva el nombre de las cuatro responsabilidades más comunes: Responsable, Aprobador, Consultado e Informado, para la gestión de los proyectos de TI es de mucha utilidad.

- **Responsable:** es la persona que realiza el trabajo hasta completar la tarea.
- **Aprobador:** es el encargado de designar a la persona responsable de la tarea, además será el responsable de que la tarea se realice con éxito. En algunos casos el aprobador y responsable pueden ser la misma persona.
- **Consultado**: se refiere a las personas que expresan su opinión sobre una actividad en concreto.
- **Informado:** designa a aquellos que buscan mantenerse al día sobre el progreso de la actividad.

Una vez que se tenga el apoyo de la alta gerencia, se realiza la designación de las tareas para establecer el desarrollo de un proyecto. Conseguir la participación de la **gerencia es algo fundamental para obtener el éxito en los proyectos de TI**. En términos de matriz RACI, esta actividad solo agregaría una complejidad innecesaria. Obtener la aprobación de la gerencia solo se realiza justo antes de comenzar con la planificación y ejecución del proyecto, y dicha actividad se puede definir dentro de los otros documentos de planificación del proyecto.

Nota: La siguiente tabla es un ejemplo de como se debe de desarrollar la matriz RACI.

	ROLES				
Responsabilidades	**Ocupaciones**	**Alta Gerencia**	**Equipo Scrum**	**Jefe De Unidad O Propietarios De proudcto**	**Empleados/Usuarios**
	Identificar los requisitos del proyecto TI	**A**	**R**	**C**	**C**
	Definir los objetivos y alcance	**A**	**R**	**C**	**I**
	Desarrollo de la metodología de evaluación de riesgos	**A**	**R**	**C**	**I**
	Selección de participante para el proyecto	**I**	**I**	**R**	**I**

Referencia. 04 Consideraciones de criptografía (Control A.10.1)

Para el desarrollo de una política debería considerar lo siguiente:

a) Un enfoque de gestión del uso de las medidas criptográficas a través de la organización, incluyendo los principios generales en base a los cuales se debería proteger la información del negocio.
b) Basados en la evaluación de riesgos, el nivel requerido de protección debe ser identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido
c) El uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación;
d) Un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves;
e) Los roles y responsabilidades de cada cual que es responsable de:

1) La implementación de la política
2) La gestión de claves, incluyendo la generación de claves

f) Los estándares a ser adoptados para una efectiva implementación a través de la organización (que solución es utilizada para cada proceso del negocio);
g) Las normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus)

Cuando se implemente la política criptográfica de la organización se debe tener en consideración las regulaciones y restricciones nacionales que pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los temas de desbordamiento de información fuera de las fronteras.

Los controles criptográficos pueden ser utilizados para alcanzar diferentes objetivos de seguridad como por ejemplo:

- Confidencialidad: utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.

- Integridad/autenticidad: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.
- No repudio: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

La documentación del modelo de manera estándar contendría los siguientes apartados:

- Objetivos, alcance y los usuarios participantes
- Documentación de referencia, tales como:
    - Norma ISO 27001, Capítulos A.10.1.1, A.10.1.2, A.18.1.5
    - Referencia legal
    - Política de clasificación de la información
    - Política de seguridad de la información
    - Vigencia

- Uso de la criptografía de acuerdo a la clasificación de la información
    - Descripción de las políticas específicas.
- Responsables del cumplimiento
- Consecuencias y sanciones
- Glosario de términos

Nota: Se puede considerar uso de la herrmamienta software Opensource llamado GNU Project.

Referencia. 05 Gestión de las vulnerabilidades técnicas. (Control A.12.6.1)

La información específica para apoyar la gestión de vulnerabilidad técnica al desarrollar proyectos, incluye el proveedor de software, números de versión, el estado actual de despliegue (por ejemplo, qué software está instalado) y la(s) persona(s) dentro de la organización responsable(s) por el software.

a) La acción apropiada y oportuna debe ser tomada en respuesta a la identificación de vulnerabilidades técnicas potenciales.
b) La organización debe establecer un proceso de gestión para vulnerabilidades técnicas.
c) En función de la urgencia necesaria para abordar una vulnerabilidad técnica, las medidas adoptadas deben llevarse a cabo de acuerdo con los controles relacionados con la gestión del cambio o siguiendo procedimientos de respuesta a incidentes de seguridad de la información;
d) La gestión de vulnerabilidades técnicas puede ser vista como una sub-función de la gestión del cambio, y como tal puede tomar ventaja de los procesos y procedimientos de gestión del cambio.
e) Análisis de los resultados y definición del proceso de remediación.
f) Aplicación de la remediación con base en el nivel de prioridad.
g) Capacitación de los funcionarios de la dirección de tecnología e información en el uso de las herramientas Microsoft, Windows update, WSUS, etc.
h) Ejecución del proceso de detección.
i) Selección de las herramientas de detección automatizada de vulnerabilidades.

Referencia. 06 Acuerdo de confidencialidad y no divulgación (Control A.13.2.4)

NOTA: se muestra una plantilla de acuerdo de confidencialidad y no divulgación para el trabajador. **Un acuerdo de naturaleza similar se debería crear para terceras personas (p.ej. proveedores)**

En virtud de la prestación de servicios de carácter laboral que <EL TRABAJADOR/PROVEEDOR> efectuará para <NOMBRE DE LA ORGANIZACIÓN>. <EL TRABAJADOR/PROVEEDOR>puede tener acceso a instalaciones, dependencias, recursos, sistemas, documentos en soporte papel, documentos electrónicos, soportes informáticos, electrónicos y telemáticos susceptibles de contener información considerada confidencial titularidad tanto de <NOMBRE DE LA ORGANIZACIÓN>. Como de otros terceros vinculados a ella a través de distintas relaciones jurídicas.

Se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores <EL TRABAJADOR/PROVEEDOR> viene obligado expresamente a cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia. En virtud de lo anterior, <EL TRABAJADOR/PROVEEDOR> declara mediante el presente documento que asume su compromiso de cumplir y respetar el deber de secreto y sigilo profesional respecto de cualquier información confidencial que pueda conocer con motivo de la prestación de servicios y ejecución de su contrato laboral.

A efectos de lo anterior <NOMBRE DE LA ORGANIZACIÓN/> pone en conocimiento de <EL TRABAJADOR/PROVEEDOR> que por “información confidencial” se entenderá toda aquella información, incluyendo datos de carácter personal relativos a personas físicas, que en cualquier momento (pasado, presente y/o futuro) y con ocasión de los servicios prestados por <EL TRABAJADOR/PROVEEDOR>, <NOMBRE DE LA ORGANIZACIÓN>. facilite, entregue o, de cualquier forma (verbal, escrita, visual u otras), y bajo cualquier tipo de soporte o canal (papel, electrónico, telemático, soportes informáticos, mensajes de correo electrónico u otros documentos o soportes), ponga a disposición de <EL TRABAJADOR/PROVEEDOR> y que, en general, y en los más amplios términos, concierna, afecte o se refiera directa, indirecta, mediata o inmediatamente, ya a <NOMBRE DE LA ORGANIZACIÓN>, ya a los terceros (personas físicas o jurídicas) con quienes se mantenga cualquier tipo de vinculación, o, sin mantenerla actualmente, pueda existir ésta en un futuro.

Segundo. –OBLIGACIONES

En cumplimiento del objeto del presente documento, <EL TRABAJADOR/PROVEEDOR > se compromete a mantener bajo el más estricto secreto profesional toda la información confidencial que pueda llegar a su conocimiento como consecuencia del desempeño de sus funciones, comprometiéndose el trabajador a no divulgarla, publicarla, cederla, revelarla ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de <NOMBRE DE LA ORGANIZACIÓN> que no estén autorizados a acceder a la citada información, en su encargo profesional o por razón del puesto que ocupan.

<EL TRABAJADOR/PROVEEDOR > se compromete usar los dispositivos, equipos tecnológicos o activos asignados para uso único y exclusivo de la gestión de la información organizacional, así como los demás medios pertenecientes a la organización.

Asimismo, declara conocer y se compromete a respetar y cumplir la normativa y medidas

de seguridad implementadas por <NOMBRE DE LA ORGANIZACIÓN> .a fin de garantizar la seguridad y protección de la información confidencial.

Tercero. –VIGENCIA DEL DEBER DE SIGILO PROFESIONAL

<EL TRABAJADOR/PROVEEDOR >garantiza que, tras la terminación de la relación laboral cualquiera que sea su causa, mantendrá vigente su deber de sigilo y secreto profesional respecto de la información confidencial a que haya tenido acceso durante el desempeño de sus funciones durante la vigencia de la relación laboral y devolverá inmediatamente a <NOMBRE DE LA ORGANIZACIÓN> cualquier soporte o documento en el que conste información confidencial que por cualquier causa obrare en su poder, o la destruirá siguiendo los procedimientos de seguridad para el borrado de información establecidos por <NOMBRE DE LA ORGANIZACIÓN>.

Cuarto. –SANCIONES

<EL TRABAJADOR/PROVEEDOR >declara conocer que las faltas por los trabajadores al servicio de <NOMBRE DE LA ORGANIZACIÓN> reguladas en este compromiso de confidencialidad, se clasificarán atendiendo a su importancia, reincidencia e intención, en leves, graves y muy graves, de conformidad con lo dispuesto en el Convenio Colectivo de aplicación y en las normas vigentes del ordenamiento jurídico laboral. En consecuencia, las sanciones que <NOMBRE DE LA ORGANIZACIÓN> podrá aplicar, según la gravedad y circunstancias de las faltas cometidas, serán las establecidas en la Legislación citada.

Quinto. – PROTECCIÓN DE DATOS

<EL TRABAJADOR/PROVEEDOR > de que los datos de carácter personal derivados de la suscripción de este documento así como los generados en virtud del objeto del mismo serán tratados con la finalidad de llevar a cabo un control de cumplimiento de su compromiso de confidencialidad respecto de toda la información reservada y confidencial que reciba durante la ejecución de la relación laboral. Dicho tratamiento tiene carácter obligatorio y resulta imprescindible a los fines indicados. Asimismo <NOMBRE DE LA ORGANIZACIÓN> informa al TRABAJADOR/PROVEEDOR de que en cualquier momento puede ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose por escrito a la siguiente dirección _____ (o indicar otros medios establecidos por la organización).

Declaro el entendimiento del presente documento, manifiesto mi conformidad con su contenido y acepto el cumplimiento de todas las normas que en el mismo se proponen y/o adjuntan, en _____a _____ de _____de _____.

Firmado por <EL TRABAJADOR/PROVEEDOR >

_____ <Fecha que recibe el documento el TRABAJADOR/PROVEEDOR >

Referencia. 07 Análisis de especificaciones de los requisitos de seguridad (Control A.14.1.1)

Para especificar los requisitos fundamentales de seguridad en la información es necesario tomar en cuenta lo siguiente:

-Uso de mecanismos para gestionar la evaluación de los riesgos

- ✓ Riesgos relacionados a utilización de software
- ✓ Riesgos relacionados con personal interno o proveedores
- ✓ Riesgos con la utilización de codificación
- ✓ Riesgos con vulnerabilidades técnicas no consideradas
- ✓ Riesgos con el uso de hardware obsoleto

-Control de cambios en el software o desarrollo del proyecto
-Protección de datos de prueba
-Establecer principios de ingeniería segura cumpliendo con estándares para el desarrollo.
-Capacitación necesaria para la seguridad

Referencia. 08 Modelo de Acta de constitución de proyecto

Datos

Empresa / Organización	
Proyecto	
Fecha de preparación	
Cliente	
Patrocinador principal	
Gerente de proyecto	

Patrocinador / Patrocinadores

Nombre	Cargo	Departamento / División	Rama ejecutiva (Vicepresidencia)

Propósito y justificación del proyecto

Descripción del proyecto y entregables

Requerimientos de alto nivel

Requerimientos del producto

Requerimientos del proyecto

Objetivos

Objetivo	Indicador de éxito
Alcance	
Cronograma (Tiempo)	
Costo	
Calidad	
Otros	

Premisas y restricciones

Riesgos iniciales de alto nivel

Cronograma de hitos principales

Hito	Fecha tope

Presupuesto inicial asignado

Lista de Interesados (stakeholders)

Nombre	Cargo	Departamento / División	Rama ejecutiva (Vicepresidencia)

Requisitos de aprobación del proyecto

Criterios de cierre o cancelación

Asignación del gerente de proyecto y nivel de autoridad

Gerente de proyecto

Nombre	Cargo	Departamento / División	Rama ejecutiva (Vicepresidencia)

Niveles de autoridad

Área de autoridad	Descripción del nivel de autoridad
Decisiones de personal (Staffing)	
Gestión de presupuesto y de sus variaciones	
Decisiones técnicas	
Resolución de conflictos	
Ruta de escalamiento y limitaciones de autoridad	

Personal y recursos pre-asignados

Recurso	Departamento / División	Rama ejecutiva (Vicepresidencia)

Aprobaciones

Patrocinador	Fecha	Firma

Referencia. 09 Política del programa de desarrollo seguro (Control A.14.2.1)

Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.
Dentro de las especificaciones para un buen desarrollo se debe considerar los siguientes aspectos:

- Apartado inicial que contenga lo siguiente:

Código:
Versión:
Fecha de la versión:
Quien lo creó:
Quien lo aprobó:
Nivel de confidencialidad:

- Objetivos, alcance
- Documentos relacionados a considerar
    - Política de seguridad de la información
    - Normas Iso 27001
    - EGSI del Ecuador
    - Metodologías para desarrollo de software
- Participante con sus Roles y Responsabilidades
- Dentro de la política de desarrollo seguro se debe considerar los siguientes aspectos:
        - Seguridad del entorno de desarrollo;
        - Orientación sobre la seguridad del ciclo de vida de desarrollo de software:
            - Seguridad en la metodología de desarrollo de software;
            - Pautas de codificación segura para cada lenguaje de programación que se utiliza;
        - Requisitos de seguridad en la fase de diseño;
        - Puntos de verificación de seguridad dentro de los hitos del proyecto;
        - Uso de herramientas para establecer el cronograma del proyecto.
        - Repositorios seguros;
        - Seguridad en el control de la versión;
        - Conocimiento de seguridad de aplicación necesario;
        - Capacidad de los desarrolladores de evitar, encontrar y solucionar la vulnerabilidad.
        - Exigir el cumplimiento de la política de desarrollo seguro de software para todos los sistemas y aplicaciones autorizados en la entidad.
- Gestión de vulnerabilidades técnicas encontradas

    Se debe de efectuar validaciones y evaluaciones constantes de seguridad en todo el ciclo de vida del proyecto
- Codificación y pruebas (control de versiones)

Fecha	Versión	Creado por	Descripción de la modificación

- Implementación
    - Implementación de controles de seguridad
    - Implementación de los componentes del proyecto, funciones,

módulos, etc.

- Difusión de la política (Uso de Medios de comunicación)
- Revisión y medición de la política luego de cada proyecto culminado.

Referencia. 010 Principios para elaborar proyectos TI (Control A.14.2.5)

Recomendaciones a tomar para la elaboración de los proyectos:

a) Se deben establecer, documentar y aplicar los procedimientos de ingeniería de sistemas de información segura en base a los principios de ingeniería de seguridad a las actividades del proyecto de TI.
b) La seguridad se debería diseñar en todos los niveles de la arquitectura (negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de la seguridad de la información con la necesidad de la accesibilidad.
c) Se debe analizar la tecnología nueva para conocer sus riesgos de seguridad y el diseño se debería revisar contra los patrones de ataque conocidos.
d) Estos principios y los procedimientos de ingeniería establecidos se deberían revisar de manera regular para asegurarse de que contribuyen de manera eficaz a las normas de seguridad mejoradas dentro del proceso de Ingeniería

Referencia. 011 Lugar adecuado para el desarrollo (Control A.14.2.6)

Es necesario garantizar un entorno de desarrollo seguro que incluye a las personas, procesos y tecnologías asociadas con el desarrollo e integración de sistemas.

La organización debe evaluar los riesgos asociados con las labores de desarrollo de sistemas individuales y establecer entornos de desarrollo seguro, considerando los siguientes elementos:

a) La sensibilidad de los datos que el sistema procesará, almacenará y transmitirá;
b) Los requisitos externos e internos correspondientes, es decir, de las normativas o políticas;
c) Controles de seguridad que ya ha implementado la organización y que soportan el desarrollo del sistema;
d) Confiabilidad del personal que trabaja en el entorno;
e) El grado de externalizarían asociado al desarrollo del sistema;
f) La necesidad de contar con segregación entre distintos entornos de desarrollo;
g) Control del acceso al entorno de desarrollo;
h) Monitoreo del cambio al entorno y al código que ahí se almacena;
i) Que los respaldos se almacenen en ubicaciones fuera del sitio;
j) Control sobre el movimiento de datos desde y hacia el entorno.

Una vez que se ha determinado el nivel de protección para un entorno de desarrollo específico, las organizaciones deberían documentar los procesos correspondientes en los procedimientos de desarrollo seguro y proporcionarlos a todas las personas que los necesiten.

Referencia. 012 Supervisión de los trabajos de proveedores. (Control A.14.2.7)

Cuando se subcontrata el desarrollo de sistemas, los siguientes puntos deben ser considerados a través de la toda la cadena de suministro externo de la organización:

a) Acuerdos de licencia, de propiedad de código y derechos de propiedad intelectual relacionados con el contenido subcontratado;
b) Los requisitos contractuales para el diseño seguro, codificación y prácticas de prueba;
c) Las pruebas de aceptación de calidad y la precisión de los entregables;
d) La provisión de evidencia de que las pruebas suficientes se han aplicado para protegerse contra la presencia de contenido malicioso (intencional o no intencional) sobre los entregables;
e) El suministro de evidencia de que las pruebas suficientes se han aplicado para proteger contra la presencia de vulnerabilidades conocidas.
f) El personal profesional que desarrollará o participará en el proyecto, cuente con las habilidades, experiencias y nivel académico adecuado en la gestión del proyecto de TI.

Los apartados descritos del a-f deben de ser expuestos de forma documental hacia el contratante para una revisión y control de lo expuesto.

Referencia. 013 Pruebas de seguridad en el desarrollo de sistemas (Control A.14.2.8)

En este apartado se recomienda seguir lo siguiente:

a) Los sistemas nuevos y actualizados se deben someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo.
b) Preparación de un programa de actividades detallado y entradas de pruebas y los resultados esperados bajo una variedad de condiciones.
c) Las pruebas de aceptación independientes se debe realizar (tanto para los desarrollos internos y externalizados) para garantizar que el sistema funciona según se espera y solo como se espera.
d) El alcance de las pruebas debería ser en proporción a la importancia y naturaleza del sistema.
e) Asegurar que no se ve impactado ningún proceso de negocio que afecte a su operativa y su seguridad.
f) Los cambios deben realizarse con suficiente antelación para que se definan pruebas previas y planes de contingencia en caso de problemas.

Referencia. 014 Revisión y aceptación de los proyectos de TI (Control 14.2.9)

Se debe de validar los nuevos desarrollos de los aplicativos en un servidor de prueba antes de ser puestos a producción. Además se recomienda establecer la política de desarrollo por terceros los criterios y pruebas de aceptación para los nuevos sistemas de información que adquiera la entidad.

a) Las pruebas de aceptación del sistema deberán incluir las pruebas de los requisitos de seguridad de la Información y la adherencia a las prácticas de desarrollo del sistema seguro.
b) Las pruebas también se deberán realizar en los componentes y sistemas integrados recibidos.
c) Las pruebas se deberán realizar en un entorno de pruebas realista para garantizar que el sistema no introducirá vulnerabilidades al entorno de la organización y que las pruebas sean confiables.
d) Definir con cada fabricante del software existente en la entidad, los protocolos de pruebas para la aceptación correspondiente previa al paso a producción.